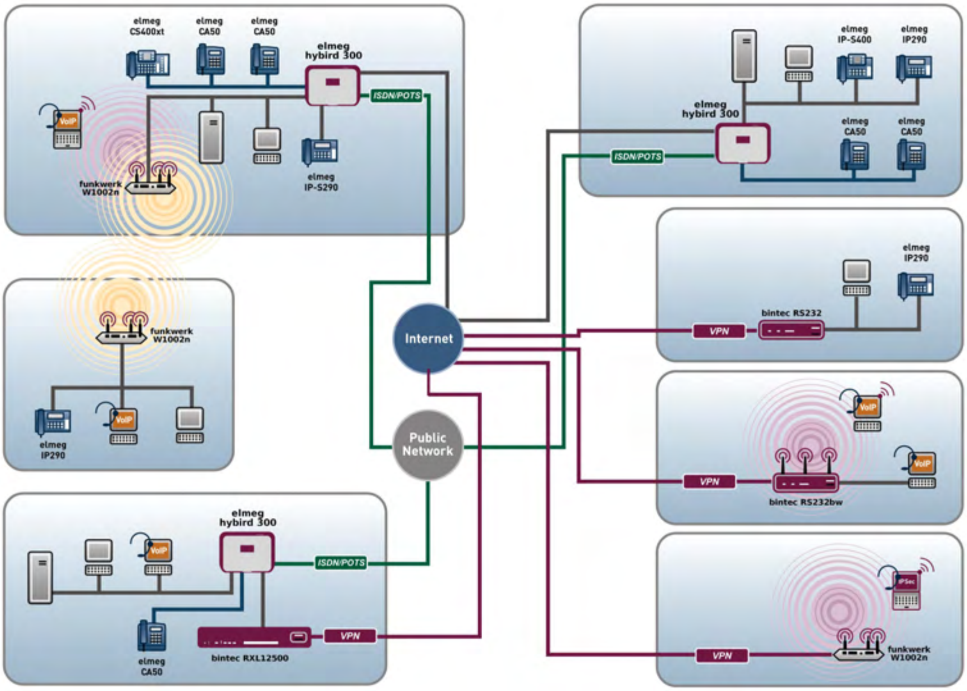


Manual
bintec R200 Series

Reference

Legal Notice

Aim and purpose

This document is part of the user manual for the installation and configuration of funkwerk devices. For the latest information and notes on the current software release, please also read our release notes, particularly if you are updating your software to a higher release version. You will find the latest release notes under *www.funkwerk-ec.com* .

Liability

This manual has been put together with the greatest possible care. However, the information contained in this manual is not a guarantee of the properties of your product. Funkwerk Enterprise Communications GmbH is only liable within the terms of its conditions of sale and supply and accepts no liability for technical inaccuracies and/or omissions.

The information in this manual can be changed without notice. You will find additional information and also release notes for funkwerk devices under *www.funkwerk-ec.com* .

Funkwerk devices make WAN connections as a possible function of the system configuration. You must monitor the product in order to avoid unwanted charges. Funkwerk Enterprise Communications GmbH accepts no responsibility for data loss, unwanted connection costs and damage caused by unintended operation of the product.

Trademarks

funkwerk trademarks and the funkwerk logo, bintec trademarks and the bintec logo, artem trademarks and the artem logo, elmeg trademarks and the elmeg logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

Company and product names mentioned are usually trademarks of the companies or manufacturers concerned.

Copyright

You will find information on guidelines and standards in the declarations of conformity under *www.funkwerk-ec.com* .

How to reach Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH, Südwestpark 94, D-90449 Nuremberg, Germany,
Phone: +49 911 9673 0, Fax: +49 911 688 07 25
Funkwerk Enterprise Communications France S.A.S., 6/8 Avenue de la Grande Lande, F-33174
Gradignan, France, Phone: +33 5 57 35 63 00, Fax: +33 5 56 89 14 05
Internet: *www.funkwerk-ec.com*

Table of Contents

Chapter 1 Introduction

The powerful gateways **bintec R230a**, **bintec R230b**, **bintec R230aw**, **bintec R232a**, **bintec R232b** and **bintec R232bw** enable you to connect small networks and your individual workstation or small company to the Internet and other partner networks (e.g. to a corporate network) at low cost.

Safety notices

The safety precautions, which are supplied with your device, tell you what you need to take into consideration when using your **bintec** gateway.

Installation

How to connect your device is shown in *Setting up and connecting* on page 6. This chapter also tells you what preliminary tasks are necessary for configuration.

Configuration

How to get your device running is explained in *Basic configuration* on page 9. There we show you how to start up your device within a few minutes from a Windows PC with the help of a Configuration Wizard and how to install other useful online assistants. At the end of the chapter, you will be in a position to surf the Internet, send or receive e-mails and set up a connection to a partner network to access data at your company head office, for example.

Password

If you are already familiar with configuring **bintec** devices and want to get started right away, all you really need to know is the factory default user name and password.

User Name: *admin*

Password: *funkwerk*

Note

Remember to change the password immediately when you log in to the device for the first time.

All **bintec** devices are supplied with the same password, which means they are not protected against unauthorised access until you change the password.

How to change the passwords is described in chapter *Modify system password* on page 14.

Workshops

Step-by-step instructions for the most important configuration tasks can be found in the separate **FEC Application Workshop** guide for each application, which can be downloaded from the *www.funkwerk-ec.com* website under **Solutions**.

Dime Manager

The devices are also designed for use with **Dime Manager**. The **Dime Manager** management tool can locate your bintec devices within the network quickly and easily. 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.

By using SNMP multicast all of the devices in your local network can be located 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 About this guide

This document is valid for **bintec** devices with system software as of software version 7.10.1.

The guide, which you have in front of you, contains the following chapters:

User's Guide - Reference

Chapter	Description
Introduction	You see an overview of the device.
About this guide	We explain the various components of this manual and how to use it.
Installation	This contains instructions for how to set up and connect your device.
Basic configuration	This chapter provides a step-by-step guide to the basic functions on your device.
Reset	This chapter explains how to reset your device to the ex works state.
Technical data	This section contains a description of all the device's technical properties.
Access and configuration	This includes explanations about the different access and configuration methods.
Assistants **System Management** **Physical Interfaces** **LAN** **Wireless LAN** **Networking** **Routing Protocols** **Multicast** **WAN** **VPN**	These chapters describe all configuration options of the **Funkwerk Configuration Interface**. The individual menus are described in the order of navigation. The individual chapters also contain more detailed explanations on the subsystem in question.

Chapter	Description
Firewall **VoIP** **Local Services** **Maintenance** **External Reporting** **Monitoring**	
Glossary	The glossary contains a reference to the most important technical terms used in network technology.
Index	The index lists all the key terms for operating the device and all the configuration options and gives page numbers so they can be found easily.

To help you locate information easily, this user's guide uses the following visual aids:

List of visual aids

Icon	Use
(!)	Indicates practical information.
☞	Indicates general and important points.
⚠	Indicates a warning of risk level "Attention" (points out possible dangers that may cause damage to property if not observed).
⚠	Indicates a warning of risk level "Warning" (points out possible dangers that may cause physical injury or even death if not observed).

The following typographical elements are used to help you find and interpret the information in this user's guide:

Typographical elements

Typographical element	Use
•	Indicates lists.

Typographical element	Use
Menu->**Submenu** **File**->**Open**	Indicates menus and sub-menus.

`non-proportional (Courier),`
`e.g. ping 192.168.1.254`
	Indicates commands that you must enter as written.

bold, e.g. **Windows Start menu**	Indicates keys, key combinations and Windows terms.
bold, e.g. **Licence Key**	Indicates fields.
italic, e.g. *none*	Indicates values that you enter or that can be configured.
Online: blue and italic, e.g. *www.funkwerk-ec.com*	Indicates hyperlinks.

Chapter 3 Installation

⚠ **Caution**

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

3.1 Setting up and connecting

☞ **Note**

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

⚠ **Caution**

The use of the wrong mains adapter may damage your device. Only use the mains adaptor supplied with the equipment. If you require foreign adapters/mains units, please contact our funkwerk service.

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

☞ **Note**

If you connect an unconfigured device to an ISDN connection in parallel to a PBX, the PBX cannot take any calls until an ISDN number is configured on the device. If no entry is specified, every incoming ISDN call is accepted by the ISDN Login service.

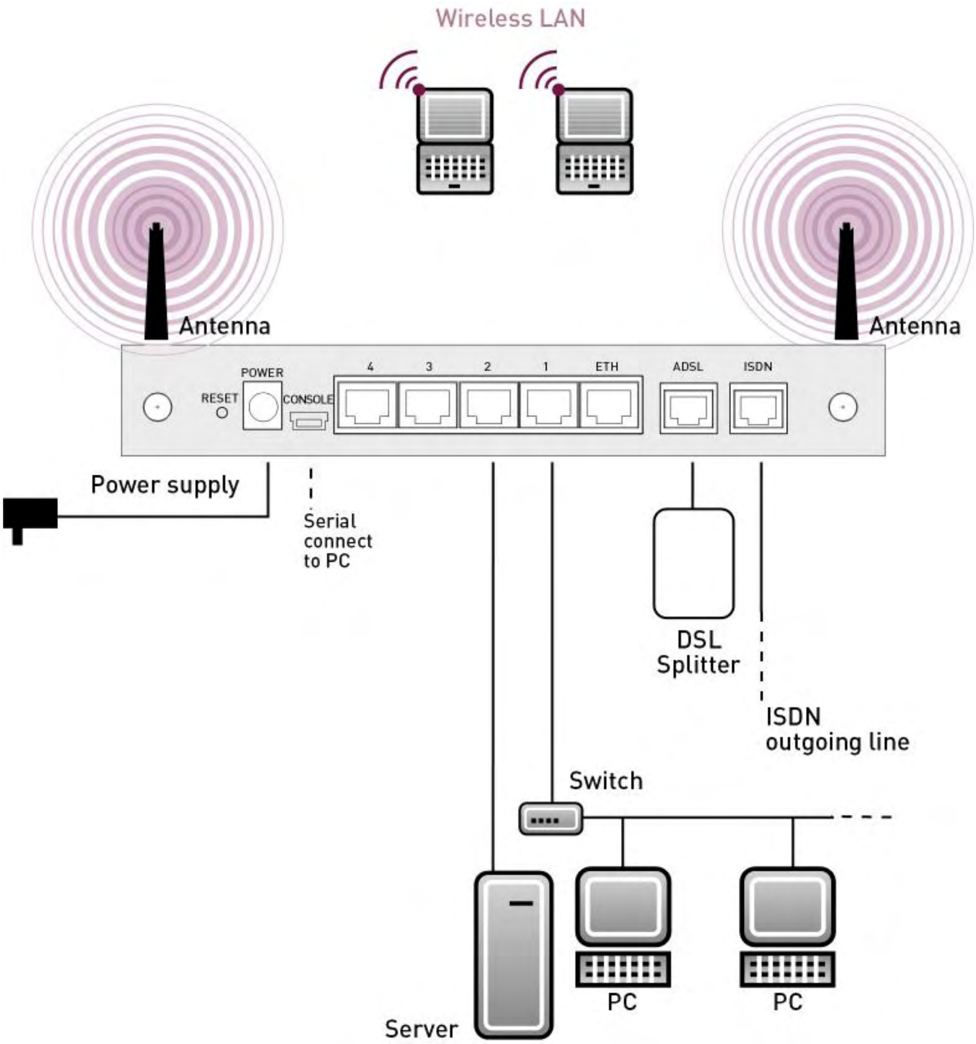


Fig. 2: Connection options using the example of **bintec R232bw**

When setting up and connecting, carry out the steps in the following sequence (refer to the connection diagrams for the individual devices in chapter *Technical data* on page 20):

(1) Antennas: Screw the two external standard antennas supplied to the RSMA connections provided for this purpose (only **bintec R230aw** and **bintec R232bw**).

(2) Place your device on a solid, level base.

(3) LAN: For the standard configuration of your device via Ethernet, connect the first switch port (**1**) of your device to your LAN using the Ethernet cable supplied. The device automatically detects whether it is connected to a switch or directly to a PC.

(4) ADSL: Connect the ADSL interface (**ADSL**) of your device to the DSL output of the

splitter using the DSL cable supplied.

(5) Mains connection: Connect the device to a mains socket using the mains adaptor supplied.

Optional connections

- ISDN: Connect the ISDN interface (**ISDN**) of the device to your ISDN socket using the ISDN cable provided (only **bintec R232a**, **bintec R232b** and **bintec R232bw**).
- DMZ: Connect the WAN interface (**ETH**) of your device to the Ethernet connection of your DMZ using another Ethernet cable (only **bintec R232a**, **bintec R232b** and **bintec R232bw**).
- Other LANs/WANs: Connect any other terminals in your network to the remaining switch ports (**2**, **3** or **4**) of your device using other Ethernet cables.
- Serial connection: For alternative configuration possibilities, connect the serial interface of your PC (**COM1** or **COM2**) to the serial interface of the gateway (**console**). Use only the serial cable supplied with the equipment. However, configuration via the serial interface is not provided by default.

The device is now prepared for configuration using the **Express Setup Wizard**.

3.2 Cleaning

You can clean your device easily. Use a damp cloth or antistatic cloth. Do not use solvents. Never use a dry cloth; the electrostatic charge could cause electronic faults. Make sure that no moisture can enter the device and cause damage.

3.3 Support information

If you have questions about your product or are looking for additional information, the Funkwerk Enterprise Communications GmbH Support Centre can be reached Monday to Friday between the hours of 8.00 am and 5 pm. They can be contacted as follows:

Email	hotline@funkwerk-ec.com
International Support Coordination	Telephone: +49 911 9673 1550 Fax: +49 911 9673 1599
End-customer Hotline	0900 1 38 65 93 (€1.10/min on land-lines in Germany)

For detailed information on our support services, contact *www.funkwerk-ec.com* .

Chapter 4 Basic configuration

You configure your device using the **Funkwerk Configuration Interface**.

A few basic configurations are required for use as a gateway. In this chapter, you will learn how to prepare the configuration, which data you have to collect first, how to perform configuration for a conventional ADSL connection, set up a WLAN, make adjustments to the PC configurations in the network if necessary and test the connection when the configuration has been completed. Detailed knowledge of networks is not necessary. A detailed online help system gives you extra support.

4.1 Presettings

4.1.1 IP configuration

Your device is shipped with a pre-defined IP configuration:

- **IP Address**: *192.168.0.254*
- **Netmask**: *255.255.255.0*

Use the following access data to configure your device in an ex works state:

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

Note

All **bintec** devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. Make sure you change the passwords to prevent unauthorised access to your device!

Furthermore, the device is factory configured as a DHCP server so that it can provide PCs on your LAN that have no IP configuration with all the information required for a connection. Steps for setting use of your PC to automatically obtain an IP configuration are described in *Configuring a PC* on page 13.

Note

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

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

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

4.1.2 Software update

Your device contains the version of the system software available at the time of production. More recent versions may have since been released. You can easily perform an update with the **Funkwerk Configuration Interface** using the **Maintenance**->**Software &Configuration**menu.

For a description of the update procedure, see *Software Update* on page 17.

4.2 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 6 or 7, Mozilla Firefox Version 1.2 or higher
- Installed network card (Ethernet)
- DVD drive
- Installed TCP/IP protocol
- High colour display (more than 256 colours) for correct representation of the graphics.

4.3 Preparations

To prepare for configuration, you need to...

- have the data for the basic configuration and the Internet connection to hand and also gather the data needed for connecting the required WLAN clients.
- Check whether the PC from which you want to perform the configuration meets the ne-

cessary requirements.

You can also...

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

4.3.1 Gathering data

You can gather the main data for configuration with the **Funkwerk Configuration Interface** quickly, because you do not need any information that requires in-depth knowledge of networks.

In addition, you can have the device assign a valid IP configuration to all PCs, so time-consuming configuration of your LAN is not necessary. If necessary, you can use the sample values.

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

- Basic configuration (obligatory if your device is in the ex works state)
- Internet access (optional)
- Wireless LAN (optional, only for **bintec R230aw** and **bintec R232bw**).

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

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

Basic configuration

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

Basic information

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

Internet access over ADSL

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

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

Data for internet access over ADSL

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

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

Additional information for T-Online

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

Note

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

Wireless LAN (only bintec R230aw and bintec R232bw)

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

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

Note the following:

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

Data for the Wireless LAN configuration

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

4.3.2 Configuring a PC

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

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

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

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

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

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

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

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

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

Note

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

4.3.3 Modify system password

All **bintec** devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. Make sure you change the passwords to prevent unauthorised access to your device!

Proceed as follows:

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

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

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

(d) Click **OK**.

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

Note the following rules on password use:

- The password must not be easy to guess. Names, car registration numbers, dates of birth, etc. should not be chosen as passwords.
- The password should contain at least one character that is not a letter (special character or number).
- The password should be at least 8 characters long.
- Change your password regularly, e.g. every 90 days.

4.4 Setting up an internet connection

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

4.4.1 Internet connection over internal ADSL modem

All devices have an integrated ADSL2+ modem for establishing a fast Internet connection. To make it easier to configure an ADSL internet connection, the **Funkwerk Configuration Interface** has a wizard to guide you through the connection set-up process simply and quickly. A selection of preconfigured connections from leading providers (T-Home, Arcor) makes configuration even easier.

(1) In **Funkwerk Configuration Interface** select the **Assistants**->**Internet Access** menu.

(2) With **New** make a new entry and take over the **Connection Type** *`Internal ADSL Modem`*.

(3) Follow the steps shown by the wizard. The wizard has its own online help, which offers all of the information you may require.

(4) Once you have exited the wizard, save the configuration by clicking on the **Save configuration** button above the menu navigation.

4.4.2 Other internet connections

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

4.4.3 Testing the configuration

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

Carry out the following steps to test your device:

(1) Test the connection from any device in the local network to your device. In the Windows Start menu, click **Run** and enter `ping` followed by a space and then the IP address of your device (e.g. *`192.168.0.254`*). A window appears with the response `"Reply from..."`.

(2) Test Internet access by entering *www.funkwerk-ec.com* in the Internet browser. Funkwerk Enterprise Communications GmbH's Internet site offers you the latest news, updates and documentation.

