Manual
hybird 300 / hybird 600

Reference

Legal Notice

Warranty

This publication is subject to change.

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

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 Introduction

The devices of the **elmeg hybird** product family constitute a combination of IP PABX system and classic PBX system. As with hybrid installations, the devices can be used as a straightforward IP PABX or PBX system. **elmeg hybird 600** is a purely rack-mounted version and supports up to 120 users, while **elmeg hybird 300**, the version for wall mounting, is appropriate for up to 60 users. The scope of functions can be upgraded with modules or software licences, e.g. by adding PBX interfaces such as S0, Up0 or analogue interfaces, or by increasing the number of possible SIP connections. Hotel and mini call centre solutions can be deployed without licence, along with language applications allowing production of a function such as "announcement before query", for example, or music-on-hold produced with your own Wave files. The **hybird** voicemail system includes two voicemail boxes by default. Additional voicemail boxes may be activated via licence packets subject to charge.

Safety notices

The **safety precautions** brochure, which is supplied with your device, tells you what you need to take into consideration when using your **elmeg hybird**.

Installation

How to connect your device is shown in *Setting up and connecting* on page 3. This chapter also tells you what preliminary tasks are necessary for configuration.

Configuration

How to create a basic configuration is shown in chapter *Basic configuration* on page 11.

Password

If you are familiar with the configuration and you wish to get started straight away, all you really need are the preset user name and password.

Note

User Name: *admin*

Password: *admin*

Standard IP *192.168.0.250*

Netmask *255.255.255.0*

Note

When you log onto your device for the first time, you are prompted to change the password. To be able to configure your device, you must modify the password. All devices are delivered with the same password. which means they are not protected against unauthorised access until you change the password. Observe the directions on your screen while performing the modification. You'll find detailed information in the *Modify system password* on page 13 chapter.

DIME Manager

The devices are designed for use with **Dime Manager**. The **Dime Manager** management tool can quickly and simply locate your **elmeg** devices in the network. The .NET-based application, which is designed for up to 50 devices, offers easy to use functions and a comprehensive overview of devices, their parameters and files.

All devices in the local network, including devices that can be reached over SNMP, are located using SNMP Multicast irrespective of their current IP address. A new IP address and password and other parameters can also be assigned. A configuration can then be initiated over HTTP or TELNET. If using HTTP, the **Dime Manager** automatically logs into the devices on your behalf.

System software files and configuration files can be managed individually as required or in logical groups for devices of the same type.

You can find the **Dime Manager** on the enclosed product DVD.

Chapter 2 Installation

Caution

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

2.1 Setting up and connecting

Warning

All areas that can only be opened using tools are classed as maintenance areas. Unauthorised opening can endanger the user.

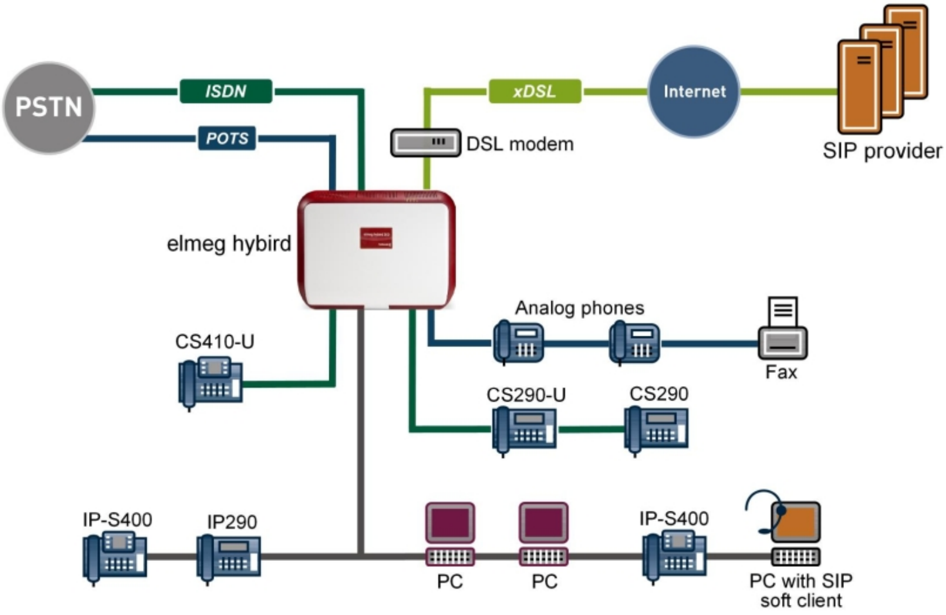
Note

Only use approved accessories!

Condensation may form on or in the device during transitions from cold to warm temperatures. Please only remove the system from the packing materials once the authorised operating ambient temperature has been reached.

Do not assemble the system in damp rooms or in areas subject to a risk of explosion.

Only fit the connection cables to the appropriate connectors.



Connection options

Set up and connect in the following sequence:

(1) Installation: In operation, the wall system must be mounted to a wall (please attentively read the **Installation instructions** included in the scope of supply).

(2) LAN: For the standard configuration of your device via Ethernet, connect the PC's Ethernet connection to the system's LAN connection via a Cat-6 or Cat-5 cable.

(3) Mains connection:

> ⚠ **Warning**
>
> Installation of the electrical connection (shockproof socket) for the system (and any additional devices) must be performed by an authorised electrician to avoid damage to persons and property.

Depending on requirements and system upgrading with expansion cards, you can set up additional connections:

- External telephone connection: Connect the external telephone interface of the device to your telephone connection.
- analog telephone/analog fax: Connect your analogue telephone or your analogue fax.
- ISDN telephone: Connect an ISDN telephone to the device connection, or several ISDN telephones to an ISDN bus connected here.

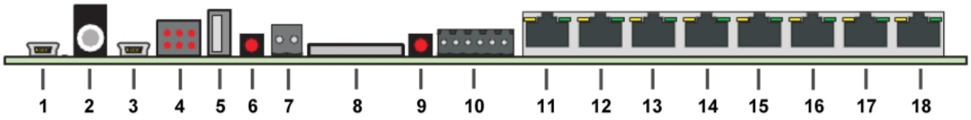
- VoIP telephone: Connect your VoIP telephones to a linked switch.
- Other LANs/WANs: Connect any other terminals in your network to the remaining connectors on the switch port of your device, or to a linked switch using other Ethernet cables.
- Serial connection: For alternative configuration options, connect the serial interface of your PC with the serial interface of the device.

> ☞ **Note**
>
> To make further connections easier, you can purchase a connection kit with the required cables and adapters from your dealer.

The device is now ready for configuration with the **GUI**. Chapter *Basic configuration* on page 11 provides a detailed step-by-step guide to the basic functions on your device.

2.2 Connectors

The connections are arranged as follows:



Basic module connections

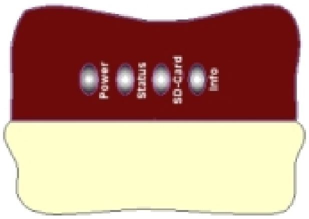
1	Serial 1	Serial interface RS232
2	Audio in / out	Jack for external and internal audio signals
3	Serial 2	Serial interface RS232
4	LED status (rack-mounted system)	LED display
5	USB	USB connector
6	Maintenance	Key for module replacement during operation (hot plug, only intended for the rack-mounted system)
7	System GND terminal	Functional earth connection for safe operation (wall-mounted system)
8	SD card	Card for data storage
9	Reset	Reset button
10	Contacts	Switch contact

11	Contacts	Switch contact
12	Option	Currently without function
13	ETH 1	10/100/1000 Base T Ethernet interface
14	ETH 2	10/100/1000 Base T Ethernet interface
15	ETH 3	10/100/1000 Base T Ethernet interface
16	ETH 4	10/100/1000 Base T Ethernet interface
17	ETH 5	10/100/1000 Base T Ethernet interface
18	Option	Currently without function

2.3 LEDs

The device LEDs provide information on certain activities and statuses of the device. The wall-mounted system LEDs are located at the upper right corner of the housing.

They are arranged as follows:



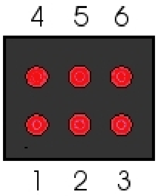
LEDs (wall-mounted system)

LED status display elmeg hybird 300

LED	Status	Information
Power	flashes red	Power Management
	lights up green	Operating voltage present
Status	flashes red	System messages exist
	flashes green	Operating status
	lights up green	The elmeg hybird is initialised
SD card	flickers green	Data being written/read
	lights up green	Memory card detected but no access

LED	Status	Information
Uploaded Excel file	currently no function	

The rack-mounted system LEDs are located at the front of the housing.



LEDs (rack-mounted system)

LED status display elmeg hybird 600

LED	Status	Information
1 Power	flashes red	Power Management
	lights up green	Operating voltage present
2 Status	flashes red	System messages exist
	flashes green	Operating status
	lights up green	The elmeg hybird is initialised
3 SD card	flickers green	Data being written/read
	lights up green	Memory card detected but no access
4	Function in module replacement	
5	Function in module replacement	
6	Function in module replacement	

☞ **Note**

For replacement of modules 1 - 6 during operation of the **elmeg hybird 600**, LEDs 1 - 6 are assigned to slots 1 - 6. You'll find information on module replacement in the installation instructions.

2.4 Scope of supply

Your device is supplied with the following parts:

Scope of supply	elmeg hybird 300	elmeg hybird 600
Cable sets/mains unit/ other	1x M 4 S/U + 6 FXS 1x MC CL 2x IP cable (3 m) Fixing screws, dowels Connection terminals	2x IP cable (3 m) Network cable 2x Angle brackets 6x Knurled screws
Software	Companion DVD	Companion DVD
Documentation	Quick Install Guide and safety notices (printed)	Quick Install Guide and safety notices (printed)
Online documentation	User's Guide **Quick Install Guide** leaflet (for printing)	User's Guide **Quick Install Guide** leaflet (for printing)

2.5 General Product Features

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

General Product Features elmeg hybird 300, elmeg hybird 600

Product name	elmeg hybird 300 (wall-mounted system)	elmeg hybird 600 (rack-mounted system)
Equipment dimensions without cable (B x H x D):	500 mm x 370 mm x 75 mm	440 mm x 88 mm x 293 mm
Weight	approx. 2.590 kg (incl. mains unit without packing and cable)	approx. 5.2 kg (incl. mains unit without packing and cable)

Product name	**elmeg hybird 300 (wall-mounted system)**	**elmeg hybird 600 (rack-mounted system)**
LEDs	4 (1x Power, 1x Status, 1x SD Card, 1x Info)	6 (1x power, 1x status, 1x SD card, 3x functions only for module replacement)
Power consumption of the device	Resting state (no module installed): ca. 12 watt Activity for 3 modules FXS16 (50 % load, ca. 24 active calls): ca. 50 W 1 Power supply	Resting state (no module installed): ca. 12 watt Activity for 6 modules FXS16 (50 % load, ca. 48 active calls): ca. 80 W 2 Power supplies
Voltage supply	230 V ~	230 V ~
Operating conditions	dry rooms, no condensation, dust-free	dry rooms, no condensation, dust-free
Storage temperature	-20 °C to +70 °C	-20 °C to +70 °C
Operating temperature	+5 °C to +40 °C	+5 °C to +40 °C
Relative atmospheric humidity	max. 85 %	max. 85 %
Available interfaces:	FXS, S0 internal/external, UP0 internal, (rel.2: FXO + PRI)	FXS, S0 internal/external, UP0 internal, (rel.2: FXO + PRI)
Serial interface V.24	Permanently installed, supports Baud rates: 1200 to 115200 Baud	Permanently installed, supports Baud rates: 1200 to 115200 Baud
Ethernet (4-port switch)	4x GB Ethernet interface configurable as LAN, WAN, according to IEEE802.3u, compatible with 100 / 10 Base T (IEEE802.3), auto-MDIX 4x GB Ethernet interface configurable as WAN, DMZ according to IEEE802.3u, compatible with 100 / 10 Base T (IEEE802.3), auto-MDIX	4x GB Ethernet interface configurable as LAN, WAN, according to IEEE802.3u, compatible with 100 / 10 Base T (IEEE802.3), auto-MDIX 4x GB Ethernet interface configurable as WAN, DMZ according to IEEE802.3u, compatible with 100 / 10 Base T (IEEE802.3), auto-MDIX
Available sockets:		
Serial interface V.24	5-pole mini USB socket	5-pole mini USB socket
Ethernet interface	5x RJ45 socket with 2 integrated LED's per socket	5x RJ45 socket with 2 integrated LED's per socket
Jack	Audio in/out (for external and in-	Audio in/out (for external and in-

Product name	**elmeg hybird 300 (wall-mounted system)**	**elmeg hybird 600 (rack-mounted system)**
	ternal audio signals)	ternal audio signals)
Standards & Guidelines	R&TTE Directive 1999/5/EC CE symbol for all EU states	R&TTE Directive 1999/5/EC CE symbol for all EU states

2.6 Reset

The **hybird** is restarted by quickly pressing the reset key (ca. one second). Pressing the key is equivalent to an interruption of the power supply. Any saved data will be retained, but all connections will be broken.

A factory reset of the **elmeg hybird** is performed if you press the reset key for approx. 30 to 40 seconds. This means that the **elmeg hybird** is returned to its ex works state. The connection data is not deleted. The boot configuration is deleted and all passwords are reset. The reset has accomplished once the **elmeg hybird** returns to operating status after 30 to 40 seconds.

2.7 Support Information

If you have any questions about your new product, please contact a local, certified retailer for prompt technical support. Resellers have been trained by us and receive privileged support.

Further information on our support and service offers can be found on our web site at *www.bintec-elmeg.com* .

Chapter 3 Basic configuration

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

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

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

3.1 Preparations

3.1.1 System Software

Your device contains the version of the system software available at the time of production. More recent versions may have since been released. You can easily perform an update with the **GUI** using the **Maintenance**->**Software &Configuration** menu. For a description of the procedure, see *Software Update* on page 17.

3.1.2 System requirements

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

- Microsoft Windows operating system Windows 2000 or higher
- Internet Explorer Version 7 or 9 (security settings may need to be customised), Mozilla Firefox Version 4 or higher
- Installed network card (Ethernet)
- Installed TCP/IP protocol
- High colour display (more than 256 colours) to show the graphics correctly

3.1.3 Gathering data

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

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

- Basic configuration

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

Basic configuration

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

Basic information

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

3.1.4 Configuring a PC

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

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

Checking the TCP/IP protocol

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

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

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

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

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

Installing the TCP/IP protocol

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

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

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

(3) Click **Add**.

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

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

Allocating PC IP address

Allocate an IP address to your PC as follows:

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

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

Enter the gateway IP address on your PC.

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

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

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

(3) Click **OK**.

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

The computer now has an IPSec configuration.

Note

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

3.2 Configuring the system

3.2.1 Modify system password

All bintec elmeg devices are delivered with the same username and password. As long as the passwords remains unchanged, you are thus not protected against unauthorised use. When first logging in, you must change the passwords to be able to configure your device.

To change the password, proceed as follows:

(a) Go to the **System Management**->**Global Settings**->**Passwords** menu.

(b) Enter a new password for **System Admin Password**.

(c) Enter the new password again under **Confirm Admin Password**.

(d) Click **OK**.

(e) Store the configuration using the **Save configuration** button above the menu navigation.

Note the following rules on password use:

- The password must not be easy to guess. Names, car registration numbers, dates of birth, etc. should not be chosen as passwords.
- The password should be at least 8 characters long.
- The password should include at least four distinct characters.
- The password should contain characters from at least three of the following four groups. Lower case letters (a - z), upper case letters (A - Z), numbers (0 - 9), symbols
- Change your password regularly, e.g. every 90 days.

3.2.2 Network settings via assistants

Select the basic configuration in the menu **Assistants**->**First steps**->**Basic Settings**. For the LAN IP configuration, the **Address Mode** is set by default to **Static** as your system is delivered ex works with a fixed IP. As **Default Gateway IP Address**, enter the IP address of your upstream router. Enter the same IP address of the upstream router under **DNS Server**.

This configures the settings for integrating your device into the local network (LAN).

3.2.3 Telephony

The **elmeg hybird** system is a PBX setup to which you can also connect IP system telephones and standard IP telephones. Below is described how to connect and log in an IP system telephone to your system.

SIP provider

In the first step, you create a SIP provider and set up a corresponding connection:

(1) In the **GUI**, select **VoIP**->**Settings**->**SIP Provider**->**New**.

(2) Enter you SIP account data. For example, the data might look as follows:

Field	Description
Description	Enter the name of your SIP provider, e.g. *Sipgate*.
Authentication ID	Enter your ID, e. g. for Sipgate: *3223174e1*

Field	Description
Password	Enter the password you received from the SIP provider.
Registrar	Enter the relevant registrar. For Sipgate: *sipgate.de*

(3) Confirm your settings by clicking **OK**.
You will see your SIP connection under **Numbering**->**Trunk Settings**->**Trunks**.

Call number

In the following step, you configure your connection's subscriber number.

(1) Select **Numbering**->**Trunk Settings**->**Trunk Numbers**->**New** in the menu and select your SIP provider under **Trunk** (in this example: *Sipgate*).

(2) Under **Displayed Name**, enter the corresponding name (e.g. *Sipgate*), and under **Single Number (MSN)**, the number assigned to you by your SIP provider. Make sure the format is correct. It's important to enter the country code (if required) without *00*; (e.g. for Germany *4951717391051*).

(3) Save your entries with **OK**.

Authorisation class

As the next step, you select the authorisations associated to this entry:

(1) To do this, select the **Numbering**->**User Settings**->**Class of Services** menu. In the authorisation class table, open *Default CoS* by clicking ✎.

(2) Under **Trunk Line Selection with Line Access Number**, go to **Add** then select your SIP provider. Confirm your choice with **Apply**.

User

A *Default User* is already entered in the **Numbering**->**User Settings**->**Users** menu.

(1) In the table, open *Default User* by clicking ✎. Then go on the **Trunk Numbers** tab to enter the internal number.

(2) Click **Add** and enter the corresponding internal number of the terminal (e.g. *120*) under **Internal Number** and enter a name under **Displayed Description** (e.g. *120-IP-S400*).

Confirm your entries with **Apply**.

Call Assignment

In the last step, you must assign an internal number to the SIP entry.

(1) Select the **Numbering**->**Call Distribution**->**Incoming Distribution** menu.

(2) Open your SIP entry, by clicking ✎. Under **Internal Number**, select the number you want.

(3) Save your entries with **OK**.

Once you've performed the settings, you're able to make internal and external calls. Save the configuration by clicking the **Save configuration** button above the menu tree and confirming the subsequent queries, if any.

Connecting telephones

Connect your IP system telephone. Confirm entries in the display, and in the telephone specify the IP address of your system **elmeg hybird** as gateway IP address. The telephone logs in as guest. The IP system telephone displays `Guest`. Under **Numbering**->**Terminals** you see under **System Phone** your system telephone, or under **VoIP** (if you log in an IP telephone), your IP telephone. Open your telephone entry by clicking ✎ and select an internal number under **Internal Number**. In a couple of minutes, the telephone is registered; `Guest` is no longer displayed on the IP system telephone.

3.3 User access

The system administrator can set up an individual configuration access for the users. You, the user, can thus display your most important personal settings and individually customise some of these.

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.

Basically, there are two differing types of user accesses: Accesses freely defined by the administrator, created in the **Numbering**->**User Settings**->**Users** menu, and those of user assigned to system telephone book, connection data, hotel function and mini call centre applications. The users created by the administrator have access to a sharply restricted configuration interface, the scope of which you can gather from the **User Access** chapter. Users that assigned to applications can view the menu corresponding to the applications, as also available to the administrator.

You can access help on available configuration options via the online help system.

3.4 Software Update

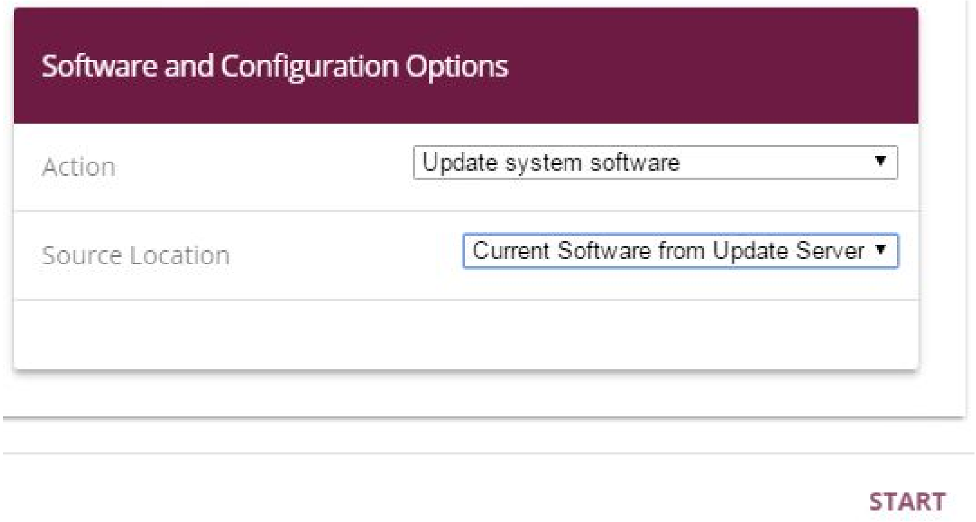
The range of functions of the **elmeg hybird** system is continuously being extended. These extensions are made available to you by bintec elmeg GmbH. Checking for new software versions and the installation of updates can be carried out easily with the **GUI**. An existing internet connection is needed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

Proceed as follows:

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

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

(3) Confirm with **Go**.



Software and Configuration Options

Action: Update system software

Source Location: Current Software from Update Server

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

Caution

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

Chapter 4 Operation via a telephone

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

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

Chapter 5 Access and configuration

This chapter describes all the access and configuration options.

5.1 Access Options

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

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

- Via your LAN
- Via the serial interface

5.1.1 Access via LAN

Access via one of your device's Ethernet interfaces allows you to open the **GUI** in a web browser for configuration.

5.1.1.1 HTTP/HTTPS

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

- *`http://192.168.0.250`*

  or

  `https://192.168.0.250`

5.1.2 Access via the Serial Interface

The **elmeg hybird** features a serial interface which allows a direct connection with a PC. The following chapter describes what you have to remember when setting up a serial connection and what you can do to configure your device in this way.

Access via the serial interface is ideal if you are performing an initial configuration on your device, and a LAN access is not possible via the pre-configured IP address (192.168.0.250/255.255.255.0).

Windows

If you are using a Windows PC, you need a terminal program for the serial connection, e.g.

HyperTerminal. Make sure that HyperTerminal was also installed on the PC with the Windows installation. However, you can also use any other terminal program that can be set to the corresponding parameters (see below).

If you have accessed and installed the **BRICKware** at *www.bintec-elmeg.com* , two links are provided in the Windows Start menu. If you use these, you do not have to make any other settings for the serial connection to your device.

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

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

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

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

Check

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

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

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

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

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

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

(5) Click **OK**.

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

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

Unix

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

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

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

5.2 Login

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

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

5.2.1 User names and passwords in ex works state

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

User names and passwords in ex works state

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

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

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

Caution

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

When you log onto your device for the first time, you are prompted to change the password. To be able to configure your device, you must modify the password.

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

5.2.2 Logging in for Configuration

Set up a connection to the device. The access options are described in *Access Options* on page 19.

GUI (Graphical User Interface)

Log in via the HTML surface as follows:

(1) Enter your user name in the **User** field of the input window.

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

(3) When you first log into your device, you're prompted to modify the password. Enter the new password again under **System Admin Password**.

(4) Enter the new password once again under **Confirm Admin Password** and click **OK**.

The status page of the **GUI** (Graphical User Interface) opens in the browser.

5.3 Configuration

The **GUI** (Graphical User Interface) is used for configuring.

5.3.1 GUI (Graphical User Interface)

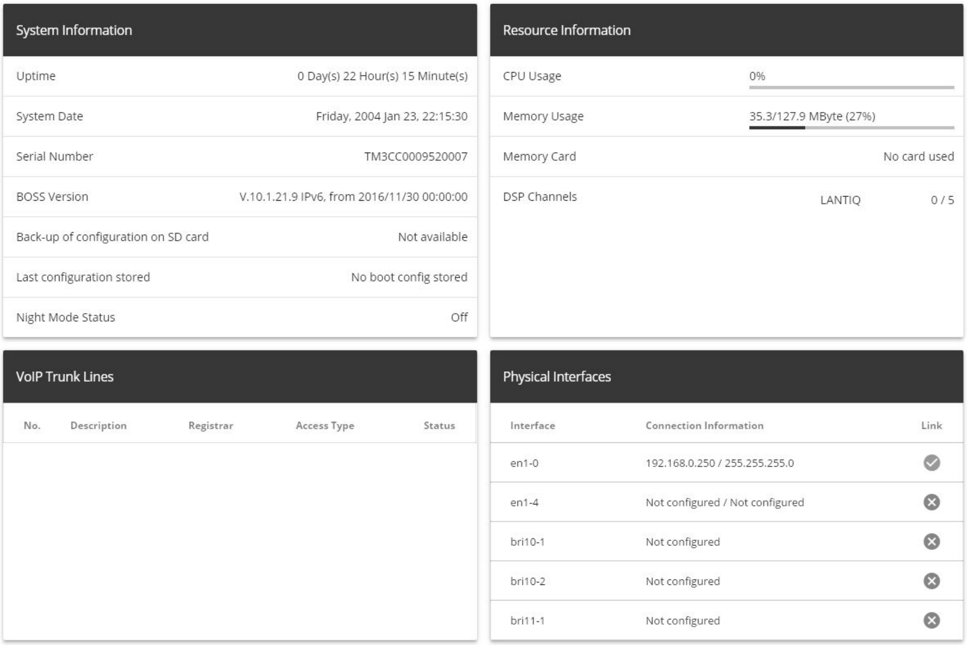
The **GUI** is a web-based graphic user surface that you can use from any PC with an up-to-date Web browser via an HTTP or HTTPS connection.

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

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

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

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



System Information	
Uptime	0 Day(s) 22 Hour(s) 15 Minute(s)
System Date	Friday, 2004 Jan 23, 22:15:30
Serial Number	TM3CC0009520007
BOSS Version	V.10.1.21.9 IPv6, from 2016/11/30 00:00:00
Back-up of configuration on SD card	Not available
Last configuration stored	No boot config stored
Night Mode Status	Off

Resource Information		
CPU Usage	0%	
Memory Usage	35.3/127.9 MByte (27%)	
Memory Card		No card used
DSP Channels	LANTIQ	0 / 5

VoIP Trunk Lines

No.	Description	Registrar	Access Type	Status

Physical Interfaces

Interface	Connection Information	Link
en1-0	192.168.0.250 / 255.255.255.0	✓
en1-4	Not configured / Not configured	⊗
bri10-1	Not configured	⊗
bri10-2	Not configured	⊗
bri11-1	Not configured	⊗

GUI Home page

5.3.1.1 Call up the GUI .

(1) Check whether the device is connected and switched on and that all the necessary cables are correctly connected (see *Setting up and connecting* on page 3).

(2) Check the settings of the PC from which you want to configure your device.

(3) Open a web browser.

(4) Enter `http://192.168.0.250` in the address field of the web browser.

(5) Enter `admin` in the **User** field and enter `admin` in the **Password** field and click **LOGIN**.

You are now in the status menu of your device's **GUI** (see *Status* on page 34).

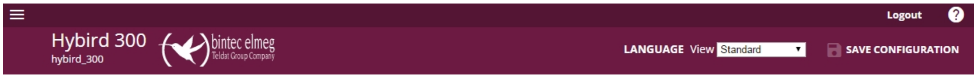
5.3.1.2 Operating elements

GUI window

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

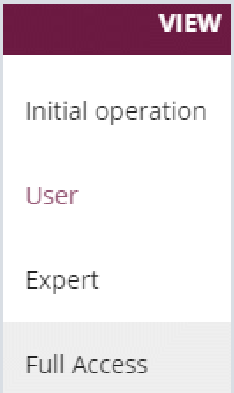
- The header
- The navigation bar
- The main configuration window

Header

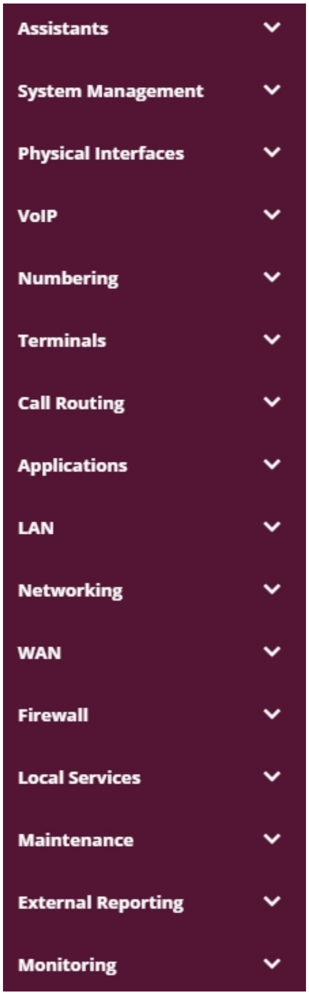


Configuration interface header bar

Menu	Function
☰	Opens the navigation bar.
Logout	**Logout**: If you want to end the configuration, click this button to log out of your device. A window is opened offering you the following options: • Continue with the configuration, • Save the configuration and close the window, • Exit the configuration without saving.
?	**Online Help**: Click this button if you want help with the menu now active. The description of the sub-menu where you are now is displayed.
LANGUAGE English Deutsch	**Language**: From the dropdown menu, select the language in which the configuration interface is to be displayed. Here, you can select the language in which you want to carry out the configuration. `German` and `English` are available.

Menu	Function
	**View**: Select the desired view from the dropdown menu. *Full Access* , *Expert* and *User*can be selected. Also the Initial operation can be start again from here.
	Save configuration button. If you click the **Save configuration** button, you will be asked "Do you really want to save the current configuration as a boot configuration?" You can • Save configuration • Save configuration with boot backup

Navigation bar



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

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

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

Status page

If you open the configuration interface the status page of your device is displayed after you log in. The most important data of your device can be seen on this at a glance.

Main configuration window

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

Configuration elements

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

Buttons

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

Symbols

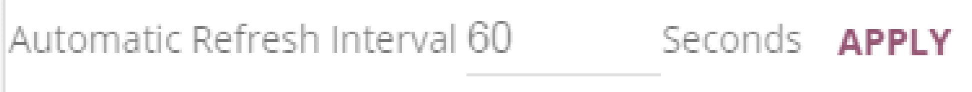
Icon	Function
🗑	Deletes the list entry.
✏	Displays the menu for changing the settings of an entry.
🔍	Displays the details for an entry.
🔊	Voicemail message can be intercepted.
💾	Messages will be saved.
📞	Select the button to go to the **elmeg** IP1x0 telephone user interface administrator page.

Icon	Function
⇅	Moves an entry. A combo box opens in which you can choose the list entry that selected entry is to be placed in front of/after.
≡+	Creates another list entry first and opens the configuration menu.
⌄	Sets the status of the entry to *Inactive* .
⌃	Sets the status of the entry to *Active*.
⏰	Indicates "Dormant" status for an interface or connection.
✔	Indicates "Up" status for an interface or connection.
✖	Indicates "Down" status for an interface or connection.
⊘	Indicates "Blocked" status for an interface or connection.
🔒	Indicates that data traffic is encrypted.
📶	Triggers a WLAN bandscan.
»	Displays the next page in a list.
«	Displays the previous page in a list.

List options

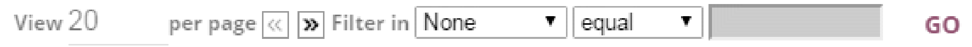
Menu	Function
Update Interval	Here you can set the interval in which the view is to be updated. To do this, enter a period in seconds in the input field and confirm it with APPLY .
Filter	You can have the list entries filtered and displayed according to certain criteria. You can determine the number of entries displayed per page by entering the required number in **Viewxper page**.

Menu	Function
	Use the « and » buttons to scroll one page forward and one page back. You can filter according to certain keywords within the configuration parameters by selecting the filter rule you want under **Filter inx <Option> y** and entering the search word in the input field. GO launches filter operation.
Configuration elements	Some lists contain configuration elements. You can therefore change the configuration of the corresponding list entry directly in the list.



Automatic Refresh Interval 60 Seconds APPLY

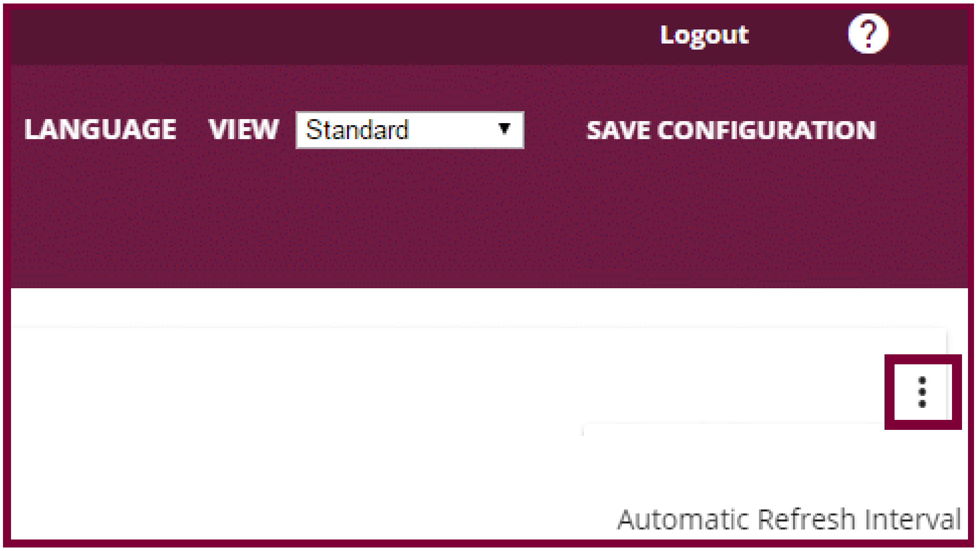
Configuration of the update interval



View 20 per page « » Filter in None ▾ equal ▾ GO

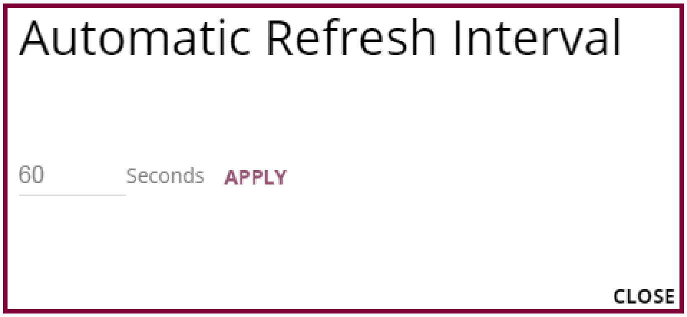
Filter list

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



Click **Automatic Refresh Interval** .

Enter the time and click APPLY .



Automatic Refresh Interval

60 Seconds APPLY

CLOSE

Structure of the GUI configuration menu

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

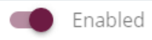
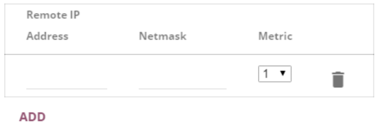
Menu structure

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

The following options are available for the configuration:

Configuration elements

Menu	Function
Eingabefelder	e.g. empty text field Description Text field with hidden input

Menu	Function
	 ********* Enter the data.
Radiobuttons	e.g. IP Address Mode ○ Static ● Get IP Address Select the corresponding option.
Checkbox	e.g. activation by selecting checkbox  Enabled
Dropdown-Menüs	e.g. Full Autonegotiation ▾ Click the arrow to open the list. Select the required option using the mouse.
Interne Listen	e.g.  Remote IP Address · Netmask · Metric 1 ▾ 🗑 ADD Click ADD . A new list entry is created. Enter the corresponding data. If list input fields remain empty, these are not saved when you confirm with **OK**. Delete the entries by clicking the 🗑 icon.

Display of options that are not available

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

⚠ **Important**

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

5.3.1.3 Menus

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

☞ **Note**

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

Chapter 6 Assistants

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

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

Chapter 7 System Management

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

You see a system status overview. In addition, global system parameters, such as the system name, date/time, passwords, timer and licences are managed, and codes and access authorisations for administration are configured.

7.1 Status

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

You see an overview of the following data:

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

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

⚠ **Caution**

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

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

Fields in the System Information menu.

Field	Value
Uptime	Displays the time past since the device was rebooted.
System Date	Displays the current system date and system time.
Serial Number	Displays the device serial number.
BOSS Version	Displays the currently loaded version of the system software.
Back-up of configuration on SD card	Indicates whether a backup configuration is available on the SD card or not.

Field	Value
Last configuration stored	Displays day, date and time of the last saved configuration (boot configuration in flash).
Night Mode Status	Indicates whether your device is in the normal mode (*Off*) or in night mode (*On*).

Fields in the Resource Information menu.

Field	Value
CPU Usage	Displays the CPU usage as a percentage.
Memory Usage	Displays the usage of the working memory in MByte in relation to the available total working memory in MByte. The usage is also displayed in brackets as a percentage.
Memory Card	Shows the status of any optional external memory card that has been inserted, and the size of the memory in GBytes or MBytes.
DSP Channels	Shows the currently used DSP channels.

Fields in the VoIP Trunk Lines menu

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

Fields in the Modules menu

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

Fields in the Physical Interfaces menu.

Field	Value
Interface - Connection	The physical interfaces are listed here and their most important

Field	Value
Information - Link	settings are shown. The system also displays whether the interface is connected or active. Interface specifics for Ethernet interfaces: • IP address • Netmask • Not configured Interface specifics for ISDN interfaces: • Configured • Not configured Interface specifics for xDSL interfaces: • Downstream/Upstream Line Speed

7.2 Global Settings

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

7.2.1 System

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

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

Fields in the menu Basic Settings

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

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

Field	Value
Maximum Number of Accounting Log Entries	Enter the maximum number of login process entries that are stored internally in the device. Possible values are `0` to `1000`. The default value is `20.`
Show Manufacturer Names	Here you can determine if the manufacturer part of a MAC address is to be "translated". The manufacturer part takes up to eight characters at the beginning of the MAC address. Instead of, e.g., `00:a0:f9:37:12:c9`, `BintecCo_37:12:c9` is displayed if this option is enabled.
Autosave Configuration	Here you can choose whether configuration changes are automatically saved. If you enable this option, settings are immediately saved so that they persist after a reboot of the device as soon as you confirm them on a configuration page (usually with the **OK** button).

Transfer to busy subscriber

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

Fields in the menu System Settings

Field	Value
Transfer Signalling	Specify how the call is to be transferred to an internal extension. Possible values: • `With the ringing tone` (the default value): Caller hears the ringing tone while being transferred. • `With music on hold (MoH)`: The caller hears the system's on-hold music while being transferred.
Transfer to busy extension	Set whether a caller may be transferred to a busy subscriber. The function is activated with `Enabled`. The function is disabled by default.

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

Country settings

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

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

Fields in the menu Country Settings

Field	Value
Country Profile	Select the country in which you want to use the system. Note: This does not change the language of the text in the system menu of system telephones. Possible values: • *Deutschland* (default value) • *Nederland* • *Great Britain*

Field	Value
	• *België* • *Italia* • *Danmark* • *España* • *Sverige* • *Norge* • *France* • *Portugal* • *Österreich* • *Schweiz* • *Česko* • *Slovenija* • *Polska* • *Magyarország* • *Ellada*
International Prefix / Country Code	Enter the country code. You need this entry if, e. g., you wish to automatically generate an international number under **SIP Provider**. You dial, as usual, the national prefix e. g. 05151 909999 and the system then automatically dials +495151 909999. If you fail to enter the country code, you may misdial, as the system will then dial +5151 909999. Without the entry **Generate international phone number** and **International Prefix / Country Code**, the full number plus the country code always has to be dialled in the case of SIP providers. Note: Not every SIP provider supports this setting.
National Prefix / City Code	Enter the national prefix and the area code for the location where your system is installed. With a point-to-point ISDN access, this area code is essential, because otherwise e. g. no automatic external callback is possible.

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

Fields in the menu Charge Settings

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

Fields in the menu Day Mode

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

Night operation

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

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

Fields in the menu Night Mode

Field	Value
Team Signalling	Select the call variants for team signalling in night operation.

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

7.2.2 Passwords

Setting the passwords is another basic system setting.

Note

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

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

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

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

fields:

Fields in the System Password menu.

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

PIN1 and PIN2

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

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

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

The following performance features are protected using PIN2:

- Remote access for Follow me, room monitoring

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

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

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

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

Fields in the SNMP Communities menu.

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

Field in the Global Password Options menu

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

Field	Value
	played as asterisks.

7.2.3 Date and Time

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

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

ISDN/Manual

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

The clock switches from summer to winter time (and back) automatically. This is independent of the exchange time or the ntp server time. Summer time starts on the last Sunday in March by switching from 2 a.m. to 3 a.m. The calendar-related or schedule-related switches that are scheduled for the missing hour are then carried out. Winter time starts on the last Sunday in October by switching from 3 a.m. to 2 a.m. The calendar-related or schedule-related switches that are scheduled for the additional hour are then carried out.

Time server

You can obtain the system time automatically, e.g. using various time servers. To ensure that the device uses the desired current time, you should configure one or more time servers.

Note

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

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

Fields in the Basic Settings menu.

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

Fields in the Manual Time Settings menu.

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

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

Field	Description
ISDN Timeserver	Determine whether the system time is to be updated via ISDN. If a time server is configured, the time is only determined over ISDN until a successful update is received from this time server. Updating over ISDN is deactivated for the period in which the time is determined by means of a time server. The function is activated with *Enabled*. The function is enabled by default.
First Timeserver	Enter the primary time server, by using either a domain name or an IP address. In addition, select the protocol for the time server request. Possible values:

Field	Description
	• *SNTP* (default value): This server uses the simple network time protocol via UDP port 123. • *Time Service / UDP*: This server uses the Time service with UDP port 37. • *Time Service / TCP*: This server uses the Time service with TCP port 37. • *None*: This time server is not currently used for the time request.
Second Timeserver	Enter the secondary time server, by using either a domain name or an IP address. In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol via UDP port 123. • *Time Service / UDP*: This server uses the Time service with UDP port 37. • *Time Service / TCP*: This server uses the Time service with TCP port 37. • *None*: This time server is not currently used for the time request.
Third Timeserver	Enter the third time server, by using either a domain name or an IP address. In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol via UDP port 123. • *Time Service / UDP*: This server uses the Time service with UDP port 37. • *Time Service / TCP*: This server uses the Time service with TCP port 37. • *None*: This time server is not currently used for the time request.