Note

Incorrect configuration of the devices in your LAN may result in unwanted connections and increased charges! Monitor your device and make sure it only sets up connections at the times you want it to. Watch the LEDs on your device (LED for ISDN, ADSL and the Ethernet interface to which you have connected WANs).

4.5 Setting up wireless LAN

Proceed as follows to use your device (only bintec **bintec R230aw** and **bintec R232bw**) as an access point:

(1) In **Funkwerk Configuration Interface** select the **Assistants**->**Wireless LAN** menu.

(2) Follow the steps shown by the wizard. The wizard has its own online help, which offers all of the information you may require.

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

Configuring the WLAN Adapter under Windows XP

After installing the drivers for your WLAN card, Windows XP set up a new connection in the network environment. Proceed as follows to configure the Wireless LAN connection:

(1) Click on **Start** -> **Settings** and double-click on **Network Connections** -> **Wireless Network Connection**.

(2) On the left-hand side, select **Change Advanced Settings**.

(3) Go to the **Wireless networks** tab.

(4) Click **Add**.

Proceed as follows:

(1) Enter a **Network Name**, e.g. *Client-1*.

(2) Set **Network Authentication** to *WPA2-PSK*.

(3) Set **Data Encryption** to *AES*.

(4) Under **Network Key** and **Confirm Network Key**, enter the configured preshared key.

(5) Exit each menu with **OK**.

Note

Windows XP allows several menus to be modified. Depending on the configuration, the path to the wireless network connection you want to configure may be different to that described above.

4.6 Software Update

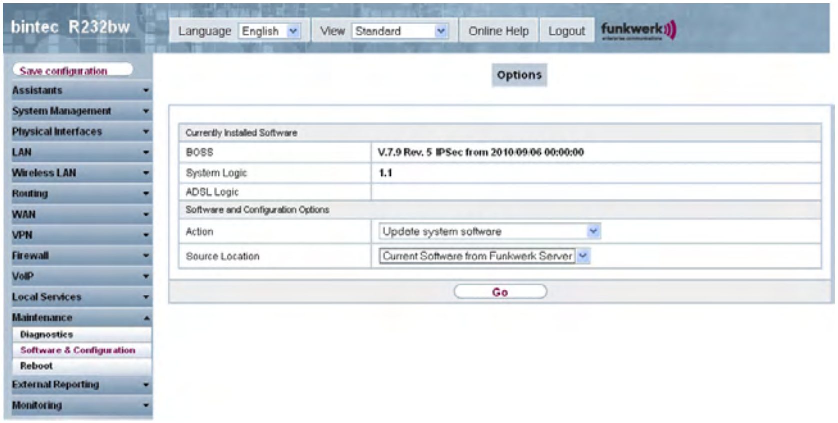
The range of functions of **bintec** devices is continuously being extended. These extensions are made available to you by Funkwerk Enterprise Communications GmbH free of charge. Checking for new software versions and the installation of updates can be carried out easily with the **Funkwerk Configuration Interface** . 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 Funkwerk Server`

(3) Confirm with **Go**.



Currently Installed Software	
BOSS	V.7.9 Rev. 5 IPSec from 2010-09-06 00:00:00
System Logic	1.1
ADSL Logic	
Software and Configuration Options	
Action	Update system software
Source Location	Current Software from Funkwerk Server

The device will now connect to the Funkwerk Enterprise Communications GmbH download server and check whether an updated version of the system software is available. If so, your device will be updated automatically. When installation of the new software is complete, you will be invited to restart the device.

Caution

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

Chapter 5 Reset

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

Practically al existing configuration data will then be ignored, only the current user passwords are retained. Configurations stored in the device are not deleted and can, if required, be reloaded when the device is rebooted.

Proceed as follows:

(1) Switch off your device.

(2) Press the **Reset** button on your device.

(3) Keep the **Reset** button on your device pressed down and switch the device back on.

(4) Look at the LEDs:
- The *Power* and *Status* LEDs come on first.
- The Ethernet LEDs (*1* to *4*) for the ports connected to the Ethernet then flash.
- The device runs through the boot sequence.
- After the *Status* LED has flashed five times, release the **Reset** button.

Proceed as follows if you also want to reset all the user passwords to the ex works state and delete stored configurations when resetting the device:

- Set up a serial connection to your device. Reboot your device and monitor the boot sequence. Start the BOOTmonitor and choose **(4) Delete Configuration** and following the instructions.

or

- Carry out the reset procedure described above with the **Reset** button. Next establish a serial connection or a Telnet connection (Telnet: Use the IP address of the ex works standard settings) for your device. At the login prompt enter `erase bootconfig` as the **Login** in the command line. Leave the password empty and press the Return key. The device runs through the boot sequence again.

Note

if you delete the boot configuration via the **Funkwerk Configuration Interface** (Menu **Maintenance**->**Software &Configuration**) all passwords are also reset and the current boot configuration is deleted. The next time, the device will boot with the standard ex works settings.

You can now configure your device again as described from *Basic configuration* on page 9

.

Chapter 6 Technical data

This chapter summarises all the hardware characteristics of the **bintec R230a**, **bintec R230b**, **bintec R230aw**, **bintec R232a**, **bintec R232b** and **bintec R232bw** devices.

6.1 Scope of supply

Your device is supplied with the following parts:

	Cable sets/mains unit/ other	**Software**	**Documentation**
bintec R230a	Ethernet cable DSL cable Serial connecting cable Mains unit	Companion DVD	Quick Install Guide (printed) User's Guide (on DVD) Release Notes, if required Safety notices
bintec R230b	Ethernet cable DSL cable Serial connecting cable Mains unit	Companion DVD	Quick Install Guide (printed) User's Guide (on DVD) Release Notes, if required Safety notices
bintec R230aw	Ethernet cable DSL cable Serial connecting cable Mains unit 2 standard antennas	Companion DVD	Quick Install Guide (printed) User's Guide (on DVD) Release Notes, if required Safety notices
bintec R232a	Ethernet cable DSL cable ISDN cable Serial connecting cable Mains unit	Companion DVD	Quick Install Guide (printed) User's Guide (on DVD) Release Notes, if required Safety notices
bintec	Ethernet cable	Companion DVD	Quick Install Guide (printed)

	Cable sets/mains unit/ other	Software	Documentation
R232b	DSL cable ISDN cable Serial connecting cable Mains unit		User's Guide (on DVD) Release Notes, if required Safety notices
bintec R232bw	Ethernet cable DSL cable ISDN cable Serial connecting cable Mains unit 2 standard antennas	Companion DVD	Quick Install Guide (printed) User's Guide (on DVD) Release Notes, if required Safety notices

6.2 General Product Features

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

The features are summarised in the following table:

General product features bintec R230a, bintec R230b, bintec R230aw

Product name	bintec R230a	bintec R230b	bintec R230aw
Dimensions and weights:			
Equipment dimensions without cable (B x H x D):	158 mm x 25.7 mm x 123.1 mm	158 mm x 25.7 mm x 123.1 mm	158 mm x 25.7 mm x 123.1 mm
Weight	approx. 550 g	approx. 550 g	approx. 550 g
Transport weight (incl. documentation, cables, packaging)	approx. 1.2 kg	approx. 1.2 kg	approx. 1.2 kg
Memory	32 MB SDRAM, 8 MB flash ROM	32 MB SDRAM, 8 MB flash ROM	32 MB SDRAM, 8 MB flash ROM
LEDs	11 (1x Power, 4x2 Ether-	11 (1x Power, 4x2 Ether-	12 (1x Power, 4x2 Ether-

Product name	**bintec R230a**	**bintec R230b**	**bintec R230aw**
	net, 1x Status, 1x ADSL)	net, 1x Status, 1x ADSL)	net, 1x WLAN, 1x Status, 1x ADSL)
Power consumption of the device	4.7 Watt	4.7 Watt	4.7 Watt
Voltage supply	12 V DC 500 mA EU PSU	12 V DC 500 mA EU PSU	12 V DC 800 mA EU PSU
Environmental requirements:			
Storage temperature	-20 # to +70 #	-20 # to +70 #	-25 # to +70 #
Operating temperature	0° to 40 #	0° to 40 #	0° to 40 #
Relative atmospheric humidity	10 % to 90 % non-condensing in operation, 5 % to 95 % non-condensing when stored	10 % to 90 % non-condensing in operation, 5 % to 95 % non-condensing when stored	10 % to 90 % non-condensing in operation, 5 % to 95 % non-condensing when stored
Room classification	Only use in dry rooms.	Only use in dry rooms.	Only use in dry rooms.
Available interfaces:			
ADSL interface	Internal ADSL modem for Annex A	Internal ADSL modem for Annex B	Internal ADSL modem for Annex A
Serial interface V.24	Permanently installed, supports Baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud	Permanently installed, supports Baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud	Permanently installed, supports Baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
Ethernet IEEE 802.3 LAN (4-port switch)	Permanently installed (twisted pair only), 10/100 mbps, auto-sensing, MDIX	Permanently installed (twisted pair only), 10/100 mbps, auto-sensing, MDIX	Permanently installed (twisted pair only), 10/100 mbps, auto-sensing, MDIX
WLAN interface (antennas)	-		802.11b and 802.11g with Antenna Diversity Data rates 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 mbps 1-, 2-, 5.5-, 6-, 9-, 11-, 12-, 18-, 24-,

Product name	**bintec R230a**	**bintec R230b**	**bintec R230aw**
			36-, 48-, 54 mbps
Available sockets:			
Serial interface V.24	5-pole mini USB socket	5-pole mini USB socket	5-pole mini USB socket
Ethernet interface	RJ45 socket	RJ45 socket	RJ45 socket
ADSL interface	RJ11 socket	RJ11 socket	RJ11 socket
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	R&TTE Directive 1999/5/EC CE symbol for all EU states
SAFERNET TM Security Technology	Community passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN with PPTP or IPSec	Community passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN with PPTP or IPSec	Community passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN with PPTP or IPSec
Software supplied	Dime Manager (on DVD)	Dime Manager (on DVD)	Dime Manager (on DVD)
Printed documentation supplied	Quick Install Guide and safety notices funkwerk Dime Manager User's Guide (on DVD)	Quick Install Guide and safety notices funkwerk Dime Manager User's Guide (on DVD)	Quick Install Guide and safety notices funkwerk Dime Manager User's Guide (on DVD)
Online documentation	User's Guide Workshops MIB reference	User's Guide Workshops MIB reference	User's Guide Workshops MIB reference

General product features bintec R232a, bintec R232b, bintec R232bw

Product name	**bintec R232a**	**bintec R232b**	**bintec R232bw**
Dimensions and weights:			
Equipment dimensions without cable (B x H x	189.2 mm x 27 mm x 123.1 mm	189.2 mm x 27 mm x 123.1 mm	189.2 mm x 27 mm x 123.1 mm

Product name	bintec R232a	bintec R232b	bintec R232bw
D):			
Weight	approx. 550 g	approx. 550 g	approx. 550 g
Transport weight (incl. documentation, cables, packaging)	approx. 1.2 kg	approx. 1.2 kg	approx. 1.2 kg
Memory	32 MB SDRAM, 8 MB flash ROM	32 MB SDRAM, 8 MB flash ROM	32 MB SDRAM, 8 MB flash ROM
LEDs	13 (1x Power, 4x2 Ethernet, 1x ETH, 1x Status, 1x ADSL, 1x ISDN)	13 (1x Power, 4x2 Ethernet, 1x ETH, 1x Status, 1x ADSL, 1x ISDN)	14 (1x Power, 4x2 Ethernet, 1x ETH, 1x WLAN, 1x Status, 1x ADSL, 1x ISDN)
Power consumption of the device	4.7 Watt	4.7 Watt	4.7 Watt
Voltage supply	12 V DC 800 mA EU PSU	12 V DC 800 mA EU PSU	12 V DC 800 mA EU PSU
Environmental requirements:			
Storage temperature	-25 # to +70 #	-20 # to +70 #	-20 # to +70 #
Operating temperature	0° to 40 #	0° to 40 #	0° to 40 #
Relative atmospheric humidity	10 % to 90 % non-condensing in operation, 5 % to 95 % non-condensing when stored	10 % to 90 % non-condensing in operation, 5 % to 95 % non-condensing when stored	10 % to 90 % non-condensing in operation, 5 % to 95 % non-condensing when stored
Room classification	Only use in dry rooms.	Only use in dry rooms.	Only use in dry rooms.
Available interfaces:			
ADSL interface	Internal ADSL modem for Annex A	Internal ADSL modem for Annex B	Internal ADSL modem for Annex B
Serial interface V.24	Permanently installed, supports Baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600,	Permanently installed, supports Baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600,	Permanently installed, supports Baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600,

Product name	bintec R232a	bintec R232b	bintec R232bw
	115200 Baud	115200 Baud	115200 Baud
Ethernet IEEE 802.3 LAN (4-port switch)	Permanently installed (twisted pair only), 10/100 mbps, auto-sensing, MDIX	Permanently installed (twisted pair only), 10/100 mbps, auto-sensing, MDIX	Permanently installed (twisted pair only), 10/100 mbps, auto-sensing, MDIX
ISDN-WAN S0	Permanently installed	Permanently installed	Permanently installed
ETH	Additional Ethernet switch port	Additional Ethernet switch port	Additional Ethernet switch port
WLAN interface (antennas)	-		802.11b and 802.11g with Antenna Diversity Data rates 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 mbps 1-, 2-, 5.5-, 6-, 9-, 11-, 12-, 18-, 24-, 36-, 48-, 54 mbps
Available sockets:			
Serial interface V.24	5-pole mini USB socket	5-pole mini USB socket	5-pole mini USB socket
Ethernet interface	RJ45 socket	RJ45 socket	RJ45 socket
ISDN interface	RJ45 socket	RJ45 socket	RJ45 socket
ADSL interface	RJ11 socket	RJ11 socket	RJ11 socket
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	R&TTE Directive 1999/5/EC CE symbol for all EU states
SAFERNET TM Security Technology	Community passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN with PPTP or IPSec	Community passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN with PPTP or IPSec	Community passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN with PPTP or IPSec

Product name	**bintec R232a**	**bintec R232b**	**bintec R232bw**
Software supplied	Dime Manager (on DVD)	Dime Manager (on DVD)	Dime Manager (on DVD)
Printed documentation supplied	Quick Install Guide and safety notices funkwerk Dime Manager User's Guide (on DVD)	Quick Install Guide and safety notices funkwerk Dime Manager User's Guide (on DVD)	Quick Install Guide and safety notices funkwerk Dime Manager User's Guide (on DVD)
Online documentation	User's Guide Workshops MIB reference	User's Guide Workshops MIB reference	User's Guide Workshops MIB reference

6.3 LEDs

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

The LEDs on **bintec R230a** / **bintec R230b** are arranged as follows:

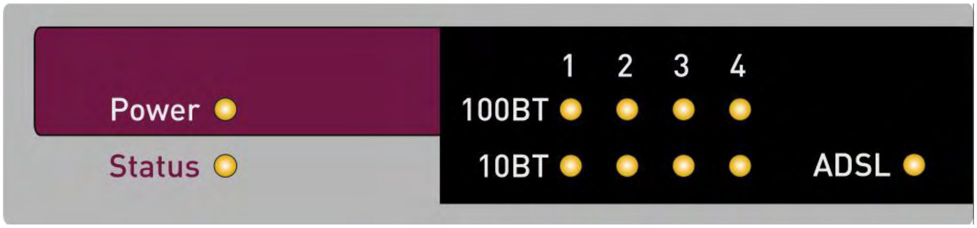


Fig. 3: LEDs of **bintec R230a** / **bintec R230b**

In operation mode, the LEDs on **bintec R230a** / **bintec R230b** display the following status information for your device:

LED status display

LED	Status	Information
Power	on	The power supply is connected.
Status	on	The device has started.
	flashing	The device is active.
1 to 4	on	The device is connected to the Ethernet (100 mbps or 10 mbps).

LED	Status	Information
	flashing	Data traffic via the Ethernet Interface (100 mbps or 10 mbps).
ADSL	on	ADSL connection is active.

The LEDs on **bintec R230aw** are arranged as follows:

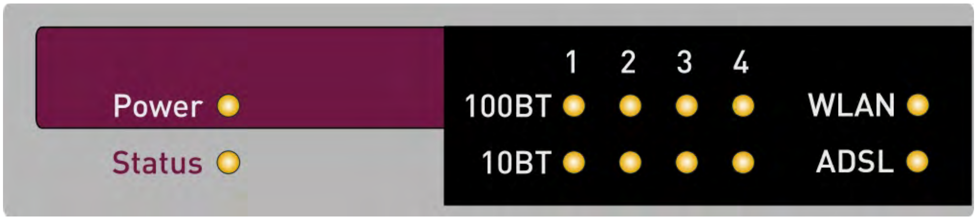


Fig. 4: LEDs of **bintec R230aw**

In operation mode, the LEDs on **bintec R230aw** display the following status information for your device:

LED status display

LED	Status	Information
Power	on	The power supply is connected.
Status	on	The device has started.
	flashing	The device is active.
1 to 4	on	The device is connected to the Ethernet (100 mbps or 10 mbps).
	flashing	Data traffic via the Ethernet Interface (100 mbps or 10 mbps).
WLAN	on	The WLAN module is active.
	flashing	Data traffic via the WLAN interface.
ADSL	on	ADSL connection is active.

The LEDs on **bintec R232a** / **bintec R232b** are arranged as follows:

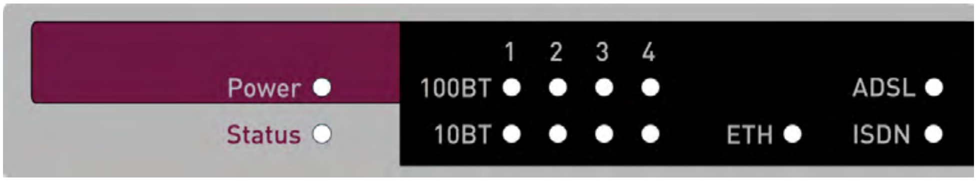


Fig. 5: LEDs of **bintec R232a** / **bintec R232b**

In operation mode, the LEDs on **bintec R232a** / **bintec R232b** display the following status information for your device:

LED status display

LED	Status	Information
Power	on	The power supply is connected.
Status	on	The device has started.
	flashing	The device is active.
1 to 4	on	The device is connected to the Ethernet (100 mbps or 10 mbps).
	flashing	Data traffic via the Ethernet Interface (100 mbps or 10 mbps).
ETH	on	The device is connected to the Ethernet.
	flashing	Data traffic via the Ethernet interface.
ADSL	on	ADSL connection is active.
ISDN	on	One B channel is used.
	flashing	Both B channels are in use.

The LEDs on **bintec R232bw** are arranged as follows:

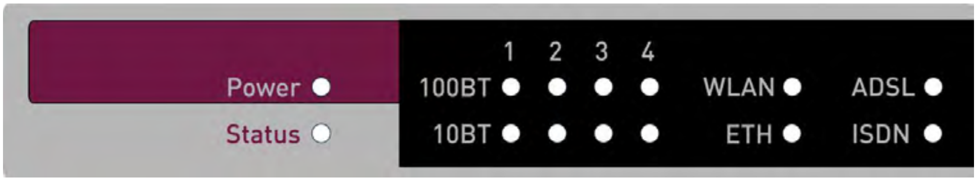


Fig. 6: LEDs of **bintec R232bw**

In operation mode, the LEDs on **bintec R232bw** display the following status information for your device:

LED status display

LED	Status	Information
Power	on	The power supply is connected.
Status	on	The device has started.
	flashing	The device is active.
1 to 4	on	The device is connected to the Ethernet (100 mbps or 10 mbps).
	flashing	Data traffic via the Ethernet Interface (100 mbps or 10 mbps).
WLAN	on	The WLAN module is active.
	flashing	Data traffic via the WLAN interface.
ETH	on	The device is connected to the Ethernet.
	flashing	Data traffic via the Ethernet interface.
ADSL	on	ADSL connection is active.
ISDN	on	One B channel is used.
	flashing	Both B channels are in use.

6.4 Connectors

All the connections are located on the back of the device.

bintec R230a and **bintec R230b** have a 4 port Ethernet switch, an ADSL interface and also a serial interface.

The connections are arranged as follows:

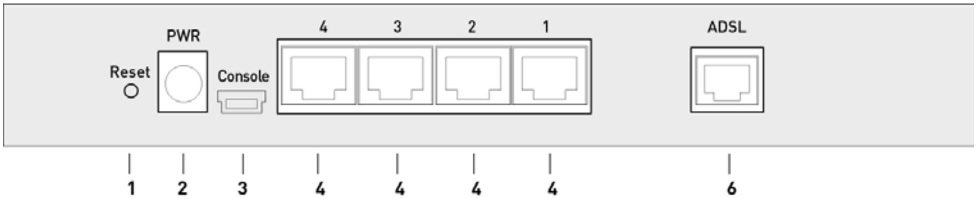


Fig. 7: **bintec R230a** / **bintec R230b** *rear panel*

Back of bintec R230a / bintec R230b

1	Reset	Reset button
2	PWR	Socket for plug-in power pack
3	Console	Serial interface
4	4/3/2/1	10/100 Base-T Ethernet interface
6	ADSL	ADSL interface

bintec R230aw has a 4 port Ethernet switch, an ADSL interface and also a serial interface.

The connections are arranged as follows:

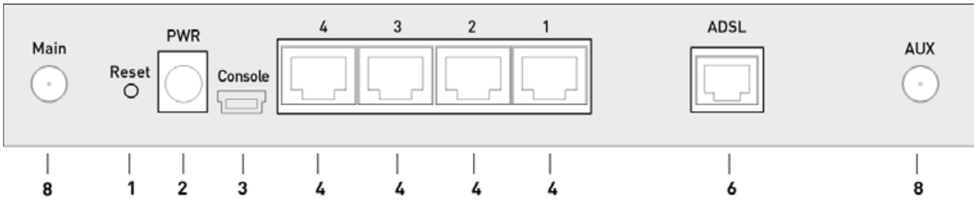


Fig. 8: **bintec R230aw** *rear panel*

Back of bintec R230aw

1	Reset	Reset button
2	PWR	Socket for plug-in power pack
3	Console	Serial interface
4	4/3/2/1	10/100 Base-T Ethernet interface
6	ADSL	ADSL interface
8	Main/AUX	RSMA connection

bintec R232a and **bintec R232b** have a 4 port Ethernet switch, an ADSL interface and also a serial interface.**bintec R232a** and **bintec R232b** also has a separate ETH/DMZ port and an ISDN interface.

The connections are arranged as follows:

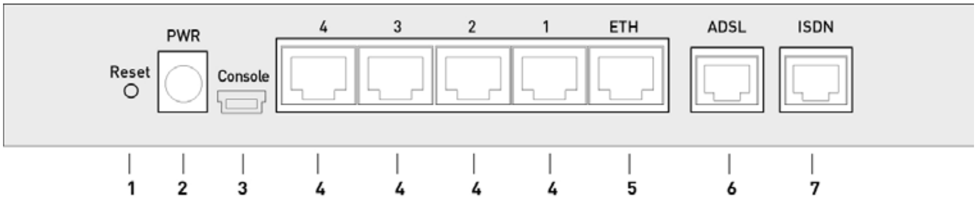


Fig. 9: **bintec R232a** / **bintec R232b** *rear panel*

Back of bintec R232a / bintec R232b

1	Reset	Reset button
2	PWR	Socket for plug-in power pack
3	Console	Serial interface
4	4/3/2/1	10/100 Base-T Ethernet interface
5	ETH	Ethernet interface
6	ADSL	ADSL interface
7	ISDN	ISDN interface

bintec R232bw has a 4 port Ethernet switch, an ADSL interface and also a serial interface. **bintec R232bw** also has a separate ETH/DMZ port and an ISDN interface.

The connections are arranged as follows:

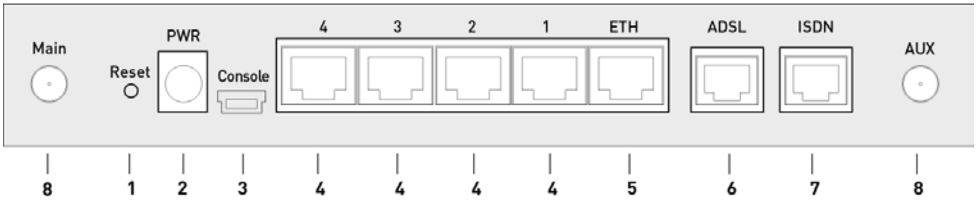


Fig. 10: **bintec R232bw** *rear panel*

Back of bintec R232bw

1	Reset	Reset button
2	PWR	Socket for plug-in power pack
3	Console	Serial interface
4	4/3/2/1	10/100 Base-T Ethernet interface
5	ETH	Ethernet interface

6	ADSL	ADSL interface
7	ISDN	ISDN interface
8	Main/AUX	RSMA connection

6.5 Pin Assignments

6.5.1 Serial interface

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

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

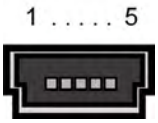


Fig. 11: 5-pole mini USB socket

The pin assignment is as follows:

Pin assignment of the mini USB socket

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

6.5.2 Ethernet interface

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

The connection is made via an RJ45 socket. **bintec R232a**, **bintec R232b** and **bintec R232bw** also have a fifth Ethernet interface.

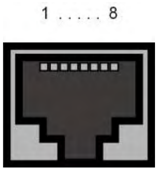


Fig. 12: Ethernet 10/100 Base-T interface (RJ45 socket)

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

RJ45 socket for LAN connection

Pin	Function
1	TD +
2	TD -
3	RD +
4	Not used
5	Not used
6	RD -
7	Not used
8	Not used

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

6.5.3 ADSL interface

The ADSL interface is connected via an RJ11 plug. The cable supplied connects the RJ11 plug needed for the device to an RJ11 plug needed for most ADSL splitters.

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

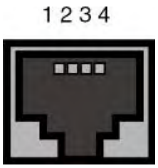


Fig. 13: ADSL interface (RJ11)

The pin assignment for the ADSL interface (RJ11 socket) is as follows:

RJ11 socket for ADSL connection

Pin	Function
1	Not used
2	a
3	b
4	Not used

6.5.4 ISDN S0 port

bintec R232a, **bintec R232b** and **bintec R232bw** have an additional ISDN-S0 interface, which can be used for backup functions, for example.

The connection is made via an RJ45 socket.

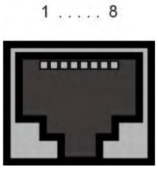


Fig. 14: ISDN S0 BRI interface (RJ45 socket)

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

RJ45 socket for ISDN connection

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

6.6 WEEE information

The waste container symbol with the »X« through it on the device indicates that the device must be disposed of separately from normal domestic waste at an appropriate waste disposal facility at the end of its useful service life.

Das auf dem Gerät befindliche Symbol mit dem durchgekreuzten Müllcontainer bedeutet, dass das Gerät am Ende der Nutzungsdauer bei den hierfür vorgesehenen Entsorgungsstellen getrennt vom normalen Hausmüll zu entsorgen ist.

Le symbole se trouvant sur l'appareil et qui représente un conteneur à ordures barré signifie que l'appareil, une fois que sa durée d'utilisation a expiré, doit être éliminé dans des poubelles spéciales prévues à cet effet, de manière séparée des ordures ménagères courantes.

Il simbolo raffigurante il bidone della spazzatura barrato riportato sull'apparecchiatura significa che alla fine della durata in vita dell'apparecchiatura questa dovrà essere smaltita separatamente dai rifiuti domestici nei punti di raccolta previsti a tale scopo.

El símbolo del contenedor con la cruz, que se encuentra en el aparato, significa que cuando el equipo haya llegado al final de su vida útil, deberá ser llevado a los centros de recogida previstos, y que su tratamiento debe estar separado del de los residuos urbanos.

Symbolen som sitter på apparaten med den korsade avfallstunnan betyder att apparaten när den tjänat ut ska kasseras och lämnas till de förutsedda sortergårdarna och skiljas från normalt hushållsavfall.

Tegnet på apparatet som viser en avfallcontainer med et kyss over, betyr at apparatet må kastet på hertil egnet avfallssted og ikke sammen med vanlig avfall fra husholdningen.

Το σύμβολο που βρίσκεται στην συσκευή με το σταυρωμένο κοντέϊνερ απορριμμάτων σημαίνει, ότι η συσκευή στο τέλος της διάρκειας χρήσης της πρέπει να διατεθεί ξεχωριστά από τα κανονικά απορρίμματα στα γι' αυτό τον σκοπό προβλεπόμενα σημεία διάθεσης.

Symbolet med gennemkrydset affaldsbeholder på apparatet betyder, at apparatet, når det ikke kan bruges længere, skal bortskaffes adskilt fra normalt husholdningsaffald på et af de dertil beregnede bortskaffelsessteder.

Znajdujący się na urządzeniu symbol przekreślonego pojemnika na śmieci oznacza, że po upływie żywotności urządzenia należy go oddać do odpowiedniej placówki utylizacyjnej i nie wyrzucać go do normalnych śmieci domowych.

Het doorgehaalde symbool van de afvalcontainer op het apparaat betekent dat het apparaat op het einde van zijn levensduur niet bij het normale huisvuil mag worden verwijderd. Het moet bij een erkend inzamelpunt worden ingeleverd.

O símbolo com um caixote de lixo riscado, que se encontra no aparelho, significa, que o aparelho no fim da sua vida útil deve ser eliminado separadamente do lixo doméstico nos centros de recolha adequados.

Chapter 7 Access and configuration

This chapter describes all the access and configuration options.

7.1 Access Options

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

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

- Via your LAN
- Via the serial interface
- Via an ISDN connection (only **bintec R232a**, **bintec R232b** and **bintec R232bw**)

7.1.1 Access via LAN

Access via one of the Ethernet interfaces of your device allows you to open the **Funkwerk Configuration Interface** in a web browser for configuration purposes and to access your device via Telnet or SSH.

⚠ **Caution**

If you carry out the initial configuration with the **Funkwerk Configuration Interface**, this can result in inconsistencies or malfunctions, as soon as you carry out additional settings using other configuration options. Therefore, it is recommended that the configuration is continued with the **Funkwerk Configuration Interface**. If you use SNMP shell commands, continue with this configuration method.

7.1.1.1 HTTP/HTTPS

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

- *http://192.168.0.254*

  or

- *https://192.168.0.254*

7.1.1.2 Telnet

Apart from configuration using a web browser, with a Telnet connection you can also access the SNMP shell and use other configuration options.

You do not need any additional software on your PC to set up a Telnet connection to your device: Telnet is available on all operating systems.

Proceed as follows:

Windows

(1) Click **Run…** in the Windows Start menu.

(2) Enter `telnet <IP address of your device>`.

(3) Click **OK**.
A window with the login prompt appears. You are now in the SNMP shell of your device.

(4) Continue with *Logging in for Configuration* on page 42.

Unix

You can also set up a Telnet connection on UNIX and Linux without any problem:

(1) Enter `telnet <IP address of your device>` in a terminal.
A window with the login prompt appears. You are now in the SNMP shell of your device.

(2) Continue with *Logging in for Configuration* on page 42.

7.1.1.3 SSH

In addition to the unencrypted and potentially viewable Telnet session, you can also connect to your device via an SSH connection. This is encrypted, so all the remote maintenance options can be carried out securely.

The following preconditions must be met in order to connect to the device via SSH:

- The encryption keys needed for the process must be available on the device.
- An SSH client must be installed on your PC.

Encryption keys

First of all, make sure that the keys for encrypting the connection are available on your device:

(1) Log in to one of the types already available on your device (e.g. via Telnet - for login

see *Logging in* on page 41).

(2) Enter `update -i` for the input prompt. You are now in the Flash Management shell.

(3) Call up a list of all the files saved on the device: `ls -al`.

If you see a display like the one below, the keys needed are already there and you can connect to the device via SSH:

```
Flash-Sh > ls -al

Flags Version Length Date Name ...

Vr-xpbc-B 7.1.04 2994754 2004/09/02 14:11:48 box150_srel.ppc860

Vrw-pl--f 0.0 350 2004/09/07 10:44:14 sshd_host_rsa_key.pub

Vrw-pl--f 0.0 1011 2004/09/07 10:44:12 sshd_host_rsa_key

Vrw-pl--f 0.0.01 730 2004/09/07 10:42:17 sshd_host_dsa_key.pub

Vrw-pl--f 0.0.01 796 2004/09/07 10:42:16 sshd_host_dsa_key

Flash-Sh >
```

Note

The device generates a key pair for each of the algorithms (RSA and DSA), i.e. two files must be stored in the flash for each algorithm (see example at above).

If no keys are available, you have to generate these first. Proceed as follows:

(1) Leave the Flash Management shell with `exit`.

(2) Launch the **Funkwerk Configuration Interface** and log on to your device (see *Calling up Funkwerk Configuration Interface* on page 45).

(3) Make sure that *Deutsch* is selected as the language.

(4) Check the key status in the **System Management**->**Administrative Access**->**SSH** menu. If both keys are available, you'll see in both fields **RSA Key Status** and **DSA Key Status** the value *Generated*

(5) If one or both of these fields contains the value *Not generated*, you must generate the relevant key. To have the device generate the key, click **Generate**.
The device generates the corresponding key and stores it in the FlashROM. *Generated* indicates successful generation.

(6) Make sure that both keys have been successfully generated. If necessary, repeat the procedure described above.

Login via SSH

Proceed as follows to log in on your device via SSH:

If you have made sure that all the keys needed are available on the device, you have to check whether an SSH client is installed on your PC. Most UNIX and Linux distributions install a SSH client by default. Additional software, e.g. PuTTY, usually has to be installed on a Windows PC.

Proceed as follows to log in on your device via SSH:

UNIX

(1) Enter `ssh <IP address of the device>` in a terminal.
The login prompt window appears. This is located in the SNMP shell of the device.

(2) Continue with *Logging in* on page 41.

Windows

(1) How an SSH connection is set up very much depends on the software used. Consult the documentation for the program you are using.
As soon as you have connected to the device, the login prompt window will appear. You are now in the SNMP shell of your gateway.

(2) Continue with *Logging in* on page 41.

Note

PuTTY requires certain settings for a connection to a **bintec** device. The support pages of *http://www.funkwerk-ec.com* include FAQs, which list the required settings.

7.1.2 Access via the Serial Interface

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

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

Windows

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

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

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

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

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

Check

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

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

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

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

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

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

(5) Click **OK**.

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

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

Unix

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

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

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

7.1.3 Access over ISDN

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

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

Note

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

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

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

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

(1) Connect your device to the ISDN.

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

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

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

Continue with *Logging in for Configuration* on page 42.

7.2 Logging in

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.

7.2.1 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

User Name	Password	Authorisations
`admin`	`funkwerk`	Read and change system variables, store configurations; use **Funkwerk Configuration Interface** .
`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 on the Setup Tool screen 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** devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. How to change the passwords is described in on page .

Make sure you change the passwords to prevent unauthorised access to your device!

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

7.2.2 Logging in for Configuration

Set up a connection to the device. The access options are described in *Access Options* on page 36.

Funkwerk Configuration Interface

Log in via the HTML surface as follows:

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

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

The status page of the **Funkwerk Configuration Interface** opens in the browser.

SNMP shell

Log into the SNMP shell as follows:

(1) Enter your user name e.g. `admin`, and confirm with **Return**.

(2) Enter your user password e.g. `funkwerk`, and confirm with **Return**.

Your device logs in with the input prompt, e.g. `r232bw:>`. The login was successful. You are now in the SNMP shell.

To leave the SNMP shell after completing the configuration, enter `exit` and press **Return**.

7.3 Configuration options

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

You can configure your device in the following ways:

- **Funkwerk Configuration Interface**
- Assistant
- SNMP shell commands

Note

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

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

Types of connections and configurations

Type of connection	Possible types of configuration
LAN	Assistant, **Funkwerk Configuration Interface** , shell command

Type of connection	Possible types of configuration
Serial connection	Shell command

The following chapters describe the configuration based on **Funkwerk Configuration Interface**.