Field	Description
Time Update Interval	Enter the time interval in minutes at which the time is automatically updated. The default value is *1440*.
Time Update Policy	Enter the time period after which the system attempts to contact the time server again following a failed time update. Possible values: • *Normal* (default value): The system attempts to contact the time server after 1, 2, 4, 8, and 16 minutes. • *Aggressive*: For ten minutes, the system attempts to contact the time server after 1, 2, 4, 8 seconds and then every 10 seconds. • *Endless*: For an unlimited period, the system attempts to contact the time server after 1, 2, 4, 8 seconds and then every 10 seconds. If certificates are used to encrypt data traffic in a VPN, it is extremely important that the correct time is set on the device. To ensure this is the case, for **Time Update Policy**, select the value *Endless*.
Internal Time Server	Select whether the internal timeserver is to be used. The function is activated by selecting *Enabled*. Time requests from a client will be answered with the current system time. This is given as GMT, without offset. The function is enabled by default. Clients' time requests are answered in the LAN.

7.2.4 Timer

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

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

Fields in the Basic Settings menu.

Field	Description
Call Forwarding (CFNR)	Enter the time in seconds after which a **Call Forwarding (CFNR)** will be executed. Possible values are *1* to *99*. The default value is *15*.
Direct Call	Enter the time in seconds after which the configured number will be dialled when the receiver is lifted. You wish to set up a telephone for which the connection to a specific number is established without entering the number (e.g. emergency telephone). You are not at home. However, there is someone at home who needs to be able to reach you quickly and easily by telephone if necessary (e. g. children or grandparents). If you have set up the "Direct Call" function for one or more telephones, the receiver of the corresponding telephone only needs to be lifted. After a time period without further entries set in configuration, the system automatically dials the configured direct call number. If you do not dial within the specified period from picking up the receiver, automatic dialling is initiated. Possible values are *1* to *30*. The default value is *5*.
External Door Connections	If an external telephone requests a door intercom call, here you can set the time in seconds after which this call is forcefully terminated. Possible values: • *infinite* • *60 seconds* • *120 seconds* • *180 seconds* (default value) • *240 seconds* • *300 seconds*

Fields in the Advanced Settings menu.

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

Field	Value
	given a call waiting. Possible values are *10* to *600*. The default value is *30*.

7.2.5 System Licences

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

The following licence types exist:

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

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

Entering licence data

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

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

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

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

Possible values for Status

Licence	Meaning
OK	Subsystem is activated.
Not OK	Subsystem is not activated.

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

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

☞ **Note**

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

7.2.5.1 Edit or New

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

Activating extra licences

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

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

Fields in the Basic Settings menu.

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

☞ **Note**

If `Not OK` is displayed as the status:

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

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

Deactivating a licence

Proceed as follows to deactivate a licence:

(1) Go to **System Management**->**Global Settings**->**System Licences**->**New**.

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

(3) Confirm with **OK**.

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

7.3 Access Codes

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

7.3.1 Alternative Access Codes

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

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

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

Fields in the Basic Settings menu.

Field	Description
Line Access Digit	Select the exchange code. Possible values: - *None* - *0* (default value)

Field	Description
	- *6* - *7* - *8* - *9*
Pick-up Group	Enter the new code for performance feature **Pick-up (group)**.
Pick-up (Extension)	Enter the new code for performance feature **Pick-up (internal subscriber)**.
Assign project codes	Enter the new code for performance feature **Assign project codes**.
Speed Dial	Enter the new code for performance feature **Speed Dial**.
Trunk Group Selection	Create the new access numbers for the **Trunk Group Selection** feature. To do this, first click **Add** to create a bundle selection, select the bundle and enter the access number you require for the bundle.
System Parking (Open Enquiry)	Create the new access numbers for the **System Parking (Open Enquiry)** feature. To do this, first click **Add** to create a queue in which the caller is to be held, and enter the access number you require for the queue. You can create a maximum of 10 entries.

7.4 Administrative Access

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

7.4.1 Access

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

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

Note

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

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

Service Login (ISDN Web-Access) is disabled by default. If the option is activated, it is deactived again after ca. 30 minutes.

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

Fields in the menu Advanced Settings

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

7.4.1.1 Add

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

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

Fields in the menu Access

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

7.4.2 SSH

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

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

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

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

Note

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

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

Fields in the menu SSH (Secure Shell) Parameters

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

Fields in the menu Authentication and Encryption Parameters

Field	Value
Encryption Algorithms	Select the algorithms that are to be used to encrypt the SSH connection. Possible options:

Field	Value
	- *3DES* - *Blowfish* - *AES-128* - *AES-256* By default *3DES*, *Blowfish* and *AES-128* are enabled.
Hashing Algorithms	Select the algorithms that are to be available for message authentication of the SSH connection. Possible options: - *MD5* - *SHA-1* - *RipeMD 160* By default *MD5*, *SHA-1* and *RipeMD 160* are enabled.

Fields in the menu Key Status

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

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

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

Fields in the menu Advanced Settings

Field	Value
Login Grace Time	Enter the time (in seconds) that is available for establishing the connection. If a client cannot be successfully authenticated during this time, the connection is terminated. The default value is *600* seconds.
Compression	Select whether data compression should be used. The function is activated by selecting *Enabled*. The function is disabled by default.
TCP Keepalives	Select whether the device is to send keepalive packets. The function is activated by selecting *Enabled*. The function is enabled by default.

Field	Value
Logging Level	Select the syslog level for the syslog messages generated by the SSH Daemon. Possible settings: • *Information* (default value): Fatal and simple errors of the SSH Daemon and information messages are recorded. • *Fatal*: Only fatal errors of the SSH Daemon are recorded. • *Error*: Fatal and simple errors of the SSH Daemon are recorded. • *Debug*: All messages are recorded.

7.4.3 SNMP

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

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

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

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

You use this menu to configure the use of SNMP.

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

Fields in the Basic Settings menu.

Field	Value
SNMP Version	Select the SNMP version your device is to use to listen for external SNMP access. Possible values:

Field	Value
	• *v1*: SNMP Version 1 • *v2c*: Community-Based SNMP Version 2 • *v3*: SNMP Version 3 By default, *v1*, *v2c* and *v3* are enabled. If no option is selected, the function is deactivated.
SNMP Listen UDP Port	Shows the UDP port (*161*) at which the device receives SNMP requests. The value cannot be changed.
SNMP multicast discovery	Enable or disable the function **SNMP multicast discovery**. The function is enabled with *Enabled*. The function is enabled by default.

Tip

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

7.5 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.

7.5.1 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 ↻.

7.5.1.1 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.
Switch to SNMP Browser	If you activate the button **Switch to SNMP Browser**, the user can switch to the SNMP browser view, access the parameters and modify all the settings displayed there.

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

Fields in the menu Navigation Entries

Field	Description
Menus	You see all the menus from the GUI's navigation bar. Menus that contain at least one sub-menu are flagged by ▲ and ▼. The icon 🗎 indicates pages. When you create a new access profile, no elements are assigned yet, i.e. all the available menus, sub-menus and pages are flagged with the icon ☒. Each element in the navigation bar can have three values. Click the icon ☒ in the row you want to display these three values. 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.

Field	Description
	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.

7.5.2 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.

7.5.2.1 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**.

Chapter 8 Physical Interfaces

8.1 Ethernet Ports

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

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

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

Note

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

ETH1 - ETH4

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

ETH5

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

VLANs for Routing Interfaces

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

8.1.1 Port Configuration

Port Separation

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

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

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

Values in the Switch Configuration list

Field	Description
Switch Port	Shows the respective switch port. The numbering corresponds to the numbering of the Ethernet ports on the back of the device.
Ethernet Interface Selection	Assign a logical Ethernet interface to the switch port. You can select from five interfaces, *en1-0* to *en1-4*. In the basic setting, switch ports **1-4** are assigned to interface *en1-0* and switch port **5** is assigned to interface *en1-4*
Configured Speed / Mode	Select the mode in which the interface is to run. Possible values: • *Full Autonegotiation* (default value) • *Auto 1000 mbps only* • *Auto 100 mbps only* • *Auto 10 mbps only* • *Auto 100 mbps / Full Duplex*

Field	Description
	- *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.

8.2 Modules

Your system features several slots for modules. These slots can accommodate various modules which allow expansion of the system and offer additional performance features.

The following modules can be installed in the system slots:

- **M 4 S/U + 6 FXS**:

The module contains four S/U interfaces that can be configured as S0 or Upn connectors. There are an additional 6 FXS interfaces available. The S connections can be configured as a S0 connection internally (NT) or externally (TE). The switch from internal to external on the S0 connection occurs only via hardware (coding plug). In the ex works state there is no configuration set. The physical changeover on the module occurs via the **coding plug**modules. The 6 FXS connectors are intended to connect analogue devices (telephone, fax).

- **M 4 S/U + 4U**:

  The module contains four S/U interfaces that can be configured as S0 or Upn connectors. There are an additional 4 U interfaces available. The S connections can be configured as a S0 connection internally (NT) or externally (TE). The switch from internal to external on the S0 connection occurs only via hardware (coding plug). In the ex works state there is no configuration set. The physical changeover on the module occurs via the **coding plug**modules.

- **M 8 FXS**:

  8 analogue terminals can be connected to the **M 8 FXS** modules.

- **M 16 FXS**:

  16 analogue terminals can be connected to the **M 16 FXS** modules.

- **M 4FXO**:

  The module provides 4 FXO connections.

☞ **Note**

You'll find a detailed description of the modules and their possible applications in the installation instructions.

8.2.1 Extension Modules

The modules inserted into and detected by the system are displayed in the **Extension Modules** menu.

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

Values in the Extension Modules list

Field	Description
Module Slot	Displays the slot in the device housing into which the module is

Field	Description
	inserted (see installation instructions and labelling on the inside of the housing cover).
Module	Displays the name of the inserted module.
Notes	Displays the function of the connection configured on the module.
Status	Displays module status.
Reconfig	An action interface is provided in this column in case an inserted module is defective or has been removed, and a new module inserted, if any. Depending on the swapped hardware, you can then perform the following actions: • If you wish to replace an inserted module with a module of another type, plug the new module into the slot and click on the action interface. The new module is detected and all previous settings associated to the old module are deleted. In this case, it is necessary to customise all configuration entries associated to the interfaces of the previous card to the functionalities of the new module. • If you wish to replace a defective module by a module of the same type, insert the new module into the slot. In this case, the existing configuration of the interface-relevant entries in automatically imported. The action interface also automatically disappears.

8.3 ISDN Ports

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

8.3.1 ISDN External

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

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

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

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

8.3.1.1 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 Type	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* • *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.

8.3.2 ISDN Internal

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

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

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

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

fields:

Values in the ISDN Internal list

Field	Description
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 interface is connected. • *`S/U`*: 4 wire (S) or 2 wire (U) Example: *`Module slot 3/1 S/U`* = The interface is located on the module inserted in slot 3 on port 1, and is used as an S or U connection.
Function	Shows the function of the ISDN interface. Possible values: • *`Upn`*: Interface for UPN terminals. • *`S0`*: Interface for ISDN S0 connection.
Default MSN	Indicates whether a default MSN is assigned for an internal S0 Bus. You can use a standard MSN to access unconfigured S0 terminals. As a standard MSN, you can dial the internal numbers configured in the **Numbering**->**User Settings**->**Users** menu and assigned to a terminal in the **Terminals** menu.
Status	Displays the status of the interface.

8.3.2.1 Edit

Choose the ✎ button to edit an entry.

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

Fields in the Basic Settings menu.

Field	Description
Default MSN	Dial the number you want. You can dial any number that you have configured in the **Numbering**->**User Settings**->**Users**->**Numbers** menu. Possible values: • *Not configured* • *<Subscriber Number>*

8.4 Analogue Ports

8.4.1 Analogue External (FXO)

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

Note

At least one 4FXO module needs to be inserted for analogue external connections to be visible.

Note

You can use up to two 4FXO modules.

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

Values in the Analogue External (FXO) list

Field	Description
Name	Shows the name of the analogue interface. Possible values: • *Module Slot*: Shows the slot which the module with the

Field	Description
	analogue interface is inserted into. • `/`: Displays the port on the module to which the analogue connection is connected. • *FXO*: Name for the analogue connection. Example: *Module slot 7/1 FXO* = The interface is located on the module inserted into slot 7 in Port 1 and is used as FXO.
Description	Shows the user-defined description of the analogue interface.
Dialling Method	Displays the dialling method used. Possible values: • *Tone Dialling (DTMF)* (default value) • *Pulse Dialling (PD)*
Status	Displays the status of the interface.
Action	Change the status of the interface by pressing the ⌃ button or ⌄ button in the **Action** column.

8.4.1.1 Edit

Choose the ✎ button to edit an entry.

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

Fields in the Basic Settings menu.

Field	Description
Description	Enter a user-defined description of the analogue interface.
Name	Shows the name of the analogue interface. Possible values: • *Module Slot*: Shows the slot which the module with the analogue interface is inserted into. • *\/*: Displays the port on the module to which the analogue con-

Field	Description
	nection is connected. • *FXO*: Name for the analogue connection. Example: *Module slot 7/1 FXO* = The interface is located on the module inserted into slot 7 in Port 1 and is used as FXO.
Dialling Method	Select which dialling method should be used. Possible values: • *Tone Dialling (DTMF)* (default value) • *Pulse Dialling (PD)*
CLIP	Select whether the CLIP feature is to be used, i. e. whether the caller's number should be displayed to the person called. Possible values: • *Off* (default value): The caller's number is not displayed to the person called. • *FSK*: The data is sent as DTMF.
Receive charges	Select whether your device is to receive charge information from the network. For this purpose, you can define the charge impulse at 12 kHz or 16 kHz. Possible values: • *Off*: Charge information is not received. • *12 kHz* • *16 kHz*

Fields in the Advanced Settings menu.

Field	Description
Busy Tone Detection	Select whether **Busy Tone Detection** should be used. The function is activated by selecting *Enabled*. The function is enabled by default.
Dial Tone Detection	Select whether **Dial Tone Detection** should be used. The function is activated by selecting *Enabled*.

Field	Description
	The function is enabled by default. If the **Dial Tone Detection** is enabled and the external dialling tone is recognised, your **hybird** begins dialling immediately.
Dial Tone Pause	Only for **Dial Tone Detection** disabled. Enter the value you want which the system is to wait for, as a maximum, when dialling a telephone number, before it begins dialling. You can switch on the **Dial Tone Pause** if the **hybird** does not recognise the external dialling tone, or no dialling tone is emitted. You must decide the duration of the **Dial Tone Pause**. Possible values are whole number values between *1* second and *5* seconds.
End-of-Selection Signal	Enter the time that the system is to wait, after dialling a number, before it considers the telephone number to be complete and makes the connection. The default value is *5* seconds.

8.4.2 Analogue Internal (FXS)

The **Analogue Internal (FXS)** menu displays all of your system's available analogue internal connections.

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

Values in the Analogue Internal (FXS) list

Field	Description
Name	Shows the name of the analogue interface. Possible values: • *Module Slot*: Shows the slot which the module with the analogue interface is inserted into. • */*: Displays the port on the module to which the analogue connection is connected. • *FXS*: Name for the analogue connection.

Field	Description
	Example: *Module slot 1/4 F* = The interface is located on the module inserted in slot 1 on port 4, and is used as FXS.
Function	Shows the function of the analogue interface. Possible values: • *Telephone* • *Doorcom Units* • *Multi Function Device/Telefax* • *Modem* • *Answering Machine* • *Emergency Phone* The function of the analogue terminal is configured in the **Terminals**->**Other phones**->**analog** menu.
Status	Displays the status of the interface.

8.5 Relay

The **elmeg hybird 300** / **elmeg hybird 600** has two independent switch contacts.

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

☞ **Note**

Switch contacts are reset to idle if the PABX is reset or has a power failure!

8.5.1 Relay Configuration

The switch contacts are configured in the **Physical Interfaces**->**Relay**->**Relay Configuration** menu.

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

Fields in the Basic Settings menu.

Field	Description
Contact 1 / **Contact 2**	Enter the desired description of the switch contact at **Description**. Only one function can be assigned to each switch contact. Select the type of usage under **Usage**. Possibe values: • *Access Codes*: The relay is switched via a dial code. • *Access Codes (period only)*: The relay is switched via acces codes for a given period (e.g. a door opener is on for three seconds). • *Access Codes (toggle only)*: The relay is toggled via acces codes. • *Alarm Output*: The relay is switched when an alarm call is received. Enter the duration of the key for **Signalling Period**. The programmed switching time for the button can be anything between 1 and 999 seconds. The default value is *3* seconds.

Chapter 9 VoIP (PABX)

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

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

9.1 Settings

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

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

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

9.1.1 SIP Provider

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

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

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

9.1.1.1 Edit or New

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

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

Fields in the Basic Settings menu.

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

Fields in the Outgoing Signalisation Settings menu.

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

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

Fields in the Registrar menu.

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

Fields in the STUN menu.

Field	Description
STUN server	Enter the name or the IP address of the STUN server. STUN = Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) A STUN server is required to allow VoIP devices access to the internet behind an active NAT. This determines the current public IP address for the connection, which is used for precise remote addressing. Maximum number of characters: 32.
Port STUN server	Enter the number of the port to be used for the connection to the STUN server. The default value is `3478`. A 5 digit sequence is possible.

Fields in the Timer menu.

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

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

Fields in the Advanced Settings menu.

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

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

Fields in the Further Settings menu

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

Field	Description
Dial End Monitoring Time	Select the time in seconds (after dialling the last digit of a call number) after which the system begins external dialling. The default value is `5`.
Call Hold inside the PBX system	The network-centric functions call hold, call switching, 3-way conference call and call waiting can be enabled by disabling the option **Call Hold inside the PBX system**. The functions are then no longer provided by the PABX, but by the public network, instead. A corresponding contract with provider and customer is required which incluides a bandwidth limitation (number of simultaneously usable voice channels). If a SIP provider - such as Deutsche Telekom - offers multiple SIP accounts / numbers via a single connection, this option should be deactivated for each of them. This is required to support the bandwidth limitation for several numbers via a single network connection. If an external call is held, no MoH is played through the PABX, but the public network provides MoH or an announcement for the remotely held party.
Call Forwarding extern (SIP 302)	Select whether calls are to be redirected externally with the SIP provider. The call is forwarded using SIP status code 302. The function is activated by selecting `Enabled`. The function is disabled by default.
Generate international phone number	If you enable this function and, under **Global Settings**, you have entered the **Country Profile** (`49` for Germany), the 0049 is generated automatically in front of the number when a number with an area code is dialled. The function is activated by selecting `Enabled`. The function is disabled by default.
Generate national subscriber number	If you enable this function and, under **Global Settings**, you have entered the **National Prefix / City Code** (e.g. `40` for Hamburg), the number dialed is automatically prefixed with 040. The function is activated by selecting `Enabled`.

Field	Description
	The function is disabled by default.
Deactivate number suppression	If you enable this function, the number is always sent, independently of whether you have switched **Suppress outgoing CLIP (CLIR)** on or off for an extension. The function is activated by selecting *Enabled*. The function is disabled by default. If the function is disabled, you have additional options. In order to ensure that your system can forward anonymous calls with SIP connections you can specify in which part of the SIP header information the string "anonymous call" is is transferred. The information can be transferred in multiple parts. For most prviders you can simply keep the preconfigured setting *Privacy ID* = *Enabled* . For the service provider 1 & 1 you need to additionally enable *Privacy Header* . Possible values: • *Display* • *Users* • *Domain* • *Privacy Header* • *Privacy User* • *Privacy ID*
SIP Header Field: FROM Display	Not for **Trunk Mode** = *Off* The sender ID is placed in the "Display" field of the SIP header. Possible values: • *None* (default value): The sender ID is not sent. • *Username*: The user-configured user name is displayed. • *Caller Address*: The user-configured number the called party is displayed. • *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.

Field	Description
SIP Header Field: FROM User	Not for **Trunk Mode** = *Off* The sender ID is sent in the "User" field of the SIP header. Possible values: • *Username*(default value): The user-configured user name is displayed. • *Caller Address*: The user-configured number the called party is displayed. • *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.
SIP Header Field: P-Preferred	Not for **Trunk Mode** = *Off* The so-called "p-preferred-identity" field is added to the SIP header and contains the sender ID. Possible values: • *None* (default value): The sender ID is not sent. • *Username*: The user-configured user name is displayed. • *Caller Address*: The user-configured number the called party is displayed. • *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.
SIP Header Field: P-Asserted	Not for **Trunk Mode** = *Off* The so-called "p-asserted-identity" field is added to the SIP header and contains the sender ID. Possible values: • *None* (default value): The sender ID is not sent. • *Username*: The user-configured user name is displayed. • *Caller Address*: The user-configured number the called party is displayed. • *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.
Substitution of Interna-	Select whether the prefix (e.g. 00) should be replaced by + for

Field	Description
tional Prefix with "+"	international numbers. The function is activated by selecting *Enabled*. The function is disabled by default.
PBX coupling	Select whether another PABX can log into your system. In this way, several PABX systems can be linked. The function is activated by selecting *Enabled*. The function is disabled by default.
Delete SIP bindings after Restart	If after registering with a provider a reset of the system should occur, for example, or a power failure, depending on the provider, another registration may prove impossible. Enabling these performance features allows re-registration after restart. The function is activated by selecting *Enabled*. The function is disabled by default.
Upstreaming Device with NAT	If you enable this function, you can use a gateway with NAT and still make VoIP calls. Without this function, it may not be possible to call you with VoIP if you use a gateway with NAT. The function is activated by selecting *Enabled*. The function is disabled by default.
Early media support	Select whether you'll allow exchange of voice and audio data before a receiver accepts a call. The function is enabled with *Enabled*. The function is enabled by default.
Registration type	Specify how registration and authentication at a provider are to be handled, or if they can omitted completely. In the latter case, the relevant data are sent to a particular IP address that is already known to the correspondent. Registration and authentication are not then needed and the Registration function is disabled. An example of this method is Microsoft Exchange SIP. If a registration is required, it can be carried out in either of two

Field	Description
	ways: • *Single*: With this option, a single MSN is registered with the SIP provider. • *Bulk (BNC)*: With this option, a SIP Trunk (DDI) is registered with the SIP provider, i.e. several numbers are registered under a single address.
T.38 FAX support	Select whether faxes shall be transmitted with T.38. The function is enabled with *Enabled*. The function is enabled by default. If the function is disabled, faxes are transmitted with G.711.
Substitution of Incoming Number Prefix	For incoming calls, if the call number should be forwarded in the system in modified form: in the first input field enter the sequence of the incoming number to be replaced by the number sequence entered in the second input field.
Send SIP UPDATE	This function ensures that after a call transfer the number of the new call partner is displayed for the initial calling party. **Note** Note that this function is not supported by all service providers. *Enabled* activates the functions. The function is not enabled by default.
Request URI	In some applications (especially in DDI connections) the target address of a SIP call needs to be extracted from the Request URI. By activating this option the address is preferably read from this field of the invite. The option is not active per default.
Check Source IP	As a response to a DNS SRV request, your SIP provider transmits the addresses of valid registration servers. If you activate this option, each SIP invite has its source IP checked against these valid addresses. If it does not originate from one of them,

Field	Description
	the invite is ignored. The option is not active per default.
TLS certificate check	Only for DDI / SIP trunk connections. If a connection is encrypted using TLS (Transport Layer Security) a validity check on the server certificate of the remote station is performed. The option is not active per default.

Fields in the Codec Settings menu

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

9.1.2 Locations

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

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

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

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

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

9.1.2.1 Edit or New

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

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

Fields in the Basic Settings menu.

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

Field	Description
	Enter the IP address or DNS name that you want under **IP Address/DNS Name**. Also enter the required **Netmask**.
Interfaces	Only for **Type** = *`Interfaces`* Indicate the interfaces to which the devices of a SIP location are connected. Click **Add** to select a new interface. Under **Interface**, select the interface you want.
Upstream Bandwidth Limitation	Determine whether the upstream bandwidth is to be restricted. The bandwidth is reduced with *`Enabled`*. The function is disabled by default.
Maximum Upstream Bandwidth	Enter the maximum data rate in the send direction in kBits per second.
Downstream Bandwidth Limitation	Determine whether the downstream bandwidth is to be restricted. The bandwidth is reduced with *`Enabled`*. The function is disabled by default.
Maximum Downstream Bandwidth	Enter the maximum data rate in the receive direction in kBits per second.

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

Fields in the Advanced Settings menu.

Field	Description
DSCP Settings for rtp Traffic	Select the Type of Service (TOS) for RTP data. Possible values: • *`DSCP Binary Value`* (default value): Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). The

Field	Description
	preconfigured value is *101110*. • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F.

9.1.3 Codec Profiles

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

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

9.1.3.1 Edit or New

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

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

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for the entry.
Codec Proposal Sequence	Choose the order in which the codecs are offered for use by the system. If the first codec cannot be used, the second is tried and so on. Possible values: • *Default* (default value): the codec in the first position in the

Field	Description
	menu will be used if possible. • *Quality*: The codecs are sorted by quality. The codec with the best quality is used if possible. • *Low Bandwidth*: The codecs are sorted by required bandwidth. If possible, the codec with the lowest bandwidth requirement is used. • *High Bandwidth*: The codecs are sorted by required bandwidth. If possible, the codec with the highest bandwidth requirement is used.
G.711 uLaw	Only for **Codec Proposal Sequence** not *default* ISDN codec with US characteristic G.711 uLaw passes audio signals in the range of 300-3500 Hz and samples them at the rate of 8,000 samples per second. At 64 kbit/s bit rate the mean opinion score (MOS) is 4,4. This audio codec uses µlaw quantization.
G.711 aLaw	Only for **Codec Proposal Sequence** not *default* ISDN codec with EU characteristic G.711 aLaw passes audio signals in the range of 300-3400 Hz and samples them at the rate of 8,000 samples per second. At 64 kbit/s bit rate the mean opinion score (MOS) is 4,4. This audio codec uses alaw quantization.
G.722	Only for **Codec Proposal Sequence** not *default* G.722 passes audio signals in the range of 50-7000 Hz and samples them at the rate of 16,000 samples per second. At 64 kbit/s bit rate the mean opinion score (MOS) is 4,5.
G.729	Only for **Codec Proposal Sequence** not *default* G.729 passes audio signals in the range of 300-2400 Hz and samples them at the rate of 8,000 samples per second. At 8 kbit/s bit rate the mean opinion score (MOS) is 3,9.
G.726 (16 kbit/s)	Only for **Codec Proposal Sequence** not *default* G.726 (16 kbit/s) passes audio signals in the range of 200-3400

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

9.1.4 Options

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

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

Fields in the Basic Settings menu.

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

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

Fields in the Advanced Settings menu.

Field	Description
DSCP Settings for sip Traffic	Select the Type of Service (TOS) for SIP data. Possible values: • *DSCP Binary Value* (default value): Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). The default value is *110000*. • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F.
SIP Port	Specify the port SIP data are to be transferred through.

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

Fields in the SIP over TLS menu

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

Chapter 10 Numbering

10.1 Trunk Settings

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

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

10.1.1 Trunks

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

Note

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

Values in the Trunks list

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

10.1.1.1 Edit or New

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

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

Fields in the Basic Settings menu

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

Fields in the Outgoing Signalisation Settings menu

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

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

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

Fields in the Advanced Settings menu

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

10.1.2 Trunk Numbers

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

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

External numbers at the point-to-point connection

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

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

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

External subscriber numbers at point-to-multipoint connection

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

10.1.2.1 Edit or New

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

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

Fields in the Basic Settings menu.

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

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

10.1.3 Trunk Groups

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

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

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

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

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

10.1.3.1 Edit or New

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

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

Fields in the Basic Settings menu.

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

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

10.1.4 X.31

Packet-switched data transmission (X.31)

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

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

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

Note

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

10.1.4.1 Edit or New

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

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

Fields in the Basic Settings menu.

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

10.2 User Settings

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

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

10.2.1 Users

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

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

Only for compact systems: The following users are predefined:

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

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

10.2.1.1 Basic Settings

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

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

Fields in the Basic Settings menu.

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

Fields in the External Numbers menu.

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

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

Fields in the Class of Service menu.

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

Fields in the Further Options menu.

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

10.2.1.2 Numbers

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

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

Fields in the Internal Numbers menu.

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

10.2.1.3 Outgoing Signalisation

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

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

Fields in the list Outgoing Signalisation

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

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

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

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

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

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

Proceed as follows to move the selected entry:

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

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

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

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

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

10.2.1.4 Optional Rerouting

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

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

Fields in the Optional Rerouting menu.

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

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

10.2.1.5 Authorizations

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

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

Fields in the Basic Settings menu.

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

Fields in the User HTML Configuration menu.

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

Call Through

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

☞ **Note**

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

Fields in the Further Options menu.

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

10.2.2 Class of Services

In the **Numbering**->**User Settings**->**Class of Services** (CoS) the functions and 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. The authorisation class *CoS Default* is configured by default.

10.2.2.1 Basic Settings

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

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

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the entry.

Fields in the Line Access Authorization menu.

Field	Description
Line Access 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. • *Region*: The telephones cannot make any national or inter-

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

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

Number display

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

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

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

Note

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

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

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

Fields in the Further Settings menu.

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

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

10.2.2.2 Features

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

Call pickup

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

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

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

Call waiting

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

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

The called party can:

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

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

Analogue terminals

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

Analogue terminals get the system call waiting tone. The number of the call-waiting party can be shown in the analogue telephone display if it features the corresponding 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, for which the Data Protection performance feature is set up (e. g. fax, modem)
- in analogue subscriber's dialling status (the receiver has been picked up, but there is no connection yet)
- for current call-waiting protection
- for dialling a team number. Then there is no call waiting for analogue team subscribers.

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

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

Fields in the Feature Authorization menu.

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

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

Simplex operation

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

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

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

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

Note

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

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

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

Message

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

Caution

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

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

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

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

System telephones

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

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

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

Individual announcement

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

Team announcement

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

Note

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

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

MWI (Message Waiting Indication)

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

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

Analogue terminals

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

ISDN terminals

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

System telephones

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

Hotel room telephone

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

Reception telephone

- MWI information can be switched on and off from a reception telephone to a room 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 *Allowed*. The function is enabled by default.
Receive Announcement Calls	Select whether this authorisation class may receive announcements. The function is activated by selecting *Allowed*. 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 *Allowed*. The function is enabled by default.
Net Direct (Keypad)	Select whether you wish to use your network operator's current ISDN functions also from older ISDN or analogue telephones by entering a key sequence. The function is activated by selecting *Allowed*. The function is disabled by default.

10.2.2.3 Applications

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

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

Fields in the Application Authorization menu.

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

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

10.2.3 Parallel Ringing

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

10.2.3.1 Edit or New

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

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

Fields in the Basic Settings menu.

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

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

10.3 Groups &Teams

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

10.3.1 Teams

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

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

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

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

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

10.3.1.1 General

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

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

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

Fields in the Basic Settings menu.

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

Fields in the Further Settings menu.

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

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

Fields in the Timer menu.

Field	Description
Team Speed Timer	Here, enter the **Team Speed Timer** following which call forwarding after time shall be performed in the team. The default value is *15* seconds.
Simultaneous after time	With linear and rotating team calls, there is the option for all team subscribers to be simultaneously called after a defined period. The default value is *60* seconds.
Wrap-up Timer	This setting is only enabled in **Signalling** *Even 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 are not included in the time calculation. The default value is *0* seconds; the range *0*... *999* seconds.

10.3.1.2 Variant 1 - 4

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

Internal numbers of a team

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

For internal team calls, a team number and team name can be assigned to the team in the configuration. If a team number is dialled, the caller sees the team name until a team 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. Only for compact systems: The numbers *10*, *20*, *21*, *22* are assigned to the *Team global*.
External Assignment	Only if **Assignment** = *External* Enter the number of the external subscriber.
Route and Charge Assignment	Only if **Assignment** = *External* Charges for the call and assignment of an external connection occur via the selected internal subscriber.

Automatic call acceptance in the team

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

If a team is called, it can be defined in configuration that the call is automatically accepted, and that the caller hears an announcement or music. The target subscriber(s) are called during this time. After the receiver is picked up, the announcement or music is turned off and the subscribers are connected to each other.

Possible settings for automatic call acceptance:

- *Simultaneous*: All assigned terminals are called simultaneously. If a terminal is busy, call waiting can be used.
- *Linear*: All assigned terminals are called in the sequence of their entry in configuration. If a terminal is engaged, the next free terminal is called. The call is signalled ca. 15 seconds per subscriber. This period can be set between 1 and 99 seconds (per team) in the configuration. If subscribers are on the phone or logged out, there is not forwarding time for these.
- *Rotating*: This call is a special case of the linear call. After all terminals are called, call signalling begins again with the first entered terminal. The call is signaled until the caller replaces the receiver or the call is ended by the exchange (after ca. 2 minutes).
- *Adding*: The terminals are called in the order of their entry in the subscriber list. Every terminal that has already been called is called again, until all entered terminals are called.
- *Linear,Simultaneous after time* or *Rotating,Simultaneous after time*: Rotating or linear is set for the team call. After defined times have run out, all team 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 corresponds to **SignallingRotating** and insures that all team subscribers receive the same number of calls. For every subscriber who has ended a call, a **Wrap-up Time** (0...999 seconds) is set up for the team/subscriber, during which she receives no more calls. Calls received by the subscriber on his number rather than via the team and self-initiated calls are not included in the even distribution calculation. Even distribution begins with the subscriber who hasn't received calls for the longest time, on restart with the first subscriber entered in the subscriber list. A subscriber who has logged out of the team (code number or 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" is to be enabled for this call option. If a team subscriber is currently engaged, you can decide whether additional calls for this team should be signalled. If "Busy on Busy" is set for a team, other callers are signalled as "engaged". The function is activated by selecting *Enabled*. The function is disabled by default.
Automatic Call Pick-up with	Select whether an incoming call should be automatically accepted, and the caller hear the desired music-on-hold or announcement. Signalling of the call to the team proceeds. The caller bears the costs for the existing connection. The function is activated by selecting *Enabled*. The function is disabled by default. Also select the desired music-on-hold or announcement. Possible values: • *<File_x>* • *MOH Intern 1* • *MOH Intern 2* • *MoH Wave 1 to 8*

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

Fields in the Rerouting Functions menu.

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

10.3.1.3 Log on / Log off

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

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

Fields in the Basic Settings menu.

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

10.4 Call Distribution

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

10.4.1 Incoming Distribution

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

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

10.4.1.1 Edit

Choose the ✎ icon to edit existing entries.

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

Fields in the Basic Settings menu.

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

Fields in the Internal Number and Rerouting Settings menu.

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

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

Fields in the Call Through Settings menu.

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

10.4.2 Misdial Routing

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

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

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

10.4.2.1 Edit

Choose the ✎ icon to edit existing entries.

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

Fields in the Basic Settings menu.

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

10.4.3 Caller number distribution

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

10.4.3.1 Edit or New

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

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

Fields in the menu Basic Settings

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

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

☞ **Note**

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

Chapter 11 Terminals

11.1 elmeg System Phones

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

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

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

11.1.1 System Phone

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

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

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

- Dialling from the system phone book
- Announcement and simplex operation with other system telephones on the system
- Function keys for control of system features (enable call options, login/logout in teams, line keys, connection keys). The status of a feature can be indicated via LED's assigned to individual function keys.
- Access to the system menu of the system. In this menu, advanced functions are offered by the PABX system.

Choose the ✎ icon to edit existing entries.

As soon as a **Description** is entered for the system telephone and an entry is selected in the **Internal Numbers** field and copied with **OK**, the entry for that device is moved to the upper part of the overview. To continue configuration, click the ✎ symbol again.

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

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

Note

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

11.1.1.1 General

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

Telephone type

Various types of telephones can be configured.

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

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

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

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

Fields in the menu Basic Settings

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

Field	Description
	tion. Possible values: • *Not defined (Unrestricted Registration)*: No location is defined. According to set default behaviour, the 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 menu Number Settings

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

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

Key extensions

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

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

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

Fields in the menu Extensions

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

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

Fields in the menu Codec Settings

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

Fields in the menu Further Settings

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

11.1.1.2 Settings

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

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

Fields in the menu Basic Settings

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

Field	Description
	• *Danish*: Not for **S530** and **S560** • *Spanish*: Not for **S530** and **S560** • *Swedish*: Not for **S530** and **S560** • *French*: Not for **S530** and **S560** • *Portugues*: Not for **S530** and **S560** • *Česko*: Not for **S530** and **S560** • *Norwegian*: Not for **S530** and **S560** • *Greek*: Not for **S530** , **S560** , **CS290** , **CS290-U** , **IP-S290** , **IP-S290plus** • *Icelandic*: Not for **S530** , **S560** , **CS400**, **CS410** , **CS410-U** , **IP-S400** • *Polish*: Not for **S530** and **S560** • *Hungarian*: Not for **S530** and **S560** • *Russian*: Not for **S530** , **S560** , **CS290** , **CS290-U** , **IP-S290** , **IP-S290plus**
Headset Support	Not for **S530** and **S560**. Select whether the headset should automatically accept calls. ☞ **Note** If you wish to use a headset, you must configure a headset key and a key for automatic call acceptance on your PABX system. On the system telephone, you must select a headset type and enable the key for automatic call acceptance.
Call Waiting	Select whether another call shall be supported for this telephone through call waiting or a display notification. The function is activated by selecting *Enabled*. The function is disabled by default. If **Call Waiting** is enabled, define for which calls you wish to allow call waiting. Possible values:

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

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

Fields in the menu Advanced Settings

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

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

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

11.1.1.3 Keys / T400 / T400/2 / T500

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

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

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

Values in the list Keys

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

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

Edit

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

You can use the following functions with system telephones:

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

- *Dial Key (Keypad sequence)*: You can store a keypad sequence on every function key.
- *Extension Key (User)*: You can set up dialling to an internal extension using a line key. After pressing the corresponding key, hands free is switched on and the internal extension entered is selected. If a call is signalled on the internal extension you have entered, you can pick this up by pressing the line key.
- *Extension Key (Team)*: You can set up dialling to a team using a line key. After pressing the corresponding key, hands-free is activated and the entered team is called according to its enabled call option. If a call is signalled for the entered team, you can pick it up by pressing this connection key.
- *Trunk Line*: An ISDN connection or a VoIP provider is set up under a connection key. If this key is pressed, automatic hands-free is enabled and the corresponding ISDN connection is assigned. You then hear the external dialling tone. If an external call is signalled on another internal telephone, you can pick it up by pressing this line key.
- *System Call (Announcement User)*: You can set up a connection to another telephone without this connection having to be actively accepted. As soon as the telephone has accepted the announcement, the connection is established and the announcement key LED is enabled. The announcement can be ended by renewed pressing of the announcement key or by pressing the loudspeaker key. The LED switches off again at conclusion of the announcement.
- *System Call (Announcement Team)*: You can configure an announcement for a team by setting up a function key. The way this works is the same as that described above.
- *Login / Log Out, Team*: If you are entered as a subscriber in the call assignments for one or more teams, you can set up a key so that you can control the call signalling of your telephone. If you're logged in, team calls are signalled to your telephone. If you are logged out, no team calls will be signalled.

  The call numbers entered in the telephone can be logged in/logged out from a team using a set function key (**MSN**-1... **MSN**-9). Before entering a team number, you must select the telephone call number index (MSN) that is entered in the corresponding team call assignments.
- *System Call (Announcement enable)*: You can also selectively deny or allow announcements using a function key. To use announcements, you must be authorised for the corresponding authorisation class.
- *Receive Intercom Calls*: You can set up a key is such a way that a connection to the specified telephone is established without this connection having to be actively accepted.
- *System Call (Intercom enable)*: You can set up a key in such a way that the simplex operation function is allowed or denied. To use simplex operation, the function must be allowed in the corresponding authorisation class.

- *Boss Key* / *Secretary Key*: You can set up a key as a special line key. The Boss telephone and Secretary telephone properties are saved in both telephones with these keys.
- *Diversion Secretary*: You can set up a key in such a way that incoming calls to the Boss telephone are automatically routed to the Secretary telephone.
- *Call Forwarding (CFNR)*: You can set up a key so that delayed call diversion is configured for a specific number (MSN) on your system telephone. Pressing the key when the phone is not in use turns call forwarding on and off. Call forwarding configuration over a programmed key is only possible for numbers 1 to 9 (MSN-1...MSN-9) of the phone. In order to be able to use call forwarding, you need to have set up at least one number.
- *Call Forwarding (CFU)*: You can set up a key so that immediate call diversion is configured for a specific number (MSN) on your system telephone. Pressing the key when the phone is not in use turns call forwarding on and off. Call forwarding configuration over a programmed key is only possible for numbers 1 to 9 (MSN-1...MSN-9) of the phone. In order to be able to use call forwarding, you need to have set up at least one number.
- *Call Forwarding (CFB)*: You can set up a key so that call diversion on engaged is configured for a specific number (MSN) on your system telephone. Pressing the key when the phone is not in use turns call forwarding on and off. Call forwarding configuration over a programmed key is only possible for numbers 1 to 9 (MSN-1...MSN-9) of the phone. In order to be able to use call forwarding, you need to have set up at least one number.
- *Macro Function*: You can configure a key so that by pressing it a saved macro is executed.

  The macro function can only be programmed at the phone.
- *Headset Control* (not with the **S5x0**): If you've connected and configured a headset to your telephone over a separate headset socket, operation of the headset occurs over a function key. Press the headset key to initiate or accept calls. If you already have an active connection over the headset, you can end the call by pressing the headset key.
- *Automatic Call Pick-up*: Your telephone can accept calls automatically without you having to lift the receiver or press the loudspeaker key. Automatic call acceptance is switched on or off using the function key assigned. You can configure a separate function key for each number ("MSN-1"..."MSN-9"), or a function key for all numbers. The period after which calls are automatically accepted is configured once for all numbers of the telephone.
- *Trunk Group Access*: Several external ISDN (if supported by you device) or IP connections to bundles can be grouped in the system. With a bundle key, you can save these connections on a function key. If this key is pressed, automatic hands-free is enabled and a free B channel of the corresponding bundle is assigned. You then hear the external dialling tone.

- *Connection Key* (not with the **S5x0**): In addition to the softkeys "Connection 1..", function keys can be configured on the system telephone or the extension for operation while brokering. At least two connection keys must be configured.
- *Hotel Rooms*: You can assign a key in such a way that when pressed, the guest is checked in or out (first level), or the selected hotel room phone is called (second level). You must configure this key on the first level, then the connected key on the second level is automatically assigned and, as the case applies, its content overwritten.
- *System Parking (Open Enquiry)*: The called party is put on hold for enquiry and dials a code. The telephone is now freed for other operations, e. g. announcements. Another party can accept the call, if he lifts the receiver and dials the relevant code of the held call. The codes assigned by the PABX can also be entered in the function keys of one or more system telephones. If a call is set to open hold for enquiry by pressing the function key, this is indicated by flashing LEDs on the function keys for the system telephones set up for this. The call is transferred by pressing the corresponding function key. This performance feature is only possible if only one call is on hold.
- *Agent wrap-up Time*: You can configure a key so that when it is pressed, an agent's post-processing time is switched on or off at a team call centre (first level), or extended (second level).
- *Night Mode*: You can configure a key so that by pressing it night operation is switched on or off.

Note

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

- *Parallel Ringing* (only **S5x0**): If a parallel call to another telephone is configured, both connections will ring when a call comes in. The call is accepted where first picked up.
- *Shift* (only **S5x0**): With this key, you can access second level functions.
- *Do not Disturb* (only **S5x0**): With this key, you enable or disable the Do not Disturb function which you have configured under **Terminals**->**elmeg System Phones**->**System Phone**->**Settings**.

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

Fields in the menu Telephone

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

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

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

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

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

Transfer key

Select the ↑↓ icon to move configured function keys.

Fields in the menu Key

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

Fields in the menu Move to

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

11.1.1.4 Device Info

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

Meaning of the list entries

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

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

Meaning of Key Extensions

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

11.1.2 elmeg IP

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

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

Note

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

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

Choose the ✎ icon to edit existing entries.

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

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

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

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

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

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

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

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

Note

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

11.1.2.1 General

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

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

Fields in the menu Basic Settings

Field	Description
Description	To clearly identify the telephone in the system, enter a description for the telephone.
Phone Type	Displays the type of your IP telephone. Possible values: • *elmeg IP120* • *elmeg IP130* • *elmeg IP140* • *elmeg IP620* • *elmeg IP630* • *elmeg IP680*
Location	Select the location of the telephone. You define locations in the **VoIP**->**Settings**->**Locations** menu. Depending on the setting in this menu, default behaviour for registration of VoIP subscribers for which no location should be defined is displayed for selection. Possible values: • *Not defined (Unrestricted Registration)*: No location is defined. According to set default behaviour, the 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 telephone.

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

Key extension modules

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

Fields n the menu Extensions

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

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

Fields in the menu Further Settings

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

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

Fields in the menu Codec Settings

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

11.1.2.2 Numbers

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

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

You can delete assigned numbers from the list with 🗑.

Values in the list Number Settings

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

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

11.1.2.3 Keys / T100

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

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

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

Values in the list Keys

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

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

Edit

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

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

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

Note

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

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

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

Fields in the menu Telephone

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

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

Transfer key

Select the ↑↓ icon to move configured function keys.

Fields in the menu Key

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

Fields in the menu Move to

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

11.1.2.4 Settings

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

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

Fields in the menu System Phone

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

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

11.1.3 elmeg DECT

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

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

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

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

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

Choose the ✎ icon to edit existing entries.

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

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

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

In order to be able to use automatic provisioning, click the ✎ icon again and add the respective 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. You require an installed SD card (if supported by you device). All languages to be deployed need to be stored on the SD card. Single-cell systems load a required language from the SD card on demand.

11.1.3.1 General

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

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

Fields in the menu Basic Settings

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

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

Fields in the menu Further Settings

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

Fields in the menu Codec Settings

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

11.1.3.2 Numbers

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

The system automatically assigns a serial number, the **Mobile Number**, to each mobile part so that you can identify the device. You can then use **Add** to assign a **Internal Number** to a mobile part from the list.

You can delete assigned numbers with 🗑.

Values in the list Numbers

Field	Description
Mobile Number	Displays the serial number of the mobile part. This number is permanently assigned to the mobile part so that it can be uniquely identified.
Internal Number	Displays the assigned internal number.
Displayed Description	Displays the description entered for the internal number. In standby mode this description is shown on the mobile part's display.
User	Displays the user's name.

11.1.3.3 Settings

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

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

Fields in the menu Basic Settings

Field	Description
Admin Password	Select whether the administrator password should be reset. The function is activated by selecting *Enabled*. The function is disabled by default. As soon as you select the **OK** button, the password is reset to the default setting.

11.2 Other phones

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

Terminals of the corresponding category (VoIP, ISDN, or analog) are sorted alphabetically in the **Description** column. Click the column title of any other column to sort entries in ascending or descending order.

11.2.1 VoIP

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

Specific instructions for configuring VoIP, see *VoIP - Configuration example (a smartphone as an internal VoIP telephone)* on page 178.

11.2.1.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to add VoIP terminals.

The **Terminals**->**Other phones**->**VoIP**->**New** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	Enter a description for the IP telephone.
Location	Select the location of the telephone. You define locations in the **VoIP**->**Settings**->**Locations** menu. Depending on the setting in this menu, default behaviour for registration of VoIP subscribers for which no location should be defined is displayed for selection. Possible values: • *Not defined (Unrestricted Registration)*: No location is defined. According to set default behaviour, the 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 Net-works Only)*: No location is defined. According to set default behaviour, the subscriber is only registered if located in a private network. • *<Location>*: A defined location is selected. The subscriber is only registered if at this location.

Fields in the menu Number Settings

Field	Description
Internal Numbers	Select the internal number for this terminal You can define several internal numbers. Possible values: • *No free Extension Available*: All configured internal numbers are already in use. First configure another user with additional numbers. • *<Internal Number>*: Select one of the existing numbers of the configured users.

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

Fields in the menu SIP Client Settings

Field	Description
SIP Client Mode	Select whether a *dynamic* SIP client or a *static* SIP client is to be used. Possible values: • *Dynamic* (default value): Your device (e. g. a standard SIP telephone) runs a SIP registration to tell the system its (dynamic) IP address. • *Static* : The system accepts an incoming call from a (statically configured) SIP client without this client needing to have been registered beforehand, if the IP address of the client matches the IP address entered under **SIP Client IP Address**. This mode is used by, for example, the MIcrosoft Office Communications Server and other unified xommunication servers.
SIP Client IP Address	Only for **SIP Client Mode** = *Static*. Enter the static local IP address of the SIP client.
Port Number	Only for **SIP Client Mode** = *Static*. Enter the number of the port to be used for connection. A 5 digit sequence is possible. For example, port *5065* must be entered for connection to a Microsoft Exchange Communication Server.
Transport Protocol	Only for **SIP Client Mode** = *Static*. Select the transport protocol for the connection. Possible values: • *UDP* (default value) • *TCP* For example, the *TCP* protocol must be entered for connection to a Microsoft Exchange Communication Server.

Fields in the menu Codec Settings

Field	Description
Codec Profile	Select the codec profile to be used if the connection is over a

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

Fields in the menu Further Settings

Field	Description
Multiple SIP Connections (Sub-Exchange)	Select whether multilinks shall be allowed from this terminals. Operation as subsystem: Only in case of connection of a subsystem to a system Here, with a disabled performance feature, only a connection via the subscriber SIP registration is possible. If a second call comes in, it is accepted and the existing call is held. With an enabled performance feature, several SIP connections are possible over the same login. If the performance feature is enabled for as system without subsystem, two simultaneous calls on the phone are not connected to each other after the receiver is replaced but released, for example. Here, the performance feature should not be set. The function is activated by selecting *Enabled*. The function is disabled by default.
No Hold and Retrieve	The performance features "hold a call" and "retrieve a held call" are not available on certain telephones. The function is activated by selecting *Enabled*. The function is disabled by default.
T.38 FAX support	Select if you want to transmit FAX documents via Voice over IP using the T.38 standard. *Enabled* activates T.38 support. Per default, the function is disabled. If the function is disabled, FAX documents are transmitted using G.711.

11.2.2 VoIP - Configuration example (a smartphone as an internal VoIP telephone)

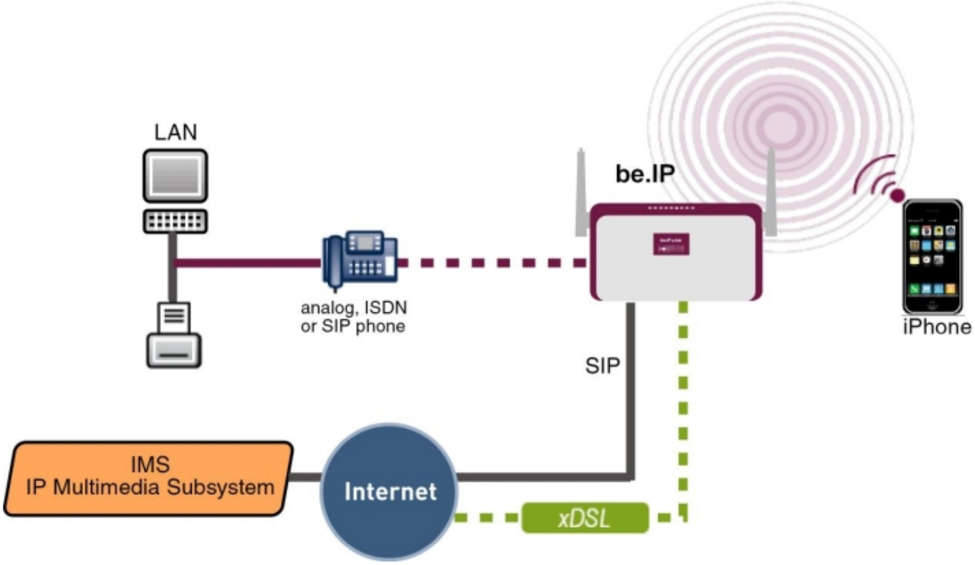
Requirements

- An **be.IP**
- A configured with the Assistents **Initial operation** SIP connection `DeutschlandLAN`
- A taken with the Assistents in operation WLAN access point
- An Smartphone e.g. **iPhone 4**
- Available connection to the WLAN access poin the **be.IP**
- SIP app, Media5-fone, installed on the smartphone

Note

Please note that the scope of settings and supported functions may vary with different versions of smartphone operating systems (iOS, Android) and the smartphone app, Media5-fone.

Example scenario



Configuration target

Integration of a smartphone as an internal VoIP phone

Overview of Configuration Steps

Creating a User and integrate Smartphone

Field	Menu	Value
Name	**N** **e** **Assistants->Telephony->Users->w**	e.g. *User 33 (iPhone)*
Description	**N** **e** **Assistants->Telephony->Users->w**	e.g. *iPhone 33*
Password	**N** **e** **Assistants->Telephony->Users->w**	e.g. *1234*
Displayed Description	**N** **e** **Assistants->Telephony->Users->w->Add**	e.g. *#33 iPhone*
Internal Number	**N** **e** **Assistants->Telephony->Users->w->Add**	e.g. *iPhone*
Description	**Terminals->Other phones->VoIP->New**	e.g. *33*
Internal Numbers	**Terminals->Other phones->VoIP->New**	*33 (#33 iPhone)*

Configuration of the smartphone app using the example Media5-fone

Field	Menu	Value
Title	**New SIP Account -> Manual Settings**	e.g. *be.IP*
User Name	**New SIP Account -> Manual Settings**	e.g. *33*
Password	**New SIP Account -> Manual Settings**	e.g. *1234*
Address	**New SIP Account -> Manual Settings-> Server**	e. g. *192.168.0.250*
Port	**New SIP Account -> Manual Set-**	*5060*

Field	Menu	Value
	tings-> Server	
Activating a proxy	**New SIP Account -> Manual Settings-> Server**	*Disabled*
SIP Transport	**New SIP Account -> Manual Settings-> Server**	*UDP*
Switch SRTP	**New SIP Account -> Manual Settings-> Server**	*Switched off*
Mailbox Number	**New SIP Account -> Manual Settings ->Advanced**	e.g. *50*
Write MWI	**New SIP Account -> Manual Settings ->Advanced**	*Enabled*
DTMF Method	**New SIP Account -> Manual Settings ->Advanced**	*RTP Input Signal Band*
Codecs Wi-Fi	**New SIP Account -> Manual Settings ->Advanced**	*G.711 µLaw, G.711 aLaw*

Configuration of external number

Field	Menu	Value
International Prefix / Country Code	**Assistants->Telephony->First steps**	e.g. *00* / *49*
National Prefix / City Code	**Assistants->Telephony->First steps**	e.g. *0* / *911*
Connection Type		*SIP Provider*

Field	Menu	Value
	New	
Type		*DeutschlandLAN*

Field	Menu	Value
	New	
Description		e.g. *SIP Connection*

Field	Menu	Value
	New->Next	
Single Number (MSN)		e.g. *111111*

Field	Menu	Value
	New->Next	
Description		e.g. *SIP number 1*

Field	Menu	Value
	New->Next	
Connection Type		*SIP Provider*

Field	Menu	Value
	New	
Type		*DeutschlandLAN*

Field	Menu	Value
	New	
Name		e.g. *`SIP Connection`*

Field	Menu	Value
	New->Next	
Single Number (MSN)		e.g. *222222*

Field	Menu	Value
	New->Next	
Description		e.g. *SIP number 2*

Field	Menu	Value
	New->Next	
Connection Type		*SIP Provider*

Field	Menu	Value
	New	
Type		*DeutschlandLAN*

Field	Menu	Value
	New	
Name		e.g. *SIP Connection*

Field	Menu	Value
	New->Next	
Single Number (MSN)		e.g. *333333*

Field	Menu	Value
	New->Next	
Description		e.g. *SIP number 3*

Field	Menu	Value
	New->Next	

Signalling of incoming calls

Feld	Menü	Wert
Assignment Type	**Assistants->Telephony->Call Distribution-> <111111>** ✎	*Team*
Team	**Assistants->Telephony->Call Distribution-> <111111>** ✎	e.g. *40 (Team global)*
Assignment Type	**Assistants->Telephony->Call Distribution-> <222222>** ✎	*Extension*
Assignment	**Assistants->Telephony->Call Distribution-> <222222>** ✎	e.g. *20 (Sys Tel 20)*
Assignment Type	**Assistants->Telephony->Call Distribution-> <333333>** ✎	*Extension*
Assignment	**Assistants->Telephony->Call Distribution-> <333333>** ✎	e.g. *33 (#33 iPhone)*

Signalling of specific number

Feld	Menü	Wert
Trunk	**Numbering->User Settings->Users-> <User 33> (iPhone)** ✎ **->Outgoing Signalisation->Internal Number-><33>** ✎	*SIP Connection*
Outgoing Signalisation	**Numbering->User Settings->Users-> <User 33> (iPhone)** ✎ **->Outgoing Signalisation->Internal Number-><33>** ✎	e.g. *333333*

Change registration timer in Media5-fone

Field	Menu	Value
Reg. Timer (Sec)	**More -> Settings -> Configure SIP Accounts -> be.IP -> Server -> Reg. Timer (Sec)**	e.g. *1200*

Configuration of codecs in Media5-fone

Field	Menu	Value
DTMF Method	**More -> Settings -> Configure SIP**	*RTP Input Signal*

Field	Menu	Value
	Accounts -> **be.IP** -> **Advanced**	*Band*
Codec Wi-Fi	**More** -> **Settings** -> **Configure SIP Accounts** -> **be.IP** -> **Advanced**	e.g. *G.711 µLaw, G.711 aLaw*

11.2.3 ISDN

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

Only for compact systems. Two predefined entries are displayed:

Description	Interface	Terminal Type	Internal Numbers	License Allocation
ISDN 1	S0 1	Telephone	30	Enabled
ISDN 2	S0 2	Telephone	35	Enabled

11.2.3.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to add ISDN terminals.

The **Terminals**->**Other phones**->**ISDN**->**New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the ISDN telephone.
Interface	Select the interface to which the ISDN telephone shall be connected.

Fields in the Basic Phone Settings menu

Field	Description
Terminal Type	Select the terminal type. Possible values: • *Telephone* (default value) • *Answering Machine* • *Voice Mail* • *Emergency Phone*

Field	Description
Internal Numbers	Select the internal number for this terminal You can define several internal numbers. Possible values: • *No free Extension Available*: All configured internal numbers are already in use. First configure another user with additional numbers. • *<Internal Number>*: Select one of the existing numbers of the configured users.

11.2.4 analog

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

Only for compact systems: Two predefined entries are displayed:

Description	Interface	Terminal Type	Internal Numbers	License Allocation
a/b 1	FXS 1	Telephone	10	Enabled
a/b 2	FXS 2	Telephone	11	Enabled
a/b 3	FXS 3	Telephone	12	Enabled
a/b 4	FXS 4	Multi Function Device/Telefax	13	Enabled

11.2.4.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to add analog terminals.

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

The **Terminals**->**Other phones**->**Analogue**->**Edit** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the analogue telephone.

Field	Description
Interface	Select the interface to which the telephone shall be connected.

Fields in the Basic Phone Settings menu

Field	Description
Terminal Type	Select the terminal type. Possible values: • *Multi Function Device/Telefax* • *Telephone* • *Modem* • *Answering Machine* • *Emergency Phone*
Internal Number	Select the internal number for this terminal. Possible values: • *No free Extension Available*: The configured internal number is already in use. First configure another user with additional numbers. • *<Internal Number>*: Select one of the existing numbers of the configured users.

Fields in the Phone Settings menu

Field	Description
Call Waiting	Select whether call waiting shall be allowed for this device. The function is activated by selecting *Enabled*. The function is enabled by default.
Do not Disturb	Select whether you wish to use the call protection (do not disturb) performance feature. With this performance feature, you can enable call signalling to your terminal. Analogue terminals use system code numbers for this. Possible values:

Field	Description
	- *Internal Calls not signaled* - *External Calls not signaled* - *No Calls signaled*

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

Fields in the CLIP Settings menu

Field	Description
Show incoming Number (CLIP)	Select whether the subscriber's number shall be transmitted. The function is activated by selecting *Enabled*. The function is enabled by default.
Show Date and Time	Only for **Show incoming Number (CLIP)** *Enabled* Select whether the time and date should be taken from your PABX system and displayed on the telephone. The function is activated by selecting *Enabled*. The function is enabled by default.
Show incoming Name (CNIP)	Only for **Show incoming Number (CLIP)** *Enabled* Select whether the caller's number shall be displayed. The caller's number can be displayed if an entry exists in the system telephone book. The function is activated by selecting *Enabled*. The function is enabled by default.
Show incoming waiting Number (CLIP off Hook)	Only for **Show incoming Number (CLIP)** *Enabled* Select whether the number of a caller waiting during an existing call shall be displayed. The function is activated by selecting *Enabled*. The function is enabled by default.

Fields in the Further Settings menu

Field	Description
Show new Messages (MWI)	Only for **Show incoming Number (CLIP)** *Enabled* Select whether new messages shall be signalled on a voice mail system. The function is activated by selecting *Enabled*. The function is enabled by default.
Transmit Charges Pulses	Select whether the system shall generate charge pulses for the terminal from the ISDN network charge information. For this purpose, you can define the charge impulse at 12 kHz or 16 kHz. Possible values: • *Off*: Charge information from the ISDN network is not transmitted. • *12 kHz* • *16 kHz* The default value is *16 kHz*
FXS Ringing Frequency	Call signalling in analogue terminals occurs by configuring a call switching voltage at the called analogue connections. This call switching voltage is converted into a specific ring tone by the analogue terminal. In the system, for the analogue connections you can set a call switching voltage with a frequency of *25 Hz* or *50 Hz*. The default value is *50* Hz.
Flash Time for DTMF Dialling	When operating analogue terminals with the multifrequency code dialling method, you can set the flashtime that the system detects as maximum flash length. If the terminal flash is longer than the defined period, "replaced receiver" is detected. Values from *100 ms* to *1000 ms* are possible. The default value is *400 ms*.

Chapter 12 Call Routing

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

12.1 Outgoing Services

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

12.1.1 Direct Call

In the **Call Routing**->**Outgoing Services**->**Direct Call** menu you configure numbers that are dialled directly without the subscriber needing to dial a number themselves on the phone.

You wish to configure a telephone for which a call to a specific number is set up even without entry of the number (e.g. emergency telephone). You are not at home. However, there is someone at home who needs to be able to reach you quickly and easily by telephone, if required (e.g. children or grandparents). If you have set up the "Direct Call" function for one or more telephones, the receiver of the corresponding telephone only needs to be lifted. After a period without further entries set in configuration, the system automatically dials the configured direct call number.

If you do not dial within the specified period from picking up the receiver, automatic dialling is initiated.

The time for Direct Call is set under **System Management**->**Global Settings**->**Timer**->**Direct Call**.

Note

In the system, up to 10 direct call destinations with names and telephone numbers can be set up by the administrator. These destinations should then only be assigned to the terminals by the user via the user configuration interface. In the configuration, system direct call, or a direct call specifically configured for the terminal, can then be set by the user.

12.1.1.1 Edit or New

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

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

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the entry.
Direct Call Number	Enter the number to be automatically dialled if no number is to be dialled for a certain time after the receiver has been picked up.

12.1.2 Call Forwarding

In the **Call Routing**->**Outgoing Services**->**Call Forwarding** menu, you configure call forwarding of external calls for an internal subscriber.

You are temporarily away from your office, but don't want to miss a call. With call forwarding to another number, e.g. your mobile, you can receive your calls even when you are not at your desk. You can forward calls on your number to any call number. It can occur *Immediately*, *On no reply* or *On Busy*. Call forwarding *On no reply* and *On Busy* can exist concurrently. If you are not near your telephone, for example, the call is forwarded to another number (e.g. your mobile phone) after a short period. If you are making a call at your desk, other caller may receive the busy signal. You can forward these callers e.g. to a colleague or the secretary by using call forwarding on busy.

Every internal subscriber to the system can forward her calls to another number. Calls can be forwarded to internal subscriber numbers, internal team numbers or external numbers When the number to which calls shall be forwarded is entered, the system automatically checks whether it's an internal or external number.

In a team, call forwarding can be set up for one subscriber in the team. This call continues to be signalled to the other team subscribers. Call forwarding to an internal or external subscriber is performed in the system.

Call forwarding to an internal number is performed in the system. If an internal call to an external number is to be forwarded, forwarding also occurs in the system. Here, the connection is on the bundle cleared for the subscriber doing the setup. If call forwarding occurs via an ISDN connection, one B channels remains in use; in case of forwarding from external to external, it's both B channels. Two possibilities exist for call forwarding of an external call to an external number:

- Call forwarding in the exchange: Call forwarding is conducted at the exchange if only one subscriber is entered in the call allocation for an external call. For call forwarding in the exchange, the performance features Call Deflection (point-to-multipoint connection) or Partial Rerouting (point-to-point connection) must be enabled with the network operator for the relevant ISDN connections.
- Call forwarding in the system: Call forwarding occurs in the system if the required performance features for call forwarding at the exchange are not available for the relevant ISDN connections. If several telephones (e. g. a team), some of which have set up call forwarding, receive an external call, the corresponding call forwarding is performed in the system. Here, the external connection is set up over a bundle's B channel, cleared for the subscriber initiating the setup. This B-channel remains assigned for the duration of active call forwarding.

Note

If the system is connected to the external ISDN (if supported by you device), for external-to-external connections, the system systematically attempts to initiate call forwarding via the exchange For teams, there can be manual definition of whether call forwarding shall occur via the exchange or the system. If the system possesses no ISDN connections, or if Call Deflection (point-to-multipoint connection) or Partial Rerouting (point-to-point connection) has not been ordered from the network operator, call forwarding occurs solely in the system.

12.1.2.1 Edit or New

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

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

Fields in the Basic Settings menu

Field	Description
Internal Number	Select the internal number to which the incoming calls shall be forwarded.
Type of Call Forwarding	Select when incoming calls shall be forwarded to the specified internal number.

Field	Description
	Possible values: • *Immediately* • *On Busy* • *On no reply* (default value) • *On busy / On no reply*
Target Number "On no reply"	Enter the number to which incoming calls shall be forwarded after time.
Target Number "On busy"	Enter the number to which incoming calls shall be forwarded on busy.
Target Number "Immediate"	Enter the number to which incoming calls shall be forwarded immediately.

12.1.3 Dial Control

In the **Call Routing**->**Outgoing Services**->**Dial Control** menu, you block specific numbers/partial numbers, or release these .

You wish to prevent dialling of specific numbers in the system, e. g. the numbers of expensive value-added services. Enter these numbers or partial numbers into the dial ranges list of blocked numbers. All subscribers subject to dial ranges cannot dial these numbers. However, if you should need specific numbers from a blocked sector, you can clear these via the dial ranges list of cleared numbers.

You can block specific numbers or prefixes with the blocked numbers list. You can clear the blocked numbers or prefixes with the cleared numbers list. If a number entered as a cleared number is longer than one entered as a blocked number, this number can be dialled. When you dial a number, dialling after the blocked digit is terminated and you hear the busy tone. You can assign each user individually to the dial ranges in the user settings.

Example: Blocked number *01*, all external numbers that begin with *01* are blocked. Cleared number *012345*, dialling can proceed. All external numbers that begin with *012345* can be dialled. If two identical numbers (same number sequence and same number of digits, e. g. *01234* and *01234*) are entered in the list of cleared numbers as well as the list of blocked numbers, dialling of the number is prevented.

Note

Subscribers who enjoy full or partial dialling access (no outside line access) are authorised for dialling of cleared numbers via the list of cleared numbers.

Please ensure that the area code is entered in the configuration, otherwise, the block can be circumvented in the local network by prefixing the area code.

12.1.3.1 Edit or New

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

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

Fields in the Basic Settings menu.

Field	Description
Inhibited number	Enter the number that cannot be dialled.
Enabled number	Enter the number for which dialling is explicitly permitted.

12.1.4 Priority Numbers

In the **Call Routing**->**Outgoing Services**->**Priority Numbers** menu you configure numbers with particular special functions, e. g. emergency functions.

In your system configuration, you can enter numbers that must be accessible in an emergency. If you now dial one of these priority numbers, it is detected by the system and an ISDN B channel is automatically cleared. If the external ISDN B channels are already in use, one of the ISDN B channels is freed up and the calling subscribers hear the busy tone. An ongoing priority call is not interrupted.

12.1.4.1 Edit or New

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

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

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the entry.
Priority Number	Enter the number which can even be dialled if all B channels are occupied. In this case, an external B channel is released for this connection and reassigned for the priority call. An ongoing priority call is not interrupted.

12.1.5 Special Numbers

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

12.1.5.1 Edit or New

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

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

Fields in the Basic Settings menu

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

12.2 Automatic Route Selection

In the **Call Routing**->**Automatic Route Selection** menu, you can set up routes for external calls in addition to configured line occupancy. Here, bundles released for users can be selectively assigned to ongoing calls according to the dialled number, or new providers entered along with their network access prefixes. You then specifically define the routing for individually created zones for every weekday.

12.2.1 General

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

The menu **Call Routing**->**Automatic Route Selection**->**General** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
ARS	Select whether to enable the ARS performance feature (Automatic Route Selection). The function is activated by selecting *Enabled*. The function is disabled by default.
Routing Stage	Select whether additional routes shall be used if an entered provider or bundle cannot be accessed. Possible values: • *1 (No Fallback)*: If the entered provider or selected bundle is (**Call Routing**->**Automatic Route Selection**->**Zones &Routing**-> **Edit/Add** -> **Mo-Su** ->**Routing Stage 1**) not available, connection setup is terminated. • *2*: If the entered provider or selected bundle (**Call Routing**->**Automatic Route Selection**->**Zones &Routing**-> **Edit/Add** -> **Mo-Su** ->**Routing Stage 1**) is not available, there is an attempt to initiate the connection over the additional entered routing variant (**Call Routing**->**Automatic Route Selection**->**Zones &Routing**-> **Edit/Add** -> **Mo-Su** ->**Routing Stage 2**). • *3* (default value): If neither of the two entered providers or bundles (**Call Routing**->**Automatic Route Selection**->**Zones &Routing**-> **Edit/Add** -> **Mo-Su** ->**Routing Stage 1** and **Routing Stage 2**) is available, dialling occurs via the provider entered as the default for the user (**Numbering**->**Class of Service**->**Add**->**Basic Settings**->**Trunk Line Selection with Line Access Number**).

12.2.2 Interfaces / Provider

In the **Call Routing**->**Automatic Route Selection**->**Interfaces / Provider** menu, enter the routes or providers along with their network access profiles.

12.2.2.1 Edit or New

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

The **Call Routing**->**Automatic Route Selection**->**Interfaces / Provider**->**New** menu 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.

12.2.3 Zones &Routing

In the menu **Call Routing**->**Automatic Route Selection**->**Zones &Routing** you define the zones via which dialling shall proceed using specific routes or providers.

Configuration of the routing tables for the defined zones occurs individually for each 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.

12.2.3.1 Trunk Numbers

In the **Trunk Numbers** area, enter the number or partial number of the zones for which you wish to configure the routing tables.

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the entry.
Zones	Configure the desired external zones which should be dialled via the desired entered provider/routes. Possible values: • `Number/Partial Number`: Enter the number or part of a number identifying a zone. • `Name`: Enter a name for this zone.

12.2.3.2 Mon - Sun

In the **Mon** - **Sun** area, select the desired times for each routing level, and the desired route or provider via which outgoing calls shall be routed from the entered time.

Fields in the <Weekday> menu

Field	Description
Routing Stage 1	Configure the switching times for routing level 1. For this, first select the **Start Time** from which routing shall occur over a specific interface or a specific network provider, and select the latter under **Interface / Provider**.
Routing Stage 2	Configure the switching times for routing level 2. For this, first select the **Start Time** from which routing shall occur over a specific interface or a specific network provider, and select the latter under **Interface / Provider**.

Chapter 13 Applications

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

13.1 Calendar

In the **Applications**->**Calendar** menu, you can decide whether to make new entries or modifications in the calendar.

Every company has fixed business hours. You can enter these in the system's internal calendar. For example, all calls outside of business hours can be signalled to a exchange or an answering machine. During this period, your employees can perform other tasks, without being interrupted by telephone calls. The individual call options of a team are automatically switched through the calendars.

You wish to modify the external calling authorisations after business hours for specific subscribers. In the system configuration, you can set individually for each user whether the authorisation for external calls is automatically switched. The switch occurs according to the data in the assigned calendar.

You can set up five types of calendars in the system. The "Authorisation Class" and "Night Operation" calendars are intended for central switching and can only be set up once. The "Team Signalling", "Intercom Signalling" and "Redirect to internal/external number" calendars can be set up repeatedly. Several different switching times can be selected for each weekday.

In the configuration, a calendar can be assigned to all performance features for which several options can be defined (e.g. teams) Switching between the individual call options then occurs at the switching times of the assigned calendar.

13.1.1 Calendar

In the menu **Applications**->**Calendar**->**Calendar** you can view, modify or copy a previously set calendar as well as create new calendars.

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

13.1.1.1 General

In the **General** area you define the name of the calendar to be created.

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

Fields in the menu Basic Settings

Field	Description
Description	Enter a description for the calendar.
Application	Select the application for which the calendar shall be used. Please note that this field cannot be edited with pre-existing entries. If another application is to be configured, you must create another entry and delete the existing one. Possible values: • *Team Signalling* (default value): Here, several calendars can be set up. • *Doorline Signalling*: Here, several calendars can be set up. • *Night Mode*: Here, only one calendar can be set up. • *Class of Service*: Here, only one calendar can be set up. • *Rerouting for internal/external Number*: Here, several calendars can be set up. • *Voice Mail System*: Here, several calendars can be set up. • *Alarm Input*: Here, several calendars can be set up.

13.1.1.2 Mon - Sun / Exception

Mon - Sun

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

The **Applications**->**Calendar**->**Calendar**->**Mon - Sun** menu consists of the following fields:

Fields in the <Weekday> menu

Field	Description
Switching Points	Enter the desired switching times. For this, under **Time**, for each weekday select the desired

Field	Description
	switching points to which switching shall occur from any divergent active switching option in the desired switching options selected under **Action**. Depending on the application, the following switching options are available: • *Team Signalling*: Call option 1 to call option 4 • *Doorcom Signalling*: Door Intercom call option 1 and door intercom call option 2 • *Night Mode*: Night operation on and night operation off • *Class of Service*: Authorisation class by default and authorisation class optional • *Rerouting for internal/external Number*: Redirect option 1 to redirect option 4 • *Voice Mail System*: Action *In the Office* and *Out of Office* • *Alarm Input*: Night operation on and night operation off
Use settings from	Only if settings have already been performed for a weekday. Select from which weekday the settings should be imported. If you require specific settings for this day, select the option *Individual*.

Exception

In the **Exception** area, select whether holidays shall be taken into account and, if so, how.

The menu **Applications**->**Calendar**->**Calendar**->**Exception** consists of the following fields:

Fields in the Settings holidays menu

Field	Description
Consider public holidays	Select whether appointments entered in the **Applications**->**Calendar**->**Public Holiday** menu shall also be considered in this calendar. The function is activated by selecting *Enabled*.

Field	Description
	The function is disabled by default.
Use settings from	Only if **Consider public holidays** is enabled. Select from which weekday the settings for holidays should be imported. Configure weekdays in menu **Applications**->**Calendar**->**Calendar**-> **Mon - Sun** If you require specific settings for holidays, select the option *Individual*.
Switching Points	Only for **Use settings from** = *Individual* Enter the desired switching times. For this, under **Time**, select the desired switching points to which switching shall occur from any divergent active switching option in the desired switching options selected under **Action**. Depending on the application, the following switching options are available: • *Team Signalling*: Call option 1 to call option 4 • *Doorcom Signalling*: Door Intercom call option 1 and door intercom call option 2 • *Night Mode*: Night operation on and night operation off • *Class of Service*: Authorisation class by default and authorisation class optional • *Rerouting for internal/external Number*: Redirect option 1 to redirect option 4 • *Voice Mail System*: Action *In the Office* and *Out of Office* • *Alarm Input*: Night operation on and night operation off

13.1.2 Public Holiday

In the **Applications**->**Calendar**->**Public Holiday** menu, you can enter holidays or any special days for which divergent settings should be made via the calendar. The holiday entries are sorted by date!

13.1.2.1 Edit or New

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

The menu **Applications**->**Calendar**->**Public Holiday**->**New** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for a holiday.
Date (DD - MM)	Enter the date with day and month in two-digit form. Incorrect entries, e. g. 31.02 are accepted and saved but not executed by the system.

13.2 Rerouting

In the **Applications**->**Rerouting** menu, you configure how incoming calls should be handled by default in the system.

13.2.1 Rerouting Functions

In the **Applications**->**Rerouting**->**Rerouting Functions** menu you can set up various redirect options for *Immediately*, *On Busy*, *On No Reply* or *On Busy and On No Reply*. You then assign these redirect options to the external connections in the **Numbering**->**Call Distribution**->**Incoming Distribution** menu.

13.2.1.1 Edit or New

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

The **Applications**->**Rerouting**->**Rerouting Functions**->**New** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the redirect function.

Field	Description
Type of Rerouting Function	Select the desired exchange function. Possible values: • *Immediately* (default value) • *On Busy* • *On No Reply* • *On Busy and On No Reply*

Fields in the On Busy Settings menu.

Field	Description
Size of Queue	Only for **Type of Rerouting Function** = *On Busy* or *On Busy and On No Reply* In this field, you can configure the maximum number of subscribers on hold. The queue may include up to 10 subscribers. Additional callers get a "busy" tone. Possible values are *0* (no queue) to *10*. The default value is *0*.
Take Waiting Calls with	Only for **Type of Rerouting Function** = *On Busy* or *On Busy and On No Reply* Define what callers on hold shall hear (internal or configured music-on-hold, announcement). Possible values: • *MoH Wave 1* to *MoH Wave 8* • *MoH internal 1* (default value) • *MOH internal 2* • *Off*
Max waiting time in the queue	Only for **Type of Rerouting Function** = *On Busy* or *On Busy and On No Reply* Define maximum time a caller can remain on hold. After expiration of this time, the caller shall be transferred to the defined redirect destination. Leave *Endless* for an unlimited queue (corresponds to value 0). Disable *Endless*, to enter the desired value.

Fields in the On No Reply Settings menu.

Field	Description
Time for Rerouting on No Reply	Define maximum time a caller can remain on hold if she cannot reach the destination number. After expiration of this time, the caller shall be transferred to the defined redirect destination. The default value is *30* seconds.

Fields in the Further Settings menu.

Field	Description
Announcement	Select whether the incoming call shall be redirected to an announcement. Possible values: • *Off* (default value): The incoming call is not redirected to an announcement. • *MoH Wave 1* to *MoH Wave 8*
Target Number	Select the internal number to which the incoming call shall be redirected. Possible values: • *No Number (Disconnect)*: The call is terminated, the connection ended. • *<Extension number>*: If a destination number is entered, the call is forwarded.
Transfer with	The caller hears the defined announcement or music while her call is being transferred. Possible values: • *Ring tone* • *MoH Wave 1* to *MoH Wave 8* • *MOH internal 1* • *MOH internal 2* • *<Wave file>*

Announcement before query

You have set up a general information call number which customers with various problems or requests ring up. Naturally, no single employee or team can provide information in every subject areas. So the caller would need to be transferred to the individual departments. If you knew beforehand which requests (subject area) a caller had, you could immediately transfer him to the competent department. Thus, your callers don't have to be initially accepted and transferred by an exchange. Every caller decides for him/herself with which employee he/she wishes to be connected.

With the performance feature **Auto Attendant with DISA** calls are automatically accepted by the system. The caller then hears an announcement with information about which entries are possible during or after the announcement. Once the entry is made, the announcement ends and the caller is transferred to an internal subscriber or team. If the caller provides a false or no entry, he/she is transferred to the defined redirect destination (internal subscriber or team). While being transferred, the caller hears a ring tone or the system's music-on-hold.

Note

DISA - Direct Inward System Access Once a call is received by the system, the caller is automatically transferred after a code number is entered. This code is assigned to an internal number in the system. Entry of a number or code must occur during the announcement. Once the announcement (Wave file) ends, no more entries are accepted. There follows redirect to a defined redirect destination. The performance feature **Auto Attendant with DISA** is an integral part of the system and can accept up to 28 calls simultaneously.

Fields in the Announcement/Auto Attendant Settings menu.

Field	Description
Call Switching	Select how incoming calls are to be transferred. Possible values: • `Announcement without DISA` (default value): The configured announcement is played. There follows either transfer to the configured internal number, or the connection is interrupted and the caller hears the busy tone. • `DISA, dial internal numbers`: The caller is prompted to enter an internal number. The call is forwarded to the number. • `DISA, dial code numbers`: The caller is prompted to enter a code number from 0 to 9. The desired internal numbers are assigned to the codes. The caller is then transferred

Field	Description
	to the configured internal number.
Number of playbacks	Select how many times the announcement shall be continuously repeated. At conclusion, the caller hears the busy tone.
Auto Attendant with DISA	Only if **Call Switching** = *`DISA, dial code numbers`* For ever desired DISA code number, select the desired internal number to which the caller shall be transferred.

13.2.2 Rerouting Applications

In the **Applications**->**Rerouting**->**Rerouting Applications** menu, you can configure when which redirect option is to be enabled. You can switch the various options either via calendar or manually.

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

13.2.2.1 General

In the **General** area, you perform basic settings for a redirect application.

The **Applications**->**Rerouting**->**Rerouting Applications**->**New** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the redirect application.
Type of Rerouting Application	Select the destination to which an incoming call shall be redirected. Possible values: • *`Trunk Number`* (default value) • *`Extension`* • *`Global`*
Switch call signalling	Select how to switch between options

Field	Description
	Possible values: • *No calendar,only manually* • *<Calendar>*

13.2.2.2 Variant 1 - 4

In the **Variant** area, you configure the redirect options. You can define up to 4 options.

The menu **Applications**->**Rerouting**->**Rerouting Applications**->**Variant** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Assignment	Choose the redirect function to which you wish to assign the selected option.

13.3 Voice Applications

In the **Applications**->**Voice Applications** menu, you configure you system's wave files.

A professional greeting, especially on the telephone, constitutes a company's visiting card. Voice applications make this possible for every business. Indeed, while being transferred, the caller receives information that's individually tailored, e. g. according to department, or is simply entertained with pleasant music-on-hold.

You wish to employ special music as music-on-hold, or specific announcements for your clients. You can load your self-produced Wave files to the system.

User-specific voice and music files can be saved in the system. Storage space for 2 MoH melodies is available in the system basic settings. The available storage space can be extended with an SD card (if supported by you device). The length of the language and music files that can be saved is based upon the SD card used. Voice and music data is saved in Wave format.

The following voice applications can be defined in the system:

- Announcement before query
- Announcement without query/Infobox
- Wake-up call

- Music on hold

You can find additional information on function, configuration and operation in the description of the individual performance features.

Basic settings of voice applications

The voice applications can be assigned to individual performance features in two different ways.

Every user employing a voice application with this connection always hears the corresponding voice announcement or music from the start. A newly-arrived user hears the voice announcement or music from the start. The number of users who can simultaneously use such a voice application is limited to 28.

Please note that externally played music or voice application music are free of third-party copyrights (GEMA free). Files in other formats must be converted into the company-specific Wave format before being saved in the system.

Note

Please note that Wave files must be available in the following format:

- Bit rate: 128 kbps
- Sampling size: 16 bits
- Channels 1 (mono)
- Sampling rate: 8 kHz
- Audio format: PCM

13.3.1 Wave Files

In the **Applications**->**Voice Applications**->**Wave Files** menu, you can configure your announcement/melody files and volume. You also have the option to play back voicemail messages or download these to your PC. To save a message, click on the 💾 icon. The download dialog then opens. To listen to a message, click on the ▶ icon.

13.3.1.1 Edit

Choose the ✎ icon to edit existing entries. Select 🗑 to change the entry.

MoH internal 1 and *MoH internal 2* are files specified in the system and can thus not be deleted.

The **Applications**->**Voice Applications**->**Wave Files**->**Edit** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the Wave file.
Select file	Click **Browse...** and select the Wave file to be loaded into the system through the Explorer window.
Volume	Select the volume at which the Wave file shall be played by default. Select *0* to play the file at a predefined default volume. You can gradually diminish the volume using the negative values, and increase it with the positive ones. Possible values: • *-5* • *-4* • *-3* • *-2* • *-1* • *0* (default value) • *+1* • *+2* • *+3*

13.4 System Phonebook

In the **Applications**->**System Phonebook** menu, you can enter and administer numbers in the system phone book.

The employees in your company must phone many customers. This is where the system phone book comes in. You need not enter the customer's number but can extract the name via the system telephone display, and dial. Customer names and telephone numbers can be centrally administered by an employee. If a customer whose number has been entered in the phone book calls, his/her name appears in the system telephone display. The system features an integrated phone book in which you can save phone book entries of up to 24-digits (numbers) and up to 20-character names (text).

When creating a telephone book entry, a **Speed Dial Number** code is assigned to each entry. Authorised telephones can initiate speed dial from the phone book via these speed dial numbers.

System telephones

System telephones can dial from the system phone book via a special menu. To search for a telephone entry, enter the first letters (max. 8) of the desired name and confirm the entry. The system always provides 8 phone book entries, which you can view successively. Select the desired entry and confirm with **OK**. You must now begin to dial within 5 seconds. The system telephone redialling list displays the name of the dialled subscriber instead of her number. If a system telephone receives a call whose number and name are saved in the system phone book, the caller's name is indicated in the system telephone display.

Note

The user's other numbers (**Mobile Number** and **Home Number**) are only displayed in the system telephone phone book menu. They are not displayed in the **System Phonebook** menu of the user interface. Entries in the system telephone phone book menu with the (M) mark refer to an entered **Mobile Number** of a user; those with the (H) mark to **Home Number**.

Note

Your PABX system supports LDAP (Lightweight Directory Access Protocol) for providing the entries of the system phonebook to other devices. Name, Number as well as mobile and private numbers can be transferred this way.

13.4.1 Entries

In the **Applications**->**System Phonebook**->**Entries** menu, all configured telephone book entries are displayed with the corresponding speeddial index. The entries in the **Description** column are sorted alphabetically. Click the column title of any column to sort entries in ascending or descending order.

13.4.1.1 Edit or New

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

The menu **Applications**->**System Phonebook**->**Entries**->**New** consists of the following

fields:

Fields in the Phonebook Entry menu.