Note

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

7.3.1 Funkwerk Configuration Interface

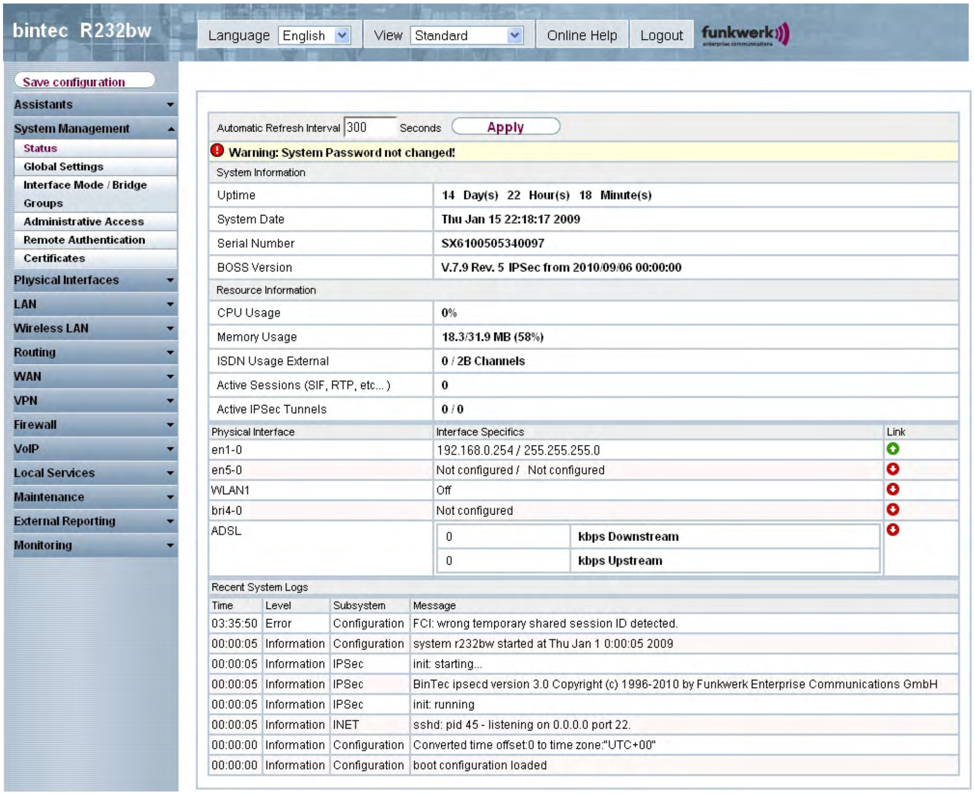
Funkwerk Configuration Interface is a web-based graphic user surface that you can use from any PC with an up-to-date Web browser via an HTTP or HTTPS connection.

With the **Funkwerk Configuration Interface** 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.funkwerk-ec.com* and installed on your device. To do this, proceed as described in *Options* on page 390.

The settings you make with the **Funkwerk Configuration Interface** are applied with the **OK** or **Apply** button of the menu, and you do not have to restart the device.

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

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



Automatic Refresh Interval 300 Seconds

Warning: System Password not changed!

System Information	
Uptime	14 Day(s) 22 Hour(s) 18 Minute(s)
System Date	Thu Jan 15 22:18:17 2009
Serial Number	SX6100505340097
BOSS Version	V.7.9 Rev. 5 IPSec from 2010/09/06 00:00:00
Resource Information	
CPU Usage	0%
Memory Usage	18.3/31.9 MB (58%)
ISDN Usage External	0 / 2B Channels
Active Sessions (SIF, RTP, etc...)	0
Active IPSec Tunnels	0 / 0

Physical Interface	Interface Specifics	Link
en1-0	192.168.0.254 / 255.255.255.0	🟢
en5-0	Not configured / Not configured	🔴
WLAN1	Off	🔴
bri4-0	Not configured	🔴
ADSL	0 kbps Downstream 0 kbps Upstream	🔴

Recent System Logs

Time	Level	Subsystem	Message
03:35:50	Error	Configuration	FCI: wrong temporary shared session ID detected.
00:00:05	Information	Configuration	system r232bw started at Thu Jan 1 0:00:05 2009
00:00:05	Information	IPSec	init: starting...
00:00:05	Information	IPSec	BinTec ipsecd version 3.0 Copyright (c) 1996-2010 by Funkwerk Enterprise Communications GmbH
00:00:05	Information	IPSec	init: running
00:00:05	Information	INET	sshd: pid 45 - listening on 0.0.0.0 port 22.
00:00:00	Information	Configuration	Converted time offset:0 to time zone:"UTC+00"
00:00:00	Information	Configuration	boot configuration loaded

Fig. 16: **Funkwerk Configuration Interface** *home page*

7.3.1.1 Calling up Funkwerk Configuration Interface

(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 6).

(2) Check the settings of the PC from which you want to configure your device (see *Configuring a PC* on page 13).

(3) Open a web browser.

(4) Enter `http://192.168.0.254` in the address field of the web browser.

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

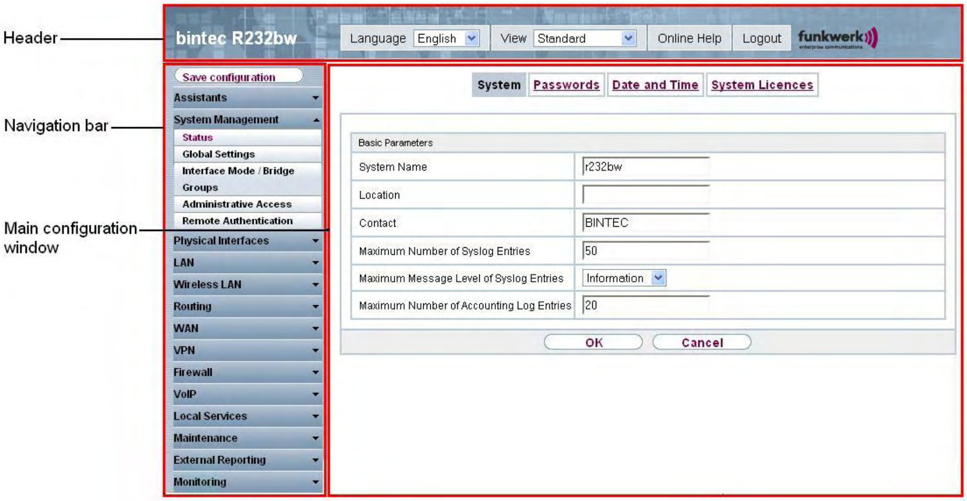
You are not in the status menu of your device's **Funkwerk Configuration Interface** (see *Status* on page 63).

7.3.1.2 Operating elements

Funkwerk Configuration Interface window

The **Funkwerk Configuration Interface** window is divided into three areas:

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



Basic Parameters

System Name	r232bw
Location	
Contact	BINTEC
Maximum Number of Syslog Entries	50
Maximum Message Level of Syslog Entries	Information
Maximum Number of Accounting Log Entries	20

Fig. 17: Areas of the **Funkwerk Configuration Interface**

Header

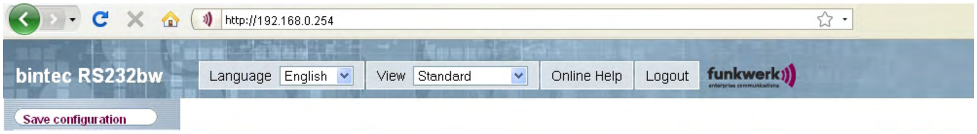


Fig. 18: **Funkwerk Configuration Interface** *header*

Funkwerk Configuration Interface header

Menu	Function
Language English	**Language selection**: In the dropdown menu, choose the language in which you want to display the **Funkwerk Configuration Interface**. Here you can choose the language in which you perform the configuration. German and English are available.
View Standard	**View**: Select the desired view from the dropdown menu. Standard and SNMP browsers can be selected.

Menu	Function
Online Help	**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.
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: • Save configuration, save previous boot configuration, then exit. • Save configuration, then exit. • Exit without saving.

Navigation bar

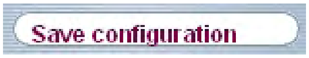


Fig. 19: Save Configuration button

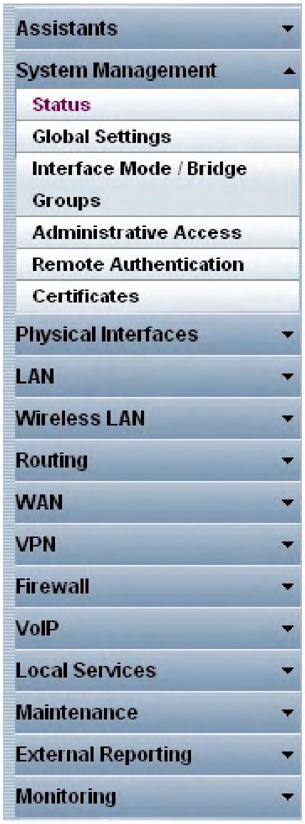


Fig. 20: Menus

The **Save configuration** button is found in the navigation bar.

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

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

You have the following two options:

- `Save configuration`, i.e. save the current configuration as the boot configuration
- `Save configuration with boot backup` i.e. save current configuration as boot configuration while also archiving previous boot configuration as backup.

If you want to load the archived boot configuration into your device, go to the **Maintenance**->**Software &Configuration** menu, select **Action** = `Import configuration` and click on **Go**. The archived backup is used as the current boot configuration.

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

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

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

Status page

If you call the **Funkwerk 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.

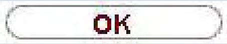
Main configuration window

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 **Funkwerk Configuration Interface** are triggered by means of the following buttons:

Funkwerk Configuration Interface buttons

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

Funkwerk Configuration Interface buttons for special functions

Button	Function
	In the **Access Point Discovery** menu, with this button you start

Button	Function
	the automatic recognition of all access points available in the network and connected by Ethernet.
Import	In the **System Management**->**Certificates**->**Certificate List** menu and the **System Management**->**Certificates**->**CRLs** menu, this button activates the sub-menus for configuration of the certificate or CRL imports.
Request	In the **System Management**->**Certificates**->**Certificate List** menu, this button activates the sub-menu for the configuration of the certificate request.
Release Call	In the **Monitoring**->**ISDN/Modem**->**Current Calls** menu, pressing this button ends the active calls selected in the 🗑 column.

Various icons indicate the following possible actions or statuses:

Funkwerk Configuration Interface symbols

Icon	Function
🗑	Deletes the list entry.
🔧	Displays the menu for changing the settings of an entry.
🔍	Displays the details for an entry.
⇕	Moves an entry. A combo box opens in which you can choose the list entry that selected entry is to be placed in front of/after.
☰	Creates another list entry first and opens the configuration menu.
⬇	Sets the status of the entry to `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 "Going up" status for an interface or connection.
🔒	Indicates that data traffic is encrypted.
📡	Triggers a WLAN bandscan.

Icon	Function
»	Displays the next page in a list.
«	Displays the previous page in a list.

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

Funkwerk Configuration Interface list options

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

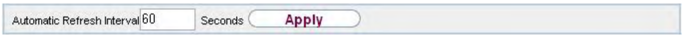

Automatic Refresh Interval 60 Seconds Apply

Fig. 21: Configuration of the update interval

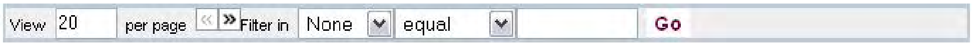
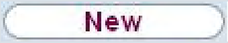
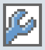
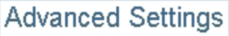

View 20 per page « » Filter in None equal Go

Fig. 22: Filter list

Structure of the Funkwerk Configuration Interface configuration menu

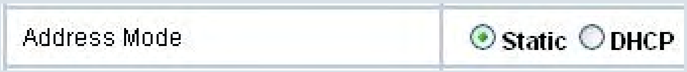
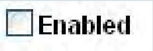
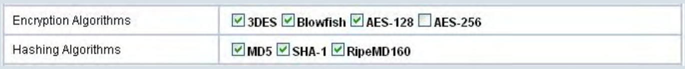
The menus of the **Funkwerk Configuration Interface** contain the following basic structures:

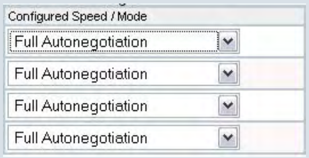
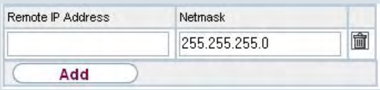
Funkwerk Configuration InterfaceMenu architecture

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:

Funkwerk Configuration Interface configuration elements

Menu	Function
Input fields	e.g. empty text field Text field with hidden input ●●●●●● Enter the data.
Radio buttons	e.g. Address Mode ● Static ○ DHCP Select the corresponding option.
Checkboxes	e.g. activation by selecting checkbox □ Enabled Selection of several possible options Encryption Algorithms ☑ 3DES ☑ Blowfish ☑ AES-128 □ AES-256 Hashing Algorithms ☑ MD5 ☑ SHA-1 ☑ RipeMD160
Dropdown menus	e.g.

Menu	Function
	 Configured Speed / Mode Full Autonegotiation Full Autonegotiation Full Autonegotiation Full Autonegotiation Click the arrow to open the list. Select the required option using the mouse.
Internal lists	e.g.  Remote IP Address | Netmask 255.255.255.0 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.

Warning symbols

Icon	Meaning
❗	This symbol appears in messages referring you to settings that were made with the Setup Tool.
⚠	This symbol appears in messages referring you to the fact that values were entered or selected incorrectly.

Pay particular attention to the following message:

"Warning: Changes not supported by the Setup Tool!" If you change them with the **Funkwerk Configuration Interface** , this can cause inconsistencies or malfunctions. Therefore, it is recommended that the configuration is continued with the Setup Tool.

7.3.1.3 Funkwerk Configuration InterfaceMenus

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.funkwerk-ec.com* .

The **Funkwerk Configuration Interface** contains the following menus:

Assistants

Menu	Function
First steps	In this menu you can make the basic settings that are required to add your gateway to your local network (LAN).
Internet Access	The wizard guides you through the individual configuration steps to connect your local network (LAN) to the internet.
VPN	In this menu you are guided through all of the settings that are required to set up your LAN-LAN connection as a virtual private network.
Wireless LAN	Wireless LAN involves the set-up of a network using wireless technology.
VoIP PBX in LAN	The assistant is required for specific PBX in the LAN, such as **Hybird** in order to guarantee SIP compatibility. To do this, external communication is carried out over a single IP address and NAT is realised as full-cone NAT.

System Management

Menu	Function
Status	In this menu, general information on your device is displayed at a glance. This information includes serial number, software version, current memory and processor use, status of the physical interfaces and the last 10 system messages.
Global Settings	In this menu, you enter the basic system settings of your device, such as, for example, system name, system date, system time

Menu	Function
	and passwords. You can also manage licences that are necessary for the use of certain functions.
Interface Mode / Bridge Groups	In this menu, you define the mode in which the interfaces of your device are to run (routing or bridging) and if necessary can define bridge groups.
Administrative Access	In this menu, you configure the access options for the individual interfaces.
Remote Authentication	In this menu, you configure the authentication via a RADIUS server or TACACS+ server.
Certificates	In this menu you can generate and import keys and have them certified.

Physical Interfaces

Menu	Function
Ethernet Ports	In this menu, you configure the Ethernet interfaces of your device. To do this, you select the speed and type of interface, for example.
ISDN Ports	Only for **R232a** , **R232b** und **R232bw**. In this menu, you configure the ISDN interface of your device. Here you enter data such as the type of ISDN connection to which your device is connected.
ADSL Modem	In this menu, you make the basic settings for your ADSL connection.

LAN

Menu	Function
IP Configuration	In this menu, you carry out the IP configuration of the LAN interfaces for your device.
VLAN	In this menu, you configure the VLANs.

Wireless LAN

Menu	Function
WLAN	In this menu, you configure your wireless modules as an access point or bridge.
Administration	In this menu, you make the basic WLAN settings.

Networking

Menu	Function
Routes	In this menu, you enter additional routes.
NAT	In this menu, you configure the NAT firewall (NAT, Network Address Translation).
Load Balancing	In this menu, you configure application-controlled bandwidth management.
QoS	In this menu, you configure all the "Quality of Service" settings.
Access Rules	In this menu, accesses to data and functions are restricted.

Routing Protocols

Menu	Function
RIP	In this menu, you configure the dynamic updating of the routing table via RIP.

Multicast

Menu	Function
General	In this menu, you enable or disable multicast routing.
IGMP	In this menu, you configure the interfaces on which IGMP is to be enabled.
Forwarding	In this menu, you specify which multicast groups are always passed between the interfaces of your device.

WAN

Menu	Function
Internet + Dialup	In this menu, you define the Internet connections for the various connection protocols or dialup connections.

Menu	Function
ATM	In this menu, you carry out configuration of the ATM profiles that are needed for all the ADSL connections and also connection monitoring (OAM) and ATM QoS.
Real Time Jitter Control	In this menu, you can optimise the low-bandwidth transmission of voice data packets.

VPN

Menu	Function
IPSec	In this menu, you configure VPN connections over IPSec.
L2TP	In this menu you configure the use of L2TP (Layer 2 Tunnelling Protocol).
PPTP	In this menu, you configure the an encrypted PPTP tunnel.
GRE	This menu shows a list of all configured GRE tunnels.

Firewall

Menu	Function
Policies	In this menu you configure the filter rules for the firewall.
Interfaces	In this menu, you can group together the interfaces to be filtered.
Addresses	In this menu, you can create the address aliases to be filtered.
Services	In this menu, you can create the service aliases to be filtered.

VoIP

Menu	Function
SIP	In this menu, you configure a network transition between various telecommunication networks.
RTSP	In this menu, you configure the use of the RealTime Streaming protocol.

Local Services

Menu	Function
DNS	In this menu, you configure the name resolution.
HTTPS	In this menu, you configure the port and certificate for a configuration session over HTTPS.
DynDNS Client	In this menu, you configure the dynamic name resolution.
DHCP Server	In this menu, you configure your device as a DHCP server.
Web Filter	In this menu, you configure the use of the URL-based Proventia Web Filter from ISS (*www.iss.net*).
CAPI Server	In this menu, you configure your device as a CAPI server.
Scheduling	In this menu, you configure time-dependent standard actions of your devices.
Surveillance	In this menu, you configure the surveillance of interfaces or hosts in the network.
ISDN Theft Protection	In this menu you can configure the ISDN theft protection function for each interface.
Funkwerk Discovery	In this menu, you can configure management functions for **bintec** Access Point.
UPnP	In this menu, you configure the UPnP settings individually for each interface of your gateway.
HotSpot Gateway	In this menu, you configure the bintec Hotspot Gateway.
BRRP	In this menu, you can configure a redundant network environment.