Field	Description
Description	Enter a description for the entry. Subsequent sorting in the phone book follows the initial letters of the entry.
Phone Number	Enter the telephone number (internal or external).
Speed Dial Number	Enter a speed dial code. If a speed dial code is entered, counting is automatic; i.e. speed dial is automatically assigned. Numbers from *0* to *999* are possible.
Call Through	Select whether the telephone number for the **Call Through** function has been activated. If a telephone number is approved for this, and the caller uses this number for the **Call Through** functions, the caller's authorisation to use the function is checked against the phonebook record. The function is activated by selecting *Enabled*. The function is disabled by default.

13.4.2 Import / Export

You can import and export phone book data in the **Applications**->**System Phonebook**->**Import / Export** menu. You can import data exported from Microsoft Outlook, for example. The phone book data stored in your device is exported to a text file.

The **Applications**->**System Phonebook**->**Import / Export** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Action	Select the desired action. Possible values: • *Export* (default value): You can export the names saved in **Applications**->**System Phonebook**->**Entries** into a text file (specifying phone number, speed dial, call through).

Field	Description
	- *Import*: You can import a text file in the following format: The file imported must consist of individual rows in the following format: name, phone number, speed dial, call through (1 = enabled, 2 = disabled). Example: Name,Phone Number,Speeddial Number,Call Through Hans,123456,1,1 Klaus,234567,2,2 Max,345678,3,1
Separator	Only for **Action** = *Import* and Default File Format not enabled Enter the separator type in the import file. Possible values: - *Comma* (default value) - *Semicolon* - *Space* - *Tabulator*
Select file	Only for **Action** = *Import* select the file to be imported.

You also have the option to import a CSV file.

If the data record consists of more than one column, you have the option to generate two address book entries from the data record for the import (e.g. one for business and one private entry.) To do this, specify the data to be used as the name and phone number in an additional import step. If you want to generate only one phonebook entry, select the blank option in all selection fields for the second record **Phonebook Import**.

Fields in the Phonebook Import menu.

Field	Description
Phone Number	Select which data is to be used from a data record as the phonenumber.
Name	Select which columns are to be used from a data record as the

Field	Description
	name. You have the option to use two elements here (e.g. forename and surname). The middle input field can be used to place a character string between the two elements here. The default separator used is a comma.

Speed dial is automatically assigned. By default, call through is disabled.

13.4.3 General

In the menu **Applications**->**System Phonebook**->**General** you define the user name and password for system phone book administration. In the phone book area, the administrator can view and modify the phone book, as well as import and export data.

The **Applications**->**System Phonebook**->**General** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Web Access Username	Enter a user name for the system telephone book administrator.
Web Access Password	Enter a password for the system telephone book administrator.
Delete Phonebook	If you wish to remove the existing system phone book with all of its entries, enable the option **Delete**. You will then be asked for confirmation **Do you really want to delete all entries of the phonebook?**. Confirm your entry by clicking **OK**. The option **Delete** is disabled by default.

13.5 Call Data Records

In the **Applications**->**Call Data Records** menu, you configure the recording of incoming and outgoing calls.

The capture of call data records provides an overview of the telephone usage in your company.

All external calls can be saved in the device in the form of call data records. These data records contain important information about the individual calls.

You must enable recording of connection data in the **Numbering**->**User Settings**->**Class**

of Services->**Applications** menu. The function is not activated in the ex works state.

13.5.1 Outgoing

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

The **Applications**->**Call Data Records**->**Outgoing** menu consists of the following fields:

Fields in the Outgoing menu.

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Duration	Displays the duration of the connection.
User	Displays the user who called.
Int. No.	Displays the user's internal number.
Called Name	Displays the name that called.
Called Number	Displays the dialled number.
Project Code	Displays the call project number, if any.
Interface	Displays the interface over which the external connection was routed.
Costs	Displays the connection charge, but only if the provider transmits the corresponding data.

13.5.2 Incoming

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

The **Applications**->**Call Data Records**->**Incoming** menu consists of the following fields:

Fields in the Incoming menu.

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Duration	Displays the duration of the connection.
User	Displays the user who was called.
Int. No.	Displays the user's internal number.
Caller Name	Displays the name of the caller.
External Number	Displays the caller's number.
Project Code	Displays the call project number, if any.
Interface	Displays the interface over which the connection from outside was routed.

13.5.3 General

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

The **Applications**->**Call Data Records**->**General** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Web Access Username	Enter a user name for the call data administrator.
Web Access Password	Enter a password for the call data administrator.
Save outgoing calls	Select which outgoing connections should be saved. Possible values: • *None* (default value) • *All* • *With Project Code only*

Field	Description
Save incoming calls	Select which incoming connections should be saved. Possible values: • *None* (default value) • *All* • *With Project Code only*
Privacy Number Truncation	Select whether to save the number in abbreviated form. If, for data privacy reasons, the number is to be only partially displayed, you can select the number of positions not to be displayed here. For **Outgoing Calls** and for **Incoming Calls** you can separately enter the number of hidden digits. The hiding of digits occurs from right to left. Possible values: • *No* (default value) • *All* • *1* to *9*
Transfer call data records via Serial 2	For modular PABX systems only Select whether to export call data records over the serial interface (Serial 2) after each call which enables you to connect an external charge metering software solution (hotel application). The function is activated by selecting *Enabled*. The function is disabled by default.

Fields in the Actions menu.

Field	Description
Export call data records	If you wish to save the current connection data record in an external file, click **Export** and save the file under the desired storage location and file name.
Delete call data records	If you wish to delete the current connection data record from the system storage, click **Delete**.

13.6 Call List

The menu **Applications**->**Call List** lists details of incoming and outgoing calls. Which kind of calls and how many of them are included can be spcified in the submenu **General**.

13.6.1 Incoming

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

The **Applications**->**Call List**->**Incoming** menu consists of the following fields:

Fields in the Incoming menu

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Type	Displays the type of the connection.
User	Displays the user who was called.
Int. No.	Displays the user's internal number.
Caller Number	Displays the caller's number.
Trunk Number	Displays the port number.
Interface	Displays the interface over which the connection from outside was routed.
Delete	You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

13.6.2 Outgoing

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

The **Applications**->**Call List**->**Outgoing** menu consists of the following fields:

Fields in the Outgoing menu

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Type	Displays the type of the connection.
User	Displays the user who was called.
Int. No.	Displays the user's internal number.
Called Number	Displays the caller's number.
Trunk Number	Displays the port number.
Interface	Displays the interface over which the connection from outside was routed.
Delete	You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

13.6.3 General

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

The **Applications**->**Call List**->**General** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Record calls	Select which kind of calls are to be included. Possible values: • *None* • *Incoming only* (default value) • *All*

Field	Description
Record connected calls	Select if accepted calls are to be included, too. This can significantly increase the number of included calls and decrease the amount of time the list can cover until the maximum number of calls is reached and the first calls are deleted from the list.
Max Call List entries for System Calls	Specify the maximum amount of system calls that are included in the list. The maximum number is *1000*. System calls include, e.g., call transfers to extern, calls being accepted by an announcement, team calls that are not accepted by a single user.
Max Call List entries per User	Specify the maximum amount of user calls (calls initated of accepted by a configured user) that are included in the list. The maximum number is *200*.

13.7 Hotel Functions

In the **Applications**->**Hotel Functions** menu, you configure the system's hotel functions.

The integrated hotel application has been especially developed for smaller hotels and B&B's. The system software already contains "Wake-up call", "Check-in", "Check-out", along with display of the "Hotel room status". With "Check-in", the room telephone dial permission is switched to "direct outward dialling". With "Check-out", dial permission is reset to "Internal".

This performance feature allows convenient printout of telephone charges accrued to the guest's room telephone between check-in and check-out. This function also includes "Check-in / Check-out" with which the room telephone is activated at arrival and blocked at departure. A wake-up call can be set up for room telephones by the guest or the reception.

A system telephone serving as "reception telephone" is required to use this performance feature. You can define up to any two system telephones as "reception telephone". A flexible 1 to 4 digit call assignment can allocate call numbers that are identical to the room number.

13.7.1 Room Status

In the **Applications**->**Hotel Functions**->**Room Status** menu, current occupancy and room status are displayed.

13.7.1.1 Edit

Choose the ✎ icon to edit existing entries.

The **Applications**->**Hotel Functions**->**Room Status**->**Edit** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Room Description	Displays the hotel room description.
Internal Number	Displays the configured hotel room internal number and the guest name.

Fields in the Room Information menu.

Field	Description
Cleaning State	Enter the hotel room status. Possible values: • *Not cleaned* • *Cleaned* • *Cleaned and checked* The hotel room status can also be set by dialling a code number from the room telephone.
Status	Enter the status of the guest occupying this hotel room. Possible values: • *Check In*: Dial permission is switched to "Unlimited". • *Check Out*: Dial permission is switched to "Internal".

Fields in the Guest Information menu.

Field	Description
Guest Name	Enter the guest name.
Additional Info	If required, enter additional guest data.

Fields in the Further Settings menu.

Field	Description
Wake-up	Select whether the guest should be woken, and if so, at what

Field	Description
	frequency. Possible values: • *Once*: The guest only wishes to be woken once, on a specific date. • *Daily*: The guest wishes to be woken daily at the same time. • *Off*: The guest doesn't wish to be woken.
Time	Enter the time at which the guest wishes to be woken. Enter hours in the first field, minutes in the second.
Date	Only for **Wake-up** = *Once* Enter the date on which the guest wishes to be woken.
Wake-up Announcement	Select the announcement with which the guest wishes to be woken. All preset and additionally-loaded Wave files in the system can be selected.
Messages existing	Select whether the guest should be informed of messages taken for him/her at the reception. When enabled, this function signals the presence of a message at the room telephone. The function is activated by selecting *Existing*. The function is disabled by default.
Communication Costs	Displays current connections charges for this telephone.

Click the **Print** button to display call data as well as due call charges for the currently selected guest. Click the **Print** button again to print the data.

13.7.2 Hotel Rooms

You define the name of the room and the internal telephone number in the **Applications**->**Hotel Functions**->**Hotel Rooms** menu.

13.7.2.1 Edit or New

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

The menu **Applications**->**Hotel Functions**->**Hotel Rooms**->**New** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the hotel room.
Internal Number	Select a configured internal telephone number to be assigned to this hotel room.

13.7.3 General

Settings for reception telephones, the rooms, wake-up calls and check-in/check-out are performed in the **Applications**->**Hotel Functions**->**General** menu. Connection charges and texts for headers and footers can also be defined. In addition, you can define the user name and password for administration of hotel functions. The administrator at the reception can view and modify the "Room Status" area.

The **Applications**->**Hotel Functions**->**General** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Web Access Username	Enter a user name for the user at the reception. The latter thus gains access to your system's reception functions.
Web Access Password	Enter a password for the user at the reception.

Fields in the Reception menu.

Field	Description
1st Number	Select the first internal telephone number for the reception.
2nd Number	Select the second internal telephone number for the reception, if applicable.

Fields in the Wake-up Settings menu.

Field	Description
Duration	Enter the time during which a wake-up call shall be signalled to the guest.

Field	Description
	The default value is *30*.
Number of Repetitions	Enter the number of repetitions for the wake-up call. Possible values are *1* to *5*. The default value is *1*.
Repeat after	Enter the time after which a wake-up call to the guest should be renewed (if he/she has accepted the first, there are no more wake-up calls). Possible values: • *No repeat* • *1* to *5* The default value is *3*.
Wake-up Announcement selectable	Select whether the reception telephone may individually set the wake-up announcement/music-on-hold for every wake-up call to be configured. The function is activated by selecting *Enabled*. The function is disabled by default.
Default Wake-up Announcement	Select the wake-up announcement to be used by default for wake-up calls. All preset and additionally-loaded Wave files in the system can be selected.

Fields in the Communication Costs menu.

Field	Description
Charge Rate Factor/ Currency	Displays the system-wide exchange rate and currency. These values are configured under **System Management**->**Global Settings**->**System**.
Conversion Factor	Enter by which cost factor an external call shall be multiplied.
Header Text	Enter your own text with a maximum of 78 characters. This text is printed as a header over every bill of charges. If you leave the text field empty, no header is printed.
Footer Text	Enter your own text with a maximum of 78 characters. This text

Field	Description
	is printed as a footer under every bill of charges. If you leave the text field empty, no footer is printed.

Note

System printer connection data:

- Baud rate 9600
- Data bits: 8
- Parity None
- RTS /CTS unused
- Xon / Xoff unused

These data are permanently set and cannot be altered!

Fields in the Further Settings menu.

Field	Description
Room to Room Call Barring	Select whether to block calls between rooms. The function is activated by selecting *Enabled*. The function is disabled by default.

13.8 Mini Call Center

The mini call centre is an integrated call centre solution for up to 16 agents. It provides the ideal solution for small groups with high dynamic telecommunication volumes (e. g insides sales, support, order acceptance/processing, customer service). Here, a specific solution with its own administrator has been integrated. The mini call centre is characterised by:

- Flexible allocation of agents and lines
- Dynamic adaptation according to call volume
- Call allocation with off-time for the agent
- Statistical data for agents and lines.

13.8.1 Status

In the **Applications**->**Mini Call Center**->**Status** menu, you can view the current status of lines and logged-in agents in a block, along with the subscribers assigned to lines.

The menu **Applications**->**Mini Call Center**->**Status** consists of the following fields:

Values in the Status list

Field	Description
View	**View** allows you to select which call centre to display.
Line	Displays the mini call centre line.
Agents assigned	Displays the number of agents assigned to this line.
Agents logged on	Displays the number of agents logged-in on this line.
Agents in Wrap-up	Displays the number of agents in post-processing time.
Active Calls	Displays the number of active connections.
Waiting Calls	Displays the number of waiting incoming calls.
Answered of Calls Today	Displays the current number of accepted calls for this day.
Lost Calls Today	Displays the current number of missed calls for this day.

13.8.2 Lines

In the **Applications**->**Mini Call Center**->**Lines** menu, lines are assigned to external and internal numbers, and the name of the call centre to which the line belongs is displayed.

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

13.8.2.1 General

In the **General** area, you perform basic settings for a line.

The menu **Applications**->**Mini Call Center**->**Lines**->**General** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the line.
External Number	Select a number configured as mini call centre for the external connection of this call centre line.
Internal Number	Enter the desired internal number for this line.
Call Center Description	Select *New* and enter a name for the new mini call centre. Or select the name of a mini call centre which has already been generated.

Fields in the Further Settings menu.

Field	Description
Switch call signalling	Select whether the call options for this line shall be switched over a configured calendar and, if so, over which. Possible values: • *No calendar,only manually* • *<Calendar>*
Active Variant	Select which call option shall be enabled by default after configuration for this line.

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

Fields in the Advanced Settings menu.

Field	Description
Team Speed Timer	Enter the time after which call forwarding to the next free agent assigned to this line shall occur.

13.8.2.2 Variant 1 - 4

In the area **Variant**, you set up call options for the mini call centre.

The menu **Applications**->**Mini Call Center**->**Lines**->**Variant** consists of the following fields:

Fields in the Settings menu.

Field	Description
Automatic Call Pick-up with	Select whether an incoming call shall be automatically accepted and, if so, with which announcement or melody. The function is activated by selecting *Enabled*. The function is disabled by default. Select the Wave file to be used for the call acceptance. All preset and additionally-loaded Wave files in the system can be selected.

Fields in the Rerouting Functions menu.

Field	Description
Rerouting on no response	Select whether and, if so, with which option an incoming call shall be redirected after the entered time. Possible values: • *None*: There shall be no redirect on no-reply. • *<Team>*: The incoming call is forwarded to the selected team after the time specified in **Time until rerouting:**.
Further Rerouting	Select additional redirect functions. You must first configure these in **Applications**->**Rerouting**->**Rerouting Functions**. Then, the following values may be selected: • *Off*: No additional redirect functions. • *Immediately*: Immediately transfers the call according to a configured redirect function . • *On Busy*: Transfers the call according to a configured redirect function on engaged.
Rerouting Function	Only for **Further Rerouting** = *Immediately* or **Further Rerouting** = *On Busy* Select a configured redirect option for immediate redirect, or on busy.
Busy when	Only for **Further Rerouting** = *On Busy* Select from how many busy agents the lines shall be con-

Field	Description
	sidered busy.

13.8.2.3 Log on / Log off

In the **Log on / Log off** area, select which of the assigned agents shall be logged into the line.

The menu **Applications**->**Mini Call Center**->**Lines**->**Log on / Log off** consists of the following fields:

Fields in the Log on / Log off menu.

Field	Description
Numbers	Displays the internal number and description of the assigned agent.
Status	Select whether the agent is logged into the line. The agent is logged in by selecting *Logged on*.

13.8.3 Agents

In the **Applications**->**Mini Call Center**->**Agents** menu, lines are assigned to agents. An agent can operate one or more mini call centre lines.

13.8.3.1 Edit or New

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

The menu **Applications**->**Mini Call Center**->**Agents**->**New** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
User	Select the configured user who shall serve as a call centre agent. You configure required users in the **Numbering**->**User Settings**->**User** menu. The following users are already created: • *User 1 to User 4 analog phones*

Field	Description
	- *User 5 and User 6 Sys Tel* - *User 7 DECT* - *User 8 and User 9 ISDN*
Internal Number	Select the user's internal number to be used for the call centre.

Fields in the Assigned Lines menu.

Field	Description
Select lines	Select the lines for which the agent shall be responsible. The name of the corresponding call centre is displayed again when lines are selected in order to improve the overview. Under **Assign** select whether the entry should be enabled.

Fields in the Wrap-up Settings menu.

Field	Description
Wrap-up Time	Enter the time available to this agent for post-processing after concluding a call. No further call can be assigned to this agent during this period. The agent has the option of temporarily extending the period with a telephone procedure.

13.8.4 General

In the **Applications**->**Mini Call Center**->**General** menu, you can set up an HTML web interface access for the mini call centre manager. The latter can then monitor the status of lines and agents, and modify the settings for lines and agents.

The **Applications**->**Mini Call Center**->**General** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Web Access Username	Enter a user name for the mini call centre administrator. When a user logs into the user interface under this name, he/she has access to the user interface with selected parameters for administration of the call centre.
Web Access Password	Enter a password for the mini call centre administrator.

13.9 Doorcom Units

You can connect a door intercom as an intercom adapter to an analogue connection of your system.

If a door intercom adapter is connected to your system, you can speak with a visitor at the door from every authorised telephone. You can assign particular telephones to each ring button. These phones then ring if the ring button is pressed. On analogue telephones, the signal on the telephone matches the intercom call. In place of the internal telephones, an external telephone can also be configured as the call destination for the ring button. Your door intercom can have up to 4 ring buttons. The door opener can be pressed during an intercom call. It is not possible activate the door opener if an intercom call is not taking place.

Note

All functions of the door intercom (intercom adapter) are controlled via the code numbers indicated in the intercom user's manual. The system does not support the intercom with specific codes.

13.9.1 Doorcom Units

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

13.9.1.1 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 con-

Field	Description
	nected. All free FXS interfaces are available.
Internal Number	Select the configured internal number to be assigned to the intercom adapter. The number is created in the **Numbering**->**User Settings**->**User** menu.
Code for Doorcom Call Acceptance	Pressing a bell button on the intercom sets off a call in the system. To establish a connection between a called subscriber and the intercom adapter, that subscriber must pick up the receiver and dial the code number for call acceptance. Enter this code for call acceptance. If a subscriber accepts a call from the intercom adapter, the PABX automatically dials the code number required to set up the connection. The subscriber need not make any more entries.

13.9.2 Doorcom Signalling

In the **Applications**->**Doorcom Units**->**Doorcom Signalling** you configure the signalling variant for call acceptance via a intercom adapter. Two intercom call options are available.

The code number for the bell button is the number the intercom adapter dials into the system when the bell button is pressed. You can perform an internal call allocation for each bell button. Please note that guidelines for connecting the intercom adapter depend on the respective manufacturer. For this, read the operating instructions provided by the manufacturer of the intercom adapter.

13.9.2.1 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

Field	Description
	bell button on the intercom adapter initiates a call to the terminals entered in the assigned intercom call option.
Bell Name	Enter a name for the bell.
Switch signalling	Select whether the intercom call options for this bell shall be switched over a configured calendar and, if so, over which. For every ring, you can create up to two intercom call variants in the **Applications**->**Doorcom Units**->**Doorcom Signalling**->**New**->**Variant** menu. Possible values: • *No calendar,only manually* • *<Calendar>*
Active Doorcom 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.

13.9.2.2 Doorcom Signalling Variant 1 and 2

In the **Doorcom Signalling Variant** area, you configure both intercom call options for this signalling profile.

The **Applications**->**Doorcom Units**->**Doorcom Signalling**->**Intercom call variant** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Assignment	Select where pressing of the bell button shall be signalled. Possible values: • *Internal*: Signalling occurs on an internal number. • *External*: Signalling occurs to an external number.
Internal Assignment	Select the internal numbers on which pressing of the door bell shall be signalled. With **Add** you add an internal number.
External Assignment	Enter the external telephone number to which pressing the door bell shall be signalled.
Signalling	You can call the internal number with a broadcast call. Possible values: • *Simultaneous* (default value): All assigned terminals are called simultaneously. If a telephone is busy, call waiting can be used. • *Linear*: All assigned terminals are called in the sequence of their entry in configuration. If a terminal is engaged, the next free terminal is called. The call is signalled ca. 15 seconds per subscriber. The period can be set between 1 and 99 seconds (per bell) in the configuration. If subscribers are on the phone or logged out, there is not forwarding time for these. • *Rotating*: This call is a special case of the linear call. After all terminals are called, call signalling begins again with the first entered terminal. The call is signalled until the caller replaces the receiver or the call is ended by the intercom adapter (after ca. 2 minutes). • *Adding*: The terminals are called in the sequence of their entry in the configuration subscriber list. Every terminal that has already been called is called again, until all entered terminals are called. In the configuration, you can define when each next terminal is called. • *Linear, simultaneous after time*: You have set linear for the door intercom call. After the defined time has run out, you can also set in the configuration that all team sub-

Field	Description
	scribers are then called in parallel (simultaneously). • *Rotating, simultaneous after time*: You have set rotating for the door intercom call. After the defined time has run out, you can also set in the configuration that all intercom subscribers are then called in parallel (simultaneously).

13.10 Alarm Calls

The PABX systems' FXS interface can be configured as an alarm input. E. g. an alarm button can be connected to one of these interfaces. When the button is pressed, an alarm call is triggered to either up to eight internal numbers or one of two external numbers. Provided your device is equipped with switch contacts, one of them can be activated during an alarm call. The function can, optionally, be switched on using a calendar or you can switch between the two possible signalling variants.

Note

If you intend to add **Alarm input**, you may first have to free an interface in the menu **Terminals**->**Other phones**->**Analogue**, i.e. delete one of the preconfigured entries with the 🗑 button.

13.10.1 Alarm Calls

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

13.10.1.1 General

In the **General** area you set up the alarm calls' basic features.

The **Applications**+**Alarm Calls**+**Alarm Calls**->**General** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Status	Enable or disable the alarm calls function. The function is enabled with *Enabled*.

Field	Description
	The function is enabled by default.
Description	Enter a unique name for the alarm.
Interface	Select the interface to be used for alarm.
Internal Number	Select an internal number to be used for the alarm.
Switch signalling	Specify how the alarm that has been set up is to be switched on. Possible values: • *No calendar,only manually*: Manual switch is enabled. • *<calendar entry>*: Select one of the calendar entries that has been configured for the alarm.
Active Variant	Select the call options that are to be enabled. You can configure the options as soon as you have confirmed the entry in the **General** tab with **OK**.

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

Fields in the menu Advanced Settings

Field	Description
Alarm Signalling Period	Enter the length of time for which an alarm is to be signalled, in seconds. The default value is *30* seconds.
Repeat after	Specify the time between the alarm repeats, in seconds. A value of between *1* and *600* seconds is possible. The default value is *10* seconds. Call repeats are not possible via an FXO interface (if an FXO interface is available).
Number of repeats	Specify the number of repeats if the alarm is not taken. A value of between 1 and 10 repeats is possible. The default value is *2*. Call repeats are not possible via an FXO interface (if an FXO in-

Field	Description
	terface is available).
External Connection Timer	Specify the maximum duration of an external call once it has been accepted (in seconds). A value of between *1* and *600* seconds is possible. The default value is *60* seconds.
Info Message (UUS1)	Optionally, a message (max. 32 characters) can be sent to ISDN terminals.
Relay Contact	Only applicable if your device is equipped with a relais! If a relay is to be switched on during the alarm: Select the relay that is to be used. Configuration of the Relay is done in the menu **Physical Interfaces**->**Relay**.
Wave-File	Select whether and which saved WAV file is to be played when the alarm call is taken. Possible values: • *Off* (default value): A caller on hold shall hear no music-on-hold. • *<WAV file>*: The subscriber called will hear the selected WAV file.
Number of playbacks	Select how many times in a row the announcement is to be played. Possible values: • *Endlessly (default value)* • *1* to *10*

13.10.1.2 Variant 1 and 2

You can configure two versions of the alarm call. One version will normally use the option to call internal extensions, while the other will use the option to call external subscribers.

Fields in the menu Basic Settings

Field	Description
Assignment	You can assign up to eight internal numbers or two external

Field	Description
	numbers to each alarm. Define whether an alarm's calls are to be signalled to the internal or external subscribers. Possible values: • *External*: The external number that was entered is called. Alternatively, two external numbers can be called for an alarm. • *Internal* (default value): The subscribers assigned to the selected numbers are called based on the signalling defined. For one alarm, eight internal subscribers can be called simultaneously.
First External Number	Only for **Assignment** = *External*Enter the first number of the external subscriber.
Second External Number	Only for **Assignment** = *External*Enter the second number of the external subscriber.
Internal Assignment	Only for **Assignment** = *Internal*Select the internal subscribers. Use **Add** to add more internal numbers.

13.11 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

If you wish to use a voicemail box, you'll need an installed SD card (if supportted by you device). You may need load the required folder structure with the announcement texts on the SD card. Choose in the **Maintenance**->**Software &Configuration** menu the option *Import Voice Mail Wave Files*.

Caution

Do not remove the SD card during any read or write access to avoid losing data or damaging the card. Watch the relevant LED on the top of the device: it will flicker during any read or write access.

13.11.1 Voice Mail Boxes

In the **Applications**->**Voice Mail System**->**Voice Mail Boxes** menu, a list of the individual voicemail boxes for specific subscribers is displayed.

Only for compact systems.

Two predefined voicemail boxes are displayed:

Internal Number	User	License Allocation
10	User 1 analog phone	Enabled
20	User 5 Sys Tel	Enabled

Values in the list Voice Mail Boxes

Field	Description
Internal Number	Displays the number of the individual subscriber for which the voicemail box is configured.
User	Displays the name of the individual subscriber for which the voicemail box is configured.
Language	Displays the language of the announcement text on the 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	Indicates 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.

13.11.1.1 Edit or New

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

The menu **Applications**->**Voice Mail System** ->**Voice Mail Boxes** ->**New** consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Internal Number	Select the internal number of the subscriber for which you wish to set up a voicemail box. You may choose among the numbers configured in the **Numbering**->**User Settings**->**User** menu.
Voice Mail Language	Select the desired language for the voicemail box announcements. Possible values: • *Deutsch*: The voicemail box uses German texts. • *Dutch*: The voicemail box uses Dutch texts. • *English*: The voicemail boxe uses English texts. • *Italian*: The voicemail box uses Italian texts. • *Spanish*: The voicemail box uses Spanish texts.

Field	Description
	• *French*: The voicemail box uses French texts. • *Portugues*: The voicemail box uses Portugues texts. • *Default* (default value): The voicemail box uses the language centrally defined for the entire voicemail system in the **Applications**->**Voice Mail System** ->**General** menu. ☞ **Note** You'll only require a setting that departs from *Default* if you wish to operate voicemail boxes with various languages within your voicemail system.
E-Mail Address (from User Settings)	Here is displayed the user e-mail address to which a notification shall be sent if a message has been left on the voicemail box. The e-mail address in saved in the **Numbering**->**User Settings**->**User**->**Basic Settings** menu.
E-Mail Notification	Once a message has been left on the voicemail box, the subscriber can be notified. Possible values: • *None* (default value): The subscriber is not notified. • *E-Mail*: The subscriber is informed of a present message via e-mail. • *E-Mail with Attachment*: Once a caller has left a message, the subscriber receives an e-mail with a recording of the message in the attachment. • *User defined*: If the administrator activates the *User defined* function, the e-mail alert settings can be changed by the user in the **User Access**. If the administrator sets a different value, a block is placed on changes from the user. ☞ **Note** Once a subscriber has received notification of a new message in an e-mail, the **Status** of the notification is changed according to the settings in the **User Access**. You can configure the status behaviour in the **User Access**->**Voice Mail System**->**Settings** menu under **E-Mail forwarding behavior**.

Field	Description
Max Recording Time	Enter the maximum recording time per message. The possible values are *5* to *300* seconds, the default value is *180* seconds.
Calendar for status "Out of Office"	When the subscriber is out, the voicemail box can be switched over a calendar. If a calendar is to be used, it needs to be configured with the setting **Application** = *Voice Mail System* in the menu **Applications**->**Calendar**. Possible values: • *No calendar,only manually* (default value): The subscriber can manually switch the voicemail box on and off. • <Calendar>: Using the selected calendar, the voicemail box can be switched on or off at the times defined there.

Fields in the menu User Settings

Field	Description
Status of Mail Box Owner	Define in which mode the mailbox shall be used when starting the voicemail system. Possible values: • *In the Office* (default value): Select this setting if the 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. You can change the PIN for the personal voice box in the **Numbering**->**User Settings**->**Users**->**Authorizations** under **PIN for Phone Access**.
Mode for status "In the Office"	The voicemail box can be operated with two different settings during office hours.

Field	Description
	Possible values: • *Announcement and Record* (default value): A caller hears an announcement and can leave a message. • *Announcement only*: A caller hears an announcement, but cannot leave a message.
Mode for status "Out of Office"	The voicemail box can be operated with two different settings outside of office hours. Possible values: • *Announcement only* (default value): A caller hears an announcement, but cannot leave a message. • *Announcement and Record* : A caller hears an announcement and can leave a message.

Select the ✎ icon to set up your own voice announcements for the selected voice mail box in addition to the settings above.

The **Applications**->**Voice Mail System** ->**Voice Mail Boxes** -> ✎ menu consists of the following fields:

Fields in the menu Voice Announcement

Feld	Beschreibung
In the Office	You can upload your own announcement for the **In the Office** state. Use the WAV file format for this annoncement. Click **New Message** to upload the file. The window **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

Feld	Beschreibung
	the announcement, the 🗑 icon to delete it.

Fields in the menu Annoucement Options

Feld	Beschreibung
Action	Displays `Update announcement` .
Source Location	For **Action** = `Update annoncement` Select the WAV file to be used for the announcement and click **Start** to upload.

13.11.2 Status

In the **Applications**->**Voice Mail System** ->**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 or stored by the subscriber.

Note

By default, the system can record a maximum of 59 calls per voicemail box. You cannot change this value in the GUI.

13.11.3 General

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

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

Fields in the menu Basic Settings

Field	Description
Voice Mail System	Select whether to activate your voicemail system. The function is enabled with *Enabled*. The function is enabled by default.
Description	Only for **Voice Mail System** enabled. Enter a description for your voicemail system. This description is displayed on the telephone when a call goes in to the voice mail system. The default value is *Voice Mail*.
Internal Number	Only for **Voice Mail System** enabled. Enter the internal number under which to access your voicemail system. The default value is *50*.
Language	Select the language for the entire voicemail system. Possible values: • *Deutsch* (default value) • *Dutch* • *English* • *Italian* • *Spanish* • *French* • *Portugues* Diverging from the language set here, a language can be indi-

Field	Description
	vidually set for each voice mail box in the **Applications**+**Voice Mail System**->**Voice Mail Boxes**->**New** menu.

Fields in the menu Mail Settings

Field	Description
SMTP Server	Enter the address (IP address or valid DNS name) of the e-mail server to be used for sending the e-mails.
SMTP Server Port	Enter the port to be used for sending e-mails. The default value is *25*.
Return Address	Enter any address to be used as sender when sending e-mails. This address merely serves to identify e-mails in the inbox.
SMTP User Name	Enter the user name for the SMTP server.
SMTP Password	Enter the password for the SNMP server user.

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

Fields in the menu Advanced Settings

Field	Description
Lifetime	Voicemail messages are deleted after an adjustable period of time. Possible values are *10* to *60* days. The default value is *60*.

Chapter 14 LAN

In this menu, you configure the addresses in your LAN.

14.1 IP Configuration

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

14.1.1 Interfaces

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

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

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

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

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

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

Note

For IPv4 note that:

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

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

Example of subnets

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

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

Here is an example for an IPv6 address:

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

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

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

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

If your device acts as host, it has a Link Prefix assigned by another router through Router Advertisements. The host address is then automatically derived through SLAAC. Additional information like, e.g., the General Prefix of the provider or the address of a time server can be received through DHCP. Use the following settings in the menu **LAN**->**IP Configuration**->**Interfaces**->**New**: **IPv6 Mode** = *Client*, **Accept Router Advertisement** = *Enabled* and **DHCP Client** = *Enabled*.

14.1.1.1 Edit or New

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

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

Fields in the Basic Parameters menu.

Field	Description
Based on Ethernet Interface	This field is only displayed if you are editing a virtual routing interface. Select the Ethernet interface for which the virtual interface is to be configured.
Interface Mode	Only for physical interfaces in routing mode and for virtual interfaces. Select the configuration mode of the interface. Possible values: • *Untagged* (default value): The interface is not assigned for a specific purpose. • *Tagged (VLAN)*: This option only applies for routing interfaces. You use this option to assign the interface to a VLAN. This is done using the VLAN ID, which is displayed in this mode and can be configured. The definition of a MAC address in **MAC Address** is optional in this mode.
VLAN ID	Only for **Interface Mode** = *Tagged (VLAN)* This option only applies for routing interfaces. Assign the interface to a VLAN by entering the VLAN ID of the relevant VLAN. Possible values are *1* (default value) to *4094*.
MAC Address	Enter the MAC address associated with the interface. For virtual interfaces, you can use the MAC address of the physical interface under which the virtual interface was created by activating **Use built-in**, but VLAN IDs must be different. You can also allocate a virtual MAC address. The first 6 characters of the MAC are preset (but can be changed). If **Use built-in** is active, the predefined MAC address of the allocated physical interface is used.

Field	Description
	Use built-in is activated by default.

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

Field	Description
Security Policy	Select the security settings to be used with the interface. Possible values: • *Trusted* (default value): All IP packets are allowed through except for those which are explicitly prohibited.. • *Untrusted*: Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone. You can configure exceptions for the selected setting in the *Firewall* on page 301 menu.
Address Mode	Select how an IP address is assigned to the interface. Possible values: • *Static* (default value): The interface is assigned a static IP address in **IP Address / Netmask**. • *DHCP*: An IP address is assigned to the interface dynamically via DHCP.
IP Address / Netmask	Only for **Address Mode** = *Static* With **Add**, add a new address entry, enter the **IP Address** and the corresponding **Netmask** of the virtual interface.

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

Field	Description
IPv6	Select whether this interface should use Internet Protocol version 6 (IPv6) for data transmission. The function is activated by selecting *Enabled*. The function is disabled by default.
Security Policy	Only for **IPv6** = *Enabled* Select the security settings to be used with the interface.

Field	Description
	Possible values: • *Trusted* (default value): All IP packets are allowed through except for those which are explicitly prohibited. We recommend you use this setting if you want to use IPv6 on your LAN. • *Untrusted*: Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone. We recommend you use this setting if you want to use IPv6 outside of your LAN. You can configure exceptions for the selected setting in the *Firewall* on page 301 menu.
IPv6 Mode	Only for **IPv6** = *Enabled* Select whether the interface is to be operated in host or in router mode. Depending on your selection different parameters are presented for you to configure. Possible values: • *Router (Transmit Router Advertisement)* (default value): Select whether Router Advertisements are to be sent via the interface. Using Router Advertisements the list of prefixes is propagated and the router propagates itself as the standard gateway. The function is activated by selecting *Enabled*. The function is enabled by default. • *Host*: The interface is operated in host mode.
DHCP Server	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Router (Transmit Router Advertisement)* Specify if your device is to act as DHCP server, i.e., if it is to transmit DHCP options in order to distribute information about the DNS servers to the clients.

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

Use **Add** to create more entries.

Fields in the Basic Parameters menu.

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

Fields in the Link Prefix menu.

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

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

Fields in the Host Address menu.

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

Field	Description
	one or more IPv6 addresses with **Add**. Its predefined length is *64*. Start any entry with *::* .

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

Fields in the Advanced IPv6 Settings menu

Field	Description
On Link Flag	Select whether the On-Link Flag (L-Flag) should be set. This allows the host to enter the prefix from the prefix list. The function is activated by selecting *True* . The function is enabled by default.
Autonomous Flag	Select whether the Autonomous Address Configuration Flag (A-Flag) should be set. This allows the host to use the prefix and the 64 bit interface ID, to derive its address. The function is activated by selecting *True* . The function is enabled by default.
Preferred Lifetime	Enter a time period in seconds. During this time, addresses derived from the prefix through SLAAC are preferred. The default value is *604800* seconds.
Valid Lifetime	Enter a time period in seconds, for which the prefix is valid. The default value is *2592000* seconds. **Note** The value for the valid lifetime should be lower than the one configured for the option **Router Lifetime** under **Advanced IPv6 Settings**.

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

Fields in the Advanced IPv4 Settings menu.

Field	Description
DHCP MAC Address	Only for **Address Mode** = *DHCP*

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

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

Field	Description
DHCP Mode	Only for **IPv6** = *Enabled*, **IPv6 Mode** = *Router (Transmit Router Advertisement)* and **Transmit Router Advertisement** = *Enabled* Select the information to be forwarded to the DHCP client. **Note** To achieve this, your router must not be set up as a DHCP server. By selecting *Other - DNS Servers, SIP Servers* (default value) no address- related information, such as i.e. DNS, VoIP, etc., is passed through. Enable this option if hosts inside of the network are to automatically create their IP addresses through SLAAC. In this case, the router sends only data via DHCP that are not address-related. By selecting *Managed - IPv6 Address Management* hosts receive IPv6 addresses as well as not address-related information through DHCP.
DNS Propagation	Only for **IPv6 Mode** = *Router (Transmit Router Advertisement)* and **Transmit Router Advertisement** *Enabled* Select if an in which way DNS server addresses are to be propagated in Router Advertisements. A maximum of two DNS server addresses is propagated. Possible values: • *Off*: No DNS server address propagation • *Self*: The device sends its own IP adderss as DSN server address. If the device has multiple addresses, they are used in the following order: • Global addresses • ULA (Unique Local Addresses) • Link local addresses • *Other*: Statically configured as well as dynamically learned DNS server entries are propagated according to their priority.

Field	Description
	If there are no entries, no address is propagated.

Chapter 15 Network

15.1 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**.

15.1.1 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.

15.1.1.1 Edit or New

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

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

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

Fields in the menu Basic Parameters

Field	Description
Route Type	Select the type of route. Possible values: - *Default Route via Interface*: Route via a specific interface which is to be used if no other suitable route is available. - *Default Route via Gateway*: Route via a specific gateway which is to be used if no other suitable route is available. - *Host Route via Interface*: Route to an individual host via a specific interface. - *Host Route via Gateway*: Route to an individual host via a specific gateway. - *Network Route via Interface* (default value): Route to a network via a specific interface. - *Network Route via Gateway*: Route to a network via a specific gateway. Only for interfaces that are operated in DHCP client mode: Even if an interface is configured for DHCP client mode, routes can still be configured for data traffic via that interface. The settings received from the DHCP server are then copied, along with those configured here, to the active routing table. This enables, e. g., in the case of dynamically changing gateway addresses, particular routes to be maintained, or routes with different metrics (i. e. of differing priority) to be specified. However, if the DHCP server sends static routes, the settings configured here are not copied to the routing. - *Default Route Template per DHCP*: The information of the gateway to be used is received via DHCP and integrated into the route. - *Host Route Template per DHCP*: The settings received by DHCP are supplemented by routing information about a particular host. - *Network Route Template per DHCP*: The settings received by DHCP are supplemented by routing information about a particular network.

Field	Description
	☞ **Note** When the DHCP lease expires or when the device is re-started, the routes that consist from the combination of DHCP settings and those made here are initially deleted once more from the active routing. If the DHCP is reconfigured they are re-generated and re-activated.
Interface	Select the interface to be used for this route.
Route Class	Select the type of **Route Class**. Possible values: • *Standard* (default value): Defines a route with the default parameters. • *Extended*: Select whether the route is to be defined with extended parameters. If the function is active, a route is created with extended routing parameters such as source interface and source IP address, as well as protocol, source and destination port, type of service (TOS) and the status of the device interface.

Fields in the menu Route Parameters

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

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

Fields in the menu Extended Route Parameters

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

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

Field	Description
	according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F. Enter the relevant value for *DSCP Binary Value*, *DSCP Decimal Value*, *DSCP Hexadecimal Value*, *TOS Binary Value*, *TOS Decimal Value* and *TOS Hexadecimal Value*.
Mode	Select when the interface defined in **Route Parameters**->**Interface** is to be used. Possible values: • *Dialup and wait* (default value): The route can be used if the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up". • *Authoritative*: The route can always be used. • *Dialup and continue*: The route can be used when the interface is "up". If the interface is "dormant", then select and use the alternative route (rerouting) until the interface is "up". • *Never dialup*: The route can be used when the interface is "up". • *Always dialup*: The route can be used when the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up". In this case, an alternative interface with a poorer metric is used for routing until the interface is "up".

15.1.2 IPv6 Route Configuration

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

15.1.2.1 Edit or New

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

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

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

Fields in the Route Parameters menu

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

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

15.1.3 IPv4 Routing Table

A list of all IPv4 routes is displayed in the **Network**->**Routes**->**IPv4 Routing Table** menu. The routes do not all need to be active, but can be activated at any time by relevant data traffic.

In the ex works state, a predefined entry with the parameters **Destination IP Address** = *192.168.0.0*, **Netmask** = *255.255.255.0*,**Gateway** = *192.168.0.250*, **Interface** = *LAN_EN1-0*, **Route Type** = *Network Route via Interface*, **Protocol** = *Local* is displayed.

Fields in the menu IPv4 Routing Table

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

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

15.1.4 IPv6 Routing Table

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

Fields in the IPv6 Routing Table menu

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

15.1.5 Options

Back Route Verify

The term Back Route Verify describes a very simple but powerful function. If a check is activated for an interface, incoming data packets are only accepted over this interface if outgoing response packets are routed over the same interface. You can therefore prevent the acceptance of packets with false IP addresses - even without using filters.

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

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

Fields in the Back Route Verify menu.

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

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

15.2 IPv6 General Prefixes

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

General Prefixes have two key advantages:

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

In order to IPv6 you need to configure how subnets and IPV6 addresses are created and distributed (see Configuring IPv6 addresses in *Interfaces* on page 258 and the menu **LAN**->**IP Configuration**->**Interfaces** for the IPv6-relevant parameters.

15.2.1 General Prefix Configuration

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

15.2.1.1 Edit or New

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

Fields in the Basic Parameters menu.

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

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

15.3 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 284).

Specific instructions for configuring NAT, see the end of the chapter *NAT - Configuration example* on page 290.

15.3.1 NAT Interfaces

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

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

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

Options in the menu NAT Interfaces

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

15.3.2 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.

15.3.2.1 New

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

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

Fields in the menu Basic Parameters

Field	Description
Description	Enter a description for the NAT configuration.
Interface	Select the interface for which NAT is to be configured. Possible values: • *Any* (default value): NAT is configured for all interfaces. • *<Interface name>*: Select one of the interfaces from the list.
Type of traffic	Select the type of data traffic for which NAT is to be configured. Possible values: • *incoming (Destination NAT)* (default value): The data traffic that comes from outside. • *outgoing (Source NAT)*: Outgoing data traffic. • *excluding (Without NAT)*: Data traffic excluded from NAT.
NAT method	Only for **Type of traffic** = *outgoing (Source NAT)* Select the NAT method for outgoing data traffic. The starting point for choosing the NAT method is a NAT scenario in which an "internal" source host has initiated an IP connection to an "external" destination host over the NAT interface, and in which an internally valid source address and internally valid source port are translated to an externally valid source address and an ex-

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

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

Fields in the menu Specify original traffic

Field	Description
Service	Not for **Type of traffic** = *outgoing (Source NAT)* and **NAT method** = *full-cone*, *restricted-cone* or *port-restricted-cone*. Select one of the preconfigured services. Possible values: • *User-defined* (default value) • *<service name>*
Action	Only for **Type of traffic** = *excluding (Without NAT)* Select which data packets are to be excluded by NAT. Possible values: • *Exclude* (default value): All the data packets that match the following parameters that are to be configured (protocol, source IP address/network mask, destination IP address/net-

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

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

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

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

Fields in the menu Replacement Values

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

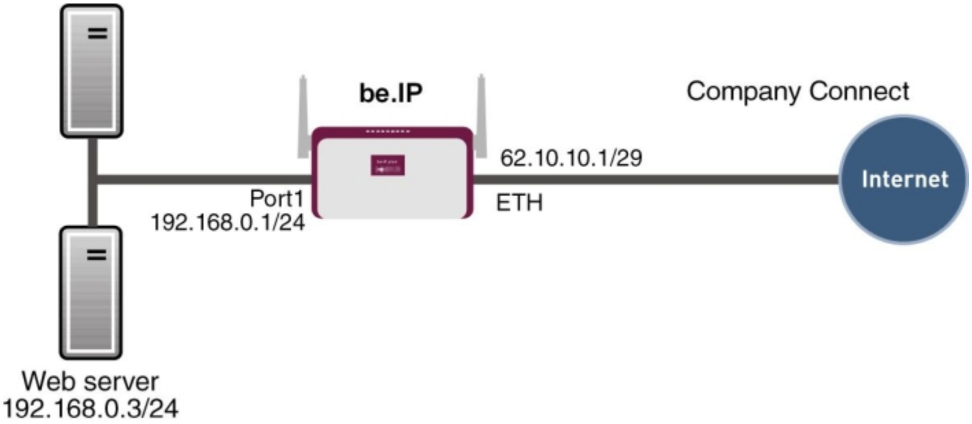
Field	Description
	UDP Leave the destination port as it appears or enter the destination port to which the original destination port is to be translated. Select *Original* to leave the original destination port. If you disable *Original*, an input field appears and you can enter a new destination port.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

15.3.3 NAT - Configuration example

Requirements

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

Example scenario



Configuration target

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

Overview of Configuration Steps

Enable NAT

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

Configured NAT enables

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

Web server

Field	Menu	Value
Description	**Network->NAT->NAT Configuration->New**	e.g. *Webserver*
Interface	**Network->NAT->NAT Configuration->New**	*LAN_EN5-0*
Type of traffic	**Network->NAT->NAT Configuration->New**	*incoming (Destination NAT)*
Service	**Network->NAT->NAT Configuration->New**	*http*
Protocol	**Network->NAT->NAT Configuration->New**	*Host*, e.g. *62.10.10.3*
Original Destination IP Address/Netmask	**Network->NAT->NAT Configuration->New**	*Host*, e.g. *192.168.0.3*
New Destination Port	**Network->NAT->NAT Configuration->New**	*Original*

Terminal Server

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

15.4 Access Rules

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

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

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

Access lists are an effective means if, for example, sites with LANs interconnected over a bintec elmeg gateway wish to deny all incoming FTP requests or only allow Telnet sessions between certain hosts.

Access filters in the gateway are based on the combination of filters and actions for filter rules (= rules) and the linking of these rules to form rule chains. They act on the incoming data packets to allow or deny access to the gateway for certain data.

A filter describes a certain part of the IP data traffic based on the source and/or destination IP address, netmask, protocol and source and/or destination port.

You use the rules that you set up in the access lists to tell the gateway what to do with the filtered data packets, i.e. whether it should allow or deny them. You can also define several rules, which you arrange in the form of a chain to obtain a certain sequence.

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

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

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

or

Allow all packets that are explicitly allowed, i.e.:

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

or

Combination of the two possibilities described above.

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

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

Caution

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

If possible, access your gateway for filter configuration over the serial console (not available for all devices) interface or ISDN Login.

15.4.1 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.

15.4.1.1 Edit or New

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

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

Fields in the Basic Parameters menu.

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

Field	Description
	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:

Field	Description
	• *Any* (default value): The destination IP address/length are not specified. • *Host*: Enter the destination IP address of the host. • *Network*: Enter the destination network address and the 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.

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

15.4.2 Rule Chains

Rules for IP filters are configured in the **Rule Chains** menu. These can be created separately or incorporated in rule chains.

In the **Networking**->**Access Rules**->**Rule Chains** menu, all created filter rules are listed.

15.4.2.1 Edit or New

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

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

Fields in the Basic Parameters menu.

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

Field	Description
	• *Ignore*: Use next rule.

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

15.4.3 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.

15.4.3.1 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

Field	Description
	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.

Chapter 16 Firewall

The Stateful Inspection Firewall (SIF) provided for bintec elmeg gateways is a powerful security feature.

The SIF with dynamic packet filtering has a decisive advantage over static packet filtering: The decision whether or not to send a packet cannot be made solely on the basis of source and destination addresses or ports but also using dynamic packet filtering based on the state of the connection to a partner.

This means packets that belong to an already active connection can also be forwarded. The SIF also accepts packets that belong to an "affiliated connection". The negotiation of an FTP connection takes place over port 21, for example, but the actual data exchange can take place over a completely different port.

SIF and other security features

The Stateful Inspection Firewall fits into the existing security architecture of bintec elmeg. The configuration work for the SIF is comparatively straightforward with systems like Network Address Translation (NAT) and IP Access Lists (IPAL).

As SIF, NAT and IPAL are active in the system simultaneously, attention must be given to possible interaction: If any packet is rejected by one of the security instances, this is done immediately. This is irrelevant whether another instance would accept it or not. Your need for security features should therefore be accurately analysed.

The essential difference between SIF and NAT/IPAL is that the rules for the SIF are generally applied globally, i.e. not restricted to one interface.

In principle, the same filter criteria are applied to the data traffic as those used in NAT and IPAL:

- Source and destination address of the packet (with an associated netmask)
- Service (preconfigured, e.g. Echo, FTP, HTTP)
- Protocol
- Port number(s)

To illustrate the differences in packet filtering, a list of the individual security instances and their method of operation is given below.

NAT

One of the basic functions of NAT is the translation of the local IP addresses of your LAN into the global IP addresses you are assigned by your ISP and vice versa. All connections initiated externally are first blocked, i.e. every packet your device cannot assign to an existing connection is rejected. This means that a connection can only be set up from inside to outside. Without explicit permission, NAT rejects every access from the WAN to the LAN.

IP Access Lists

Here, packets are allowed or rejected exclusively on the basis of the criteria listed above, i.e. the state of the connection is not considered (except for **Services** = *TCP*).

SIF

The SIF sorts out all packets that are not explicitly or implicitly allowed. The result can be a "deny", in which case no error message is sent to the sender of the rejected packet, or a "reject", where the sender is informed of the packet rejection.

The incoming packets are processed as follows:

- The SIF first checks if an incoming packet can be assigned to an existing connection. If so, it is forwarded. If the packet cannot be assigned to an existing connection, a check is made to see if a suitable connection is expected (e.g. as affiliated connection of an existing connection). If so, the packet is also accepted.
- If the packet cannot be assigned to any existing or expected connection, the SIF filter rules are applied: If a deny rule matches the packet, the packet is discarded without sending an error message to the sender of the packet; if a reject rule matches, the packet is discarded and an ICMP Host Unreachable message sent to the sender of the packet. The packet is only forwarded if an accept rule matches.
- All packets without matching rules are rejected without sending an error message to the sender when all the existing rules have been checked (=default behaviour).

Specific instructions for the configuration of Stateful Inspection Firewall (SIF), see the end of the chapter *Configuration* on page 315.

16.1 Policies

16.1.1 IPv4 Filter Rules

The default behaviour with **Action** = *`Access`* consists of two implicit filter rules: If an incoming packet can be assigned to an existing connection and if a suitable connection is expected (e.g. such as an affiliated connection of an existing connection), the packet is allowed.

The sequence of filter rules in the list is relevant: The filter rules are applied to each packet in succession until a rule matches. If overlapping occurs, i.e. more than one filter rule matches a packet, only the first rule is executed. This means that if the first rule denies a packet, whereas a later rule allows it, the packet is rejected. A deny rule also has no effect if a relevant packet has previously been allowed by another filter rule.

The security concept is based on the assumption that an infrastructure consists of trusted and untrusted zones. The security policies *`Trusted`* and *`Untrusted`* describe this assumption. They define the filter rules **Trusted Interfaces** and **Untrusted Interfaces** which are created by default and cannot be deleted.

If you use the **Security Policy** *`Trusted`*, all data packets are accepted. You can create additional filter rules that discard specific packets. In the same way, you can allow specific packets when using the *`Untrusted`* policy.

A list of all configured filter rules is displayed in the **Firewall**->**Policies**+**IPv4 Filter Rules** menu.

Using the ✎ button in the line **Trusted Interfaces**, you can determine which interfaces are **Trusted**. A new window opens with an interface list. You can mark individual interfaces as trusted.

You can use the ≡+ button to insert another policy above the list entry. The configuration menu for creating a new policy opens.

You can use the ⇅ button to move the list entry. A dialog box opens, in which you can select the position to which the policy is to be moved.

16.1.1.1 New

Note

Informationen on the selection of Trusted Interfaces can be found here: *IPv4 Filter Rules* on page 303.

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.

16.1.2 IPv6 Filter Rules

The default behaviour with **Action** = *Access* consists of two implicit filter rules: If an incoming packet can be assigned to an existing connection and if a suitable connection is expected (e.g. such as an affiliated connection of an existing connection), the packet is allowed.

The sequence of filter rules in the list is relevant: The filter rules are applied to each packet in succession until a rule matches. If overlapping occurs, i.e. more than one filter rule matches a packet, only the first rule is executed. This means that if the first rule denies a packet, whereas a later rule allows it, the packet is rejected. A deny rule also has no effect if a relevant packet has previously been allowed by another filter rule.

The security concept is based on the assumption that an infrastructure consists of trusted and untrusted zones. The security policies *Trusted* and *Untrusted* describe this assumption. They define the filter rules **Trusted Interfaces** and **Untrusted Interfaces** which are created by default and cannot be deleted.

If you use the **Security Policy** *Trusted*, all data packets are accepted. You can create additional filter rules that discard specific packets. In the same way, you can allow specific packets when using the *Untrusted* policy.

A list of all configured filter rules is displayed in the **Firewall**->**Policies**->**IPv6 Filter Rules** menu.

Using the ✎ button in the line **Trusted Interfaces**, you can determine which interfaces are **Trusted**. A new window opens with an interface list. You can mark individual interfaces as trusted.

You can use the ≡+ button to insert another policy above the list entry. The configuration menu for creating a new policy opens.

You can use the ⇅ button to move the list entry. A dialog box opens, in which you can select the position to which the policy is to be moved.

16.1.2.1 New

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

The menu **Firewall**->**Policies**->**IPv6 Filter Rules**->**New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Source	Select one of the preconfigured aliases for the source of the packet. In the list, all WAN/LAN interfaces, interface groups (see **Firewall**->**Interfaces**->**IPv6 Groups**), adresses (see **Firewall**->**Addresses**->**Address List**) and address groups (see **Firewall**->**Addresses**->**Groups**) are available for selection for IPv6.
Destination	Select one of the preconfigured aliases for the destination of the packet. In the list, all WAN/LAN interfaces, interface groups (see **Firewall**->**Interfaces**->**IPv6 Groups**), addresss (see **Firewall**->**Addresses**->**Address List**) and address groups (see **Firewall**->**Addresses**->**Groups**) are available for selection for IPv6.
Service	Select one of the preconfigured services to which the packet to be filtered must be assigned. The extensive range of services configured ex works includes the following: • *ftp* • *telnet* • *smtp* • *dns* • *http* • *nntp*

Field	Description
	Additional services are created in **Firewall**->**Services**->**Service List**. In addition, the service groups configured in **Firewall**->**Services**->**Groups** can be selected.
Action	Select the action to be applied to a filtered packet. Possible values: • *Access* (default value): The packets are forwarded on the basis of the entries.. • *Deny* : The packets are rejected. • *Reject* : The packets are rejected. An error message is issued to the sender of the packet.

16.1.3 Options

In this menu, you can disable or enable the IPv4 firewall and can log its activities. In addition, you can define after how many seconds of inactivity a session shall be ended.

Note

The IPv6 firewall is always active and cannot be disabled.

The menu **Firewall**->**Policies**->**Options** consists of the following fields:

Fields in the Global Firewall Options menu

Field	Description
IPv4 Firewall Status	Enable or disable the IPv4 firewall function. The function is enabled with *Enabled* The function is enabled by default.
Logged Actions	Select the firewall syslog level. The messages are output together with messages from other subsystems. Possible values:

Field	Description
	• *All* (default value): All firewall activities are displayed. • *Deny*: Only reject and deny events are shown, see "Action". • *Accept*: Only accept events are shown. • *None*: Syslog messages are not generated.
IPv4 Full Filtering	With TCP sessions, the SIF first verifies if a session has been established completely and correctly. The filtering itself is carried out in a second step. The default setting **IPv4 Full Filtering** has been designed to meet this "standard" case. If - in a two-way communication - one traffic direction is sent through the router, but the counter direction takes a different route, the data traffic of this connection will be blocked because the session is interpreted as "incomplete" by the SIF. This will happen even if there is a rule that allows the same kind data traffic in a complete session. In order to allow the data traffic of "incomplete" sessions you have to disable **IPv4 Full Filtering**.
STUN Handler	Enable this option if you intend to allow network devices (esp. SIP clients) to use STUN in order to identify the network address translation mode and the public IP address. The firewall creates temporary rules that allow RTP data traffic for SIP phone calls.
Port STUN server	Only for **STUN Handler**= Enabled Enter the number of the port to be used for the connection to the STUN server. The default value is 3478. A 5 digit sequence isd possible.

Fields in the Session Timer menu.

Field	Description
UDP Inactivity	Enter the inactivity time after which a UDP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *180*.
TCP Inactivity	Enter the inactivity time after which a TCP session is to be re-

Field	Description
	garded as expired (in seconds). Possible values are *30* to *86400*. The default value is *3600*.
PPTP Inactivity	Enter the inactivity time after which a PPTP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *86400*.
Other Inactivity	Enter the inactivity time after which a session of another type is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *30*.

Fields in the Factory Reset Firewall

Field	Description
Factory Reset Firewall	Click **Reset** to reset the firewall to factory defaults.

16.2 Interfaces

16.2.1 IPv4 Groups

A list of all configured IPv4 interface routes is displayed in the **Firewall**->**Interfaces**->**IPv4 Groups** menu.

You can group together the interfaces of your device. This makes it easier to configure firewall rules.

16.2.1.1 New

Choose the **New** button to set up new IPv4 interface groups.

The menu **Firewall**->**Interfaces**->**IPv4 Groups**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the IPv4 interface group.
Members	Select the members of the group from the available interfaces. To do this, activate the field in the **Selection** column.

16.2.2 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.

16.2.2.1 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.

16.3 Addresses

16.3.1 Address List

A list of all configured addresses is displayed in the **Firewall**->**Addresses**->**Address List** menu.

16.3.1.1 New

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

The menu **Firewall**->**Addresses**->**Address List**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the address.
IPv4	Allows configuration of IPv4 address lists. The function is enabled with *Enabled* . The function is enabled by default.
Address Type	Only for **IPv4** = *Enabled* Select the type of address you want to specify. Possible values: • *Address / Subnet* (default value): Enter an IP address with subnet mask. • *Address Range*: Enter an IP address range with a start and end address.
Address / Subnet	Only for **IPv4** = *Enabled* and **Address Type** = *Address / Subnet* Enter the IP address of the host or a network address and the related netmask. The default value is *0.0.0.0*.
IPv6	Allows configuration of IPv6 address lists. The function is enabled with *Enabled* . The function is disabled by default.
Address / Prefix	Only for **IPv6** = *Enabled* Enter IPv6 address and the related prefix.

16.3.2 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.

16.3.2.1 New

Choose the **New** button to set up additional address groups.

The menu **Firewall**->**Addresses**->**Groups**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the address group.
IP Version	Select the IP version used. Possible values: • *IPv4* • *IPv6* *IPv4* is selected by default.
Selection	Select the members of the group from the available **Addresses**. To do this, activate the Fields in the **Selection** column.

16.4 Services

16.4.1 Service List

In the **Firewall**->**Services**->**Service List** menu, a list of all available services is displayed. Choose the ✎ icon to edit existing entries. You can delete existing entries with the icon 🗑 .

Note

Service is also removed from NAT service list! Recreation possible only by factory reset.

16.4.1.1 New

Choose the **New** button to set up additional services.

The menu **Firewall**->**Services**->**Service List**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter an alias for the service you want to configure.
Protocol	Select the protocol on which the service is to be based. The most important protocols are available for selection.
Destination Port Range	Only for **Protocol** = *TCP*, *UDP/TCP* or *UDP* In the first field, enter the destination port via which the service is to run. If a port number range is specified, in the second field enter the last port of the port range. By default the field does not contain an entry. If a value is displayed, this means that the previously specified port number is verified. If a port range is to be checked, enter the upper limit here. Possible values are *1* to *65535*.
Source Port Range	Only for **Protocol** = *TCP*, *UDP/TCP* or *UDP* In the first field, enter the source port to be checked, if applicable. If a port number range is specified, in the second field enter the last port of the port range. By default the field does not contain an entry. If a value is displayed, this means that the previously specified port number is verified. If a port range is to be checked, enter the upper limit here. Possible values are *1* to *65535*.
Type	Only for **Protocol** = *ICMP* The **Type** field shows the class of ICMP messages, the **Code** field specifies the type of message in greater detail. Possible values: • *Any* (default value) • *Echo Reply*

Field	Description
	• *Destination unreachable* • *Source Quench* • *Redirect* • *Echo* • *Time Exceeded* • *Parameter Problem* • *Timestamp* • *Timestamp Reply* • *Information Request* • *Information Reply* • *Address Mask Request* • *Address Mask Reply*
Code	Selection options for the ICMP codes are only available for **Type** = *Destination unreachable* Possible values: • *Any* (default value) • *Net Unreachable* • *Host Unreachable* • *Protocol Unreachable* • *Port Unreachable* • *Fragmentation Needed* • *Communication with Destination Network is Administratively Prohibited* • *Communication with Destination Host is Administratively Prohibited*

16.4.2 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.

16.4.2.1 New

Choose the **New** button to set up additional service groups.

The menu **Firewall**->**Services**->**Groups**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the service group.
Members	Select the members of the group from the available service aliases. To do this, activate the Fields in the **Selection** column.

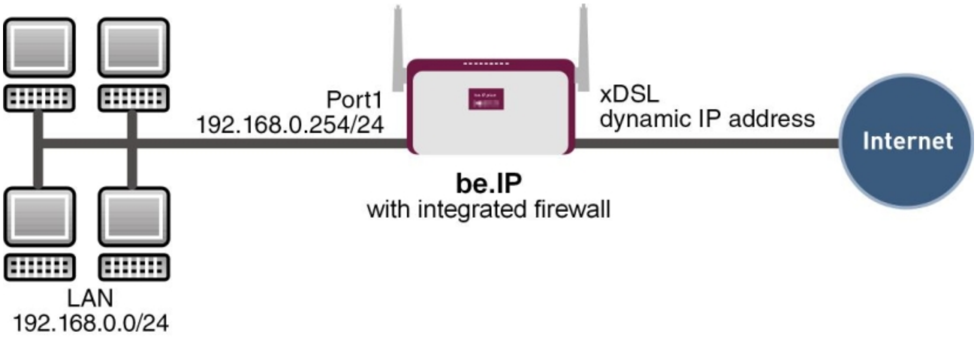
16.5 Configuration

16.5.1 SIF - Configuration example

Requirements

- Internet connection
- Your LAN must be connected to one of ports 1, 2, 3 or 4 on the gateway.

Example scenario



Configuration target

- Only certain Internet services are to be available for the staff of a company (HTTP, HT-

TPS, FTP, DNS).

- The gateway should operate as a DNS proxy, which means that the clients use the gateway as a DNS server.
- Only the system administrator and the director should be able to established an HTTP and a Telnet connection to the gateway.
- The director must be able to use all services in the Internet..
- All other data traffic will be blocked.

⚠ **Important**

An incorrect configuration of the firewall can significantly disrupt the functionality of the gateway or drop the connections.

The usual principle for firewalls also applies: Everything that is not explicitly allowed is prohibited.

This means accurate planning of the filter rules and filter rule chain is necessary to ensure correct operation.

Overview of Configuration Steps

Aliases for IP addresses and network address

Field	Menu	Value
Description	**Firewall**-> **Addresses** ->**Address List**-> **New**	e.g. *Administrator*
Address Type	**Firewall** ->**Addresses**-> **Address List** ->**New**	*Address / Subnet*
Address / Subnet	**Firewall**-> **Addresses** ->**Address List**-> **New**	e.g. *192.168.0.2* with *255.255.255.255*
Description	**Firewall**-> **Addresses** ->**Address List** ->**New**	e.g. *Director*
Address Type	**Firewall**-> **Addresses** ->**Address List**-> **New**	*Address / Subnet*
Address / Subnet	**Firewall** ->**Addresses**-> **Address List** ->**New**	e.g. *192.168.0.3* with *255.255.255.255*
Description	**Firewall**-> **Addresses** ->**Address List**-> **New**	e.g. *be.IP*
Address Type	**Firewall**-> **Addresses** ->**Ad-**	*Address / Subnet*

Field	Menu	Value
	dress List ->New	
Address / Subnet	**Firewall-> Addresses ->Address List-> New**	e.g. *192.168.0.254* with *255.255.255.255*
Description	**Firewall ->Addresses-> Address List ->New**	e.g. *Network Internal*
Address Type	**Firewall-> Addresses ->Address List-> New**	*Address / Subnet*
Address / Subnet	**Firewall-> Addresses ->Address List ->New**	e.g. *192.168.0.0* with *255.255.255.0*

Address groups

Field	Menu	Value
Description	**Gro Firewall->Addresses->ups->New**	e.g. *be.IP*
IP Version	**Gro Firewall->Addresses->ups->New**	*IPv4*
Selection	**Gro Firewall->Addresses->ups->New**	e.g. *Administrator* and *Director*

Service Sets

Field	Menu	Value
Description	**Group Ne Firewall->Services->s->w**	e.g. *Internet Ports*
Members	**Group Ne Firewall->Services->s->w**	e.g. *http*, *http (SSL)* and *ftp*
Description	**Group Ne Firewall->Services->s->w**	e.g. *Administration Ports*
Members	**Group Ne Firewall->Services->s->w**	e.g. *http* and *telnet*

Filter rules 1: Manage Gateway (System administrator)

Field	Menu	Value
Source Location	**Firewall ->Policies ->IPv4 Filter Rules-> New**	*be.IP*
Destination	**Firewall-> Policies ->IPv4 Filter Rules-> New**	*be.IP*
Service	**Firewall ->Policies ->IPv4 Filter Rules-> New**	*Administration Ports*
Action	**Firewall-> Policies ->IPv4 Filter Rules-> New**	*Access*

Filter rules 2: Use gateway as DNS proxy

Field	Menu	Value
Source Location	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*LOCAL*
Destination	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*ANY*
Service	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*dns*
Action	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*Access*
Source Location	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*Netzwerk_Intern*
Destination	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*be.IP*
Service	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*dns*
Action	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*Access*

Filter rules 3: Deny access from outside to the Gateway

Field	Menu	Value
Source Location	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*ANY*
Destination	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*be.IP*
Service	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*any*
Action	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*Deny*

Filter rules 4: Allow access to all services on the Internet (Director)

Field	Menu	Value
Source Location	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*Director*
Destination	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*ANY*
Service	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*any*
Action	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*Access*

Filter rules 5: Allow access to the Internet (Staff)

Field	Menu	Value
Source Location	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*Network_Internal*
Destination	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*ANY*
Service	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*Internet Ports*
Action	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*Access*

Chapter 17 Local Services

This menu offers services for the following application areas:

- Name resolution (DNS)
- Configuring the parameters of the backed up configuration connection via HTTPS.
- Configuration of system as a DHCP server (assignment of IP addresses)
- Automation of tasks according to schedule (scheduling).
- Start network devices that are switched off via an integrated network card (Wake-On-LAN)

17.1 DNS

Each device in a TCP/IP network is usually located by its IP address. Because host names are often used in networks to reach different devices, it is necessary for the associated IP address to be known. This task can be performed by a DNS server, which resolves the host names into IP addresses. Alternatively, name resolution can also take place over the HOSTS file, which is available on all PCs.

Your device offers the following options for name resolution:

- DNS Proxy, for forwarding DNS requests sent to your device to a suitable DNS server. This also includes specific forwarding of defined domains (Forwarded Domains).
- DNS cache, for saving the positive and negative results of DNS requests.
- Static entries (static hosts), to manually define or prevent assignments of IP addresses to names.
- DNS monitoring (statistics), to provide an overview of DNS requests on your device.

Name server

Under **Local Services**->**DNS**->**DNS Servers**->**New** you enter the IP addresses of name servers that are queried if your device cannot answer requests itself or by forwarding entries. Global name servers and name servers that are attached to an interface can both be entered.

Your device can also receive the global name servers dynamically via PPP or DHCP and transfer them dynamically if necessary.

Strategy for name resolution on your device

A DNS request is handled by your device as follows:

(1) If possible, the request is answered directly from the static or dynamic cache with IP address or negative response.

(2) Otherwise, if a suitable forwarding entry exists, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If the DNS server can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(3) Otherwise, if name servers have been entered, taking into account the priority configured and if the relevant interface status is "up", the primary DNS server is queried and then the secondary DNS server. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(4) Otherwise, if a suitable Internet or dialin connection is selected as the standard interface, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(5) Otherwise, if overwriting the addresses of the global name servers is allowed in the **WAN**->**Internet + Dialup** menu (**Interface Mode** = *Dynamic*), a connection is set up – if necessary at extra cost – to the first Internet or dialin connection configured to enable DNS server addresses to be requested from DNS servers (**DNS Negotiation** = *Enabled*), if this has not been already attempted. When the name servers have been negotiated successfully, these name servers are then available for more queries.

(6) Otherwise the initial request is answered with a server error.

If one of the DNS servers answers with `non-existent domain`, the initial request is immediately answered accordingly and a corresponding negative entry is made in the DNS cache of your device.

17.1.1 Global Settings

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**	Enter the IP address of the first and, if necessary, alternative global Windows Internet Name Server (=WINS) or NetBIOS Name Server (=NBNS).

Field	Description
Secondary	

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

Fields in the Advanced Settings menu

Field	Description
Positive Cache	Select whether the positive dynamic cache is to be activated, 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**. 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`.

Field	Description
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.

17.1.2 DNS Servers

A list of all configured DNS servers is displayed in the **Local Services**->**DNS**->**DNS Servers** menu.

17.1.2.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to set up additional DNS servers.

Here you can configure both global DNS servers and DNS servers that are to be assigned to a particular interface.

Configuring a DNS server for a particular interface can be useful, for example, if accounts with different providers have been set up via different interfaces and load balancing is being used.

The **Local Services**->**DNS**->**DNS Servers**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Admin Status	Select whether the DNS server should be enabled. The function is activated by selecting *Enabled*. The function is enabled by default.
Description	Enter a description for DNS server.
Priority	Assign a priority to the DNS server. You can assign more than one pair of DNS servers (**Primary DNS Server** and **Secondary DNS Server**) to an interface (i. e. for example, to an Ethernet port or a PPPoE WAN partner). 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)

Field	Description
Interface	Select the interface to which the DNS server pair is to be assigned. For **Interface Mode** = *Dynamic* A global DNS server is created with the setting *None*. For **Interface Mode** = *Static* A DNS server is configured for all interfaces with the *Any* setting.
IP Version	Select the IP version used. Possible values: • *IPv4* • *IPv6* *IPv4* is selected by default.
Primary IPv4 DNS Server	Only if **Interface Mode** = *Static* Enter the IPv4 address of the first name server for Internet address name resolution.
Secondary IPv4 DNS Server	Only if **Interface Mode** = *Static* Optionally, enter the IPv4 address of an alternative name server.
Primary IPv6 DNS Server	Only if **Interface Mode** = *Static* Enter the IPv6 address of the first name server for Internet address name resolution.
Secondary IPv6 DNS Server	Only if **Interface Mode** = *Static* Optionally, enter the IPv6 address of an alternative name server.

17.1.3 Static Hosts

A list of all configured static hosts is displayed in the **Local Services**->**DNS**->**Static Hosts** menu.

17.1.3.1 New

Choose the **New** button to set up new static hosts.

The menu **Local Services**->**DNS**->**Static Hosts**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Default Domain	Here, the domain is displayed that you have specified in the menu **DNS**->**Global Settings** as Domain Name.
DNS Hostname	Enter the host name to which the **IP Address** defined in this menu is to be assigned if a positive response is sent upon a DNS request. If a negative response is sent upon a DNS request, no address is specified. The entry can also start with the wildcard *, e.g. *.bintec-elmeg.com. If you specify a simple name (e.g. `router`), it is expanded by the Default Domain to form a complete DNS name (Fully Qualified Domain Name, FQDN). If you enter a name with the structure of a FQDN (i.e. character sequences separated by "."), the entry is interpreted as a FQDN and is not expanded. The closing "." which is mandatory for a complete FQDN is automatically appended if required. Entries with spaces are not allowed.
Response	In this entry, select the type of response to DNS requests. 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.

Field	Description
IPv4 Address	Only if **Response** = *Positive* Enter the IPv4 address assigned to **DNS Hostname**.
IPv6 Address	Only if **Response** = *Positive* Enter the IPv6 address assigned to **DNS Hostname**.

17.1.4 Domain Forwarding

In the **Local Services**->**DNS**->**Domain Forwarding** menu, a list of all configured forwardings for defined domains is displayed.

17.1.4.1 New

Choose the **New** button to set up additional forwardings.

The menu **Local Services**->**DNS**->**Domain Forwarding**->**New** consists of the following fields:

Fields in the Forwarding Parameters menu.

Field	Description
Forward	Select whether requests for a host or domain are to be forwarded. Possible values: • *Host* (default value) • *Domain*
Host	Only for **Forward** = *Host* Enter the name of the host for which requests are to be forwarded. 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*

Field	Description
	Enter the name of the domain for which requests are to be forwarded. The entry can start with the wildcard "*", e.g. "*.bintec-elmeg.com". If you enter a name without a leading wildcard "*" a leading wildcard "*" is supplemented as soon as you confirm with **OK**.
Forward to	Select if matching DNS requests are to be forwarded to the DNS server of an **Interface** or to a manually specified **DNS Server**. Possible values: • *Interface* (default value): Requests are forwarded to the DNS server assigned to either an automatically selected or to a user-selected interface. • *DNS Server*: Requests are forwarded to the specified **DNS Server**.
Interface	Only for **Forward to** = *Interface* Select the interface that has the DNS server assinged which is to receive the DNS requests.
Primary DNS Server (IPv4/IPv6)	Only for **Forward to** = *DNS Server* Enter the IPv4/IPv6 address of the primary DNS server.
Secondary DNS Server (IPv4/IPv6)	Only for **Forward to** = *DNS Server* Enter the IPv4/IPv6 address of the secondary DNS server.

17.1.5 Dynamic Hosts

In the menu **Local Services**->**DNS**->**Dynamic Hosts**, you can find relevant information on dynamic DNS entries.

17.1.6 Cache

In the **Local Services**->**DNS**->**Cache** menu, a list of all available cache entries is displayed.

You can select individual entries using the checkbox in the corresponding line, or select them all using the **Select all** button.

A dynamic entry can be converted to a static entry by marking the entry and confirming with **Make static**. This corresponding entry disappears from the list and is displayed in the list in the **Static Hosts** menu. The TTL is transferred.

17.1.7 Statistics

In the **Local Services**->**DNS**->**Statistics** menu, the following statistical values are displayed:

Fields in the DNS Statistics menu.

Field	Description
Received DNS Packets	Shows the number of received DNS packets addressed direct to your device, including the response packets for forwarded requests.
Invalid DNS Packets	Shows the number of invalid DNS packets received and addressed direct to your device.
DNS Requests	Shows the number of valid DNS requests received and addressed direct to your device.
Cache Hits	Shows the number of requests that were answered with static or dynamic entries from the cache.
Forwarded Requests	Shows the number of requests forwarded to other name servers.
Cache Hitrate (%)	Indicates the number of **Cache Hits** pro DNS request in percentage.
Successfully Answered Queries	Shows the number of successfully answered requests (positive and negative).
Server Failures	Shows the number of requests that were not answered by any name server (either positively or negatively).

17.2 HTTPS

You can operate the user interface of your device from any PC with an up-to-date Web browser via an HTTPS connection.

HTTPS (HyperText Transfer Protocol Secure) is the procedure used to establish an encrypted and authenticated connection by SSL between the browser used for configuration and the device.

17.2.1 HTTPS Server

In the **Local Services**->**HTTPS**->**HTTPS Server** menu, configure the parameters of the backed up configuration connection via HTTPS.

The **Local Services**->**HTTPS**->**HTTPS Server** menu consists of the following fields:

Fields in the HTTPS Parameters menu.

Field	Description
HTTPS TCP Port	Enter the port via which the HTTPS connection is to be established. Possible values are *0* to *65535*. The default value is *443*.
Local Certificate	Select a certificate that you want to use for the HTTPS connection. Possible values: • *Internal* (default value): Select this option if you want to use the certificate built into the device. • *<Certificate name>*: Under **System Management**->**Certificates**->**Certificate List** select entered certificate.

17.3 DHCP Server

You can configure your device as a DHCP (Dynamic Host Configuration Protocol) server.

Your device and each PC in your LAN requires its own IP address. One option for allocating IP addresses in your LAN is the Dynamic Host Configuration Protocol (DHCP). If you configure your device as a DHCP server, the device automatically assigns IP addresses to requesting PCs in the LAN from a predefined IP address pool.

If a client requires an IP address for the first time, it sends a DHCP request (with its MAC address) to the available DHCP server as a network broadcast.* The client then receives its IP address from bintec elmeg (as part of a brief exchange).

You therefore do not need to allocate fixed IP addresses to PCs, which reduces the amount of configuration work in your network. To do this, you set up a pool of IP addresses, from which your device assigns IP addresses to hosts in the LAN for a defined period of time. A DHCP server also transfers the addresses of the domain name server entered statically or by PPP negotiation (DNS), NetBIOS name server (WINS) and default gateway.

For specific instructions how to use your device as a DHCP server, DHCP client or DHCP relay agent, see the ent of the chapter *DHCP - Configuration example* on page 337.

17.3.1 IP Pool Configuration

The **Local Services**->**DHCP Server**->**IP Pool Configuration** menu displays a list of all the configured IP pools. This list is global and also displays pools configured in other menus.

17.3.1.1 Edit or New

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

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	**Primary**: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. **Secondary**: Optionally, enter the IP address of an alternative DNS server.

17.3.2 DHCP Configuration

To activate your device as a DHCP server, you must first define IP address pools from which the IP addresses are distributed to the requesting clients.

A list of all configured DHCP pools is displayed in the **Local Services**->**DHCP Server**->**DHCP Configuration** menu.

In the list, for each entry, you have the possibility under **Status** of enabling or disabling the configured DHCP pools.

> **Note**
>
> In the ex works state the DHCP pool is preconfigured with the IP addresses 192.168.0.10 to 192.168.0.49 and is used if there is no other DHCP server available in the network.

17.3.2.1 Edit or New

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

The **Local Services**->**DHCP Server**->**DHCP Configuration**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Select the interface over which the addresses defined in **IP Pool Name** are to be assigned to DHCP clients. When a DHCP request is received over this **Interface**, one of the addresses from the address pool is assigned.
IP Pool Name	Select an IP pool name configured in the **Local Services**->**DHCP Server**->**IP Pool Configuration** menu.
Pool Usage	Select if the DHCP pool is to be used for requests from clients in a network directly connected to an Ethernet interface, or if it is to be used for DHCP requests from a remote network that are sent to your device via a DHCP relay station. In the second case, it is possible to use an IP address pool for

Field	Description
	the remote network. Possible values: • *Local* (default value): The DHCP pool is only used for DHCP requests from a network directly connected to an Ethernet interface. • *Relay*: The DHCP pool is only used for DHCP requests forwarded from remote networks. • *Local/Relay*: The DHCP pool can be used for both kinds of requests.
Description	Enter any description to uniquely identify the DHCP pool.

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

Fields in the menu Advanced Settings

Field	Description
Gateway	Select which IP address is to be transferred to the DHCP client as gateway. Possible values: • *Use router as gateway* (default value): Here, the IP address defined for the **Interface** is transferred. • *No gateway*: No IP address is sent. • *Specify*: Enter the corresponding IP address.
Lease Time	Enter the length of time (in minutes) for which an address from 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.

Field	Description
	• *DNS Server*: Enter the IP address of the DNS server to be sent to the client. • *DNS Domain Name*: Enter the DNS domain to be sent to the client. • *WINS/NBNS Server*: Enter the IP address of the WINS/NBNS server to be sent to the client. • *WINS/NBT Node Type*: Select the type of the WINS/NBT node to be sent to the client. • *TFTP Server*: Enter the IP address of the TFTP server to be sent to the client. • *CAPWAP Controller*: Enter the IP address of the CAPWAP controller to be sent to the client. • *URL (provisioning server)*: This option enables you to send a client any URL. Use this option to send querying **IP1x0** telephones the URL of the provisioning server if the telephones are to be provisioned automatically. The URL then needs to take the form *http://<IP address of the provisioning server>/eg_prov*. Multiple entries are possible. Add additional entries with the **Add** button.

Vendor Specific Information (DHCP Option 43)

The options for a **Vendor String** or a vendor-specific group of DHCP options (**Vendor Group**) enable you to transmit any manufacturer-specific information or configuration parameters to DHCP clients. You can also define entire groups of DHCP options to be transmitted.

Note

For some products settings have already been predefined in this section. These are required for the seamless integration of telephones or LTE access routers and should not be changed or deleted.

Choose the ✎ icon to edit an existing entry or one of the **Add** buttons to add an entry. In the popup menu, you configure manufacturer-specific settings in the DHCP server for specific telephones, for example.

Fields in the Basic Parameters menu for vendor strings

Field	Description
Select vendor	Here, you can select for which manufacturer specific values shall be transmitted for the DHCP server. Possible values: • *Other* (default value) • *-bintec-*
APN	Only für **Select vendor** = *-bintec-* Enter the Access Point Namen (APN) of the SIM card.
PIN	Only für **Select vendor** = *-bintec-* Enter the PIN of the SIM card.
Vendor Description	Only für **Select vendor** = *Other* Type in the name of the manufacturer for which you want to transfer specific DHCP server settings.
Vendor ID	Only für **Select vendor** = *Other* To identify the device, enter the manufacturer ID.
Vendor Option String	Only für **Select vendor** = *Other* Enter the manufacturer specific configuration parameters.

Fields in the Basic Parameters menu for vendor groups

Field	Description
Select vendor	Here, you can select for which manufacturer specific values shall be transmitted for the DHCP server. Possible values: • *Siemens* (default value) • *Other*
Provisioning Server	Only für **Select vendor** = *Siemens* Enter which manufacturer value shall be transmitted.

Field	Description
	For the setting **Select vendor** = *Siemens*, the default value *sdlp* is displayed. You can complete the IP address of the desired server.
Vendor Description	Only für **Select vendor** = *Other* Type in the name of the manufacturer for which you want to transfer specific DHCP server settings.
Vendor ID	Only für **Select vendor** = *Other* To identify the device, enter the manufacturer ID.
Custom DHCP Options	Only für **Select vendor** = *Other* Use **Add** to add more entries. You can add custom DHCP options.

17.3.3 IP/MAC Binding

The **Local Services**->**DHCP Server**->**IP/MAC Binding** menu displays a list of all clients that received an IP address from your device via DHCP.

You can allocate an IP address from a defined IP address pool to specific MAC addresses. You can do this by selecting the **Static Binding** option in the list to convert a list entry as a fixed binding, or you manually create a fixed IP/MAC binding by configuring this in the **New** sub-menu.

Note

You can only create new static IP/MAC bindings if IP address ranges were configured in **Local Services**->**DHCP Server**->**DHCP Pool**, and in the **Local Services**->**DHCP Server**->**IP Pool Configuration** menu is assigned a valid IP Pool.

17.3.3.1 New

Choose the **New** button to set up new IP/MAC bindings.

The menu **Local Services**->**DHCP Server**->**IP/MAC Binding**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the host to which the **MAC Address** the **IP Address** is to be bound. A character string of up to 256 characters is possible.
IP Address	Enter the IP address to be assigned to the MAC address specified in **MAC Address** is to be assigned.
MAC Address	Enter the MAC address to which the IP address specified in **IP Address** is to be assigned.

17.3.4 DHCP Relay Settings

If your device for the local network does not distribute any IP addresses to the clients by DHCP, it can still forward the DHCP requests on behalf of the local network to a remote DHCP server. The DHCP server then assigns the your device an IP address from its pool, which in turn sends this to the client in the local network.

The menu **Local Services**->**DHCP Server**->**DHCP Relay Settings** consists of the following fields:

Fields in the Basic Parameters menu.