Maintenance

Menu	Function
Diagnostics	In this menu you can test the accessibility of hosts, DNS servers or routing.
Software &Configuration	In this menu, you manage your device's software version, configuration files and interface language.
Reboot	In this menu, you can initiate the rebooting of the device.

External Reporting

Menu	Function
Syslog	In this menu, you configure the host to which the data logged internally on the device is forwarded for saving and further processing.
IP Accounting	In this menu, you decide for which interfaces accounting messages are to be generated.
E-mail Alert	Depending on the configuration, in this menu e-mails are sent to the administrator as soon as relevant syslog messages occur.
SNMP	In this menu, you configure whether the device is to listen for external SNMP accesses and send SNMP traps.
Activity Monitor	In this menu, you configure the monitoring of your device with the Windows Tool Activity Monitor.

Monitoring

Menu	Function
Internal Log	In this menu, the system messages are displayed.
IPSec	In this menu, the IPSec connections and connection statistics that are currently active are displayed.
ISDN/Modem	In this menu, the ISDN connections are displayed.
Interfaces	In this menu, connection statistics and status of all interfaces are displayed.
WLAN	This menu shows you the WLAN connections statistics.
Bridges	In this menu you can view the current values of the configured bridges.
HotSpot Gateway	This menu shows a list of all bintec Hotspot users.
QoS	In this menu, statistics are displayed for all interfaces for which QoS has been configured.

SNMP Browser

If you select the *SNMP Browser* option under **View** header, you will see an HTML view of all internal system MIB tables and can modify the saved values. This view is only provided for professional configuration and extended monitoring.

SNMP (Simple Network Management Protocol) is a protocol that allows access for configuring your device. All configuration parameters are stored in the MIB (Management Information Base) in the form of MIB tables and MIB variables. You can read and modify these directly via the SNMP browser.

⚠ **Caution**

This configuration method assumes an in-depth system knowledge of Funkwerk devices!

7.3.2 SNMP shell

SNMP (Simple Network Management Protocol) is a protocol that defines how you can access the configuration settings.

All configuration settings are stored in the MIB (Management Information Base) in the form of MIB tables and MIB variables. You can access these directly from the SNMP shell via SNMP commands. This type of configuration requires a detailed knowledge of our devices.

7.4 BOOTmonitor

The BOOTmonitor is only available over a serial connection to the device.

The BOOTmonitor provides the following functions, which you select by entering the corresponding number:

(1) Boot System (reboot the system):
The device loads the compressed boot file from the flash memory to the working memory. This happens automatically on starting.

(2) Software Update via TFTP:
The devices performs a software update via a TFTP server.

(3) Software Update via XMODEM:
The device performs a software update via a serial interface with XMODEM.

(4) Delete configuration:
The device is reset to the ex works state. All configuration files are deleted and the BOOTmonitor settings are set to the default values.

(5) Default BOOTmonitor Parameters:
You can change the default settings of the BOOTmonitor of the device, e.g. the baud rate for serial connections.

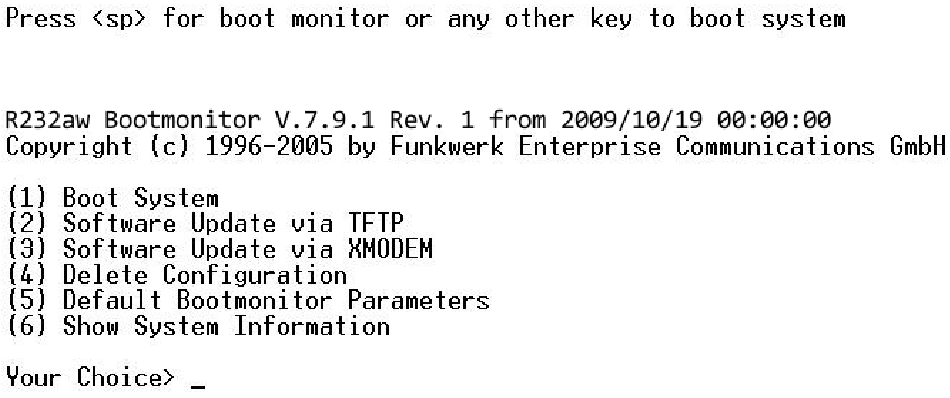
(6) Show System Information:
Shows useful information about your device, e.g. serial number, MAC address and software versions.

The BOOTmonitor is started as follows.

The devices passes through various functional states when starting:

- Start mode
- BOOTmonitor mode
- Normal mode

After some self-tests have been successfully carried out in the start mode, your device reaches the BOOTmonitor mode. The BOOTmonitor prompt is displayed if you are serially connected to your device.



```
Press <sp> for boot monitor or any other key to boot system


R232aw Bootmonitor V.7.9.1 Rev. 1 from 2009/10/19 00:00:00
Copyright (c) 1996-2005 by Funkwerk Enterprise Communications GmbH

(1) Boot System
(2) Software Update via TFTP
(3) Software Update via XMODEM
(4) Delete Configuration
(5) Default Bootmonitor Parameters
(6) Show System Information

Your Choice> _
```

After display of the BOOTmonitor prompt, press the space bar within four seconds to use the functions of the BOOTmonitor. If you do not make an entry within four seconds, the device changes back to normal operating mode.

Note

If you change the baud rate (the preset value is 9600 baud), make sure the terminal program used also uses this baud rate. If this is not the case, you will not be able to establish a serial connection to the device.

Chapter 8 Assistants

The **Assistants** menu offers step-by-step instructions for the following basic configuration tasks:

- **First steps**
- **Internet Access**
- **VPN**
- **Wireless LAN**
- **VoIP PBX in LAN**

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

Chapter 9 System Management

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

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

9.1 Status

If you log into the **Funkwerk Configuration Interface**, 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, WLAN, and ADSL interfaces
- The last 10 system messages

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

⚠ **Caution**

Under **Automatic Refresh Interval** do not enter a value below *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.
Last configuration stored	Displays day, date and time of the last saved configuration (boot

Field	Value
	configuration in flash).

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.
ISDN Usage External	Shows the number of active B channels and the maximum number of available B channels for external connections.
Active Sessions (SIF, RTP, etc...)	Displays the total of all SIF, TDRC, and IP load balancing sessions.
Active IPSec Tunnels	Displays the number of currently active IPSec tunnels in relation to the number of configured IPSec tunnels.

Additional fields in the StatusPhysical Interfaces menu

Field	Value
Interface - **Connection Information** - **Link**	The physical interfaces are listed here and their most important settings are shown. The system also displays whether the interface is connected or active. Interface specifics for Ethernet interfaces: • IP address • Netmask Interface specifics for ISDN interfaces: • Configured • Not configured Interface specifics for xDSL interfaces: • Downstream/Upstream Line Speed Interface Specifics for WLAN Interfaces: Access Point Mode: • Operation Mode: Access Point or Off • The channel used on this wireless module

Field	Value
	• Number of connected clients • Number of WDS links • Software version of the wireless card

Fields in the StatusWAN Interfaces menu

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

9.2 Global Settings

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

9.2.1 System

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

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

Fields in the SystemBasic Settings menu

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

Field	Value
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.
Maximum Number of Accounting Log Entries	Enter the maximum number of accounting entries that are stored internally in the device. Possible values are `0` to `1000`. The default value is `20`.

9.2.2 Passwords

Setting the passwords is another basic system setting.

Note

All **bintec** devices are delivered with the same username and password. As long as the password remains unchanged, they are not protected against unauthorised use.

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

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

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

Fields in the PasswordsSystem Password menu

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

Fields in the PasswordsSNMP Communities menu

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

Field in the PasswordsGlobal 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`*

Field	Value
	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. The WLAN and IPSec keys are one exception here. They can only be entered in plain text. If you press **OK** or call the menu again, they are displayed as asterisks.

9.2.3 Date and Time

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

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

ISDN/Manual

The system time is updated via ISDN, i.e. the date and time are taken from the ISDN when the first outgoing call is made, or is set manually on the device.

If the correct location of the device (country/city) is set for the **Time Zone**, switching from summer time to winter time (and back) is automatic. This is independent of the exchange time or the ntp server time. Summer time starts on the last Sunday in March by switching from 2 a.m. to 3 a.m. The calendar-related or schedule-related switches that are scheduled for the missing hour are then carried out. Winter time starts on the last Sunday in October by switching from 3 a.m. to 2 a.m. The calendar-related or schedule-related switches that are scheduled for the additional hour are then carried out.

If a value other than Universal Time Coordinated (UTC), option *UTC+-x*, has been chosen for the **Time Zone**, the switch from summer to winter time must be carried out manually when required.

Time server

You can obtain the system time automatically, e.g. using various time servers. To ensure that the device uses the desired current time, you should configure one or more time servers. Switching from summer time to winter time (and back) must be carried out manually if the time is derived using this method by changing the value in the **Time Zone** field with an option UTC+ or UTC-.

Note

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

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

Fields in the Date and TimeBasic 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, e.g. *`Europe/Berlin`*.
Current Local Time	The current date and current system time are shown here. The entry cannot be changed.

Fields in the Date and TimeManual Time Settings menu

Field	Description
Set Date	Enter a new date. Format: • **Day**: dd • **Month**: mm • **Year**: yyyy
Set Time	Enter a new time. Format: • **Hour**: hh • **Minute**: mm

Fields in the Date and TimeAutomatic Time Settings (Time Protocol) menu

Field	Description
ISDN Timeserver	Define whether the time information received at an incoming ISDN connection is used to update the system time. If a time

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

Field	Description
	In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol with UDP port 123. • *Time Service / UDP*: This server uses the time service with UDP port 37. • *Time Service / TCP*: This server uses the time service with TCP port 37. • *Disabled*: This time server is not currently used for the time request.
Time Update Interval	Enter the time interval in minutes at which the time is automatically updated. The default value is *1440*.
Time Update Policy	Enter the time period after which the system attempts to contact the time server again following a failed time update. Possible values: • *Normal* (default value): The system attempts to contact the time server after 1, 2, 4, 8, and 16 minutes. • *Aggressive*: For ten minutes, the system attempts to contact the time server after 1, 2, 4, 8 seconds, then every 10 seconds. • *Endless*: For an unlimited period, the system attempts to contact the time server after 1, 2, 4, 8 seconds, then every 10 seconds. If certificates are used to encrypt data traffic in a VPN, it is extremely important that the correct time is set on the device. To ensure this is the case, for **Time Update Policy**, select the value *Endless*.
Internal Time Server	Select whether the internal timeserver is to be used. The function is activated by selecting *Enabled*. Time requests from a client will be answered with the current system time. This is given as GMT, without offset.

Field	Description
	The function is disabled by default. Time requests from a client are not answered.

9.2.4 System Licences

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

The following licence types exist:

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

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

Entering licence data

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

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

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

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

Possible values for Status

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

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

Note

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

9.2.4.1 Edit or New

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

9.3 Interface Mode / Bridge Groups

In this menu, you define the operation mode for your device's interfaces.

Routing versus bridging

Bridging connects networks of the same type. In contrast to routing, bridges operate at layer 2 of the OSI model (data link layer), are independent of higher-level protocols and transmit data packets using MAC addresses. Data transmission is transparent, which means the information contained in the data packets is not interpreted.

With routing, different networks are connected at layer 3 (network layer) of the OSI model and information is routed from one network to the other.

Conventions for port/interface names

The names of wireless ports in the user interface of your device are made up of the following parts:

(a) WLAN

(b) Number of the physical port (1 or 2)

Example: *WLAN1*

The name of the Ethernet port is made up of the following parts:

(a) ETH, where en stands for Ethernet

(b) Number of the port

Example: *ETH1*

The names of the interfaces connected to an Ethernet port are made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the Ethernet port

(c) Number of the interface

Example: *en1-0* (first interface on the first Ethernet port)

The name of the bridge group is made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the bridge group

Example: *br0* (first bridge group)

The name of the wireless network is made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the wireless module

(c) Number of the interface

Example: *vss1-0* (first wireless network on the first wireless module)

The names of the virtual interfaces connected to an Ethernet port are made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the Ethernet port

(c) Number of the interface connected to the Ethernet port

(d) Number of the virtual interface

Example: *en1-0-1* (first virtual interface based on the first interface on the first Ethernet port)

9.3.1 Interfaces

You define separately whether each interface is to operate in routing or bridging mode.

If you want to set bridging mode, you can either use existing bridge groups or create a new bridge group.

The default setting for all existing interfaces is routing mode. When selecting the *New Bridge Group* option for **Mode / Bridge Group**, a bridge group, i.e. *br0*, *br1* etc. is automatically created.

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

Fields in the Interfaces menu

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

9.4 Administrative Access

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

9.4.1 Access

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

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

9.4.1.1 Add

Press 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 Access menu

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

9.4.2 SSH

Your devices offers encrypted access to the shell. You can enable or disable this access in the **System Management**->**Administrative Access**->**SSH** menu (**Enabled**, standard value) and have access to the options for configuration of 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.funkwerk-ec.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 includes the following fields:

Fields in the SSHSSH (Secure Shell) Parameters menu

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.
Compression	Select whether data compression should be used. The function is activated by selecting `Enabled`. The function is disabled by default.

Field	Value
TCP Keepalives	Select whether the device is to send keepalive packets. The function is activated by selecting *Enabled*. The function is enabled by default.
Logging Level	Select the syslog level for the syslog messages generated by the SSH Daemon. Possible settings: • *Information* (default value): Fatal and simple errors of the SSH Daemon and information messages are recorded. • *Fatal*: Only fatal errors of the SSH Daemon are recorded. • *Error*: Fatal and simple errors of the SSH Daemon are recorded. • *Debug*: All messages are recorded.

Fields in the SSHAuthentication and Encryption Parameters menu

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

Fields in the SSHKey Status menu

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 in red and a link *Generate* displayed. If you select the link, the generation process is triggered and the view is updated. The status *Generating* is now displayed in green. When generation is completed successfully, the status changes from *Generating* to *Generated*. If an error has occurred during generation, *Not generated* is displayed again with link *Generate*. You can then repeat generation. If the status *Unknown* 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 an DSA key has not been generated yet, *Not generated* is displayed in red, along with a link *Generate*. If you select the link, the generation process is triggered and the view is updated. The status *Generating* is now displayed in green. When generation is completed successfully, the status changes from *Generating* to *Generated*. If an error has occurred during generation, *Not generated* is displayed again with link *Generate*. You can then repeat generation. If the status *Unknown* is displayed, generation of a key is not possible, for example because there is not enough space in the FlashROM.

9.4.3 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 SNMPBasic Settings menu

Field	Value
SNMP Version	Select the SNMP version your device is to use to listen for external SNMP accesses. Possible values: • *v1*: SNMP Version 1 • *v2c*: Community-Based SNMP Version 2 • *v3*: SNMP Version 3 By default *v1*, *v2c* and *v3* are enabled. If no option is selected, the function is deactivated.
SNMP Listen UDP Port	Shows the UDP port (*161*) at which the device receives SNMP requests. The value cannot be changed.

Tip

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

9.5 Remote Authentication

This menu contains the settings for user authentication.

9.5.1 RADIUS

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

RADIUS can be used for:

- Authentication
- Accounting
- Exchange of configuration data

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

If the RADIUS server is used for accounting, your device sends an accounting message at the start of the connection and a message at the end of the connection. These start and end messages also contain statistical information about the connection (IP address, user name, throughput, costs).

RADIUS packets

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

Packet types

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

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

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

9.5.1.1 Edit or New

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

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

Fields in the RADIUSBasic Parameters menu

Field	Value
Authentication Type	Select what the RADIUS server is to be used for. Possible values: • *PPP Authentication*(standard value, for PPP connections only): The RADIUS server is used for controlling access to a network. • *Accounting*(for PPP connections only): The RADIUS server is used for recording statistical call data.

Field	Value
	• *Login Authentication*: The RADIUS server is used for controlling access to the SNMP shell of your device. • *IPSec Authentication*: The RADIUS server is used for sending configuration data for IPSec peers to your device. • *WLAN (802.1x)*: The RADIUS server is used for controlling access to a wireless network. • *XAUTH*: The RADIUS server is used for authenticating IPSec peers via XAuth.
Vendor Mode	Only for **Authentication Type** = *Accounting*. In hotspot applications, select the mode define by the provider. In standard applications, leave the value set to *Default*. Possible values for hotspot applications: • *France Telecom*: For France Telecom hotspot applications. • *bintec HotSpot Server*: For bintec hotspot applications.
Server IP Address	Enter the IP address of the RADIUS server.
RADIUS Secret	Enter the shared password used for communication between the RADIUS server and your device.
Default User Password	Some Radius servers require a user password for each RADIUS request. Enter the password that your device sends as the default user password in the prompt for the dialout routes on the RADIUS server.
Priority	If a number of RADIUS server entries were created, the server with the highest priority is used first. If this server does not answer, the server with the next-highest priority is used. Possible values from *0* (highest priority) to *7* (lowest priority). The default value is *0*. See also **Policy** in the **Advanced Settings**.
Entry active	Select whether the RADIUS server configured in this entry is to be used. The function is activated by selecting *Enabled*.

Field	Value
	The function is enabled by default.
Group Description	Define a new RADIUS group description or assign the new RADIUS entry to a predefined group. The configured RADIUS servers for a group are queried according to **Priority** and the **Policy**. Possible values: • *New* (default value): Enter a new group description in the text field. • *Default Group 0*: Select this entry for special applications, such as Hotspot Server configuration. • *<Group Name>*: Select a predefined group from the list.

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

Fields in the Advanced Settings menu

Field	Value
Policy	Select how your device is to react if a negative response to a request is received. Possible values: • *Authoritative* (default value): A negative response to a request is accepted. • *Non-authoritative* : A negative response to a request is not accepted. A request is sent to the next RADIUS server until your device receives a response from a server configured as authoritative.
UDP Port	Enter the UDP port to be used for RADIUS data. RFC 2138 defines the default ports 1812 for authentication (1645 in older RFCs) and 1813 for accounting (4,180.84 cm older RFCs). You can obtain the port to be used from the documentation for your RADIUS server. The default value is *1812*.
Server Timeout	Enter the maximum wait time between ACCESS_REQUEST and response in milliseconds.