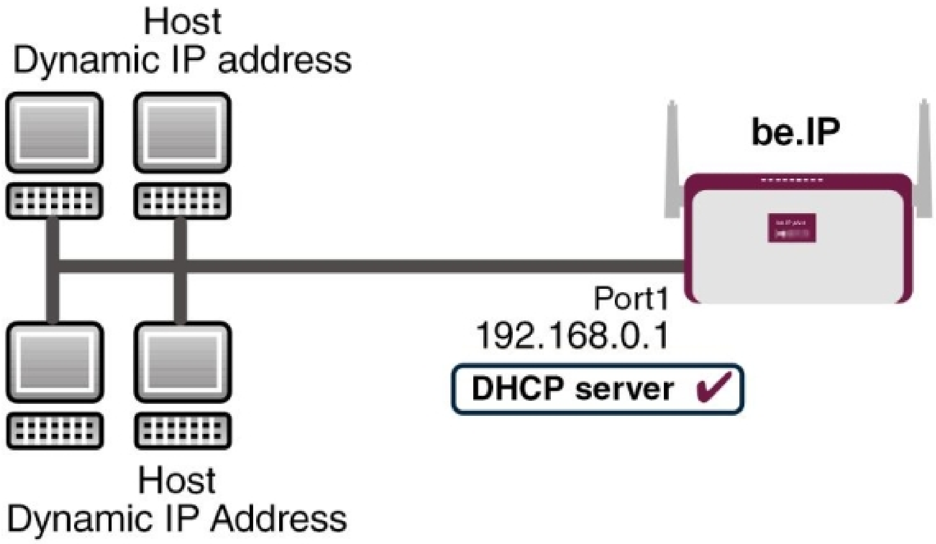
Field	Description
Primary DHCP Server	Enter the IP address of a server to which BootP or DHCP requests are to be forwarded. The default value is `0.0.0.0`.
Secondary DHCP Server	Enter the IP address of an alternative BootP or DHCP server. The default value is `0.0.0.0`.

17.3.5 DHCP - Configuration example

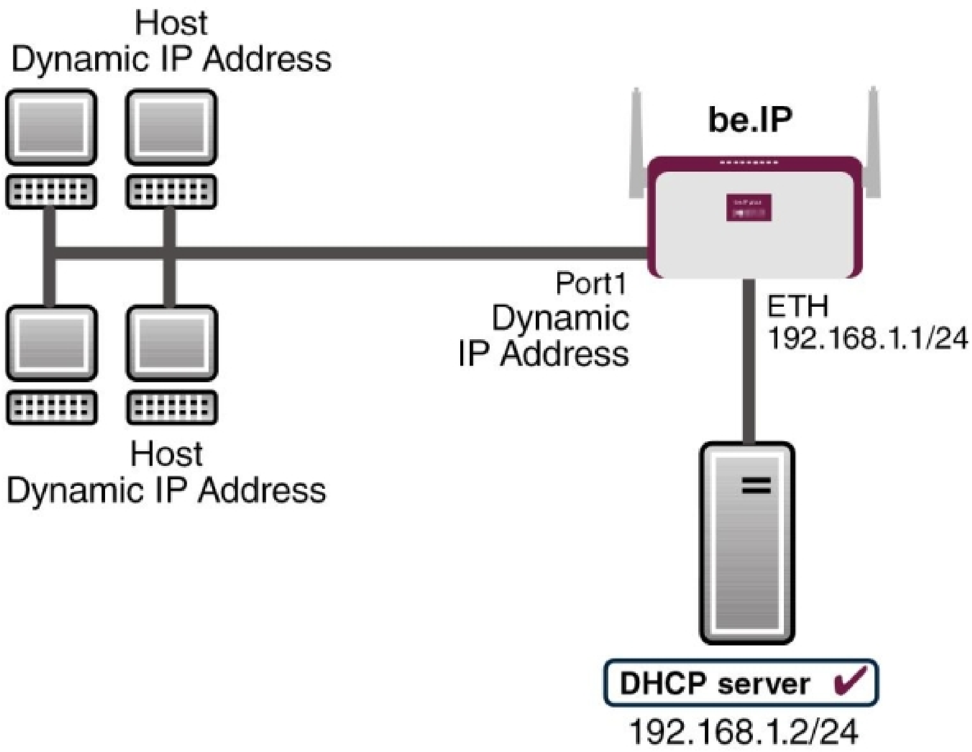
Requirements

- An optional DHCP server

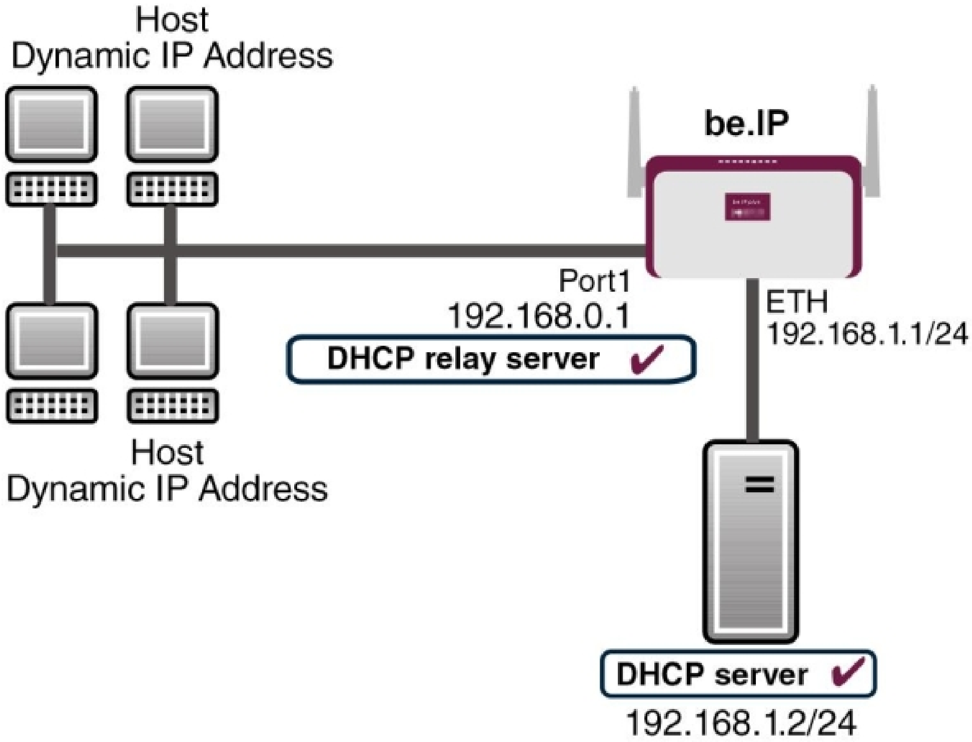
Example scenaria



Example scenario as DHCP Server



Example scenario as DHCP Client



Example scenario as DHCP Relay Server

Configuration target

You can use your device as a DHCP server, DHCP client or DHCP relay agent.

Overview of Configuration Steps

DHCP Server

Field	Menu	Value
IP Pool Name	**Local Services->DHCP Server->IP Pool Configuration->New**	e.g. *IP-Pool-1*
IP Address Range	**Local Services->DHCP Server->IP Pool Configuration->New**	e.g. *192.168.0.2* and *192.168.0.10*
Interface	**Local Services->DHCP Server->DHCP Configuration->New**	e.g. *en1-0*
IP Pool Name	**Local Services->DHCP Server->DHCP Configuration->New**	*IP-Pool-1*
Pool Usage	**Local Services->DHCP Server->DHCP Configuration->New**	*Local*

Field	Menu	Value
Gateway	**Local Services**->**DHCP Server**->**DHCP Configuration**->**New**->**Advanced Settings**	*Use Router as Gateway*
Lease Time	**Local Services**->**DHCP Server**->**DHCP Configuration**->**New**->**Advanced Settings**	e.g. *120*
IP address to use for DNS/WINS server assignment	**Local Services**->**DNS**->**Global Settings**->**Advanced Settings**	e.g. *Own IP address*

DHCP Client

Field	Menu	Value
Address Mode	**LAN**->**IP Configuration**->**Interfaces**-> **<en1-4>**-> ✎	*DHCP*
DHCP MAC Address (optional)	**LAN**->**IP Configuration**->**Interfaces**-> **<en1-4>** -> ✎ ->**Advanced Settings**	MAC address for a specific DHCP server

DHCP Relay Server

Field	Menu	Value
Primary DHCP Server	**Local Services**->**DHCP Server**->**DHCP Relay Settings**	e.g. *192.168.1.2*
Secondary DHCP Server (optional)	**Local Services**->**DHCP Server**->**DHCP Relay Settings**	if one exists

17.4 DHCPv6 Server

You can operate your device as a DHCPv6 server. The DHCPv6 server can either assign IP addresses as well as DHCPv6 options or DHCPv6 options only without any addresses. These parameters are collected in a so called "Option Set". An option set can be linked to an interface (see **Local Services**->**DHCPv6 Server**->**DHCPv6 Server**->**New**), or it can be configured globally (see **Local Services**->**DHCPv6 Server**->**DHCPv6 Global Options**->**New**). DHCP options can, e.g., contain information about DNS or time servers.

Note

An IPv6 address pool is created by assigning an IPv6 Link Prefix (a subnet with a length of /64) to an DHCPv6 option set. The definition of a separate set of IP addresses like, e.g. fc00:1:2:3::1..fc00:1:2:3::100, is - in contrast with IPv4 - not specified for IPv6.

The following requirements must be met for the configuration of an IPV6 address pool:

(a) IPv6 has to be activated for the respective interface.

(b) An IPv6 Link Prefix (subnet) with a length of /64 has to be configured for the respective interface. An IPv6 link prefix can be defined in either of two ways:

- The IPv6 Link Prefix is derived from a General IPv6 Prefix (a prefix with a length of, e.g., /56 or /48). In this case, the General IPv6 Prefix has to be configured in the menu **Networking**->**IPv6 General Prefixes**->**General Prefix Configuration**.
- The IPv6 Link Prefix with a length of /64 is manually configured for the respective interface and is not derived from a General IPv6 Prefix.

(c) The **DHCP Server** option has to be enabled for the interface.

Moreover, the following settings are recommended:

- The options **Preferred Lifetime** and **Valid Lifetime** should be set to values higher than the value configured for the option **Router Lifetime**.

  With a **Router Lifetime** of 600 seconds a **Preferred Lifetime** of, e.g., 900 seconds and a **Valid Lifetime** of 1800 seconds are reasonable settings.
- The option **DHCP Mode** should be enabled.

In order to make the settings mentioned above, go to the menu **LAN**->**IP Configuration**->**Interfaces**. Choose the intended interface with the ✎ icon. Activate IPv6 and set the **IPv6 Mode** to `Router (Transmit Router Advertisement)`. In the field **IPv6-Adressen**, click **Add** and configure the Link Prefix. Confirm your configuration with **Accept**. The configuration of the recommended settings s then carried out in the following menus:

- **Router Lifetime**: **LAN**->**IP Configuration**->**Interfaces**->**New**->**Advanced Settings**->**Advanced IPv6 Settings**
- **Preferred Lifetime** and **Valid Lifetime**: **LAN**->**IP Configuration**->**Interfaces**->**New**->**Basic IPv6 Parameters**->**Add**->**Advanced**

17.4.1 DHCPv6 Server

Here you can create interface-related address pools and define DHCP options inside of an DHCP Option Set.

17.4.1.1 Edit or New

Use the **New** button in order to create an Option Set. Use the ✎ icon in order to edit an existing entry.

The menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Name	Enter a name for the Option Set.
Interface	Select the IPv6 interface the Option Set is assigned to. You can choose from interfaces with the following configuration: • IPv6 is enabled. • The option **DHCP Server** is enabled. In the ex works state, IPv6 is disabled for all interfaces. If the intended interface is not offered for selection, configure it according to the requirements detailed in the introduction of this section. Configuration is done on the menu **LAN**->**IP Configuration**->**Interfaces**.
Address assignment	The definition of an IPv6 address pools is carried out by assigning an IPv6 Link Prefix (subnet with a length of /64) to a DHCPv6 Option Set. The IPv6 address pool always comprises the complete 64 Bit address space of the selected IPv6 Link Prefix. Address assignment is random. Use **Add** to assign one or more IPv6 Link Prefixes to the IPv6 Option Set. **Note** Note that only such IPv6 Link Prefixes are available for selection that are assigned to the selected interface.

Fields in the menu Server Options

Field	Description
DNS domains search list	Use **Add** to create a list of domain names which is queried by the client during name resolution (DHCPv6 Option 24 "Domain Search List"). Domain names will be transmitted to the clients in the order defined by the list.

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

Fields in the menu Advanced Server Options

Field	Description
DNS Server	Here you can configure the DNS servers that are propagated by DHCPv6. (DHCPv6 Option 23 "DNS Recursive Name Server"). Per default, the global DNS server of the system are propagated. (Global DNS servers are configured by the field **DNS Propagation** in the menu **LAN**->**IP Configuration**->**Interfaces**-> ✎ ->**Advanced Settings** if **IPv6** = *Enabled* .) You can also manually specify DNS servers and have them propagated to the clients. To do this disable the option **Use RA or Global Fallback DNS Server** and create the desired DNS server entries using **Add**.
SNTP Server	Here you can configure the time servers to be propagated by DHCPv6 (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Use **Add** to create the desired time server entries.

17.4.2 DHCPv6 Global Options

In this menu, you can configure those DHCPv6 options which are globally valid for the DHCPv6 server. An option that has been configured here will be propagated if there is no more specific definition is available (e.g., no interface- or vendor-ID-specific definition).

The menu consist of the following fields:

Fields in the menu Basic Parameters

Field	Description
DNS domains search list	Use **Add** to create a list of domain names which is queried by the client during name resolution (DHCPv6 Option 24 "Domain

Field	Description
	Search List"). Domain names will be transmitted to the clients in the order defined by the list. The domain name (e.g. dev.bintec.de.) mast end with a dot (.).

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

Fields in the menu Server preference

Field	Description
Server preference	The DHCPv6 advertisements sent by the DHCPv6 server to the clients may contain the DHCPv6 option 7 "Preference". Possible values are *0...255*. In a network with multiple DHCPv6 servers this option controls which server takes the highest priority. If a client receives DHCPv6 advertisements with different priorities from different servers, it will usually accept the parameters from the highest priority server. The client can, however, also accept DHCPv6 advertisements with a lower priority if the set of parameters in the advertisement provides more of the options requested by the client. A value of *0* means "not specified" (lowest priority), *255* denotes the highest priority.

Fields in the menu Advanced Server Fallback Options

Field	Description
DNS Server	Here you can configure the DNS servers that are propagated by DHCPv6. (DHCPv6 Option 23 "DNS Recursive Name Server"). Per default, the global DNS server of the system are propagated. (Global DNS servers are configured by the field **DNS Propagation** in the menu **LAN**->**IP Configuration**->**Interfaces**-> ✎ ->**Advanced Settings** if **IPv6** = *Enabled*.) You can also manually specify DNS servers and have them propagated to the clients. To do this disable the option **Use RA or Global Fallback DNS Server** and create the desired DNS server entries using **Add**.
SNTP Server	Here you can configure the time servers to be propagated by DHCPv6 (DHCPv6 Option 31 "Simple Network Time Protocol

Field	Description
	Server"). Use **Add** to create the desired time server entries.

17.4.3 Stateful Clients

Here you see an entry for each Stateful Client that has contacted the server and has been assigned an IPv6 address.

17.4.4 Stateful Clients Configuration

During a stateful configuration of IPv6 clients not only the DHCP options, but also the IPv6 prefix is transmitted to the client.

17.4.4.1 Edit or New

Use **New** to create entries for Stateful Clients. Normally, you do not have to create any entries.Use ✎ in order to edit existing entries. You should check each automatically created entry once to verify the settings and adjust them if required.

The menu consists of the following fields.

Fields in the menu Basic Parameters

Field	Description
DUID	Clients use the **DUID field** (DHCP Unique Identifier) in order to identify themselves and request an IP address from the DHCPv6 server. If you create an entry using **New** you can specify the **DUID** as a 16 - 20 digit HEX number. You can enter them using a "-" (minus) as separator (Windows style), or you can enter them in a single block (Linux style).
Accept Client FQDN	If **Accept Client FQDN** is enabled, the client is entered into the cache of the Domain Name Server with the parameter FQDN (Fully Qualified Domain Name).
Administrative FQDNs	With **Add**, you can specify an FQDN (Fully Qualified Domain Name) - even for automatically created entries.
Static Interface Identifier	The field **Static Interface Identifier** is the host portion of the

Field	Description
	IPv6 address, i.e., the last 64 Bit of the IP address. This prefix must start with ::.

17.5 Scheduling

Your device has an event scheduler which enables certain standard actions (activation or deactivation of interfaces, for example) to be carried out. In addition, every existing MIB variable can be configured with any value.

You configure the desired **Actions** and define the triggers controlling the date and other conditions of the **Actions**. A trigger may be a single event or a sequence of events collected in an **Event List**. For a single event, create an **Event List** containing only one element.

It is possible to trigger operations on a time-controlled basis. What's more, the status or accessibility of interfaces, or their data traffic can lead to performance of the configured operations, as also the validity of licences. Here again, it is possible to configure every MIB variable with any value as initiator.

Activate the **Schedule Interval** option under **Options** to put the event scheduler into operation. The system uses this time interval to check if at least one event has occurrred. This triggers the configured action.

Specific instructions for configuring Time-controlled Tasks (Scheduling), see the end of the chapter *Configuration example - Time-controlled Tasks (Scheduling)* on page 364.

Caution

The configuration of actions that are not available as defaults requires extensive knowledge of the method of operation of bintec elmeg gateways. An incorrect configuration can cause considerable disruption during operation. If applicable, save the original configuration on your PC.

Note

To run the event scheduler, the date configured on your device must be 1.1.2000 or later.

17.5.1 Trigger

All configured event lists are displayed in the **Local Services**->**Scheduling**->**Trigger** menu. Each event list contains at least one event intended to trigger a configured action.

17.5.1.1 New

Choose the **New** button to create additional event lists.

The menu **Local Services**->**Scheduling**->**Trigger**->**New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Event List	You can create a new event list with *New* (default value). You give this list a name with **Description**. You use the remaining parameters to create the first event in the list. If you want to add to an existing event list, select the event list you want and add at least one more event to it. You can use event lists to create complex conditions for initiating an action. The events are processed in the same order in which they are created in the list.
4Description	Only for **Event List** *New* Enter your chosen designation for the **Event List**.
Event Type	Select the type of initiator. Possible values: • *Time* (default value): The operations configured and assigned in **Actions** are initiated at specific points in time. • *MIB/SNMP*: The operations configured and assigned in **Actions** are initiated when the defined MIB variables assumes the assigned values. • *Interface Status*: Operations configured and assigned in **Actions** are initiated, when the defined interfaces take on a specified status. • *Interface Traffic*: Operations configured and assigned in **Actions** are initiated when the data traffic on the specified

Field	Description
	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 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

Field	Description
	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.

Field	Description
Source IP Address	Only for **Event Type** *Ping Test* Enter an IP address to be used as sender address for the ping test. Possible values: • *Automatic* (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address. • *Specific*: Enter the desired IP address in the input field.
Status	Only for **Event Type** *Ping Test* Select whether **Destination IP Address** *Reacheable* must be (default value) or *Unreacheable* in order to initiate the operation.
Interval	Only for **Event Type** *Ping Test* Enter the time in **Seconds** after which a ping must be resent. The default value is *60* seconds.
Trials	Only for **Event Type** *Ping Test* Enter the number of ping tests to be performed until **Destination IP Address** as *Unreacheable* applies. The default value is *3*.
Monitored Certificate	Only for **Event Type** *Certificate Lifetime* Select the certificate whose validity should be checked.
Remaining Validity	Only for **Event Type** *Certificate Lifetime* Indicate the remaining validity of the certificate in percentage.
Function Button Status	Only for **Event Type** *Function Button*. When creating the trigger the dropdown selection **Function Button Status** allows you to choose which status of the function button activates or deactivates the trigger. If you set the status to *On*, the trigger becomes active if the status of the func-

Field	Description
	tion 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*. 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. Activa-

Field	Description
	tion is carried on the next scheduling interval. the default value of this interval is 55 seconds.
Stop Time	Enter the time from which the initiator is to be deactivated. Deactivation is carried on the next scheduling interval. If you do not enter a **Stop Time** or set a **Stop Time** = **Start Time**, the initiator is activated, and deactivated after 10 seconds.

17.5.2 Actions

In the **Local Services**->**Scheduling**->**Actions** menu is displayed a list of all operations to be initiated by events or event chains configured in **Local Services**->**Scheduling**->**Trigger**.

17.5.2.1 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,

Field	Description
	deleted or entered. • *5 GHz WLAN Bandscan*: Only for devices with a wireless LAN. A scan of the 5 GHz frequency band is performed. • *5.8 GHz WLAN Bandscan*: Only for devices with a wireless LAN. A scan of the 5.8 GHz frequency range is performed. • *WLC: New Neighbor Scan*: Only for devices with a WLAN controller. A Neighbor Scan is initiated by the WLAN network controlled by the WLAN controller. • *WLC: VSS State*: Only for devices with a WLAN controller. The status of a wireless network is modified. • *WLAN: Operation Mode*: The operating mode of a WLAN radio module is modified.
Event List	Select the event list you want which has been created in **Local Services**->**Scheduling**->**Trigger**.
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.

Field	Description
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. 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**.

Field	Description
	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.

Field	Description
	• *HTTP Server*: The latest software will be downloaded from an HTTP server that you define in *Server URL*. • *HTTPS Server*: The latest software will be downloaded from an HTTPS server that you define in *Server URL*. • *TFTP Server*: The latest software will be downloaded from an TFTP server that you define in *Server URL*.
Server URL	Where **Command Type** = *Software Update* if **Source Location** not *Current Software from Update Server* Enter the URL of the server from which the desired software version is to be retrieved. Where **Command Type** = *Configuration Management* with **Action** = *Import configuration* or *Export configuration* 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*

Field	Description
	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 **Action** = *Import configuration* or *Export configuration* Select whether the file is to be sent in the CSV format. The CSV format can easily be read and modified. In addition, you can view the corresponding file clearly using Microsoft Excel for example. The function is enabled by default.
Remote File Name	Only if **Command Type** = *Configuration Management* For **Action** = *Import configuration* Enter the name of the file under which it is saved on the server from which it is to be retrieved. For **Action** = *Export configuration* Enter the file name under which it should be saved on the server.

Field	Description
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.

Field	Description
Reboot after execution	Only if **Command Type** = *Configuration Management* Select whether your device should restart after the intended **Action**. The function is disabled by default.
Version Check	Only where **Command Type** = *Configuration Management* and **Action** = *Import configuration* Select whether, when importing a configuration file, to check on the server for the presence of a more current version of the already loaded configuration. If not, the file import is interrupted. The function is disabled by default.
Destination IP Address	Only if **Command Type** = *Ping Test* Enter the IP address whose accessibility is to be checked.
Source IP Address	Only if **Command Type** = *Ping Test* Enter an IP address to be used as sender address for the ping test. Possible values: • *Automatic* (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address. • *Specific*: Enter the desired IP address in the input field.
Interval	Only if **Command Type** = *Ping Test* Enter the time in **Seconds** after which a ping must be resent. The default value is *1* second.
Count	Only if **Command Type** = *Ping Test* Enter the number of ping tests to be performed until **Destination IP Address** is considered unreachable. The default value is *3*.

Field	Description
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 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

Field	Description
	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 enrol-

Field	Description
	ment cannot be concluded immediately. If the status has not been saved, the incomplete registration cannot be completed. As soon as the enrolment is completed and the certificate has been downloaded from the CA server, it is automatically saved in the device configuration. The function is enabled by default.
Use CRL	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Define the extent to which certificate revocation lists (CRLs) are to be included in the validation of certificates issued by the owner of this certificate. Possible values: • *Auto* (default value): In case there is an entry for a CDP, CRL distribution point this should be evaluated in addition to the CRLs globally configured in the device. • *Yes*: CRLs are always checked. • *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*

Field	Description
	Select the required operating mode for the selected radio module if it currently has the status *Down*. You may select from any of the operating modes that your device supports. So the choice may vary from device to device.

17.5.3 Options

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

The **Local Services**->**Scheduling**->**Options** menu consists of the following fields:

Fields in the Scheduling Options menu

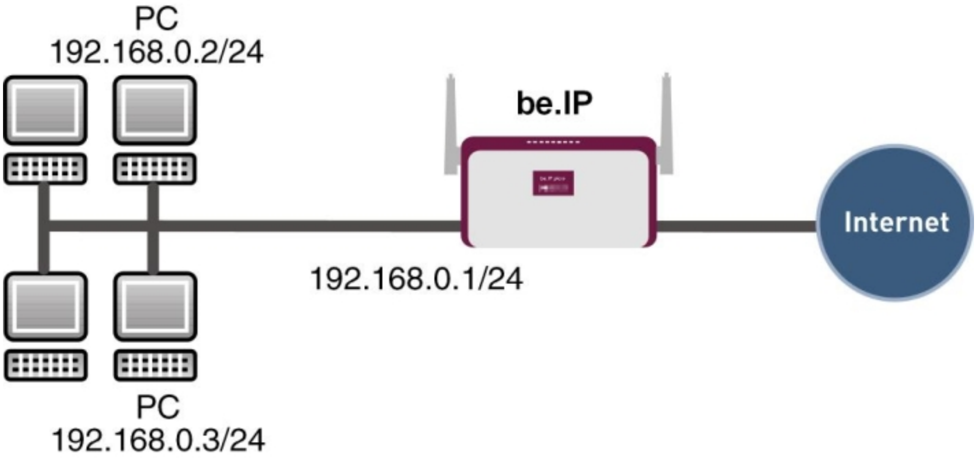
Field	Description
Schedule Interval	Select whether the schedule interval is to be enabled. Enter the interval in seconds after which the system checks whether events have occured. Possible values are *0* to *65535*. The value *300* is recommended (5 minute accuracy).

17.5.4 Configuration example - Time-controlled Tasks (Scheduling)

Requirements

- Basic configuration of the gateway.

Example scenario



Example scenario Time-controlled Tasks

Configuration target

- You want to reboot your gateway automatically overnight.
- The WLAN interface is to be suspended at the weekend.
- In addition, the configuration is to be backed up automatically once a month on a TFTP server.

Overview of Configuration Steps

Daily reboot

Field	Menu	Value
Event List	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	*New*
Description	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	e.g. *Trigger Reboot*
Event Type	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	*Time*
Time Condition	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Condition Type = *Periods*, Condition Settings = *Daily*
Start Time	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Hour *02* Minute *00*
Description	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *Reboot the devicet*

Field	Menu	Value
Command Type	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Reboot*
Event List	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Trigger Reboot*
Event List Condition	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*All*
Reboot device after	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *60* Seconds
Schedule Interval	**Local Services** -> **Scheduling** -> **Options**	*Enabled*, *55* sec

Suspending the WLAN interface

Field	Menu	Value
Event List	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	*New*
Description	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	e.g. *Trigger switch off WLAN interface*
Event Type	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	*Time*
Time Condition	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Condition Type = *Periods*, Condition Settings = *Saturday - Sunday*
Start Time	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Hour *00* Minute *00*
Stop Time	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Hour *23* Minute *59*
Description	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *Switch off WLAN interface*
Command Type	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Interface Status*
Event List	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Trigger switch off WLAN interface*
Event List Condition	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*All*
Interface	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *vss1-0*
Set interface status	**Local Services** -> **Scheduling** ->	*Down*

Field	Menu	Value
	Actions -> **New**	
Schedule Interval	**Local Services** -> **Scheduling** -> **Options**	*Enabled*, *55* sec

Monthly configuration backup

Field	Menu	Value
Event List	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	*New*
Description	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	e.g. *Trigger configuration backup*
Event Type	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	*Time*
Time Condition	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Condition Type = *Day of Month*, Condition Settings = *1*
Start Time	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Hour *03* Minute *00*
Description	**Local Services** -> **Scheduling** -> **Actions** -> **New**	Configuration backup
Command Type	**Local Services** -> **Scheduling** -> **Actions** -> **New**	Configuration Management
Event List	**Local Services** -> **Scheduling** -> **Actions** -> **New**	Trigger configuration backup
Event List Condition	**Local Services** -> **Scheduling** -> **Actions** -> **New**	All
Action	**Local Services** -> **Scheduling** -> **Actions** -> **New**	Export configuration
Server URL	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *tftp://192.168.2.5*
CSV File Format	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Enabled*
Remote File Name	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *monthly-backup.cf*
File Name in Flash	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*boot*
Configuration contains certificates/keys	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Enabled*

Field	Menu	Value
Schedule Interval	**Local Services -> Scheduling -> Options**	*Enabled*, *55* sec

17.6 Wake-On-LAN

With the function **Wake-On-LAN** you can start network devices that are switched off via an integrated network card. The network card also needs a power supply, even when the computer is switched off. You can use filters and rule chains to define the conditions that need to be met to send the so-called magic packet, and select the interfaces that are to be monitored for the defined rule chains. Configuring the filters and rule chains is largely like configuring filters and rule chains in the menu **Access Rules**.

17.6.1 Wake-On-LAN Filter

The menu **Local Services**->**Wake-On-LAN**->**Wake-On-LAN Filter** displays a list of all the WOL filters that have been configured.

17.6.1.1 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*

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

Field	Description
	• *Any* (default value): The destination IP address/length are not specified. • *Host*: Enter the destination IP address of the host. • *Network*: Enter the destination network address and the 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*.

17.6.2 WOL Rules

The menu **Local Services**->**Wake-On-LAN**->**WOL Rules** displays a list of all the WOL rules that have been configured.

17.6.2.1 Edit or New

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

The **Local Services**->**Wake-On-LAN**->**WOL Rules**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Wake-On-LAN Rule Chain	Select whether to create a new rule chain or to edit an existing one. Possible values: • *New* (default value): You can create a new rule chain with this setting. • *<Name of the rule chain>*: Shows a rule chain that has already been created, which you can select and edit.
Description	Only where **Wake-On-LAN Rule Chain** = *New* Enter the name of the rule chain.
Wake-On-LAN Filter	Select a WOL filter. If the rule chain is new, select the filter to be set at the first point of the rule chain. If the rule chain already exists, select the filter to be attached to the rule chain. To select a filter, at least one filter must be configured in the **Local Services**->**Wake-On-LAN**->**WOL Rules** menu.
Action	Define the action to be taken for a filtered data packet. Possible values: • *Invoke WOL if filter matches*: Run WOL if the filter matches. • *Invoke if filter does not match*: Run WOL if the filter does not match.

Field	Description
	• *Deny WOL if filter matches*: Do not run WOL if the filter matches. • *Deny WOL if filter does not match*: Do not run WOL if the filter does not match. • *Ignore rule and skip to next rule*: This rule is ignored and the next one in the chain is examined.
Type	Select whether the Wake on LAN magic packet is to be sent as a UDP packet or as an Ethernet frame via the interface specified in **Send WOL packet over Interface**.
Send WOL packet over Interface	Select the interface which is to be used to send the Wake on LAN magic packet.
Target MAC-Address	Only where **Action** = *Invoke WOL if filter matches* and *Invoke if filter does not match* Enter the MAC address of the network device that is to be enabled using WOL.
Password	Only where **Action** = *Invoke WOL if filter matches* and *Invoke if filter does not match* If the network device that is to be enabled supports the "SecureOn" function, enter the corresponding password for this device here. The device is only enabled if the MAC address and password are correct.

17.6.3 Interface Assignment

In this menu, the configured rule chains are assigned to individual interfaces which are then monitored for these rule chains.

A list of all configured interface assignments is displayed in the **Local Services**->**Wake-On-LAN**->**Interface Assignment** menu.

17.6.3.1 Edit or New

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

The **Local Services**->**Wake-On-LAN**->**Interface Assignment**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Select the interface for which a configured rule chain is to be assigned.
Rule Chain	Select a rule chain.

17.7 Trace Interface

The menu **Trace Interface** allows recording the data traffic of a specific interface and allows you to save the recording as a PCAP file once the process has been stopped.

17.7.1 Trace Interface

Fields in the Trace Settings menu

Field	Description
Interface Selection	Select the interface the data traffic of which is to be recorded.
Trace Mode	Here you can choose the layers on which the data traffic of the selected interface is to be recorded. Available choices are: • *Layer 2* • *PPP* • *Layer 3* • *IP*

As soon as you start the recording with the **START** button, a window informs you about the recording. During recording you can leave the menu and use the GUI as usual. Once you stop the recording with the **STOP** button, information on the created file is displayed and you can either delete ot save it as a PCAP file.

17.7.2 Trace VoIP/SIP

The menu **Trace VoIP/SIP** allows you to capture VoIP/SIP messages at various levels and save them to a text file on your computer. You can choose from the following capture levels, a description what information is written to the file is provided depending on your selection:

- State information: The device writes the current state of the VoIP/SIP subsystem to a file you can then download.

- Events: The device continuously writes VoIP/SIP information to the capture buffer as soon as you click the Start button. Once you click the Stop button, you are presented with the download option.
- SIP: The device continuously writes all SIP messages (only) to the capture buffer as soon as you click the Start button. Once you click the Stop button, you are presented with the download option.

Chapter 18 Maintenance

This menu provides you with numerous functions for maintaining your device. It firstly provides a menu for testing availability within the network. You can manage your system configuration files. If more recent system software is available, you can use this menu to install it. If you require additional languages for the configuration interface, or wish to use a voicemail system, you can import the corresponding files. You can also trigger a system reboot in this menu.

18.1 Log out Users

It can happen that an incompletely terminated configuration session affects functions of the configuration interface. In this case, all active configurations can be checked and - if applicable - terminated.

18.1.1 Log out Users

In this menu, you are presented with a list of all active configuration sessions.

Fields in the manu Log out Users

Field	Description
Class	Dislays the class the signed-on user belongs to.
User	Displays the user name.
Remote IP Address	Displays the IP address from which the connection has been established. This may be the address ofa PC, but it may also be the address of an intermediate router.
Expires	Displays when the connection will be automatically terminated by the device.
Log out immediately	If you activate the check box, this user will be disconnected from the system when you click **Logout**.

18.1.1.1 Logout Options

After you have confirmed your selection of connections to be terminated with **Logout** you can choose if any configuration related to the connections is to be saved before the user is actually disconnected, and in which way.

18.2 Diagnostics

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

18.2.1 Ping Test

You can use the ping test to check whether a certain host in the LAN or an internet address can be reached.

Fields in the Ping Test menu

Field	Description
Test Ping Mode	Select the IP version to be used for the ping test. Possible values: • *IPv4* • *IPv6*
Test Ping Address	Enter the IP address to be tested.
Use Interface	Only for **Test Ping Mode** = *IPv6* For link local addresses select the interface to be used for the ping test. *Default* can be used for global addresses.

Pressing the **Go** button starts the ping test. The **Output** field displays the ping test messages.

18.2.2 DNS Test

The DNS test is used to check whether the domain name of a particular host is correctly resolved. The **Output** field displays the DSN test messages. The ping test is launched by entering the domain name to be tested in **DNS Address** and clicking the **Go** button.

18.2.3 Traceroute Test

You use the traceroute test to display the route to a particular address (IP address or domain name), if this can be reached.

Fielder in the Traceroute Test menu

Field	Description
Traceroute Mode	Select the IP version to be used for the Traceroute test. Possible values: • *IPv4* • *IPv6*
Traceroute Address	Enter the IP address to be tested.

Pressing the **Go** button starts the Traceroute test. The **Output** field displays the traceroute test messages.

18.3 Software &Configuration

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

18.3.1 Options

Your device contains the version of the system software available at the time of production. More recent versions may have since been released. You may therefore need to carry out a software update.

Every new system software includes new features, better performance and any necessary bugfixes from the previous version. You can find the current system software at *www.bintec-elmeg.com* . The current documentation is also available here.

⚠ **Important**

If you want to update your software, make sure you consider the corresponding release notes. These describe the changes implemented in the new system software.

The result of an interrupted update (e.g. power failure during the update) could be that your gateway no longer boots. Do not turn your device off during the update.

An update of BOOTmonitor and/or Logic is recommended in a few cases. In this case, the release notes refer expressly to this fact. Only update BOOTmonitor or Logic if bintec elmeg GmbH explicitly recommends this.

Flash

Your device saves its configuration in configuration files in the flash EEPROM (Electrically Erasable Programmable Read Only Memory). The data even remains stored in the flash when your device is switched off.

RAM

The current configuration and all changes you set on your device during operation are stored in the working memory (RAM). The contents of the RAM are lost if the device is switched off. So if you modify your configuration and want to keep these changes for the next time you start your device, you must save the modified configuration in the flash memory before switching off: The **Save configuration** button over the navigation area of the **GUI**. This configuration is then saved in the flash in a file with the name `boot`. When you start your device, the `boot` configuration file is used by default.

Actions

The files in the flash memory can be copied, moved, erased and newly created. It is also possible to transfer configuration files between your device and a host via HTTP.

Configuration file format

The file format of the configuration file allows encryption and ensures compatibility when restoring the configuration on the gateway in various system software versions. This is a CSV format, which can be read and modified easily. In addition, you can view the corresponding file clearly using Microsoft Excel for example. The administrator can store encrypted backup files for the configuration. When the configuration is sent by e-mail (e.g for support purposes) confidential configuration data can be protected fully if required. You can save or import files with the actions "Export configuration", "Export configuration with status information" and "Load configuration". If you want to save a configuration file with the action "Export configuration" or "Export configuration with status information", you can choose whether the configuration file is saved encrypted or without encryption.

⚠ **Caution**

If you have saved a configuration file in an old format via the SNMP shell with the `put` command, there is no guarantee that it can be reloaded to the device. As a result, the old format is no longer recommended.

The **Maintenance**->**Software &Configuration** ->**Options** menu consists of the following fields:

Fields in the Currently Installed Software menu.

Field	Description
BOSS	Shows the current software version loaded on your device.
System Logic	Shows the current system logic loaded on your device.
xDSL Logic	Shows the current version of the xDSL logic loaded on your device.

Fields in the Software and Configuration Options menu.

Field	Description
Action	Select the action you wish to execute. After each task, a window is displayed showing the other steps that are required. Possible values: • `No Action` (default value): • `Export configuration`: The configuration file **Current File Name in Flash** is transferred to your local host. If you click the **Go** button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name. • `Import configuration`: Under **Filename** select a configuration file you want to import. Please note: Click **Go** to first load the file under the name `boot` in the flash memory for the device. You must restart the device to enable it. Please note: The files to be imported must be in CSV format! • `Copy configuration`: The configuration file in the **Source File Name** field is saved as **Destination File Name**. • `Delete configuration`: The configuration in the **Select file** field is deleted. • `Rename configuration`: The configuration file in the **Select file** field is renamed to **New File Name**. • `Restore backup configuration`: Only if, under **Save configuration** with the setting `Save configuration and back up previous boot configuration` the current configuration was saved as boot configuration and the previous boot configuration was also archived.

Field	Description
	You can load back the archived boot configuration. • *Delete software/firmware*: The file in the **Select file** field is deleted. • *Import language*: You can import additional language versions of the **GUI** into your device. You can download the files to your PC from the download area at *www.bintec-elmeg.com* and from there import them to your device • *Update system software*: You can launch an update of the system software, the xDSL logic and the BOOTmonitor. • *Export configuration with state information*: The active configuration from the RAM is transferred to your local host. If you click the **Go** button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name. The following options require that an MMC/SD card is inserted (if supported by your device) or that your device is equipped with an additional internal storage. • *Import Voice Mail Wave Files*: In **file name**, select the *vms_wavfiles.zip* file that you wish to import. • *Import Additional Files (to usb storage)*: You can upload additional files to the USB memory. Choose which file to load under **File Name** • *Format MMC/SD Card*: Occasionally, the additional internal Flash memory has to be formatted. All stored data are deleted.
Current File Name in Flash	For **Action** = *Export configuration* Select the configuration file to be exported.
Include certificates and keys	For **Action** = *Export configuration*, *Export configuration with state information* Define whether the selected **Action** should also be applied for certificates and keys. The function is activated by selecting *Enabled*. The function is enabled by default.

Field	Description
Configuration Encryption	Only for **Action** = *Import configuration*, *Export configuration*, *Export configuration with state information*. Define whether the data of the selected **Action** are to be encrypted. The function is activated by selecting *Enabled*. The function is disabled by default. If the function is enabled, you can enter the **Password** in the text field.
Filename	Only for **Action** = *Import configuration*, *Import language Update system software*. Enter the path and name of the file or select the file with **Browse...** via the explorer/finder.
Source File Name	Only for **Action** = *Copy configuration* Select the source file to be copied.
Destination File Name	Only for **Action** = *Copy configuration* Enter the name of the copy.
Select file	Only for **Action** = *Rename configuration*, *Delete configuration* or *Delete software/firmware* Select the file or configuration to be renamed or deleted.
New File Name	Only for **Action** = *Rename configuration* Enter the new name of the configuration file.
Source Location	Only for **Action** = *Update system software* Select the source of the update. Possible values: • *Local File* (default value): The system software file is stored locally on your PC. • *HTTP Server*: The file is stored on a remote server specified in the **URL**.

Field	Description
	• *Current Software from Update Server*: The file is on the official update server.
URL	Only for **Source Location** = *HTTP Server* Enter the URL of the update server from which the system software file is loaded.

In the **Advanced Settings** menu, the version of the currently installed system flash files will be displayed.

18.4 Update System Phones

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

Note

Before beginning with the software update of your system telephone, you must load the software in the **Maintenance**->**Update System Phones**->**Firmware Files** menu on your SD card (if supported by you device) or in your system.

18.4.1 elmeg System Phones

In the **Maintenance**->**Update System Phones**->**elmeg System Phones** menu, you will see a list of the connected elmeg system telephones. You can select telephones for immediate updating of the software, or you can have the software updated on a scheduled basis.

In the case of immediate updating, there is no version control.

With time-controlled updating, a check is performed to determine whether a newer version of the system software is saved on the SD card or in your system than on the telephone. It's only in that case that an update takes place. The **Update by time** setting remains after the update has been received, i.e. within the configured period a daily check is performed to determine whether a newer version of the system software is available on the SD card or in your system.

Values in the list elmeg System Phones

Field	Description
Description	Displays the description entered for the system telephone.
Phone Type	Displays the system telephone type.
Serial Number	Displays the system telephone serial number.
Systel Version	Displays the system telephone software version.
Internal Storage Vers.	Displays the inserted SD card version (if supported by you device) or the version stored in internal storage.
Status/Update Status	Displays the system telephone status, or a progress bar during the update progress. ✔ identifies a connected system telephone whose system software is supported by your PABX. ✖ identifies a system telephone that is either not connected, or whose system software is not supported by your PABX. ⏰ identifies an update currently not performed because the maximum number of possible simultaneous updating processes is momentarily exceeded. As soon as another updating process is complete, the telephone is updated in the ⏰ status. For IP telephone, there is no restriction on simultaneous updating of system software. With ISDN telephones, the number of simultaneous updates is dependent on system upgrades. Per digital module, two telephones can be simultaneously updated. If the system telephone system software is not supported by your PABX, there is still a way to update the system software. During system software updating, you see a progress bar.
Update by time	Displays whether, at a certain point, the system telephone software should be updated. This function is enabled on an individual device by setting a checkmark. The function is disabled by default. You can use the **Select all** and **Deselect all** buttons for all the

Field	Description
	devices displayed.
Update immediately	Displays whether the system telephone software should be updated immediately. This function is enabled on an individual device by setting a checkmark. The function is disabled by default. You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

18.4.2 elmeg OEM

In the **Maintenance**->**Update System Phones**->**elmeg OEM** menu, you will see a list of the connected elmeg OEM telephones or base stations. This view displays both elmeg IP1x telephones and elmeg DECT base stations, if there are any. You can select devices to have their software updated immediately or allow them to download completely new software from the system.

In the case of immediate updating, there is no version control.

Note

Note that immediate software updates for DECT multi-cell systems are only available via the system's web configurator and that they cannot be initiated by the PABX GUI.

Values in the list Update from internal Server

Field	Description
Description	Displays the description entered for the system telephone.
Phone Type	Displays the system telephone type.
MAC Address	Shows the system telephone's MAC address.
Phone Version	Displays the software version of the telephone.
Internal Storage Vers.	Displays the inserted SD card version (if supported by you device) or the version stored in internal storage .
Status/Update Status	Displays the system telephone status, or a progress bar during

Field	Description
	the update progress. ✔ identifies a connected system telephone whose system software is supported by your PABX. ⊗ identifies a system telephone that is either not connected, or whose system software is not supported by your PABX. For IP telephone, there is no restriction on simultaneous updating of system software. If the system telephone system software is not supported by your PABX, there is still a way to update the system software. During system software updating, you see a progress bar.
Update enabled	Shows whether connected telephones can independently download new software from the system. You can select individual entries using the checkbox in the corresponding line, or select them all using the **Select all** button or the **Deselect all** button.
Update by time	Displays whether, at a certain point, the system telephone software should be updated. This function is enabled on an individual device by setting a checkmark. The function is disabled by default. You can use the **Select all** and **Deselect all** buttons for all the devices displayed.
Update immediately	Displays whether the system telephone software should be updated immediately. This function is enabled on an individual device by setting a checkmark. The function is disabled by default. You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

Values in the list Update from external Server

Field	Description
Automatic Update from external Server	Enable or disable the automatic update from external server function. The function is enabled with *`Enabled`*. The function is enabled by default.
Description	Displays the description entered for the system telephone.
Phone Type	Displays the system telephone type.
MAC Address	Shows the system telephone's MAC address.
Phone Version	Displays the software version of the telephone.
Status	Displays the system telephone status, or a progress bar during the update progress. ✓ identifies a connected system telephone whose system software is supported by your PABX. ⊗ identifies a system telephone that is either not connected, or whose system software is not supported by your PABX.
Update immediately	Displays whether the system telephone software should be updated immediately. This function is enabled on an individual device by setting a checkmark. The function is disabled by default. You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

18.4.3 Firmware Files

In the **Maintenance**->**Update System Phones**->**Firmware Files** menu, you see the system software files that are currently available on your SD card (if supported by you device) or into the internal storage. You can load additional files on the SD card or into the internal storage.

Note

You will find current system software files in the download area, at *www.bintec-elmeg.com* .

For DECT systems there is a ZIP file available which contains the system software files and, for **elmeg DECT150**, language files too.

Note

One version of the system software file per telephone type can be saved on the SD card or into the internal storage.

Values in the list Firmware Files

Field	Description
Load firmware	Save the system software files on your SD card (if supported by you device) or into the internal storage.
No.	Displays the serial number of the system software file.
Phone Type	Displays the system telephone type.
Version	Displays the version of the system software.
Status	✓ indicates that a system software file is saved in the correct directory.

18.4.4 Settings

In the **Maintenance**->**Update System Phones**->**Settings** menu, you can set a period for the time-dependent updating of the system software. You can save a telephone number that may be used in case a system software update has failed. You can dial this number with the telephone in order to update the system software once the telephone is in boot mode following a failed update.

The **Maintenance**->**Update System Phones**->**Settings** menu consists of the following fields:

Fields in the menu Time Settings for System Phone Firmware Update

Field	Description
Internal Number	For ISDN system telephones only Enter the number of the PABX update server that you wish to call from the telephone if the system software update fails. In this case, you can perform the update from the telephone. This number is automatically sent to the system telephone when the telephone logs into the PABX. When it has been sent, the number is displayed on the telephone under **Menu**->**Service**->**Software Update**. If you press the **OK** button, the number is available in redial.
Firmware Update	Set a period for updating the system software. To do this, select the **Start Time** and the **Stop Time**.
ISDN Remote Access	Select whether a ISDN remote access shall be permitted on your system. The function is enabled with *Enabled* The function is disabled by default.

18.5 Reboot

18.5.1 System Reboot

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

Pay attention to the LEDs on your device. For information on the meaning of the LEDs, see the **Technical Data** chapter of the manual.

Note

Before a reboot, make sure you confirm your configuration changes by clicking the **Save configuration** button, so that these are not lost when you reboot.

If you wish to restart your device, click the **OK** button. The device will reboot.

18.6 Factory Reset

In the menu **Maintenance**->**Factory Reset**, you can reset your device to the ex works state without having to have physical access to it.

Chapter 19 External Reporting

In this system menu, you define what system protocol messages are saved on which computers, and whether the system administrator should receive an e-mail for certain events. Information on IP data traffic can also be saved--depending on the individual interfaces. In addition, SNMP traps can be sent to specific hosts in case of error.

19.1 Syslog

Events in various subsystems of your device (e.g. PPP) are logged in the form of syslog messages (system logging messages). The number of messages visible depends on the level set (eight steps from *Emergency* over *Information* to *Debug*).

In addition to the data logged internally on your device, all information can and should be transmitted to one or more external PCs for storage and processing, e.g. to the system administrator's PC. The syslog messages saved internally on your device are lost when you reboot.

Warning

Make sure you only pass syslog messages to a safe computer. Check the data regularly and ensure that there is always enough spare capacity available on the hard disk of your PC.

Syslog Daemon

All Unix operating systems support the recording of syslog messages. For Windows PCs, the Syslog Demon included in the **DIME Tools** can record the data and distribute to various files depending on the contents (can be called in the download area at *www.bintec-elmeg.com*).

19.1.1 Syslog Servers

Configure your device as a syslog server so that defined system messages can be sent to suitable hosts in the LAN.

In this menu, you define which messages are sent to which hosts and with which conditions.

A list of all configured system log servers displayed in the **External Reporting**->**Syslog**->**Syslog Servers** menu.

19.1.1.1 New

Select the **New** button to set up additional syslog servers.

The menu **External Reporting**->**Syslog**->**Syslog Servers**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
IP Address	Enter the IP address of the host to which syslog messages are passed.
Level	Select the priority of the syslog messages that are to be sent to the host. Possible values: • *Emergency* (highest priority) • *Alert* • *Critical* • *Error* • *Warning* • *Notice* • *Information* (default value) • *Debug* (lowest priority) Syslog messages are only sent to the host if they have a higher or identical priority to that indicated, i.e. at syslog level *Debug* all messages generated are forwarded to the host.
Facility	Enter the syslog facility on the host. This is only required if the **Log Host** is a Unix computer. Possible values: *local0 - 7* . The default value is *local0*.

Field	Description
Timestamp	Select the format of the time stamp in the syslog. Possible values: • *None* (default value): No system time indicated. • *Time*: System time without date. • *Date &Time*: System time with date.
Protocol	Select the protocol for the transfer of syslog messages. Note that the syslog server must support the protocol. Possible values: • *UDP* (default value) • *TCP*
Type of Messages	Select the message type. Possible values: • *System &Accounting* (default value) • *System* • *Accounting*

19.2 IP Accounting

In modern networks, information about the type and number of data packets sent and received over the network connections is often collected for commercial reasons. This information is extremely important for Internet Service Providers that bill their customers by data volume.

However, there are also non-commercial reasons for detailed network accounting. If, for example, you manage a server that provides different kinds of network services, it is useful for you to know how much data is generated by the individual services.

Your device contains the IP Accounting function, which enables you to collect a lot of useful information about the IP network traffic (each individual IP session).

19.2.1 Interfaces

In this menu, you can configure the IP Accounting function individually for each interface.

In the **External Reporting**->**IP Accounting**->**Interfaces** menu, a list of all interfaces configured on your device is shown. For each entry, you can activate IP Accounting by setting the checkmark. In the **IP Accounting** column, you do not need to click each entry individually. Using the options **Select all** or **Deselect all** you can enable or disable the IP accounting function for all interfaces simultaneously.

19.2.2 Options

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

In the **External Reporting**->**IP Accounting**->**Options** menu, you can define the **Log Format** of the IP accounting messages. The messages can contain character strings in any order, sequences separated by a slash, e.g. *\t* or *\n* or defined tags.

Possible format tags:

Format tags for IP Accounting messages

Field	Description
%d	Date of the session start in the format DD.MM.YY
%t	Time of the session start in the format HH:MM:SS
%a	Duration of the session in seconds
%c	Protocol
%i	Source IP Address
%r	Source Port
%f	Source interface index
%I	Destination IP Address
%R	Destination Port
%F	Destination interface index
%p	Packets sent
%o	Octets sent
%P	Packets received
%O	Octets received
%s	Serial number for accounting message
%%	%

By default, the following format instructions are entered in the **Log Format** field: *INET: %d%t%a%c%i:%r/%f -> %I:%R/%F%p%o%P%O[%s]*

19.3 Alert Service

It was previously possible to send syslog messages from the router to any syslog host. Depending on the configuration, e-mail alerts are sent to the administrator as soon as relevant syslog messages appear.

19.3.1 Alert Recipient

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

19.3.1.1 New

Select the **New** to create additional alert recipients.

The menu **External Reporting**->**Alert Service**->**Alert Recipient**->**New** consists of the following fields:

Fields in the Add / Edit Alert Recipient menu.

Field	Description
Alert Service	Displays the alert service. You can select an alert service for devices with UMTS. Possible values: • E-mail • SMS
Recipient	Enter the recipient's e-mail address. The entry is limited to 40 characters.
Message Compression	Select whether the text in the alert E-mail is to be shortened. The e-mail then contains the syslog message only once plus the number of relevant events. Enable or disable the field. The function is enabled by default.
Subject	You can enter a subject.
Event	This feature is available only for devices with Wireless LAN Controller.

Field	Description
	Select the event to trigger an email notification. Possible values: • *Syslog contains string* (default value): A Syslog message includes a specific string. • *New Neighbor AP found*: A new adjacent AP has been found. • *New Rogue AP found*: A new Rogue AP has been found, i.e. an AP using an SSID of its own network, yet is not a component of this network. • *New Slave AP (WTP) found*: A new unconfigured AP has reported to the WLAN. • *Managed AP offline*: A managed AP is no longer accessible.
Matching String	You must enter a "Matching String". This must occur in a syslog message as a necessary condition for triggering an alert. The entry is limited to 55 characters. Bear in mind that without the use of wildcards (e.g. "*"), only those strings that correspond exactly to the entry fulfil the condition. The "Matching String" entered therefore usually contains wildcards. To be informed of all syslog messages of the selected level, just enter "*".
Severity	Select the severity level which the string configured in the **Matching String** field must reach to trigger an e-mail alert. Possible values: *Emergency* (default value), *Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Information*, *Debug*
Monitored Subsystems	Select the subsystems to be monitored. Add new subsystems with **Add**.
Message Timeout	Enter how long the router must wait after a relevant event before it is forced to send the alert mail. Possible values are *0* to *86400*. The value *0* disables the timeout. The default value is *60*.

Field	Description
Number of Messages	Enter the number of syslog messages that must be reached before an E-mail can be sent for this case. If timeout is configured, the mail is sent when this expires, even if the number of messages has not been reached. Possible values are *0* to *99*; the default value is *1*.

19.3.2 Alert Settings

The menu **External Reporting**->**Alert Service**->**Alert Settings** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Alert Service	Select whether the alert service is to be enabled for the interface. The function is enabled with *Enabled*. The function is enabled by default.
Maximum E-mails per Minute	Limit the number of outgoing mails per minute. Possible values are *1* to *15*, the default value is *6*.

Fields in the E-mail Parameters menu.

Field	Description
Sender E-mail Address	Enter the mail address to be entered in the sender field of the E-mail.
SMTP Server	Enter the address (IP address or valid DNS name) of the mail server to be used for sending the mails. The entry is limited to 40 characters.
SMTP Port	Encryption of e-mails (SSL / TLS). The field **SMTP Port** is per default preset to *25* and **SSL** Encryption is enabled.
SMTP Authentication	Authentication expected by the SMTP server.

Field	Description
	Possible values: • *None* (default value): The server accepts and send emails without further authentication. • *ESMTP*: The server only accepts e-mails if the router logs in with the correct user name and password. • *SMTP after POP*: The server requires that e-mails are called via POP3 by the sending IP with the correct POP3 user name and password before sending an e-mail.
User Name	Only if **SMTP Authentication** = *ESMTP* or *SMTP after POP* Enter the user name for the POP3 or SMTP server.
Password	Only if **SMTP Authentication** = *ESMTP* or *SMTP after POP* Enter the password of this user.
POP3 Server	Only if **SMTP Authentication** = *SMTP after POP* Enter the address of the server from which the e-mails are to be retrieved.
POP3 Timeout	Only if **SMTP Authentication** = *SMTP after POP* Enter how long the router must wait after the POP3 call before it is forced to send the alert mail. The default value is *600* seconds.

Fields in the SMS Parameters menu (for devices with UMTS only)

Field	Description
SMS Device	You can receive notification of system alerts in text messages. Select the device to be used to send the text message.
Maximum SMS per Day	Limit the maximum number of SMS sent during a single day. Activating *No Limitation* allows any number of SMS to be sent. The defualt value is 10 SMS per day. Note: Entering a value of *0* is equivalent to activating *No Limitation*.

19.4 SNMP

SNMP (Simple Network Management Protocol) is a protocol from the IP protocol family for transporting management information about network components.

Every SNMP management system contains an MIB. SNMP can be used to configure, control and administrate various network components from one system. Such an SNMP tool is included on your device: the Configuration Manager. As SNMP is a standard protocol, you can use any other SNMP managers, e.g. HPOpenView.

For more information on the SNMP versions, see the relevant RFCs and drafts:

- SNMP V. 1: RFC 1157
- SNMP V. 2c: RFC 1901 - 1908
- SNMP V. 3: RFC 3410 - 3418

19.4.1 SNMP Trap Options

In the event of errors, a message - known as a trap packet - is sent unrequested to monitor the system.

In the **External Reporting**->**SNMP**->**SNMP Trap Options** menu, you can configure the sending of traps.

The menu **External Reporting**->**SNMP**->**SNMP Trap Options** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
SNMP Trap Broadcasting	Select whether the transfer of SNMP traps is to be activated. Your device then sends SNMP traps to the LAN's broadcast address. The function is activated by selecting `Enabled`. The function is disabled by default.
SNMP Trap UDP Port	Only if **SNMP Trap Broadcasting** is enabled. Enter the number of the UDP port to which your device is to send SNMP traps.

Field	Description
	Any whole number is possible. The default value is *162*.
SNMP Trap Community	Only if **SNMP Trap Broadcasting** is enabled. Enter a new SNMP code. This must be sent by the SNMP Manager with every SNMP request so that this is accepted by your device. A character string of between *0* and *255* characters is possible. The default value is *SNMP Trap*.

19.4.2 SNMP Trap Hosts

In this menu, you specify the IP addresses to which your device is to send the SNMP traps.

In the **External Reporting**->**SNMP**->**SNMP Trap Hosts** menu, a list of all configured SNMP trap hosts is displayed.

19.4.2.1 New

Select the **New** button to create additional SNMP trap hosts.

The menu **External Reporting**->**SNMP**->**SNMP Trap Hosts**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
IP Address	Enter the IP address of the SNMP trap host.

19.5 SIA

19.5.1 SIA

In the menu **External Reporting**->**SIA**->**SIA**, you can create and download a file that provides extensive support information about the status of your device like, e.g., the current configuration, available memory, uptime etc.

Chapter 20 Monitoring

This menu contains information that enables you to locate problems in your network and to monitor activities, e.g. at your system's interfaces, users, teams, internal protocols and Ethernet connections.

20.1 Status Information

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

20.1.1 Users

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

20.1.1.1 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. If a voicemail system is active, `Voice Mail System` is displayed.
Current Class of Service	Displays the all of the authorisation classes assigned to the user. The currently enabled authorisation class is marked appropriately with a green arrow (✔).
Terminal	Displays the interface assigned to this subscriber.
Charges	Displays calculated charges for accrued connection units.
Status	Displays the status of the interface to which the subscriber is connected.

Values in the System Settings list

Field	Description
Parallel Ringing	Displays whether parallel call is set up for the user.
Call Forwarding	Displays current call forwarding for this user.
Do not Disturb	Displays whether call waiting protection is set up for the user. (Only for system telephones)
Call Waiting	Displays whether call waiting is allowed for internal and/or external calls.
Direct Call	Displays whether direct call on receiver pickup is configured for the user.
Room Monitoring	Displays whether room monitoring is enabled for the user.
Receive Announcement Calls	Displays whether the announcement is allowed for the user.
Receive Intercom Calls	Displays whether simplex operation is allowed for the user.
Automatic Call Pick-up	Displays whether automatic call acceptance is configured for the user.

20.1.2 Teams

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

20.1.2.1 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.

Field	Description
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.
Rerouting on no response	Displays whether redirect on no reply is enabled and, if so, the time period after which it occurs and the destination team.
Further Rerouting	Displays which of the redirect functions are enabled and which subscriber is the redirect destination.

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

Values in the Advanced Settings list

Field	Description
Assigned Users	Displays all logged-in and logged-out subscribers in the team.

20.2 Internal Log

20.2.1 System Messages

In the **Monitoring**->**Internal Log**->**System Messages** menu, a list of all internally stored system messages is displayed. Above the table you will find the configured vales for the **Maximum Number of Syslog Entries** and **Maximum Message Level of Syslog Entries** fields. These values can be changed in the **System Management**->**Global Settings**->**System** menu.

Values in the System Messages list

Field	Description
No.	Displays the serial number of the system message.
Date	Displays the date of the record.
Time	Displays the time of the record.
Level	Displays the hierarchy level of the message.
Subsystem	Displays which subsystem of the device generated the message.
Message	Displays the message text.

20.3 Interfaces

20.3.1 Statistics

In the **Monitoring**->**Interfaces**->**Statistics** menu, current values and activities of all device interfaces are displayed.

With the filter bar, you can select whether to display **Transfer Totals** or **Transfer Throughput**. The values per second are shown on the **Transfer Throughput** display.

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

Values in the Statistics list

Field	Description
No.	Shows the serial number of the interface.
Description	Displays the name of the interface.
Type	Displays the interface text.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Tx Errors	Shows the total number of errors sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.
Rx Errors	Shows the total number of errors received.
Status	Shows the operating status of the selected interface.
Unchanged for	Shows the length of time for which the operating status of the interface has not changed.
Action	Enables you to change the status of the interface as displayed.

Click the 🔍 button to display the statistical data for the individual interfaces in detail.

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.

Field	Description
NAT	Indicates if NAT is activated for this interface.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.

Fields in the TCP Connections menu

Field	Description
Status	Displays the status of an active TCP connection.
Local Address	Displays the local IP address of the interface for an active TCP connection.
Local Port	Displays the local port of the IP address for an active TCP connection.
Remote Address	Displays the IP address to which an active TCP connection exists.
Remote Port	Displays the port to which an active TCP connection exists.

20.3.2 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.

Chapter 21 User Access

The system administrator can set up an individual configuration access interface for the users. You, the user, can thus display your most important personal settings and individually customise some of these.

To log in to the configuration interface with your assigned access data, enter your **User Name** and **Password** in the login window.

After successful login, the **Status** page is displayed. It includes an overview of your most important settings.

In the **Phonebook** menu, you can access the **System Phonebook** and create, edit as well as delete entries in a user-specific telephone book.

In the **Call Data Records** menu, you get a detailed overview of the calls you have conducted and accepted.

The **Settings** menu contains an overview of current settings of performance features **Direct Call**, **Call Forwarding** and **Parallel Ringing**. You can individually customise these here. In addition, you can view general settings and customise access and contact data.

You can also view the settings of the **elmeg System Phones** assigned to you, and modify these to your needs.

In the **Voice Mail System**->**Settings** menu, you'll see the current configuration of your individual voicemail box, as well as the number of messages present. You can modify several frequently used voicemail box parameters here. The **Voice Mail System**->**Messages** menu displays a detailed overview of all received calls.

21.1 Status

The **User Access**->**Status** menu displays the most important settings performed for you by the system administrator.

The **User Access**->**Status** menu consists of the following fields:

Values in the User Data list

Field	Description
Name, First Name	Displays the configured surname and name, if applicable, of your user.

Field	Description
Description	Displays the configured additional description for your user.

Values in the Internal Numbers &Communication Cost list

Field	Description
<Internal Number>	Displays the connection charges for the internal numbers assigned to your user.

Values in the Further Settings list

Field	Description
Current Class of Service	Displays the name of the authorisation class to which your user is assigned.
Dialling Authorization	Displays the dial permission for your telephones. This derives from the setting for the corresponding user class. Possible values: • *International*: The telephones have unrestricted dialling authorisations and can initiate all connections. • *National*: The telephones can initiate all calls except international calls. If a number starts with the code for international dialling, the number cannot be dialled. • *Incoming*: The telephones can receive incoming external calls, but cannot initiate any external calls. Internal calls are possible. • *Region*: The telephones cannot make any national or international calls. For this dial permission, 10 exception numbers allowing national or international dialling can be configured. An exception number can consist of complete call numbers or sections thereof (e. g. the first numerals). • *Local*: The telephones can make local calls. National and international calls are not possible. • *Internal*: The telephones do not have authorisation for incoming or outgoing external calls. Only internal telephone calls are possible.
Allow manual trunk group selection	Indicates whether your user is assigned to an authorisation class for which manual bundle assignment is allowed. If so, authorised bundles or external connections are displayed.

Field	Description
	Besides general exchange access, a telephone can also 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.

21.2 Phonebook

In the **Phonebook** menu, telephone book entries are displayed separately according to **System Phonebook** and **User Phonebook**. In **User Phonebook** the user can create, modify or delete up to 50 own entries. These entries can only be viewed by the respective user. These entries are updated via the **GUI**.

21.2.1 System Phonebook

In the **System Phonebook**, entries of the overall system created by the administrators are displayed You cannot modify these.

Values in the System telephone book list

Field	Description
Description	Displays the subscriber's description. The **System Phonebook** is sorted according to these entries.
Phone Number	Displays the telephone number.
Speed Dial Number	Displays the speed-dial number.

Field	Description
Call Through	Indicates whether the telephone number for the **Call Through** function is activated.

21.2.2 User Phonebook

In the **User Phonebook**, your user entries are displayed. You can add, edit or delete entries.

21.2.2.1 Edit or New

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

The menu **User Access**->**Phonebook**->**User Phonebook**->**New** consists of the following fields:

Fields in the Phonebook Entry menu.

Field	Description
Description	Enter a description for the entry. Sorting in **User Phonebook** follows the initial letters of the entry.
Phone Number	Enter the telephone number (internal or external).

21.3 Call Data Records

The **Call Data Records** menu displays your user's incoming and outgoing connections recorded to date.

21.3.1 Outgoing

The **Call Data Records**->**Outgoing**menu consists of the following fields:

Values in the Outgoing list

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.

Field	Description
Duration	Displays the duration of the connection.
User	Displays the user who called.
Int. No.	Displays the user's internal number.
Called Number	Displays the dialled number.
Project Code	Displays the call project number, if any.
Interface	Displays the interface over which the external connection was routed.
Costs	Displays the connection charge, but only if the provider transmits the corresponding data.

21.3.2 Incoming

The **Call Data Records**->**Incoming** menu consists of the following fields:

Values in the Incoming list

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Duration	Displays the duration of the connection.
User	Displays the user who was called.
Int. No.	Displays the user's internal number.
External Number	Displays the caller's number.
Project Code	Displays the call project number, if any.
Interface	Displays the interface over which the connection from outside was routed.

21.4 Call List

The menu **Applications**->**Call List** lists details of incoming and outgoing calls. Which kind of calls and how many of them are included can be spcified in the submenu **General**.

21.4.1 Incoming

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

The **Applications**->**Call List**->**Incoming** menu consists of the following fields:

Fields in the Incoming menu

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Type	Displays the type of the connection.
Int. No.	Displays the user's internal number.
Caller Number	Displays the caller's number.
Trunk Number	Displays the port number.
Interface	Displays the interface over which the connection from outside was routed.
Delete	You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

21.4.2 Outgoing

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

The **Applications**->**Call List**->**Outgoing** menu consists of the following fields:

Fields in the Outgoing menu

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Type	Displays the type of the connection.
User	Displays the user who was called.
Int. No.	Displays the user's internal number.
Called Number	Displays the caller's number.
Trunk Number	Displays the port number.
Interface	Displays the interface over which the connection from outside was routed.
Delete	You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

21.5 Settings

In the **Settings** menu, you can perform personal settings to performance features direct call, call forwarding (CF), parallel call and do not disturb, as well as customise general settings.

21.5.1 Feature Settings

In the **Settings**->**Feature Settings** menu, the settings for performance features direct call, call forwarding (CF), parallel call and do not disturb can be customised.

21.5.1.1 Call Forwarding

In the **Settings**->**Feature Settings**->**Call Forwarding** menu, you configure forwarding of incoming calls to your internal number onto the entered destination number.

You are temporarily away from your office, but don't want to miss a call. With call forwarding to another number, e.g. your mobile, you can receive your calls even when you are not at your desk. You can forward calls on your number to any call number. It can occur `Imme-`

diately, *On no reply* or *On Busy*. Call forwarding *On no reply* and *On Busy* can exist concurrently. If you are not near your telephone, for example, the call is forwarded to another number (e.g. your mobile phone) after a short period. If you are making a call at your desk, other caller may receive the busy signal. You can forward these callers e.g. to a colleague or the secretary by using call forwarding on busy.

Calls can be forwarded to internal subscriber numbers, internal team numbers or external numbers When the number to which calls shall be forwarded is entered, the system automatically checks whether it's an internal or external number.

To continue with configuring, click the ✎ symbol.

Select the ▤ button to go to the **IP1x0** telephone user interface administrator page. This is described in the telephone user guide!

The **Settings**->**Feature Settings**->**Call Forwarding** menu consists of the following fields:

Fields in the Call Forwarding menu.

Field	Description
Active Function	Select whether to enable the call forwarding (CF) function for your telephone. The function is enabled with *Enabled* The function is disabled by default.
Type	Select when incoming calls shall be forwarded to the specified internal number. Possible values: • *Immediately* • *On Busy* • *On no reply* (default value) • *On busy / On no reply*
Destination on no Reply	Enter the number to which incoming calls shall be forwarded after time.
Destination on Busy	Enter the number to which incoming calls shall be forwarded on busy.
Destination immediately	Enter the number to which incoming calls shall be forwarded immediately.

21.5.1.2 Parallel Ringing

In the **Settings**->**Feature Settings**->**Parallel Ringing** menu, you configure which calls should be signalled to your terminal.

The **Settings**->**Feature Settings**->**Parallel Ringing** menu consists of the following fields:

Fields in the Parallel Ringing menu.

Field	Description
Active Function	Select whether to enable the parallel call function for your telephone. The function is enabled with `Enabled` The function is disabled by default.
External Number	Under `Individual Number` enter the external telephone number to which a call should be signalled in parallel. If a mobile number and a call number are configured for personal use, these are displayed in `Configured Home Number` or `Configured Mobile Number` and can be selected.

21.5.1.3 Direct Call

You wish to install your telephone in such a way that connection to a specific call number is set up even without entry of the number (e. g. emergency phone). You are not at home. However, there is someone at home who needs to be able to reach you quickly and easily by telephone if necessary (e. g. children or grandparents). If you have set up the Direct Call function for your telephone, the telephone receiver only needs to be picked up. After a time period without further entries set in configuration, the system automatically dials the configured direct call number.

If you do not dial within the specified period from picking up the receiver, automatic dialling is initiated.

The **Settings**->**Feature Settings**->**Direct Call** menu consists of the following fields:

Fields in the Direct Call menu.

Field	Description
Active Function	Select whether to enable the direct call function for your telephone.

Field	Description
	The function is enabled with *Enabled* The function is disabled by default.
Number	Select which number to use for direct call. Possible values: • *Preconfigured Number*: Select the desired number for which to set up direct call from the dropdown list. • *Invidual Number*: Enter the desired number for which to set up direct call into the input field.

21.5.1.4 Do not Disturb

You can use the "station guarding" (do not disturb) feature to configure which calls will be signalled to your terminal.

The **Settings**->**Feature Settings**->**Do not Disturb** menu consists of the following fields:

Fields in the menu Do not Disturb

Field	Description
Active Function	Select whether to enable the "station guarding" function for your telephone. The function is enabled with *Enabled*. The function is disabled by default.
Do not Disturb	With the station guarding feature, you can enable call signalling to your terminal. Analogue terminals use system code numbers for this. Select the calls for which you wish to use the feature. Possible values: • *Internal Calls not signaled* • *External Calls not signaled* • *No Calls signaled*

21.5.1.5 Log on / Log off

With system telephones, it is only possible to log out of a team using the **Log on / Log off** function key. The team administrator must run this function manually if standard telephones are used.

The **Settings**->**Feature Settings**->**Log on / Log off** menu consists of the following fields:

Fields in the menu Log on / Log off

Field	Description
Description	Shows which teams the user belongs to.
Status	Select whether the team member shall be logged in or out of the team. The function is activated by selecting `Logged on`. The function is enabled by default.

21.5.2 General Settings

Your user's most important settings are listed in the **Settings**->**General Settings** menu. Personal access data (configuration password, IP phone password) as well as mobile and home office numbers can be customised.

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

Fields in the User Data menu.

Field	Description
Name	Displays your user's name.
Description	Displays the additional description for your user.
Login Name	Displays your user name for login to the user configuration interface.
Password for HTML Configuration Access	If you wish to change your password for access to the user configuration interface, enter a new password here. To check, you can display the password in plain text by clicking the **Show** option.

Field	Description
Password for IP Phone Registration	If you wish to change your password for IP telephone login, enter a new password here. To check, you can display the password in plain text by clicking the **Show** option.
PIN for Phone Access	If you wish to change the PIN for your personal voicebox, enter a new PIN here. To check, you can display the password in plain text by clicking the **Show** option.
Mobile Number	Here, you can enter the mobile number under which you can be reached.
Home Office Number	Here, you can enter the home office number under which you can be reached.
Busy on busy	Indicates whether performance feature Busy on Busy is enabled for the currently selected user. If a subscriber for whom multiple telephone numbers have been configured makes a call, you can decide whether additional calls for this user shall be signalled. If "Busy on Busy" is set for this user, other callers get an **Engaged** signal if the user is calling on one of her numbers. The function is activated by selecting *Enabled*. The function is disabled by default.

Fields in the Status Information menu.

Field	Description
Extension Numbers	Displays the internal numbers assigned to you.
Current Class of Service	Displays the authorisation class to which you're currently assigned.
Dialling Authorization	Displays your dial permission.
Allow manual trunk group selection	Displays whether you're allowed to assign additional bundles to outside lines and, if so, which.
Pick-up Group	Displays the number of the group in which calls may be picked up.

21.6 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.

21.6.1 Assigned elmeg Phones

The **Assigned elmeg Phones**->**Assigned elmeg Phones** menu shows a list with the key information about your telephone. The ▤ symbol takes you to the **IP1x0** phone's configuration interface.

Select the ✎ symbol to reset the phone's user password.

The **Assigned elmeg Phones**->**Assigned elmeg Phones** ✎ menu consists of the following fields:

Fields in the System Phone menu

Field	Description
User password	Select whether the user password should be reset. The function is activated by selecting `Enabled`. The function is disabled by default. As soon as you select the **OK** button, the password is reset to the default setting.

21.7 elmeg System Phones

The menu **elmeg System Phones** displays the system telephones assigned to you by the system administrator.

Note

The **elmeg System Phones** menu is only displayed if you've already been assigned system telephones by the administrator.

21.7.1 Assigned System Phones

The system telephone offers typical system performance features associated with bintec elmeg systems. For example:

- Dialling from the system phone book
- Announcement and simplex operation with other system telephones on the system
- Function keys for control of system performance features (enable call options, login/ logout in teams, line keys, connection keys). The status of defined performance features can be indicated via LED's assigned to individual function keys.

Note

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

21.7.1.1 Settings

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

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

Fields in the menu Basic Settings

Field	Description
Headset Support	Not for **S530** and **S560**. Select whether the headset should automatically accept calls.

Field	Description
	☞ **Note** If you wish to use a headset, you must configure a headset key and a key for automatic call acceptance on your PABX system. On the system telephone, you must select a headset type and enable the key for automatic call acceptance.
Call Waiting	Select whether another call shall be supported for this telephone through call waiting or a display notification. The function is activated by selecting *Enabled*. The function is disabled by default. If **Call Waiting** is enabled, define for which calls you wish to allow call waiting. Possible values: - *Internal Calls* - *External Calls* - *Internal and External Calls* Under **Repeat Call Waiting Signal**, also decide whether the call waiting tone or the display notification should only be signalled once, or repeated.
Do not Disturb	Only for telephones in the **CS4xx** series, the **S530** telephones and **S560** and the **IP-S400** telephone. For the **S530** and **S560** telephones, you merely configure the function here. With these telephones, enable *Do not Disturb* via the function key. Select whether you wish to use the call protection (do not disturb) performance feature. With this performance feature, you can enable call signalling to your terminal. Select for which number you wish to use the station guarding performance feature. Possible values:

Field	Description
	• *First Number only* (**CS4xx** series only): Call protection applies only to the first configured MSN. • *All Numbers* (**CS4xx** series only): Call protection applies to all configured MSN's. Select whether incoming calls shall be signalled: • *Off*: Calls are signalled. • *On* (**CS4xx** series only): Calls are not signalled. • *Acknowledgement Tone only* (**CS4xx** series only): An attention tone is heard once for a call • *Attention tone 1* (only **S530** and **S560**) • *Attention tone 2* (only **S530** and **S560**) • *Attention tone 3* (only **S530** and **S560**) • *Attention tone 4* (only **S530** and **S560**) • *No attention tone* (only **S530** and **S560**)

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

Fields in the menu Advanced Settings

Field	Description
Status LED	Select whether and, if so, which events should be signalled by the system telephone status LED. Possible values: • *Off*: The status LED function is not used. • *Caller List*: The status LED signals calls and new messages. • *Messages only*: The status LED only signals new messages (MWI). • *New Message* (only **S5x0**) • *New Call* (only **S5x0**) • *Active Call* (only **S5x0**) You can use the options *New Message*, *New Call* and *Active Call* individually, or combine them freely.
Directory Softkey	Only for telephones in the **CS4xx** series

Field	Description
	Select whether calls shall be made with the softkey entries from the system phone book (*System*) or from the telephone phone book (*Telephone*).
Conversation Display	Not for **S5x0** Select which information shall be indicated in the system telephone display during a call. Possible values: • *Number and Charge or Duration* • *Number and Charge* • *Number and Duration* • *Number and Time* • *Number only* • *Date and Time only*
Default Signalling during Calls	Select whether DTMF signals or keypad functions shall be transmitted into the system in call status. You can use special functions during a call by entering character and numerical sequences. These entries must be made as keypad or MFV sequences, depending on the function to be used. You can define whether MFV or keypad functions are possible in the basic setting during a call. Possible values: • *DTMF* (default value) • *Keypad*
Automatic Call Pick-up	Select the period after which calls to this system telephone should be automatically accepted without you having to pick up the receiver or press the loudspeaker key. *Please note that to be able to use this function at least one telephone key must be assigned to automatic call acceptance.* Possible values: • *Immediately* • *After 5 seconds*

Field	Description
	• *After 10 seconds* • *After 15 seconds* (only **S5x0**) • *After 20 seconds* (only **S5x0**) • *Off* (only **S5x0**)
Mute after hands-free Calling	Not for **S5x0**, **CS290**, **CS290-U** You can dial the number of a subscriber without picking up the receiver (e. g. hands-free). Here, you have the choice of whether the built-in microphone shall be switched on immediately or only after pressing of the corresponding softkey. If the microphone is turned off during dialling, the corresponding softkey must be pressed, even if the connection is already active. The function is activated by selecting *Enabled*. The function is disabled by default.
Receiving UUS	Select whether performance feature UUS (User to User Signalling) can be used for this telephone. With this performance feature, you can receive short text messages from other telephones. In this way, you can send written information within the system, e. g. *Meeting at 9:30 AM* or *Will be on holiday on Monday*. Possible values: • *Off, UUS are blocked*: The UUS performance feature is not used. • *Internal only*: Text messages can only be received internally. • *External only*: Text messages can only be received externally. • *Internal and External* (default value): Text messages can only be received internally and externally.
Receive System Intercom Call	Select whether the system telephone assigned may accept simplex connections. If the system has more than one number then the settings are only applied to the first MSN. The function is activated by selecting *Enabled*. The function is disabled by default.

Field	Description
Receive Announcement Calls	Select whether the system telephone assigned may receive announcements. If the system has more than one number then the settings are only applied to the first MSN. The function is activated by selecting *Enabled*. The function is disabled by default.

21.7.1.2 Keys / T400 / T400/2 / T500

In the menu **elmeg System Phones**->**Assigned System Phones**->**Keys** configuration of system telephone keys is displayed.

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

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

Values in the list Keys

Field	Description
Key	Displays the name of the key.
Label Description	Displays the text which you have entered for the labelling page. The text contains the configured key name
Key Type	Displays the key type.
Settings	Displays the additional settings with a summary

You can use **Print** to print out a label sheet for the label field on your system telephone or your key extension.

Edit

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

You can use the following functions with system telephones:

- *Dial Key (Standard)*: You can store a call number on every function key.
- *Dial Key (DTMF)*: You can store a MFV sequence on every function key.
- *Dial Key (Keypad sequence)*: You can store a keypad sequence on every function key.
- *Extension Key (User)*: You can set up dialling to an internal extension using a line key. After pressing the corresponding key, hands free is switched on and the internal extension entered is selected. If a call is signalled on the internal extension you have entered, you can pick this up by pressing the line key.
- *Extension Key (Team)*: You can set up dialling to a team using a line key. After pressing the corresponding key, hands-free is activated and the entered team is called according to its enabled call option. If a call is signalled for the entered team, you can pick it up by pressing this connection key.
- *Trunk Line*: An ISDN connection or a VoIP provider is set up under a connection key. If this key is pressed, automatic hands-free is enabled and the corresponding ISDN connection is assigned. You then hear the external dialling tone. If an external call is signalled on another internal telephone, you can pick it up by pressing this line key.
- *Login / Log Out, Team*: If you are entered as a subscriber in the call assignments for one or more teams, you can set up a key so that you can control the call signalling of your telephone. If you're logged in, team calls are signalled to your telephone. If you are logged out, no team calls will be signalled.

  The call numbers entered in the telephone can be logged in/logged out from a team using a set function key (**MSN**-1... **MSN**-9). Before entering a team number, you must select the telephone call number index (MSN) that is entered in the corresponding team call assignments.
- *System Call (Announcement User)*: You can set up a connection to another telephone without this connection having to be actively accepted. As soon as the telephone has accepted the announcement, the connection is established and the announcement key LED is enabled. The announcement can be ended by renewed pressing of the announcement key or by pressing the loudspeaker key. The LED switches off again at conclusion of the announcement.
- *System Call (Announcement Team)*: You can configure an announcement for a team by setting up a function key. The way this works is the same as that described above.
- *System Call (Announcement enable)*: You can also selectively deny or allow announcements using a function key. To use announcements, you must be authorised for the corresponding authorisation class.
- *System Call (Intercom)*: You can set up a key is such a way that a connection to the specified telephone is established without this connection having to be actively accepted.
- *System Call (Intercom enable)*: You can set up a key in such a way that the sim-

plex operation function is allowed or denied. To use simplex operation, the function must be allowed in the corresponding authorisation class.

- *Boss Key* / *Secretary Key*: You can set up a key as a special line key. The Boss telephone and Secretary telephone properties are saved in both telephones with these keys.
- *Diversion Secretary*: You can set up a key in such a way that incoming calls to the Boss telephone are automatically routed to the Secretary telephone.
- *Call Forwarding (CFNR)*: You can set up a key so that delayed call diversion is set up for a specific number (MSN) on your system telephone. Pressing the key when the phone is not in use turns call forwarding on and off. Configuring call forwarding with a programmed key is only possible for numbers 1 to 9 (MSN-1...MSN-9) on the phone. In order to be able to use call forwarding, you need to have set up at least one number.
- *Call Forwarding (CFU)*: You can set up a key so that immediate call diversion is set up for a specific number (MSN) on your system telephone. Pressing the key when the phone is not in use turns call forwarding on and off. Call forwarding configuration over a programmed key is only possible for numbers 1 to 9 (MSN-1...MSN-9) of the phone. In order to be able to use call forwarding, you need to have set up at least one number.
- *Call Forwarding (CFB)*: You can set up a key so that call diversion on engaged is set up for a specific number (MSN) on your system telephone. Pressing the key when the phone is not in use turns call forwarding on and off. Call forwarding configuration over a programmed key is only possible for numbers 1 to 9 (MSN-1...MSN-9) of the phone. In order to be able to use call forwarding, you need to have set up at least one number.
- *Macro Function*: You can configure a key so that by pressing it a saved macro is executed.

  The macro function can only be programmed at the phone.
- *Headset Control* (not with the **S5x0**): If you've connected and configured a headset to your telephone over a separate headset socket, operation of the headset occurs over a function key. Press the headset key to initiate or accept calls. If you already have an active connection over the headset, you can end the call by pressing the headset key.
- *Automatic Call Pick-up*: Your telephone can accept calls automatically without you having to lift the receiver or press the loudspeaker key. Automatic call acceptance is switched on or off using the function key assigned. You can configure a separate function key for each number ("MSN-1"..."MSN-9"), or a function key for all numbers. The period after which calls are automatically accepted is configured once for all numbers of the telephone.
- *Trunk Group Access*: Several external ISDN (if supported by you device) or IP connections to bundles can be grouped in the system. With a bundle key, you can save these connections on a function key. If this key is pressed, automatic hands-free is enabled and a free B channel of the corresponding bundle is assigned. You then hear the external dialling tone.

- `Connection Key` (not with the **S5x0**): In addition to the softkeys "Connection 1..", function keys can be configured on the system telephone or the extension for operation while brokering. At least two connection keys must be configured.
- `Hotel Room`: You can assign a key in such a way that when pressed, the guest is checked in or out (first level), or the selected hotel room phone is called (second level). You must configure this key on the first level, then the connected key on the second level is automatically assigned and, as the case applies, its content overwritten.
- `System Parking`: The called party is put on hold for enquiry and dials a code. The telephone is now freed for other operations, e. g. announcements. Another party can accept the call, if he lifts the receiver and dials the relevant code of the held call. The codes assigned by the PABX can also be entered in the function keys of one or more system telephones. If a call is set to open hold for enquiry by pressing the function key, this is indicated by flashing LEDs on the function keys for the system telephones set up for this. The call is transferred by pressing the corresponding function key. This performance feature is only possible if only one call is on hold.
- `Agent wrap-up Time`: You can configure a key so that when it is pressed, an agent's post-processing time is switched on or off at a team call centre (first level), or extended (second level).
- `Night Mode`: You can configure a key so that by pressing it night operation is switched on or off.