Field	Value
	After timeout, the request is repeated according to **Retries** or the next configured RADIUS server is requested. Possible values are whole numbers between *50* and *50000*. The default value is *1000* (1 second).
Alive Check	Here you can activate a check for accessibility of a RADIUS server in **Status** *Down* . An Alive Check is carried out regularly (every 20 seconds) by sending an ACCESS_REQUEST to the IP address of the RADIUS server. If the server is accessible, **Status** is reset to *alive* . If the RADIUS server is only reachable over a switched line (dialup connection), this can cause additional costs if the server is *down* for a long time. The function is activated by selecting *Enabled*. The function is enabled by default.
Retries	Enter the number of retries for cases when there is no response to a request. If an response has still not been received after these attempts, the **Status** is set to *down*. In **Alive Check** = *Enabled* your device attempts to reach the server every 20 seconds. If the server responds, **Status** is set back to *alive* . Possible values are whole numbers between *0* and *10*. The default value is *1*. To prevent **Status** being set to *down*, set this value to *0*.
RADIUS Dialout	Only for **Authentication Type** = *Authentication* and *IPSec Authentication*. Select whether your device receives requests from RADIUS server dialout routes. This enables temporary interfaces to be configured automatically and your device can initiate outgoing connections that are not configured permanently. The function is activated by selecting *Enabled*. The function is disabled by default. If the function is active, you can enter the following options:

Field	Value
	• *Reload Interval*: Enter the time period in seconds between update intervals. The default entry here is *0* i.e. an automatic reload is not carried out. • *Default User Password*: Some Radius servers require a user password for each RADIUS request. Enter the password that your device sends as the default user password in the prompt for the dialout routes on the RADIUS server. By default, *Default User Password* is empty.

9.5.2 TACACS+

TACACS+ permits access control for your device, network access servers (NAS) and other network components via one or more central servers.

Like RADIUS, TACACS+ is an AAA protocol and offers authentication, authorisation and accounting services (TACACS+ Accounting is currently not supported by **bintec** devices).

The following TACACS+ functions are available on your device:

- Authentication for login shell
- Command authorisation on the shell (e.g. telnet, show)

TACACS+ uses TCP port 49 and establishes a secure and encrypted connection.

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

9.5.2.1 Edit or New

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

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

Fields in the TACACS+Basic Parameters menu

Field	Description
Authentication Type	Displays which TACACS+ function is to be used. The value cannot be changed.

Field	Description
	Possible values: • *Login Authentication*: Here, you can define whether the current TACACS+ server is to be used for login authentication to your device.
Server IP Address	Enter the IP address of the TACACS+ server that is to be requested for login authentication.
TACACS+ Secret	Enter the password to be used to authenticate and, if applicable, encrypt data exchange between the TACACS+ server and the network access server (your device). The maximum length of the entry is 32 characters.
Priority	Assign a priority to the current TACACS+ server. The server with the lowest value is the one used first for TACACS+ login authentication. If there is no response or access is denied (only if **Policy** = *Non-authoritative*), the entry with the next-lowest priority is used. The available values are *0* to *9*, the default value is *0*.
Entry active	Select whether this server is to be used for login authentication. The function is activated by selecting *Enabled*. The function is enabled by default.

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

Fields in the Advanced Settings menu

Field	Description
Policy	Select the interpretation of the TACACS+ response. Possible values: • *Non-authoritative* (default value): The TACACS+ servers are queried in order of their priority (see **Priority**) until a positive response is received or a negative response is received from an authoritative server. • *Authoritative*: A negative response to a request is accepted, i.e. a request is not sent to another TACACS+ server. The device's internal user administration is not turned off by TACACS+. It is checked after all TACACS+ servers have been

Field	Description
	queried.
TCP Port	Shows the default TCP port (*49*) used for the TACACS+ protocol. The value cannot be changed.
Timeout	Enter time in seconds for which the NAS is to wait for a response from TACACS+. If a response is not received during the wait time, the next configured TACACS+ server is queried (only if **Policy** = *Non-authoritative*) and the current server is set to status *Blocked*. The possible values are *1* to *60*, the default value is *3*.
Block Time	Enter the time in seconds for which the current server is to remain in blocked status. At the end of the block time, the server is set to the status specified in the **Entry active** field. The possible values are *0* to *3600*, the default value is *60*. The value *0* means that the server is never set to *Blocked* status and thus no other servers are queried.
Encryption	Select whether data exchange between the TACACS+ server and the NAS is to be encrypted with MD5. The function is activated by selecting *Enabled*. The function is enabled by default. If the function is not enabled, the packets and all related information are transferred unencrypted. Unencrypted transfer is not recommended as a default setting and should only be used for debugging.

9.5.3 Options

This setting possible here causes your device to carry out authentication negotiation for incoming calls, if it cannot identify the calling party number (e.g. because the remote terminal does not signal the calling party number). If the data (password, partner PPP ID) obtained by executing the authentication protocol is the same as the data of a listed remote terminal or RADIUS user, your device accepts the incoming call.

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

Fields in the OptionsGlobal RADIUS Options menu

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

9.6 Certificates

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

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

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

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

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

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

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

9.6.1 Certificate List

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

9.6.1.1 Edit

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

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

The **System Management**->**Certificates**->**Certificate List**->🔧 menu includes the following fields:

Fields in the menu

Field	Description
Description	Shows the name of the certificate, key, or request.
Certificate is CA Certificate	Mark the certificate as a certificate from a trustworthy certification authority (CA). Certificates issued by this CA are accepted during authentication. The function is enabled with *True*. The function is disabled by default.
Certificate Revocation List (CRL) Checking	Only for **Certificate is CA Certificate** = *True*. Define the extent to which certificate revocation lists (CRLs) are to be included in the validation of certificates issued by the own-

Field	Description
	er of this certificate. Possible settings: • *Disabled*: No CRLs check. • *Always*: CRLs are always checked. • *Only if a CRL Distribution Point is present* (default value): A check is only carried out if a CRL Distribution Point entry is included in the certificate. This can be determined under "View Details" in the certificate content. • *Use settings from superior certificate*: The settings of the higher level certificate are used, if one exists. It is does not, the same procedure is used as that described under "Only if a CRL Distribution Point is present".
Force certificate to be trusted	Define that this certificate is to be accepted as the user certificate without further checks during authentication. The function is enabled with *True*. The function is disabled by default.

Caution

It is extremely important for VPN security that the integrity of all certificates manually marked as trustworthy (certification authority and user certificates) is ensured. The displayed "fingerprints" can be used to check this integrity: Compare the displayed values with the fingerprints specified by the issuer of the certificate (e.g. on the Internet). It is sufficient to check one of the two values.

9.6.1.2 Certificate Request

Registration authority certificates in SCEP

If SCEP (Simple Certificate Enrollment Protocol) is used, your device also supports separate registration authority certificates.

Registration authority certificates are used by some Certificate Authorities (CAs) to handle certain tasks (signature and encryption) during SCEP communication with separate keys, and to delegate the operation to separate registration authorities, if applicable.

When a certificate is downloaded automatically, i.e. if **CA Certificate** = *-- Download --* is selected, all the certificates needed for the operation are loaded automatically.

If all the necessary certificates are already available in the system, these can also be selected manually.

Select the **Certificate Request** button to request or import more certificates.

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

Fields in the Certificate ListCertificate Request menu

Field	Description
Certificate Request Description	Enter a unique description for the certificate.
Mode	Select the way in which you want to request the certificate. Possible settings: • *Manual* (default value): Your device generates a PKCS#10 for the key. This file can then be uploaded directly in the browser or copied in the 🔧 menu using the **View details** field. This file must be provided to the CA and the received certificate must then be imported manually to your device. • *SCEP* : The key is requested from a CA using the Simple Certificate Enrolment Protocol.
Generate Private Key	Only for **Mode** = *Manual* Select an algorithm for key creation. *RSA* (standard value) and *DSA* are available. Also select the length of the key to be created. Possible values: *512*, *768*, *1024*, *1536*, *2048*, *4096*. Please note that a key with a length of 512 bits could be rated as unsecure, whereas a key of 4096 bits not only needs a lot of time to create, but also occupies a major share of the resources during IPSec processing. A value of 768 or more is, however, recommended and the default value is 1024 bits.

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

Field	Description
	If you use one of your own certificates to sign communication with the RA, you can select another one here to encrypt communication. The default value is `-- Use RA Sign Certificate --`, i.e. the same certificate is used as for signing.
Password	Only for **Mode** = *SCEP* You may need a password from the certification authority to obtain certificates for your keys. Enter the password you received from the certification authority here.

Fields in the Certificate ListSubject Name menu

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

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

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

Fields in the Advanced SettingsSubject Alternative Names menu

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

Field in the Advanced SettingsOptions menu

Field	Description
Autosave Mode	Select whether your device automatically stores the various

Field	Description
	steps of the enrolment internally. This is an advantage if enrolment cannot be concluded immediately. If the status has not been saved, the incomplete registration cannot be completed. As soon as the enrolment is completed and the certificate has been downloaded from the CA server, it is automatically saved in the device configuration. The function is enabled with *Enabled*. The function is enabled by default.

9.6.1.3 Import

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

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

Fields in the Certificate ListImport menu

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

9.6.2 CRLs

In the **System Management**->**Certificates**->**CRLs** menu, a list of all CRLs (Certification Revocation List) is displayed.

If a key is no longer to be used, e.g. because it has fallen into the wrong hands or has been lost, the corresponding certificate is declared invalid. The certification authority revokes the certificate and publishes it on a certificate blacklist, so-called CRL. Certificate users should always check against these lists to ensure that the certificate used is currently valid. This check can be automated via a browser.

The Simple Certificate Enrollment Protocol (SCEP) supports the issue and revocation of certificates in networks.

9.6.2.1 Import

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

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

Fields in the CRLsCRL Import menu

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

9.6.3 Certificate Servers

A list of all certificate servers is displayed in the **System Management**->**Certificates**->**Certificate Servers** menu.

A certificate server provides CRL's which for checking certificates can be queried by the device either per LDAP or HTTP.

9.6.3.1 New

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

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

Fields in the Certificate ServersBasic Parameters menu

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

Chapter 10 Physical Interfaces

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

10.1 Ethernet Ports

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

The Ethernet ports **1** to **4** are assigned to a single logical Ethernet interface in ex works state. The logical Ethernet interface *en1-0* is assigned, and preconfigured with **IP Address** *192.168.0.254* and **Netmask** *255.255.255.0* .

The logical Ethernet interface *en5-0* is assigned to the **ETH** port and is not preconfigured.

Note

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

1 - 4

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

ETH

The logical Ethernet interface *en5-0* is assigned to the **ETH5** port. The configuration options are the same as those for the ports **1** - **4**.

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.

10.1.1 Port Configuration

Port Separation

Your device makes it possible to run the switch ports **1** - **4** 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. 100 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. 100 mbps full duplex is available for all the ports together.

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

Fields in the Port ConfigurationSwitch Configuration menu

Field	Description
Switch Port	Shows the respective switch port. The numbering corresponds to the numbering of the Ethernet ports on the back of the device.
Ethernet Interface Selection	Assign an Ethernet interface to the switch port. You can select from four interfaces, *en1-0* to *en1-3* . In the basic setting, interface *en1-0* is assigned to all switch ports.
Configured Speed / Mode	Select the mode in which the interface is to run. Possible values: • *Full Autonegotiation* (default value) • *Auto 1000 mbps only*

Field	Description
	• *Auto 100 mbps only* • *Auto 10 mbps only* • *Auto 100 mbps / Full Duplex* • *Auto 100 mbps / Half Duplex* • *Auto 10 mbps / Full Duplex* • *Auto 10 mbps / Half Duplex* • *Fixed 1000 mbps / Full Duplex* • *Fixed 100 mbps / Full Duplex* • *Fixed 100 mbps / Half Duplex* • *Fixed 10 mbps / Full Duplex* • *Fixed 10 mbps / Half Duplex* • *None* : The interface is created but remains inactive.
Current Speed / Mode	Shows the actual mode and actual speed of the interface. Possible values: • *1000 mbps / Full Duplex* • *100 mbps / Full Duplex* • *100 mbps / Half Duplex* • *10 mbps / Full Duplex* • *10 mbps / Half Duplex* • *Down*

Fields in the Port ConfigurationPort Configuration menu

Field	Description
Interface	Shows the interface name of the separate Ethernet port ETH.
Configured Speed / Mode	Select the mode in which the interface is to run. Possible values: • *Full Autonegotiation* (default value) • *Auto 100 mbps only* • *Auto 10 mbps only* • *Auto 100 mbps only*

Field	Description
	• *Auto 100 mbps / Full Duplex* • *Auto 100 mbps / Half Duplex* • *Auto 10 mbps / Full Duplex* • *Auto 10 mbps / Half Duplex* • *Fixed 100 mbps / Full Duplex* • *Fixed 100 mbps / Half Duplex* • *Fixed 10 mbps / Full Duplex* • *Fixed 10 mbps / Half Duplex* • *Disabled* : 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*

10.2 ISDN Ports

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

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

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

10.2.1 ISDN Configuration

Note

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

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

10.2.1.1 Working with 🔧

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

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

Fields in the ISDN ConfigurationBasic Parameters menu

Field	Description
Port Name	Shows the name of the ISDN port.
Autoconfiguration on Bootup	Select whether the ISDN switch type (D channel detection for switched line) is to be automatically identified. The function is enabled with *Enabled*. The function is enabled by default.
Result of Autoconfiguration	Shows the status of the ISDN Auto Config. Automatic D-channel detection runs until a setting is found, or until the ISDN protocol is selected manually under **Port Usage**. This field cannot be edited. The result of automatic configuration for the **Port Usage** and the **ISDN Configuration Type** is displayed. Possible values: • All possible values for the **Port Usage** and the **ISDN Configuration Type**.

Field	Description
	• *Running*: Detection is still running.
Port Usage	Only if **Autoconfiguration on Bootup** is disabled. Select the protocol that you want to use for the ISDN port. Possible values: • *Not used*: The ISDN connection is not used. • *Dialup (Euro ISDN)* • *Leased Line* • *Q-SIG*
ISDN Configuration Type	Only if **Autoconfiguration on Bootup** is disabled and for **Port Usage** = *Dialup (Euro ISDN)* or *Q-SIG* Select the ISDN connection type. Possible values: • *Point-to-Multipoint* (default value): Point-to-multipoint connection • *Point-to-Point*: Point-to-point ISDN access.

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

Fields in the Advanced Settings menu

Field	Description
X.31 (X.25 in D Channel)	Select whether you want to use X.31 (X.25 in the D channel) e.g. for CAPI applications. The function is enabled with *Enabled*. The function is disabled by default.
X.31 TEI Value	Only if **X.31 (X.25 in D Channel)** is enabled With the ISDN autoconfiguration, the X.31-TEI is detected automatically. If the autoconfiguration has not detected TEI, you can manually enter the value assigned by the exchange. Possible values are *0* to *63*. The default value is *-1* (for automatic detection).

Field	Description
X.31 TEI Service	Only for **X.31 (X.25 in D Channel)** enabled Select the service for which you want to use X.31 TEI. Possible values: • *CAPI* • *CAPI Default* • *Packet Switch* (default value) *CAPI* and *CAPI Default* are only for the use of X.31 TEI for CAPI applications. For *CAPI*, the TEI value set in the CAPI application is used. For *CAPI Default*, the value of the CAPI application is ignored and the default value set here is always used. *Packet Switch* is set if you want to use X.31 TEI for the X.25 device.

10.2.2 MSN Configuration

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

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

The device supports the following services:

- PPP (routing): The PPP (routing) service is your device's general routing service. This enables ISDN remote terminals to establish data connections with your LAN, among other things. This enables partners outside your own local network to access hosts within your LAN. It is also possible to establish outgoing data connections to ISDN remote terminals.
- ISDN Login: The ISDN login service enables both incoming data connections with access to the SNMP shell of your device, and outgoing data connections to other **bintec** devices. As a result, your device can be remotely configured and administrated.
- IPSec: **bintec** devices support the DynDNS service to enable hosts without fixed IP addresses to obtain a secure connection over the Internet. With the IPSec Callback function and using a direct ISDN call to an IPSec peer with a dynamic IP address you can signal

to this IPSec peer that you are online and waiting for the setup of an IPSec tunnel over the Internet. If the called peer currently has no connection to the Internet, the ISDN call causes a connection to be set up. The identification of the caller from his or her ISDN number is enough information to initiate setting up a tunnel.

- X.25 PAD: X.25 PAD is used to provide a protocol converter, which converts non-packet-oriented protocols to packet-oriented communication protocols and vice versa. Data terminal equipment sending or receiving data on a non-data-packet-oriented basis can this be adapted in line with Datex-P (public data packet network based on the principle of a packet switching exchange).

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

Note

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

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

10.2.2.1 New

Choose the **New** button to edit the MSN's.

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

Fields in the MSN ConfigurationBasic Parameters menu

Field	Description
ISDN Port	Select the ISDN port for which the MSN is to be configured.
Service	Select the service to which a call is to be assigned on the **MSN** below. Possible values: • *ISDN Login* (default value): Enables login with *ISDN Login*

Field	Description
	• *PPP (Routing)*: Default setting for PPP routing. Contains automatic detection of the PPP connections stated below except *PPP DOVB*. • *IPSec*: Enables a number to be defined for IPSec callback. • *Other (PPP)*: Other services can be selected: *PPP 64k* (Allows 64 kpbs PPP data connections), *PPP 56k* (Allows 56 kpbs PPP data connections), *PPP V.110(9600) PPP V.110(14400)*, *PPP V.110(19200)*, *PPP V.110(38400)* (Allows PPP connections with V.110 and bitrates of 9,600 bps, 14,400 bps, 19,200 bps, 38,400 bps), *PPP V.120* (Allows PPP connections with V.120).
MSN	Enter the number used to check the called party number. For the call to be accepted, it is sufficient for the individual numbers in the entry to agree, taking account of **MSN Recognition**.
MSN Recognition	Select the mode your device is to use for the number comparison for **MSN** with the called party number of the incoming call. Possible values: • *Right to Left* (default value) • *Left to Right (DDI)*: Always select if your device is connected to a point-to-point connection.
Bearer Service	Select the type of incoming call (service detection). Possible values: • *Data + Voice* (default value): Both data and voice calls. • *Data*: data call • *Voice*: Voice call (modem, voice, analog fax)

10.3 ADSL Modem

The ADSL modem on the **bintec R232x** and **bintec R232xw** is compatible with ANNEX A and ANNEX B standards (see chapter **Technical Data**) and so can be used universally in several countries. It is particularly suitable for high-speed Internet access and remote access use in SMEs or remote offices.

10.3.1 ADSL Configuration

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

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

Fields in the ADSL ConfigurationDSL Port Status menu

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

Fields in the ADSL ConfigurationCurrent Line Speed menu

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

Field	Description
	router to CO/DSLAM) in bits per second. The value cannot be changed.

Fields in the ADSL ConfigurationDSL Parameter menu

Field	Description
DSL Mode	Select the ADSL synchronization type. Possible values: • `ADSL Automode` (default value): The ADSL mode is automatically adapted for the remote terminal. • `ADSL1` :ADSL1 / G.DMT is used. • `ADSL2`: ADSL2 / G.992.3 is used. • `ADSL2 Plus`: ADSL2 Plus / G.992.5 is used. • `Inactive`: The ADSL interface is not active.
Transmit Shaping	Select whether the data rate in the send direction is to be reduced. This is only needed in a few cases for special DSLAMs. Possible values: • `Default (Line Speed)`: The data rate in the send direction is not reduced. • `128000 bps`, `192000 bps`, `256000 bps`, `512000 bps`, `768000 bps`, `1024000 bps`, `1536000 bps` and `2048000 bps`: The data rate in the send direction is reduced to a maximum of 128,000 bps to 2,048,000 bps in defined steps. • `User-defined`:The data rate is reduced to the value entered in **Maximum Upstream Bandwidth**. The default value is `Default (Line Speed)`.
Maximum Upstream Bandwidth	Only for **Transmit Shaping** = `User-defined` Enter the maximum data rate in the send direction in bits per second.

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

Fields in the ADSL ConfigurationAdvanced Settings menu

Field	Description
ADSL Line Profile	Select the ADSL line profile required for your provider. Possible values: • *`Default`* (default value): If no special ADSL line profile is required, leave this setting. • *`<Provider>`*: Select one of the preset providers from the list.

Chapter 11 LAN

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

11.1 IP Configuration

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

11.1.1 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.

The default setting for all existing interfaces of your device is routing mode. The interface, **en1-0**, is pre-configured with IP address *192.168.0.254* and netmask *255.255.255.0* .

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.

11.1.1.1 Edit or New

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

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

Fields in the InterfacesBasic 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.
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.
Interface Mode	Only for physical interfaces in routing mode. 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 module.

Field	Description
MAC Address	Only with virtual interfaces and only for **Interface Mode** = *Untagged* 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, but this is not necessary. You can also allocate a virtual MAC address. The first 6 characters of the MAC are preset (but can be changed).
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*.

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

Fields in the Advanced Settings menu

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

Field	Description
	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.
Proxy ARP	Select whether your device is to respond to ARP requests from its own LAN on behalf of defined remote terminals. The function is activated by selecting `Enabled`. The function is disabled by default.
TCP-MSS Clamping	Select whether your device is to apply MSS Clamping. To prevent IP packets fragmenting, the MSS (Maximum Segment Size) is automatically decreased by the device to the value set here. The function is activated by selecting `Enabled`. The function is disabled by default. Once enabled, the default value `1350` is entered in the input field.

11.2 VLAN

By implementing VLAN segmentation in accordance with 802.1Q, you can configure VLANs on your device. The wireless ports of an access point, in particular, are able to remove the VLAN tag of a frame sent to the clients and to tag received frames with a predefined VLAN ID. This functionality makes an access point nothing less than a VLAN-aware switch with the enhancement of grouping clients into VLAN groups. In general, VLAN segmenting can be configured with all interfaces.

VLAN for Bridging and VLAN for Routing

In the **LAN**->**VLAN** menu, VLANs (virtual LANs) are configured with interfaces that operate in Bridging mode. Using the **VLAN** menu, you can make all the settings needed for this and query their status.

Caution

For interfaces that operate in Routing mode, you only assign a VLAN ID to the interface. You define this via the parameters **Interface Mode** = *Tagged (VLAN)* and field **VLAN ID** in menu **LAN**->**IP Configuration**->**Interfaces**->**New**.

11.2.1 VLANs

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

11.2.1.1 Edit or New

Choose the 🔧 icon to edit existing entries. Choose the **New** button to configure other VLANs.

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

Fields in the VLANsConfigure VLAN menu

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

11.2.2 Port Configuration

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

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

Fields in the Port Configuration menu

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

11.2.3 Administration

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

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

Fields in the VLANAdministration menu

Field	Description
Enable VLAN	Enable or disable the specified bridge group for VLAN. The function is enabled with `Enabled`. The function is not activated by default.
Management VID	Select the VLAN ID of the VLAN in which your device is to operate.

Chapter 12 Wireless LAN

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

Network functions

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

Currently applicable standard: IEEE 802.11

In the case of 802.11-WLANs, all the functions of a wired network are possible. WLAN transmits inside and outside buildings with a maximum of 100 mW.

IEEE 802.11g is currently the most widespread standard for wireless LANs and offers a maximum data transmission rate of 54 mbps. This procedure operates in the radio frequency range of 2.4 GHz, which ensures that parts of the building are penetrated as effectively as possible with a low transmission power that poses no health risks.

A 802.11g-compatible standard is 802.11b, which operates in the 2.4 GHz range (2400 MHz - 2485 MHz) and offers a maximum data transmission rate of 11 mbps. 802.11b and 802.11g WLAN systems involve no charge or login.

With 802.11a, bandwidths of up to 54 mbps can be used in the 5150 GHz to 5725 MHz range. With the higher frequency range, 19 non-overlapping frequencies are available (in Germany). This frequency range can also be used without a licence in Germany. In Europe, transmission power of not just 30 mW but 1000 mW can be used with 802.11h, but only if TPC (TX Power Control, method for controlling transmission power in wireless systems to reduce interferences) and DFS (Dynamic Frequency Selection) are used. The purpose of TPC and DFS is to ensure that satellite connections and radar devices are not interfered with.

12.1 WLAN

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

12.1.1 Radio Settings

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

12.1.1.1 Radio Settings->🔧

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

Choose the 🔧 button to edit the configuration.

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

Fields in the Radio SettingsWireless Settings menu

Field	Description
Operation Mode	Define whether your device is to be run as an *Access Point*, or whether the wireless module must be deactivated (*Off*, default value).
Operation Band	Displays the operation band and usage area of the access point. Possible values: • *2.4 GHz Indoor-Outdoor* (default value): The access point is run within or outside buildings.
Channel	Select the channel to be used. The number of channels that can be selected depends on the country setting. Please consult the data sheet for your device. Possible values are *1* to *13*. The default value is *11*. Configuring the network name (SSID) in Access Point mode means that wireless networks can be logically separated from each other, but they can still physically interfere with each other if they are operating on the same or closely adjacent wireless channels. So if you are operating two or more radio networks close to each other, it is advisable to allocate the networks to different channels. Each of these should be spaced at least four channels apart, as a network also partially occupies the adja-

Field	Description
	cent channels. In the case of manual channel selection, please make sure first that the clients actually support these channels.
Transmit Power	Select the maximum value for the radiated antenna power. The actually radiated antenna power may be lower than the maximum value set, depending on the data rate transmitted. The maximum value for Transmit Power is country-dependent. Possible values: • *Max.* (default value): The maximum antenna power is used. • *7 dBm* • *9 dBm* • *12 dBm* • *15 dBm*

Fields in the Radio SettingsPerformance Settings menu

Field	Description
Wireless Mode	Select the wireless technology that the access point is to use. Possible values: • *802.11g*: Your device operates only in accordance with 802.11g. 802.11b clients have no access. • *802.11b*: Your device operates only in accordance with 802.11b and forces all clients to adapt to it. • *802.11 mixed (b/g)* (default value) / *802.11 mixed short (b/g)*: Your device adapts to the client technology. The following applies for mixed-short: The data rates 5.5 and 11 mbps must be supported by all clients (basic rates). • *802.11 mixed long (b/g)*: Your device adapts to the client technology. Only a data rate of 1 and 2 mbps needs to be supported by all clients (basic rates). This mode is also needed for Centrino clients if connection problems occur.
Max. Transmission Rate	Select the transmission speed. Possible values:

Field	Description
	• `Auto` (default value): The transmission speed is determined automatically. • `<Value>`: According to setting for **Operation Band**, **Bandwidth**, **Number of Spatial Streams** and **Wireless Mode** various fixed values in mbps are available.
Burst Mode	Activate this function to increase the transmission speed for 802.11g through frame bursting. As a result, several packets are sent one after the other without a waiting period. This is particularly effective in 11b/g mixed operation. The function is enabled with `Enabled`. The function is activated by default. If problems occur with older WLAN hardware, this function should be deactivated.

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

Fields in the Advanced Settings menu

Field	Description
Beacon Period	Enter the time in milliseconds between the sending of two beacons. This value is transmitted in Beacon and Probe Response Frames. Possible values are `1` to `65535`. The default value is `100` msec.
DTIM Period	Enter the interval for the Delivery Traffic Indication Message (DTIM). The DTIM field is a data field in transmitted beacons that informs clients about the window to the next broadcast or multicast transmission. If clients operate in power save mode, they come alive at the right time and receive the data. Possible values are `1` to `255`. The default value is `2`.

Field	Description
RTS Threshold	Select how the RTS/CTS mechanism is to be switched on/off. If you choose *User-defined*, you can specify in the input field the data packet length threshold in bytes (1..2346) as of which the RTS/CTS mechanism is to be used. This makes sense if several clients that are not in each other's wireless range are run in one access point. The mechanism can also be switched on/off independently of the data packet length by selecting the value *Always on* or *Always off*(default value).
Short Retry Limit	Enter the maximum number of attempts to send a frame with length less than or equal to the value defined in **RTS Threshold**. After this many failed attempts, the packet is discarded. Possible values are *1* to *255*. The default value is *7*.
Long Retry Limit	Enter the maximum number of send attempts for a data packet that is longer than the value defined in **RTS Threshold** After this many failed attempts, the packet is discarded. Possible values are *1* to *255*. The default value is *4*.
Fragmentation Threshold	Enter the maximum size as of which the data packets are to be fragmented (i.e. split into smaller units). A low value is recommended for this field in areas with poor reception and in the event of radio interference. Possible values are *256* to *2346*. The default value is *2346* bytes.
Max. Receive Lifetime	Enter the time from receipt of the first fragment of a data packet as of which no further attempts are made. The data packet is discarded. Possible values are *1* to *4294967295*. The default value is *512* msec.

Field	Description
Max. Transmit MSDU Lifetime	Enter the time from sending of the first fragment of a data packet as of which no further send attempts are made. The data packet is discarded. Possible values are `1` to `4294967295`. The default value is `512` msec.

12.1.2 Virtual Service Sets

If you're operating your device in Access Point mode (**Wireless LAN**->**WLAN**->**Radio Settings**->🔧->**Operation Mode** = *Access Point*), you can edit or create the desired wireless networks in the menu **Wireless LAN**->**WLAN**->**Virtual Service Sets**->🔧+**New**.

Note

The preset wireless network Funkwerk-EC has the following security settings in the ex works state:

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

Setting network names

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

Protection of wireless networks

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

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

WEP

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

IEEE 802.11i

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

WPA

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

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

WPA2

WPA2 is the enhancement of WPA. In WPA2, the 802.11i standard is not only implemented for the first time in full, but another encryption algorithm AES (Advanced Encryption Standard) is also used.

Access control

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

Security measures

To protect the data transferred on the WLAN, the following configuration steps should be carried out in the **Wireless LAN**->**WLAN**->**Virtual Service Sets**->**New**->**/**🔧 menu, where necessary:

- Change the access passwords for your device.
- Change the default SSID, **Network Name (SSID)** = *Funkwerk-ec*, of your access point. Set **Visible** = *Enabled*. This will exclude all WLAN clients that attempt to establish a connection with the general value for **Network Name (SSID)** *Any* and do not know the SSID settings.
- Use the available encryption methods. For this, select **Security Mode** = *WEP 40*, *WEP 104*, *WPA-PSK* or *WPA Enterprise* or both, and enter the corresponding key into the access point under **WEP Key** 1 - 4 or **Preshared Key** in the WLAN clients.
- The WEP key should be changed regularly. To do this, change **Transmit Key**. Select the longer 104 Bit WEP key.
- For transmission of information with very high security relevance, configure **Security Mode** = *WPA Enterprise* with **WPA Mode** = *WPA 2*. This method contains hardware-based encryption and RADIUS authentication of the client. In special cases, combination with IPSec is possible.
- Restrict WLAN access to permitted clients. Enter the MAC addresses of the wireless network cards for these clients in the **Allowed Addresses** list in the **MAC-Filter** menu (see *Fields in the MAC-Filter menu* on page 122).

A list of all WLAN networks is displayed in the **Wireless LAN**->**WLAN**->**Virtual Service Sets** menu.

12.1.2.1 Edit or New

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

The **Wireless LAN**->**WLAN**->**Virtual Service Sets**->🔧->**/New** menu consists of the following fields:

Fields in the Virtual Service SetsService Set Parameters menu

Field	Description
Network Name (SSID)	Enter the name of the wireless network (SSID). Enter an ASCII string with a maximum of 32 characters.

Field	Description
	Also select whether the **Network Name (SSID)** is to be transmitted. The network name is displayed by selecting *Visible*. It is visible by default.
Intra-cell Repeating	Select whether communication between the WLAN clients is to be permitted within a radio cell. The function is activated by selecting *Enabled*. The function is enabled by default.
ARP Processing	Select whether the ARP processing function should be enabled. The ARP data traffic is reduced in the network by the fact that ARP broadcasts that have been converted to ARP unicasts are forwarded to IP addresses that are known internally. Unicasts are quicker and clients with an enabled power save function are not addressed. The function is activated by selecting *Enabled*. The function is disabled by default. Make sure that ARP processing cannot be applied in conjunction with the MAC bridge function.

Fields in the Virtual Service SetsSecurity Settings menu

Field	Description
Security Mode	Select the security mode (encryption and authentication) for the wireless network. Possible values: • *Inactive* (default value): Neither encryption nor authentication • *WEP 40*: WEP 40 bits • *WEP 104*: WEP 104 bits • *WPA-PSK*: WPA Preshared Key • *WPA Enterprise*: 802.11i/TKIP

Field	Description
Transmit Key	Only for **Security Mode** = *WEP 40*, *WEP 104* In **WEP Key** select 1 - 4 of the configured keys as a standard key. The default value is *Key 1*.
WEP Key 1-4	Only for **Security Mode** = *WEP 40*, *WEP 104* Enter the WEP key. Enter a character string with the right number of characters for the selected WEP mode. For *WEP 40* you need a character string with 5 characters, for *WEP 104* with 13 characters, e. g. *hello* for *WEP 40*, *funkwerk-wep1* for *WEP 104*.
WPA Mode	Select the security mode (encryption and authentication) for the wireless network. Possible values: • *Inactive* (default value): Neither encryption nor authentication • *WEP 40*: WEP 40 bits • *WEP 104*: WEP 104 bits • *WPA-PSK*: WPA Preshared Key • *WPA Enterprise*: 802.11i/TKIP
WPA Cipher	Only for **Security Mode** = *WEP 40*, *WEP 104* In **WEP Key** select 1 - 4 of the configured keys as a standard key. The default value is *Key 1*.
WPA2 Cipher	Only for **Security Mode** = *WEP 40*, *WEP 104* Enter the WEP key. Enter a character string with the right number of characters for the selected WEP mode. For *WEP 40* you need a character string with 5 characters, for *WEP 104* with 13 characters, e. g. *hello* for *WEP 40*, *funkwerk-wep1* for *WEP 104*.

Field	Description
Preshared Key	Only for **Security Mode** = *WPA-PSK* Enter the WPA password. Enter an ASCII string with 8 - 63 characters. Note: Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!
EAP Preauthentification	Only for **Security Mode** = *WPA Enterprise* Select whether the EAP preauthentification function is to be activated. This function tells your device that WLAN clients, which are already connected to another access point, can first carry out 802.1x authentication as soon as they are within range. Such WLAN clients can then simply connect over the existing network connection with your device. The function is activated by selecting *Enabled*. The function is enabled by default.

Fields in the MAC-Filter menu

Field	Description
ACL Mode	Select whether only certain clients are to be permitted for this wireless network. The function is activated by selecting *Enabled*. The function is disabled by default.
Allowed Addresses	Use **Add** to make entries and enter the MAC addresses (**MAC Address**) of the clients to be permitted.

12.2 Administration

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

12.2.1 Basic Settings

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

Field in the Basic SettingsWLAN Administration menu

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

Chapter 13 Networking

13.1 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**.

13.1.1 IP Routes

A list of all configured routes is displayed in the **Networking**->**Routes**->**IP Routes** menu.

13.1.1.1 Edit or New

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

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

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

Field in the IP RoutesRoute Class menu

Field	Description
Extended Route	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.

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

Fields in the IP RoutesRoute Parameters menu

Field	Description
Route Type	Select the type of route. Possible values: • *Network Route* (default value): Route to a network. • *Default Route* : Is used if no other suitable route is available. • *Host Route* : Route to a single host.
Destination IP Address/NetmaskDestination IP Address/Netmask	Only for **Route Type** *Host Route* or *Network Route* Enter the IP address of the destination host. In **Route Type** = *Network Route*, you additionally enter the corresponding netmask in the second field. If no entry is made, your device uses a default netmask.
Interface	If necessary, enter the interface to be used for this route.
Network Type	Not for **Route Type** = *Default Route* Also select the network type. Possible values: • *Direct* (default value): • in the LAN: You define another IP address for the interface. • in the WAN: You define a route without a transit network. • *Indirect*: • in the LAN: You define a gateway route. • in the WAN: You define a route with a transit network.
Local IP Address	Only for **Network Type** = *Direct* Enter the IP address of the gateway to which your device is to

Field	Description
	forward the IP packets.
Gateway	Only for **Network Type** = *Indirect* Enter the IP address of the host 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 IP RoutesExtended Route Parameters menu

Field	Description
Source Interface	Select the interface over which the data packets are to reach the device. The default value is *None*.
New 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: *ICMP* , *TCP* , *UDP* , *GRE* , *ESP* , *AH* , *OSPF* , *L2TP*, *Any* . The default value is *Any*.
Source Port	Only for **Layer 4 Protocol** = *TCP* or *UDP*. Enter the source port. First select the port number range. Possible values: • *Any* (default value): The route is valid for all port numbers. • *Single*: Enables the entry of a port number. • *Range*: Enables the entry of a range of port numbers. • *Privileged*: Entry of privileged port numbers: 0 ... 1023.