Note

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

- `Parallel Ringing` (only **S5x0**): If a parallel call to another telephone is configured, both connections will ring when a call comes in. The call is accepted where first picked up.
- `Shift` (only **S5x0**): With this key, you can access second level functions.
- `Do not Disturb` (only **S5x0**): With this key, you enable or disable the Do not Disturb function which you have configured under **Terminals**->**elmeg System Phones**->**System Phone**->**Settings**.

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

Fields in the menu Phone: Type x

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

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

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

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

Field	Description
	Where **Key Type** = *System Call (Announcement Team)* Select the internal number of a team to whose telephone an announcement shall be sent. When **Key Type** = *Login / Log Out, Team* Select the internal number of a team to be logged in/out when this key is pressed.
Trunk Line	Only where **Key Type** = *Trunk Line* Select the external connection over which an external call shall be set up when this key is pressed.
Number of Secretary Phone	Only where **Key Type** = *Boss Key* Select the internal number of the secretary telephone. The secretary telephone is called when this key is pressed.
Number of Boss Phone	Only where **Key Type** = *Secretary Key* Select the internal number of the Boss telephone. The Boss telephone is called when this key is pressed.
Target Number "On no reply"	Only where **Key Type** = *Call Forwarding (CFNR)* Enter the number to which calls shall be forwarded immediately when call forwarding is enabled.
Target Number "Immediate"	Only where **Key Type** = *Call Forwarding (CFU)* Enter the number to which calls shall be forwarded when call forwarding when busy is enabled.
Target Number "On busy"	Only where **Key Type** = *Call Forwarding (CFB)* Enter the number to which calls shall be forwarded when call forwarding is enabled when the call is not answered.
Trunk Group Access	Only where **Key Type** = *Trunk Group Access* Select the bundle via which an outside call shall be set up.
Waiting Queue	Only where **Key Type** = *System Parking*

Field	Description
	Select the queue in which the current call should be held.

Move

Select the ↑↓ icon to move configured function keys.

Fields in the menu Phone

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

Fields in the menu Move to

Field	Description
Phone	Displays your system telephone. In **User Access** you can only move keys within your own telephone key extension combination.
Module	Select telephone or a key extension module.
Key	Select the key to which you wish to transfer the configured function.

21.7.1.3 Device Info

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

Meaning of the list entries

Description	Meaning
Description	Displays the entered description of the telephone.
Phone Type	Displays the type of telephone.
Serial Number	Displays the serial number of the telephone.

Description	Meaning
Software Version	Displays the current version of the telephone software.
Release Date and Time	Displays the date and time of the telephone software version.
Last Device Configuration	Displays the date and time of the last telephone configuration.
Answering Machine	Displays whether an answering machine module is inserted in the telephone (Yes) or not (No).

Meaning of the key extension

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

21.8 Voice Mail System

You can access information on you voicemail box in the **Voice Mail System** menu.

Note

The **Voice Mail System** menu is only displayed once a personal voicemail box has been set up for you.

21.8.1 Settings

In the **Voice Mail System** ->**Settings** menu, your voicemail box settings are displayed.

Values in the Settings list

Field	Description
Internal Number	Displays your internal number.
User	Displays your user name.
Status of Mail Box Owner	Displays your status.
Check PIN	Indicates whether access to your voicemail box is protected by a PIN.
Mode for status "In the Office"	Indicates in which mode your voicemail box operates for the "In Office" status.
Mode for status "Out of Office"	Indicates in which mode your voicemail box operates for the "Out of Office" status.
New Calls	Indicates the number of new calls.
Old Calls	Indicates the number of old calls.
Saved Calls	Indicates the number of saved calls.

21.8.1.1 Edit

Choose the ✎ icon to edit existing entries. You can change the settings of selected parameters.

The menu **Voice Mail System** ->**Settings** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Status of Mail Box Owner	Define in which mode your mailbox shall be used when starting the voicemail system.

Field	Description
	Possible values: • *In the Office* (default value): Select this setting if you're in the office when the voicemail system is started. • *Out of Office* : Select this setting if you're out of the office when the voicemail system is started.
Check PIN	Select whether your voicemail box should be protected with a PIN.
Mode for status "In the Office"	Your voicemail box can be operated with two different settings during office hours. Possible values: • *Announcement only*: A caller hears an announcement, but cannot leave a message. • *Announcement and Record*: A caller hears an announcement and can leave a message.
Mode for status "Out of Office"	Your voicemail box can be operated with two different settings outside office hours. Possible values: • *Announcement only*: A caller hears an announcement, but cannot leave a message. • *Announcement and Record*: A caller hears an announcement and can leave a message.

Fields in the Voice Mail Message via E-Mail menu.

Field	Description
E-Mail Notification	Once a message has been left on the voicemail box, the subscriber can be notified. Possible values: • *None* (default value): The subscriber is not notified. • *E-Mail*: The subscriber is informed of a present message via e-mail. • *E-Mail with Attachment*: Once a caller has left a message, the subscriber receives an e-mail with a recording of the

Field	Description
	message in the attachment. **Note** After a subscriber has been informed about a new message through an E-Mail, the **Status** of the message is chnaged according to the configuration in **User Access**->**Voice Mail System**->**Settings** under **E-Mail forwarding behavior**.
E-Mail forwarding behavior	Only for **E-Mail Notification** = *E-Mail* or *E-Mail with Attachment* Select an option for forwarded messages. Possible values: • *Keep Message in 'new' after forwarding*: Following an e-mail alert or forwarding, the status of the voicemail message is set to *New*. • *Move Message to 'old' after forwarding*: Following an e-mail alert or forwarding, the status of the voicemail message is set to *Old*. • *Remove Message after forwarding*: The voicemail message is deleted following an e-mail alert or forwarding.

21.8.2 Messages

In the **Voice Mail System**->**Messages** menu, a list of your messages is displayed. You also have the option to play back voicemail messages or download these to your PC. To save a message, click on the 💾 icon. The download dialog then opens. To listen to a message, click on the ▶ icon.

Individual or all wave files can be deleted by clicking the **Select all** / **Deselect all** checkbox then pressing **Delete Selected**.

Values in the Messages list

Field	Description
Internal Number	Displays the internal number of a voicemail box.

Field	Description
	Several internal numbers can be assigned to a single user. The user can operate a separate voicemail box under each internal number.
User	Displays the name of the voicemail box user.
Call from	Displays the caller's number.
Date/Time	Displays the date and time of the call.
Call Status	Indicates whether the call is `New`, `Old` or `Saved`.
Select all / Deselect all	You can select individual entries using the checkbox in the corresponding line, or select them all using the **Select all** button or **Deselect all**. You can delete the selected entries by pressing the **Delete Selected** option.

Glossary

3DES See DES.

A-subscriber The A-subscriber is the caller.

a/b interface An a/b interface is used to connect an analogue terminal. In the case of an ISDN terminal (terminal adapter) with a/b interface, a connected analogue terminal is enabled to use the supported ISDN performance features.

Accounting Accounting refers to the recording of connection data, e.g. date, time, connection duration, charging information and number of data packets transferred.

AES Advanced Encryption Standard (AES, Rijndael) is an encryption method (see Cipher). AES uses a fixed block length of 128 bits. The key length is 128, 192 or 256 bits. AES is a very fast and secure algorithm.

Agent The call centre agent is a member of a call centre.

Analogue Analogue signals are used to transmit data. They are more susceptible to errors than digital signals.

Analogue terminals Terminals that transmit voice and other information analogously, e.g. telephones, fax machines, answering machines and modems. Performance features can only be used with terminals that dial using the MFC dialling method and that have an R or flash key.

Announcement The announcement is a performance feature. The announcement function enables a connection to be established to other phones which is automatically accepted by the subscribers called. The caller speaks and those called hear the announcement. If one of those called lifts the receiver, a normal connection is established.

Answering machine Analogue answering machines are configured as an analogue terminal and selected via the terminal type. The PABX voice mail system is used as the answering machine.

ARP The Address Resolution Protocol (ARP) supplies the associated MAC addresses to IPv4 addresses. The information required is shared between the network nodes, stored in the device's cache, and deleted again after the ARP lifetime has expired. For IPv6 this functionality is provided by the Neighbor Discovery Protocol (NDP).

ARS The PABX uses Automatic Route Selection (ARS) to determine the ideal route to the called party, depending on the provider, service, QoS, …

Authorisation class See CoS.

Automatic callback on busy (CCBS) Callback on busy is a performance feature. If the connection of the subscriber called is engaged, a callback can be requested. When the called subscriber's phone call ends, the caller is phoned and automatically connected to the called subscriber.

Automatic callback on no reply (CCBS) Callback on no reply is a performance feature. If the called subscriber fails to take the call, a callback can be requested. When the called subscriber ends a call, the caller is phoned and automatically connected to the called subscriber.

Automatic outside line Automatic outside line enables the phone number of an external party to be dialled (without entering a code).

Automatic redialling If the connection of the called party is engaged, an automatic redial can be initiated. This notifies the caller as soon as the line is free.

Automatic Route Selection Automatic route selection can be used to route calls whatever the number (zone) dialled, via specified providers or bundles.

B channel See Basic Rate Interface and Primary Rate Interface.

B channel See B channel.

B subscriber The B subscriber is the called party.

Back Route Verify If a Back Route Verify is activated for an interface, incoming data packets are only accepted over this interface if outgoing response packets are routed over the same interface.

Basic Rate Interface The Basic Rate Interface is a network connection to the ISDN. This type of connection is often abbreviated to BRI. A basic rate interface includes two basic channels (B channels) each with 64 kbps and one control and signalling channel (D channel) with 16 kbps. There are two operating modes for the Basic Rate Interface: Point-to-point ISDN and Point-to-multipoint The Primary Rate Interface (PRI) is used with larger installations.

Bit A binary digit (bit) is the smallest unit of data in computing technology. Signals are represented in the logical states "0" and "1".

Black / White List Entries in the Black List are blocked, entries in the White List are allowed through. (Example: Any telephone number beginning with 01234 is blocked in the Black List. The number 01234987 can nonetheless be approved in the White List.)

Blowfish Blowfish is an encryption method (see Cipher). Blowfish uses a fixed block length of 64 bits. The key length can be between 32 and 448 bits.

BRI See Basic Rate Interface

Bridge A bridge is a network component for connecting the same types of network at Level 2 of the OSI model. Data packets are transmitted using MAC addresses. The use of bridges divides up the network and reduces the load.

Broker Brokering makes it possible to switch between two subscribers without the waiting subscriber being able to hear the other conversation.

Bundle The external connections of a PABX can be grouped into bundles.

Busy On Busy If Busy on Busy is enabled, anyone who calls an engaged subscriber hears the engaged tone. Call waiting or call forwarding to a team are not possible.

Cache The device temporarily stores data used in name resolution in the cache. See also ARP.

Call allocation With call allocation, calls coming into the PBX are assigned to particular numbers or applications (remote access, ISDN login, ...).

Call centre A call centre provides support, shares information and sells over the telephone.

Call deflection Call deflection (CD) is a performance feature. A call can be forwarded without it having been taken.

Call deflection (CD) See Call forwarding.

Call forwarding Call forwarding is a performance feature. When call forwarding (CF) is used, incoming calls can be routed to another, internal or external, phone number. The call can be forwarded in the telephone system or the switchboard, or by the SIP provider.

Call pickup See pickup

Call Through Call Through refers to dialling into the system via an external connection and the system putting the call through to a different external connection. This can reduce call costs.

Call variant The call variant specifies which terminals a call is signalled to. The calendar can be used to control the individual call variants on a time basis.

Call waiting Call waiting is a performance feature. Another caller is signalled during a phone call.

Call waiting protection When call waiting protection is enabled, other callers are not signalled on the terminal. The caller hears the engaged tone.

Callback on Busy See Automatic callback on busy (CCBS)

Callback on no reply See Automatic callback on no reply (CCBS)

Called party number The number of the party being phoned.

Caller list On system telephones, missed calls are saved in a caller list. To achieve this, calling line identification presentation (CLIP) needs to be enabled.

Calling party number The number of the calling terminal.

CAPI The Common ISDN Application Programming Interface (CAPI) is a programming interface for ISDN. It enables application programs to access ISDN hardware from a PC. See also TAPI.

CAPWAP Control And Provisioning of Wireless Access Points Protocol (CAPWAP) is used to have wireless access points (slaves) monitored by a WLAN controller (master). It uses UDP port 5246 for monitoring and 5247 to send data.

CFB Call Forwarding Busy (CFB) is a performance feature. CFB forwards callers to a different connection if the connection of the party called is engaged.

CFNR Call Forwarding No Reply (CFNR) is a performance feature. CFNR forwards callers to a different connection if the call is not taken.

Channel bundling When channels are bundled, the B channels in an ISDN connection are combined to increase data throughput.

Cipher A block cipher is an encryption algorithm. In this encryption method, a data block of a fixed size (normally 64 bit) is rewritten to a block of the same size using a so-called key. The longer the key, the more secure the algorithm.

CLID Calling Line Identification (CLID), also known as Caller ID, is used for authentication. A caller is identified by means of his or her ISDN extension number before the connection is established.

Client A client uses the services provided by a server. Clients are usually workstations.

CLIP See Display caller number (CLIP / CLIR).

CLIP no Screening See also Display caller number (CLIP / CLIR). With CLIP no Screening, as well as the normal caller number, another number is also sent, e. g. the number of the switchboard or a service number. The normal number can also be suppressed using CLIP, so that the party called only sees the other number.

CLIP off Hook See Display caller number (CLIP / CLIR).

CLIR See Display caller number (CLIP / CLIR).

Code procedure A sequence (code procedure) (consisting of 0 - 9, *, # and R) can be entered on the telephone keypad in order to access the PBX's functions.

COLP See Display called party number (COLP / COLR).

COLP no Screening See also Display called party number (COLP / COLR). With COLP no Screening, as well as the normal caller number, another number is also sent, e. g. the number of the switchboard or a service number. The normal number can also be suppressed using COLP, so that the party called only sees the other number.

COLR See Display called party number (COLP / COLR).

Conference call With a conference call, multiple internal subscribers can speak to one another on the phone at the same time.

Configuration The configuration refers to all of a device's settings. It is stored internally, in MIB tables. This data can be backed up, loaded and deleted externally. The configuration is edited using the HTTP(S) user interface, an SNMP client or connected telephones.

CoS The term Class of Service (CoS) means different things depending on the area in which it is applied. In telecommunications CoS refers to the permission class assigned to the user. The permission class defines the user's rights, e. g. exchange access right, features that can be used, access to applications, ... In network technology CoS refers to the classification of certain services as per IEEE 802.1p. CoS enables priorities to be set in a targeted way, while Quality of Service (QoS) is used to set up explicit bandwidth guarantees or restrictions. Data packets are classified using a DSCP (Differentiated Services Code Point) value.

D channel See Basic Rate Interface and Primary Rate Interface.

Daemon A daemon refers to a program that runs in the background and provides certain services.

DCN DCN stands for data communication network.

DDI DDI stands for Direct Dial In. See Point-to-point ISDN access and Direct dial-in (VoIP).

DECT Digital Enhanced Cordless Telecommunications (DECT) is a standard for cordless telephones and wireless PABX systems.

Default route See Standard route

Default route The default route is used when no other suitable route is available.

DES The Data Encryption Standard (DES) is an encryption method (see Cipher). DES uses a fixed block length of 64 bits. The key length is 56 bits. Triple DES or 3DES is based on using DES three times (three different, independent keys).

DHCP The Dynamic Host Configuration Protocol (DHCP) allows IP addresses to be assigned dynamically. A DHCP server allocates each client in a network an IP address from a defined address pool. The clients need to be configured accordingly.

Dial preparation Dial preparation describes the entering of the telephone number before initiating the call, e. g. by lifting the receiver.

Dialling control See Black / White List.

Digital Digital signals are used to transmit data. They are less susceptible to errors than analogue signals.

DIME Desktop Internetworking Management Environment (DIME) is used to configure and monitor gateways.

Direct call If the direct call function is set up, the user merely has to lift the telephone receiver to, after a short wait, automatically get a connection to a particular phone number.

Direct dial exception See Point-to-point ISDN access and Direct dial-in (VoIP).

Direct dial-in (VoIP) Direct dial-in is a VoIP connection that is also known as point-to-point. It is used to connect a PBX. A main phone number and a number block are issued. Each of the numbers in the number block is called a direct dial exception. (Example: Main number 1234, number block: 1 - 99, numbers of the individual extensions: 1234-1, 1234-2, 1234-3, …)

Direct dialling range See number block in Point-to-point ISDN access and Direct dial-in (VoIP)

DISA DISA - Direct Inward System Access A call, after it has been taken by the PBX, is automatically forwarded after a code has been entered. In the PBX, this code is assigned to an internal telephone number.

Display called party number (COLP / COLR). Connected Line Identification Presentation (COLP) is used to send the phone number of the called party (B phone number) to the caller. Connected Line Identification Restriction (COLR) is used to suppress the transmission of the phone number of the called party to the caller.

Display caller number (CLIP / CLIR). Calling Line Identification Presentation (CLIP) is used to send the caller's phone number (A phone number) to the called party. CLIP off Hook sends the phone number of the caller waiting. Calling Line Identification Restriction (CLIR) is used to suppress the transmission of the phone number of the caller to the called party.

DNS The Domain Name System (DNS) is used to convert the domain name (e. g. www.example.org) to an IP address (name resolution).

Do not disturb See Station guarding.

Domain A domain is a contiguous sub-set of the DNS (e. g. example.org).

Door intercom A door intercom is mounted on entrances, and may be part of a PBX.

Downstream The gateway receives the data from a higher-level network and forwards it to its connected network.

DSA The Digital Signature Algorithm (DSA) is used to create digital signatures and encrypt data packets. Signatures can be used to verify changes made to the information in the data packet. DSA is used for public-key cryptography (IPSec). See also RSA. Key generation is quicker with DSA than with RSA, but key processing is slower.

DSCP Data packets can be marked with a Differentiated Services Codepoint (DSCP). DSCP values classify data packets in such a way that important packets can be routed through the network more quickly. See also QoS.

DSP A digital signal processor (DSP) converts analogue, ISDN and VoIP signals to one another. So, e. g., analogue terminals can also be used on an SIP connection.

DSS1 Digital Subscriber Signalling System No. 1 (DSS1) is a signalling protocol for the D channel in the ISDN. It is also known as Euro ISDN.

DTMF See Multifrequency code dialling method.

DTMF Inband / Outband See also Multifrequency code dialling method. With inband, the DTMF signal is transmitted in the voice band (G.711) With outband, the DTMF signal is transmitted as specified in RFC 2833.

Dynamic IP address In contrast to a static IP address, a dynamic IP address is assigned temporarily by DHCP. Network components such as the web server or printer usually have static IP address, while clients such as notebooks or workstations usually have dynamic IP addresses.

Engaged when busy See Busy on Busy.

Ethernet Ethernet is a specification for cable data networks. Ethernet works on the first and second layer of the OSI model.

Euro ISDN Standard ISDN in Europe, based on the DSS1 signalling protocol.

Eurofile transfer Eurofile transfer (EFT) is a protocol for sharing files over ISDN.

Exchange access right The telephone system distinguishes between the following exchange access rights: Unlimited: Any international, national or internal connection is permitted. National long-distance calls: Only domestic connections may be established - i. e. dialling any number that begins with 0 but not with 00. Incoming external calls can be received without restrictions. Locality: Only connections to the same area code may be established. So the number may not begin with a 0. Incoming external calls can be received without restrictions. Incoming: Only connections to other terminals in the telephone system may be established. Incoming external calls can be received without restrictions. Internal: Only connections within the telephone system are permitted.

Extension In PBX systems, an extension refers to the terminal connected to the system.

Extension number See Point-to-point ISDN access and Direct dial-in (VoIP).

Extension number block See Point-to-point ISDN access and Direct dial-in (VoIP).

Extension numbers range See Extension number block in Point-to-point ISDN access.

Fax Fax is used to send text, graphics and documents over the phone network. A distinction is drawn between Group 3 fax machines for the analogue network (transmission rate: 9.6 or 14,4 kbit/s) and Group 4 fax machines for ISDN (transmission rate: 64 kbit/s). To connect Group 3 fax machines to ISDN, a terminal adapter or a suitable PBX is required.

Filter A filter comprises a number of criteria (e.g. protocol, port number, source and destination address). If these criteria match a data packet, the data packet can be subjected to a particular action (forward, reject, ...). This creates a filter rule.

Filter rule A rule that defines which data packets should or should not be transmitted by the gateway.

Firmware The firmware (system software) is programming code that is permanently embedded in the device. It provides the device's functions.

Flash key The flash key on a telephone is the R button. The key interrupts the line briefly to start certain functions such as inquiries.

Follow-me Follow-me is a performance feature. This function can be used to route incoming calls from a different extension to one's own terminal.

FTP The File Transfer Protocol (FTP) regulates data transmission in IP networks. It regulates the exchange between FTP server and client.

Function keys Function keys are special keys on system telephones which can be assigned phone numbers or functions.

FXO Foreign Exchange Office (FXO) refers to the connection to the analogue terminal. See also FXS.

FXS

Foreign Exchange Station (FXS) refers to the analogue connection to the connection socket or PBX. See also FXO.

G.711

G.711 is an audio codec. Audio signals from the frequency range between 300 Hz and 3400 Hz are passed with a sampling rate of 8 kHz. At a data transmission rate of 64 kbit/s, the codec achieves excellent voice quality (MOS value: 4.4). The A-law quantisation method is used in Europe, and the µ-law method in the USA.

G.722

G.722 is an audio codec. Audio signals from the frequency range between 50 Hz and 7000 Hz are passed with a sampling rate of 16 kHz. At a data transmission rate of 64 kbit/s, the codec achieves outstanding voice quality (MOS value: 4.5).

G.726

G.726 is an audio codec. Audio signals from the frequency range between 200 Hz and 3400 Hz are passed with a sampling rate of 8 kHz. The codec achieves an acceptable voice quality. MOS value: 3.7 (16 kbit/s), 3.8 (24 kbit/s), 3.9 (32 kbit/s), 4.2 (40 kbit/s). There are two different coding methods: I.366 and X.420

G.729

G.729 is an audio codec. Audio signals from the frequency range between 300 Hz and 2400 Hz are passed with a sampling rate of 16 kHz. At a data transmission rate of 8 kbit/s, the codec achieves an acceptable voice quality (MOS value: 3.9).

Gateway

The gateway is a network component for connecting different types of network.

Hands-free calling

With hands-free calling, calls can be made without lifting the receiver. Other people in the room can participate in the conversation using a microphone and loudspeakers.

Hash

To ensure data integrity, the information needs to be protected from unauthorised manipulation while it is being transmitted. To ensure that this happens, every item of communication received has to match the information originally sent. Therefore erratic mathematical value functions (hash functions) are used to calculate checksums (hash values). These are encrypted and sent as a digital signature with the message. The recipient, in turn, checks the signature before opening the packet. If the signature and, thus, the content of the data packet has changed, the packet is discarded. The hash algorithms used most frequently are Message Digest Version 5 (MD5) and Secure Hash Algorithm (SHA1).

Hold

A telephone call is put on hold without breaking the connection (inquiry/brokering). A distinction is drawn between holding the connection in the PBX (holding in the system) and holding in the switchboard or by the SIP provider.

Hold for enquiry With hold for enquiry, the phone call with the first party is held while one conducts a second call.

Host A host is a computer system that provides its services to the network.

Host name The domain name of a host. See DNS.

Host route A host route is the name for the route to a single host.

HTTP The HyperText Transfer Protocol (HTTP) is a protocol for transmitting HTML pages (web pages) between server and client. By default it uses port 80.

HTTPS The HyperText Transfer Protocol Secure (HTTPS) is a protocol which protects against eavesdropping when transmitting HTML pages (web pages) between server and client. HTTPS is schematically identical to HTTP. SSL / TLS is used for additional data encryption. The standard port for HTTPS connections is 443.

IAE IAE refers to the standard socket (ISDN connection unit) to which ISDN terminals are connected.

ICMP The Internet Control Message Protocol (ICMP) is used to exchange information and error messages over IPv4. The version ICMPv6 exists for IPv6.

Internal call tone The internal call tone on a PBX is used to differentiate between internal and external calls.

Internal telephone numbers Internal phone numbers are used for calls within the PBX.

IP The Internet Protocol (IP) is a network protocol and it is the basis for the Internet. It works on the network layer of the OSI model. The TCP and UDP protocols are based on IP. There are two versions, Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).

IP address IP addresses are used to navigate in an IP network, to unambiguously identify the source and destination. IPv4 addresses consist of 32 bits, IPv6 addresses of 128 bits. So, with IPv4 232, i.e. 4.294.967.296 addresses can be represented, with IPv6 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 addresses.

Dotted decimal notation, e. g. 192.168.0.250, is used for IPv4. Hexadecimal notation, e. g. 2001:db8:85a3::8a2e:370:7344, is used for IPv6. See also netmask.

IPCP The Internet Protocol Control Protocol (IPCP) is used, in a similar way to DHCP, to configure a host with an IP address, gateway and DNS server, when a PPP network connection is being used. With the extension Robust Header Compression over PPP, the header can be compressed for faster data transmission. Similarly, in IPv6 networks, the functionality is provided by the Internet Protocol version 6 Control Protocol (IPV6CP).

IPv6 See IP.

ISDN Integrated Services Digital Network (ISDN) is a data transmission standard that includes telephony, fax and data transmission. There are two ISDN connection variants: Basic Rate Interface and Primary Rate Interface.

ISDN address The ISDN address of an ISDN device comprises an ISDN number followed by other numbers that relate to the specific terminal.

ISDN login The ISDN login is used to remotely configure the device via SNMP. To do so, it needs to have a configured ISDN or wireless connection.

ISDN number The ISDN number is the network address of the ISDN interface.

ISDN-BRI See BRI.

ISDN-Internal/External Alternative name for the So bus.

ISDN-PRI See PRI.

ITU The International Telecommunication Union (ITU) coordinates the setting up and operating of telecommunications networks and services.

Keepalive Keepalive packets are used to check that the communication partner can be contacted.

Keypad The keypad protocol (network direct) is used to access and manage performance features provided by the switchboard.

LAN A Local Area Network (LAN) refers to a network that is geographically very limited and normally spans one building or a company head office.

Layer A layer refers to a layer in the OSI model.

LDAP The Lightweight Directory Access Protocol (LDAP) regulates the communication between a client and the directory server. LDAP is used for sharing and updating directories, e. g. a phone book.

Lease time The lease time refers to the validity period of a dynamic IP address that a client has been given by a DHCP server.

Line access authorisation See Exchange access right.

Loopback In a loopback switch the sender and recipient are identical.

MAC address The Media Access Control address (MAC address) is the hardware address of the network adapter and is used to identify the device at the hardware level.

MD5 Message Digest Algorithm 5 (MD5) is a hash function that generates a 128 bit hash value (checksum). See also Hash.

Media gateway A media gateway converts the network type of digital voice, audio or image information. For example, the signals from an ISDN network can be converted to an IP network.

Metric The metric is a measure for the properties of the route. The fastest route has the lowest metric (costs). Simplified, this is connecting with the smallest number of node points (routers).

MFC See Multifrequency code dialling method.

MFV See Multifrequency code dialling method.

MIB The Management Information Base (MIB) describes the data that can be queried or modified via a network management protocol (e. g. SNMP). The MIB is a database that describes all the devices and functions in the network.

Mobile subscriber If the mobile subscriber is enabled, an external telephone, e. g. a mobile phone can be called in parallel (parallel calling). The system's functions, e. g. callback, can also be used externally. For these functions, the external telephone's star key is interpreted as the R key.

MOH See Music on hold.

MSN See Multiple subscriber number

MSS The Maximum Segment Size (MSS) defines the maximum number of bytes that can be used as user data in a TCP segment. The MSS must be smaller than the Maximum Transmission Unit (MTU) to avoid fragmenting the IP packets.

MSS clamping MSS clamping reduces the Maximum Segment Size (MSS) in order to connect networks with different Maximum Transmission Units (MTU).

Multicast With a multicast, data packets are sent from one point to particular subscribers in a network. In IPv4 this is controlled via the address range 224.0.0.0 to 239.255.255.255 and the IGMP protocol, while in IPv6 it is controlled by ff00::/8 addresses and ICMPv6.

Multifrequency code dialling method The multifrequency code dialling method, also known as tone dialling, MFV, MFC and DTMF, is a signalling method for automatic telephone routing. Key inputs are represented by overlaid, sinusoidal signals. See also Pulse dialling.

Multiple subscriber number Multiple subscriber numbers are the individual phone numbers in the ISDN point-to-multipoint connection.

Music on Hold The term Music On Hold (MOH) refers to automated announcements or hold music on the PBX.

Music on hold See Music on hold.

MWI The Message Waiting Indicator (MWI) signals that a new message is available.

NAT Network Address Translation (NAT) is used to replace the source and destination IP addresses of a data packet with others. This enables different networks to be connected to one another. See also PAT.

NBNS Like DNS, NetBIOS Name Service (NBSN) is used in centralised name resolution. See also WINS and DNS.

Netmask With IPv4 in connection with the IP address, the netmask, also network mask and subnet mask, defines the network by dividing the IP address into network and device parts and thus determining which addresses need to be routed. Example of a netmask: 255.255.255.0. With IPv6 one refers to prefix length.

Network direct See Keypad.

Network route The network route refers to the route to a particular network.

Network termination Network termination (NT) refers to a connection or operating type. A terminal is given access to a communication network at the NT interface (connection socket). The connector is called a TAE with an analogue connection, an NTBA with the basic ISDN connection, and NTPMGF with the ISDN Primary Rate Interface. In the NT operation, the gateway is connected to the PABX's external S0 and is an external exchange connection for it. See also TE.

NT See Network termination.

NTBA See Network termination.

NTPMGF See Network termination.

Open hold for enquiry With open hold for enquiry, a call is put on hold and either party can then resume it once more.

OSI model The OSI model divides the flow of communication between the physical medium and the user level into layers. The requirements at each layer are met by relevant protocols.

PABX Private Automatic Branch Exchange (PABX) is another expression for a telephone system.

PABX PABX is another term for a telephone system.

Parallel call See Mobile subscriber.

Park When a call is parked, the connection is held even if the receiver of the terminal involved is replaced or the cable connection is cut off.

PAT Port and Address Translation (NAT) is used to replace the source and destination IP addresses and source and destination ports of a data packet with others. This enables different networks to be connected to one another. See also NAT.

PBX Private Branch Exchange (PABX) is another expression for a telephone system.

PDM See Pulse dialling

Pick-up With pick-up, calls can be received using code procedures on an internal terminal that is not part of active call allocation.

PIN A personal identification number (PIN) can be used to authenticate oneself on the device so that one can use the device's functions.

Point-to-multipoint Point-to-multipoint connection is an ISDNB connection. It is used to connect ISDN terminals. Multiple subscriber numbers (MSNs) are provided. See also Point-to-point ISDN access

Point-to-multipoint See Single phone number (VoIP).

Point-to-point See Point-to-point ISDN access and Direct dial-in (VoIP).

Point-to-point connection number: See Point-to-point ISDN access

Point-to-point ISDN access Point-to-point ISDN access refers to an ISDN connection that is also called point-to-point. It is used to connect a PBX. A point-to-point number and a number block are issued. Each of the numbers in the number block is called a direct dial exception. (Example: Point-to-point connection number: 1234, number block: 1 - 99, numbers of the individual extensions: 1234-1, 1234-2, 1234-3, …) See also Point-to-multipoint connection.

Port The port number is used to decide the service (telnet, FTP, ...) to which an incoming data packet should be sent.

POTS Plain Old Telephone System (POTS) refers to the analogue telephone network.

PPTP The Point-to-Point Tunneling Protocol (PPTP) is a network protocol for encapsulating other protocols so that they can be transported via the Internet Protocol (IP) in the form of a tunnel (VPN). PPTP uses protocol number 1723. The PPTP architecture is divided into two logical systems. The PPTP Access Concentrator (PAC) and the PPTP Network Server (PNS). The PAC is usually integrated into the Windows client. It establishes the connection to the PNS and manages it. The PNS is responsible for routing and controlling the packets received by the PNS.

Prefix length See netmask.

PRI See Primary Rate Interface.

Primary Rate Interface The Primary Rate Interface is a network connection to the ISDN. This type of connection is often also called a PRI or S2Minterface. A Primary Rate Interface offers 30 user channels (B channels), each with 64 kbits/s, in Europe and 23 in the USA, one control channel (D channel) with 64 kbits/s and one synchronisation channel with 64 kbits/s in Europe and 8 64 kbits/s in the USA. See also Basic Rate

Interface.

Protocol Protocols regulate the flow of a data communication on different levels of the OSI model. Protocols control addressing, coding, authentication, formatting, etc. Examples: Ethernet, IP, TCP, HTTP

Proxy A proxy is a network component. The proxy is an agent. It routes a query from the source with its own IP address to the destination.

Pulse dialling Pulse dialling is a signalling method for automated telephone routing. Key inputs are represented by a defined number of dc pulses. See also Multifrequency code dialling method (MF).

QoS Quality of Service (QoS) describes the properties of the communication service. It is defined using bandwidth, delay, packet losses and jitter. To transmit time-critical data packets for VoIP or video streaming as quickly as possible, QoS is used to sort all the data packets into groups and forward them on in the network either more quickly or slowly, depending on their priority.

Registrar The SIP server (registrar) needs to be used in case the subscribers to a VoIP call are not using static IP addresses The SIP server registers the clients' IP addresses and sends this data to the SIP proxy, which connects the calls. The SIP proxy and SIP registrar are usually identical.

Reject / reject function When a phone number that has not been set up in the telephone system is dialled, or if the connection of the party called is engaged, or the party called does not take the call, the reject function determines how to proceed with the call. The call can be routed to a different destination or discarded.

Reset This returns the device to its unconfigured state.

RFC A Request For Comments (RFC) is a document that describes the standards and guidelines for the Internet.

Rijndael See AES.

RipeMD 160 RACE Integrity Primitives Evaluation Message Digest (RipeMD 160) is a hash function that generates a 160 bit hash value (checksum). See also Hash.

RJ45 RJ45 refers to a jack or connector with a maximum of eight wires to the digital terminals' connection.

Room monitoring Room monitoring is a performance feature. One can listen in to the sounds in a room.

Router

A router is a network component for connecting different types of network at the network layer of the OSI model. Data packets are transmitted using IP addresses. Routing tables are used to identify the best routes through the network. In order to keep the routing tables up to date, the routers exchange information via routing protocols (e.g. OSPF, RIP).

Routing

Routing refers to the identifying of routes for sending messages.

RSA

The RSA algorithm (named after its inventors, Rivest, Shamir and Adleman) is used to create digital signatures and encrypt data packets. The signature can be used to verify changes made to the information in the data packet. RSA is used for public-key cryptography (IPSec). See also DSA. Key generation is slower with RSA than with DSA, but key processing is faster.

RTP

The Real-Time Transport Protocol (RTP) is used to transmit audio and video data (streams) via IP-based networks.

Rule chain

A rule chain contains a combination of different filter rules. A filter rule selects part of the data traffic based on particular features, e. g. the source IP address, and applies an action, e. g. block, on this part.

S0 bus

The S0 bus is an interface for the ISDN Basic Rate Interface, and links multiple ISDN terminals to the NTBA. The bus is implemented by a four-wire circuit. See also UP0.

S2M interface

See Primary Rate Interface.

SCEP

The Simple Certificate Enrollment Protocol (SCEP) is used to manage digital certificates.

Scheduling

Scheduling refers to the planning of tasks. Particular actions (e. g. deactivating an interface) are triggered by events (e. g. time or changing a MIB variable).

Serial interface

The serial interface is used to exchange data between computers and peripheral devices. It can be used to configure the device or to transmit data via an IP infrastructure (Serial over IP).

Server

A server offers services used by clients.

SHA1

Secure Hash Algorithm version 1 (SHA1) is a hash function that generates a 160 bit hash value (checksum). See also Hash.

Shell

The shell is an input interface (e. g. command line or graphic user interface) between computer and user.

SIF

With a Stateful Inspection Firewall (SIF), the routing of a data packet is not determined only by source and destination addresses but also using dynamic packet filtering based on the connection status.

Simplex operation

Simplex operation is a performance feature. Simplex operations are used to take a call automatically and switch the speaker function on. If the called party lifts the receiver, a normal voice connection is established.

Single phone number (VoIP)

Single phone number access is a VoIP connection that is also known as a point-to-multipoint connection. It is used to connect VoIP terminals. Multiple subscriber numbers (MSNs) are provided. See also Direct dial-in (VoIP)

SIP

The Session Initiation Protocol is a network protocol for setting up a communication session between two or more subscribers. The protocol is used for IP telephony (VoIP).

SIP provider

A SIP provider does the switching between a SIP connection and other analogue, ISDN and VoIP connections.

SMTP

The Simple Mail Transfer Protocol (SMTP) is used to exchange emails.

SNMP

The Simple Network Management Protocol (SNMP) is used to configure, control and monitor different network components (e. g. routers, servers, etc.) from a single, central system. The network component settings that can be changed are stored in a database – the Management Information Base (MIB). SNMP uses UDP. The network component receives requests to port 161 while the managing system receives confirmation messages (TRAPs) at port 162.

SNTP

The Simple Network Time Protocol (SNTP) is used to transmit the time and to synchronise the server and client.

Softkey

A softkey refers to a key whose function is determined by the associated screen display.

Speaker function

With the speaker function, the people present in the room can listen in to the telephone call.

Speed dial number

A speed dial index (000...999) is assigned to every number in the phone book. This speed dial index can be used to dial instead of the long phone number.

Splitter

A broadband access unit, commonly known as a splitter, is used to split signals that come via a subscriber loop into data and telephone lines.

SSH

Secure Shell (SSH) is a network protocol that can be used to establish an encrypted connection to a device's shell.

Static IP Address

In contrast to a dynamic IP address, the static IP address is assigned permanently by the user. Network components such as the web server or printer usually have static IP address, while clients such as notebooks or workstations usually have dynamic IP addresses.

Station guarding

When station guarding is enabled, acoustic call signalling is switched off. This function is also known as Do not disturb.

STUN Server

Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). A STUN server enables VoIP devices behind an active NAT to access the network.

Suppress telephone number

See Display caller number (CLIP / CLIR) and Display called party number (COLP / COLR).

Switch

A switch is a network component that connects individual network segments to one another. On the one hand, a switch can be operated as a bridge to the data link layer in the OSI model. Unlike the bridge, however, a switch has more than one input and output. On the other hand, the switch can be operated as a gateway to the network layer in the OSI model. The device comparable to the switch in the physical layer is known as the hub.

Switch contact

A telephone can be used to switch a device connected to the switch contact, e. g. a door opener, on and off.

Syslog

The syslog protocol is used to transmit status messages in an IP network. In this way, different network components can be monitored from a single, central system. Syslog messages are sent as unencrypted text messages over the UDP port 514.

System telephone

A system telephone has multiple function and special keys and can use the performance features of a PBX.

T.38

T.38 or Fax over IP (FoIP) refers to fax transmission via an IP network.

TA

See Terminal adapter

TAPI

The Telephony Applications Programming Interface (TAPI) is a programming interface for ISDN. It enables application programs to access ISDN hardware from a PC. See also CAPI.

TCP

The Transmission Control Protocol (TCP) is a connection-oriented protocol. It works on the transport layer of the OSI model. With a connection-oriented protocol, a logical connection is established before transmission and maintained. This enables data to be transmitted reliably. Nonetheless, control information is constantly being sent alongside the actual data packets. This causes the data volume sent to increase. See also UDP.

TCU

See Network termination. A distinction is drawn between F-coded connectors for telephones and N-coded connectors for fax machines, modems and answering machines.

TE

Terminal equipment (TE) refers to a connection or operating type. The TE connector is a terminal's connector. In TE operation, the gateway is connected to the PABX's internal S0 and thus constitutes an ISDN terminal. See also NT.

TEI

Under ISDN protocol DSS1, the Terminal Endpoint Identifier (TEI) is an identifier for terminals.

Telefax

See Fax.

Telnet

Telecommunication Network (Telnet) is a network protocol. It enables communication with another, remote device in the network, e. g. PCs, routers, etc.

Terminal adapter

A terminal adapter (TA) can be used to connect terminals to an interface on which they cannot be operated directly, e. g. analogue terminals to an ISDN connection.

TFTP

The Trivial File Transfer Protocol (TFTP) regulates the transmission of files. Compared with FTP, there is no option to display data, issue permissions or authenticate users.

Three-party conference

The three-party conference is a performance feature. Three subscribers can speak to one another on the phone simultaneously.

Tiger 192

Tiger 192 is a hash function that generates a 192 bit hash value (checksum). See also Hash.

Time service

The Time protocol is used to synchronise the date and time. The protocol uses port 37 via TCP and UDP.

Tone dialling See Multifrequency code dialling method.

TOS Type of Service (TOS) is a field in the header of IP data packets. It specifies the priority of the data packet. See also QoS.

Trigger This refers to a trigger impulse.

Triple DES See DES.

Trunk A trunk consists of bundled connections or transmission channels. See also Bundle.

Twofish Twofish is an encryption method (see Cipher). Twofish uses a fixed block length of 128 bits. The key length is 128, 192 or 256 bits.

UDP The User Datagram Protocol (UDP) is a connectionless protocol. It works on the transport layer of the OSI model. With a connectionless protocol, no control is integrated for delivering the packet. The control must take place in the application layer. Conversely, UDP is faster than connection-oriented protocols.

UP0 The UP0 connection is an interface for the ISDN Basic Rate Interface, and links one ISDN terminal to the NTBA. The connection is implemented via a two-wire circuit, and offers a greater range than the S0 bus.

Upstream The gateway forwards the data from its own network.

URL A Uniform Resource Locator (URL) identifies a file's storage location. Example: http://www.example.org/index.htp (Internet website)

UUS With User to User Signalling (USS), text messages can be exchanged with other subscribers.

VLAN A network can be divided up into one or more logical sub-networks– so-called Virtual Local Area Networks (VLAN) – by the network components no longer forwarding the data packet of a defined subnetwork to other sub-networks. Each VLAN is assigned a unique number, This number is called a VLAN ID (VID) and assigned to the data packets in the VLAN tag.

Voice mailbox A voice mailbox is a user's personal answering machine in a voicemail system.

Voicemail system A voicemail system enables voice messages to be stored, accessed and forwarded, like an answering machine, but with more options.

VoIP

Voice over IP (VoIP), also known as IP telephony, refers to the transmitting of voice via an IP network. The telephone is connected and disconnected using signalling protocols, e. g. SIP.

WAN

A Wide Area Network (WAN) refers to a network that is spread over a large geographic area. Global WAN networks provide access to the Internet.

WINS

The Windows Internet Name Service (WINS) is a translation of the NetBIOS over TCP/IP network protocol by Microsoft. Like DNS, WINS is used for centralised name resolution. See also DNS.

X.31

The X.31 standard describes the connecting of ISDN and X.25 systems. It is a standard for connecting card terminals.

Zone

A zone refers to a phone number or numbers that begin with the same sequence.

Index