Field	Description
	• *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 priviliged*: 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 priviliged*: Entry of unprivileged port numbers: 1024 ... 65535. Enter the appropriate values for the individual port or start port of a range in **Port** and, for a range, the end port in **to Port**.
DSCP / TOS Value	Select the Type of Service (TOS). Possible values: • *Ignore* (default value): The type of service is ignored. • *DSCP Binary Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format). • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format).

Field	Description
	- *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. - *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. Enter the relevant value for *DSCP Binary Value*, *DSCP Decimal Value*, *TOS Binary Value* and *TOS Decimal 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".

13.1.2 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.

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

Fields in the OptionsBack Route Verify menu

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

Fields in the OptionsGeneral menu

Field	Description
Allow deleting/editing all routing entries	Define whether all the routes entered on your device can be edited and deleted in the **Networking**->**Routes**->**IP Routes** menu. The function is enabled with *Enabled*. By default, the function is deactivated for all interfaces.

13.2 NAT

13.2.1 NAT Interfaces

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 131).

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

For every NAT interface, the `NAT active`, `Silent Deny` and `PPTP Passthrough` options 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.
Silent Deny	Select whether IP packets are to be silently denied by NAT. If this function is deactivated, the sender of the denied IP packet is informed by means of an ICMP or TCP RST message. The function is disabled by default.
PPTP Passthrough	Select whether the setup and operation of several simultaneous, outgoing PPTP connections from hosts in the network are also to be permitted if NAT is activated. The function is disabled by default. If **PPTP Passthrough** is enabled, the device itself cannot be configured as a tunnel endpoint.
Port	Shows the number of portforwarding rules configured in **Networking**->**NAT**->**NAT Configuration** .

13.2.2 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.

13.2.2.1 New

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

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

Field in the NAT ConfigurationBasic Parameters menu

Field	Description
Description	Enter a description for the NAT configuration.
Interface	Select the interface for which NAT is to be configured. Possible values: • `Any` (default value): NAT is configured for all interfaces. • `<Interface name>`: Select one of the interfaces from the list.
Type of traffic	Select the type of data traffic for which NAT is to be configured. Possible values: • `incoming (Destination NAT)` (default value): The data traffic that comes from outside. • `outgoing (Source NAT)`: Outgoing data traffic. • `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 NAT ConfigurationSpecify original traffic menu

Field	Description
Service	Not for **Type of traffic** = *outgoing (Source NAT)* and **NAT method** = *full-cone*, *restricted-cone* or *port-restricted-cone*. Select one of the preconfigured services. Possible values: • *User-defined* (default value) • *<service name>*
Protocol	Only for certain services. Not for **Type of traffic** = *outgoing (Source NAT)* and **NAT method** = *full-cone*, *restricted-cone* or *port-restricted-cone*. In this case UDP is automatically defined. Select a protocol. According to the selected **Service**, different protocols are available.

Field	Description
	Possible values: - *Any* (default value) - *AH* - *Chaos* - *EGP* - *ESP* - *GGP* - *GRE* - *HMP* - *ICMP* - *IGP* - *IGRP* - *IP* - *IPinIP* - *IPv6* - *IPX in IP* - *ISO-IP* - *Kryptolan* - *L2TP* - *OSPF* - *PUP* - *RDP* - *RSVP* - *SKIP* - *TCP* - *TLSP* - *UDP* - *VRRP* - *XNS-IDP*
Source IP Address/ Netmask	Enter the source IP address and corresponding netmask of the original data packets, as the case arises.

Field	Description
Source Port	Only for **Type of traffic** = *outgoing (Source NAT)*, **NAT method** = *symmetric* and **Service** = *User-defined*. Enter the source port of the original data packets. The default setting *-All-* means that the port remains unspecified.
Source Port/Range	Not for **Type of traffic** = *outgoing (Source NAT)* Enter the source port or the source port range of the original data packets. The default setting *-All-* means that the port remains unspecified.
Original Destination IP Address/Netmask	Enter the destination IP address and corresponding netmask of the original data packets, as the case arises.
Original Destination Port/Range	Only for **Service** = *User-defined*. Enter the destination port or the destination port range of the original data packets. The default setting All means that the port is not specified.

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

Fields in the NAT ConfigurationReplacement Values menu

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)*. Leave the destination port as it appears or enter the destination port to which the original destination port is to be translated. Selecting *Original* leaves the original destination port. If you disable *Original*, an input field appears in which you can enter a new destination port. *Original*is active by default.
New Source IP Address/Netmask	Only for **Type of traffic** = *outgoing (Source NAT)*.

Field	Description
	Enter the source IP address and corresponding netmask to which the original source IP address is to be translated.
New Source Port	Only for **Type of traffic** = *outgoing (Source NAT)*. 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 q-port. *Original*is active by default.

13.3 Load Balancing

13.3.1 Load Balancing Groups

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

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

A list of all configured load balancing groups is displayed in the **Networking**->**Load Balancing**->**Load Balancing Groups** menu. Clicking the magnifier icon opens an overview of basic parameters pertaining to this group.

Note

Note that all interfaces collected under a Load Balancing Group must have routes with identical metrics. If applicable, go to **Networking**->**Routes** and verify the relevant entries.

13.3.1.1 New

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

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

Fields in the Load Balancing GroupsBasic Parameters menu

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

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

Use **Add** to create more entries.

Fields in the Load Balancing GroupsInterface Selection for Distribution menu

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

13.4 QoS

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

The QoS configuration consists of three parts:

- Creating IP filters
- Classifying data
- Prioritising data.

13.4.1 QoS Filter

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

13.4.1.1 New

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

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

Fields in the QoS FilterBasic Parameters menu

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

Field	Description
	• *Any* (default value): All TCP packets match the filter.
Destination IP Address/Netmask	Enter the destination IP address of the data packets and the corresponding netmask.
Destination Port/Range	Only for **Protocol** = *tcp* or *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 IP Address/ Netmask	Enter the source IP address of the data packets and the corresponding netmask.
Source Port/Range	Only for **Protocol** = *tcp* or *udp* Enter a source port number or a range of source port numbers. Possible values: • *-All-* (default value): The destination port is not specified. • *Specify port*: Enter a destination port. • *Specify port range*: Enter a destination port range.
DSCP/TOS Filter (Layer 3)	Specify how the priority of the IP packets is signalled. Possible values: • *Ignore* (default value): No priority signalling is used. • *DSCP Binary Value*: Differentiated Services Code Point is used to signal the priority of IP packets (indicated in binary format, 6 bit). • *DSCP Decimal Value*: Differentiated Services Code Point is used to signal the priority of IP packets (indicated in decimal format). • *TOS Binary Value*: Type of Service is used to signal the priority of IP packets (indicated in binary format 8 bit). • *TOS Decimal Value*: Type of Service is used to signal the

Field	Description
	priority of IP packets (indicated in decimal format). Additional information on DSCP and TOS in RFC's 3260 and 1349.
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*. Value range *0* to *7*. The default value is *0*.

13.4.2 QoS Classification

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

13.4.2.1 New

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

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

Fields in the QoS ClassificationBasic Parameters menu

Field	Description
Class map	Choose the class plan you want to create or edit. Possible values: • *New* (default value): You can create a new class plan with this setting. • *<Name of class plan>*: Shows a class plan that has already been created, which you can select and edit. You can add new filters.
Description	Only for **Class map** = *New*. Enter the name of the class plan.

Field	Description
Filter	Select an IP filter. If the class plan is new, select the filter to be set at the first point of the class plan. If the class plan already exists, select the filter to be attached to the class plan. To select a filter, at least one filter must be configured in the **Networking**->**QoS**->**QoS Filter** menu.
Direction	Select the direction of the data packets to be classified. Possible values: • *Incoming*: Incoming data packets are assigned to the **Class ID** specified below . • *Outgoing* (default value): Outgoing data packets are assigned to the **Class ID** specified belowd. • *Both*: Incoming and outgoing data packets are assigned to the **Class ID** specified below.
High Priority Class	Enable or disable the high priority class. If the high priority class is active, the data packets are associated with the class with the highest priority and priority 0 is set automatically. The function is enabled with *Enabled*. The function is disabled by default.
Class ID	Only for **High Priority Class** not active. Choose a number which assigns the data packets to a class. Note: The class ID is a label to assign data packets to specific classes. (The class ID defines the priority.) Possible values are whole numbers between *1* and *254*.
Set DSCP/TOS value (Layer 3)	Here you can set or modify the DSCP/TOS value of IP datagrams according to the specified class (**Class ID**). Possible values: • *Preserve* (default value): The DSCP/TOS value of the IP da-

Field	Description
	tagrams remains unchanged. • `DSCP Binary Value`: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 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). • `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.
Set COS value (802.1p/Layer 2)	Here you can set or change the Class of Service (Layer 2 Priority) within the VLAN Ethernet header of the IP datagrams in correspondence to the class (**Class ID**) they have been assigned to. Possible values are whole numbers between `0` and `7`. The default value is `Preserve`.
Interfaces	Only for **Class map** = `New`. When creating a new class plan, select the interfaces to which you want to link the class plan. A class plan can be assigned to multiple interfaces.

13.4.3 QoS Interfaces/Policies

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

Note

Data can only be prioritized in the outgoing direction.

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

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

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

13.4.3.1 New

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

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

Fields in the QoS Interfaces/PoliciesBasic Parameters menu

Field	Description
Interface	Select the interface for which QoS is to be configured.
Priorisation algorithm	Select the algorithm according to which the queues are to be processed. This activates and deactivates QoS on the selected interface. Possible values: • *Priority Queueing*: QoS is activated on the interface. The available bandwidth is distributed strictly according to the queue priority. • *Weighted Round Robin*: QoS is activated on the interface. The available bandwidth is distributed according to the weighting (weight) of the queue. Exception: High-priority packets are always handled with priority. • *Weighted Fair Queueing*: QoS is activated on the interface. The available bandwidth is distributed as “fairly” as possible among the (automatically detected) traffic flows in a queue. Exception: High-priority packets are always handled with priority. • *Disabled* (default value): QoS is deactivated on the interface. The existing configuration is not deleted, but can be activated again if required.
Traffic shaping	Activate or deactivate data rate limiting in the send direction. The function is enabled with *Enabled*.

Field	Description
	The function is disabled by default.
Maximum Upload Speed	Only for **Traffic shaping** enabled. Enter a maximum data rate for the queue in the send direction in kbits. Possible values are *0* to *1000000*. The default value is *0*, i.e. no limits are set, the queue can occupy the maximum bandwidth.
Protocol Header Size below Layer 3	Choose the interface type to include the size of the respective overheads of a datagram when calculating the bandwidth. Possible values: • *User defined*(value in bytes; possible values are *0* to *100*.) • *Ethernet* (default value) Only for Ethernet interfaces: • *Ethernet* • *Ethernet and VLAN* • *PPP over Ethernet* • *PPP over Ethernet and VLAN* Only for IPSec interfaces: • *IPSec over Ethernet* • *IPSec over Ethernet and VLAN* • *IPSec via PPP over Ethernet* • *IPSec via PPPoE and VLAN*
Real Time Jitter Control	Only for **Traffic shaping** enabled Real Time Jitter Control optimises latency when forwarding real time datagrams. The function ensures that large data packets are fragmented according to the available upload bandwidth. Real Time Jitter Control is useful for small upload bandwidths (< 800 kbps). Activate or deactivate Real Time Jitter Control.

Field	Description
	The function is enabled with *Enabled*. The function is disabled by default.
Control Mode	Only for **Real Time Jitter Control** enabled. Select the mode for optimising voice transmission. Possible values: • *All RTP Streams*: All RTP streams are optimised. The function activates the RTP stream detection mechanism for the automatic detection of RTP streams. In this mode, the Real Time Jitter Control is activated as soon as an RTP stream has been detected. • *Inactive*: Voice data transmission is not optimised. • *Controlled RTP Streams only*: This mode is used if either the VoIP Application Layer Gateway (ALG) or the VoIP Media Gateway (MGW) is active. Real Time Jitter Control is activated by the control instances ALG or MGW. • *Always*: Real Time Jitter Control is always active, even if no real time data is routed.
Queues/Policies	Configure the desired QoS queues. For each class created from the class plan, which is associated with the selected interface, a queue is generated automatically and displayed here (only for data traffic classified as outgoing and for data traffic classified as moving in both directions). Add new entries with **Add**. The **Edit Queue/Policy** menu opens.

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

Fields in the Edit Queue/Policy menu

Field	Description
Description	Enter the name of the queue/policy.
Outbound Interface	Shows the interface for which the QoS queues are being configured.
Priorisation queue	Select the queue priority type.

Field	Description
	Possible values: • *Class Based* (default value): Queue for data classified as “normal”. • *High Priority*: Queue for data classified as “high priority”. • *Default*: Queue for data that has not been classified or data of a class for which no queue has been configured.
Class ID	Only for **Priorisation queue** = *Class Based*. Select the QoS packet class to which this queue is to apply. To do this, at least one class ID must be given in the **Networking**->**QoS**->**QoS Classification** menu.
Priority	Only for **Priorisation queue** = *Class Based*. Choose the priority of the queue. Possible values are *1 (high priority)* to *254 (low priority)*. The default value is *1*.
Weight	Only for **Priorisation algorithm** = *Weighted Round Robin* or *Weighted Fair Queueing* Choose the priority of the queue. Possible values are *1* to *254*. The default value is *1*.
RTT Mode (Realtime Traffic Mode)	Active or deactivate the real time transmission of the data. The function is enabled with *Enabled*. The function is disabled by default. RTT mode should be activated for QoS classes in which real time data has priority. This mode improves latency when forwarding real time datagrams. It is possible to configure multiple queues when RTT mode is enabled. Queues with enabled RTT mode must always have a higher priority than queues with disabled RTT mode.
Traffic Shaping	Activate or deactivate data rate (=Traffic Shaping) limiting in the send direction.

Field	Description
	The data rate limit applies to the selected queue. (This is not the limit that can be defined on the interface.) The function is enabled with *Enabled*. The function is disabled by default.
Maximum Upload Speed	Only for **Traffic Shaping** enabled. Enter a maximum data rate for the queue in kbits. Possible values are *0* to *1000000*. The default value is *0*.
Overbooking allowed	Only for **Traffic Shaping** enabled. Enable or disable the function. The function controls the bandwidth limit. If **Overbooking allowed** is activated, the bandwidth limit set for this queue can be exceeded, as long as free bandwidth exists on the interface. If **Overbooking allowed** is deactivated, the queue can never occupy bandwidth beyond the bandwidth limit that has been set. The function is enabled with *Enabled*. The function is disabled by default.
Burst size	Only for **Traffic Shaping** enabled. Enter the maximum number of bytes that may still be transmitted temporarily when the data rate permitted for this queue has been reached. Possible values are *0* to *64000*. The default value is *0*.

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

Fields in the Advanced Settings menu

Field	Description
Dropping Algorithm	Choose the procedure for rejecting packets in the QoS queue, if the maximum size of the queue is exceeded. Possible values: • *Tail Drop* (default value): The newest packet received is dropped. • *Head Drop*: The oldest packet in the queue is dropped. • *Random Drop*: A randomly selected packet is dropped from the queue.
Congestion Avoidance (RED)	Select the process according to which packets are preventively dropped between **Min. queue size** and **Max. queue size** to prevent queue overflow (Random Early Detection). Possible values: • *None* (default value): No packets are dropped. • *weighted-random*: Packets are dropped according to the level of the queue. This procedure ensures a smaller long-term queue size for TCP-based data traffic, so that traffic bursts can also usually be transmitted without large packet losses.
Min. queue size	Enter the lower threshold value for the process **prevention of data congestion (RED)** in bytes. Possible values are *0* to *262143*. The default value is *0*.
Max. queue size	Enter the upper threshold value for the process **prevention of data congestion (RED)** in bytes. Possible values are *0* to *262143*. The default value is *16384*.

13.5 Access Rules

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

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

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

Access lists are an effective means if, for example, sites with LANs interconnected over a **bintec** gateway wish to deny all incoming FTP requests or only allow Telnet sessions between certain hosts.

Access filters in the gateway are based on the combination of filters and actions for filter rules (= rules) and the linking of these rules to form rule chains. They act on the incoming data packets to allow or deny access to the gateway for certain data.

A filter describes a certain part of the IP data traffic based on the source and/or destination IP address, netmask, protocol and source and/or destination port.

You use the rules that you use in the access lists to tell the gateway what to do with the filtered data packets, i.e. whether it should allow or deny them. You can also define several rules, which you arrange in the form of a chain to obtain a certain sequence.

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

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

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

or

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

or

- Combination of the two possibilities described above.

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

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

Caution

Make sure you don't lock yourself out when configuring filters.

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

13.5.1 Access Filter

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

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

13.5.1.1 Edit or New

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

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

Fields in the Access FilterBasic 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*

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

Field	Description
	Possible values: • *Any* (default value) • *Host*: Enter the IP address of the host. • *Network*: Enter the network address and the related netmask.
Destination Port/Range	Only if **Protocol** = *tcp*, *udp* Enter the destination port number or range of destination port numbers that matches the filter. Possible values: • *-All-* (default value): The route 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 IP Address/ Netmask	Enter the source IP address and netmask of the data packets.
Source Port/Range	Only if **Protocol** = *tcp*, *udp* Enter the source port number or range of source port numbers. Possible values: • *-All-* (default value): The route 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

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

13.5.2 Rule Chains

Rules for IP filters are configured in the access list menu. These can be created separately or incorporated in rule chains.

In the **Networking**->**Access Rules**+**Rule Chains** menu, all created filter rules are listed.

13.5.2.1 Edit or New

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

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

Fields in the Rule ChainsBasic Parameters menu

Field	Description
Rule Chain	Select whether to create a new rule chain or to edit an existing one. Possible values:

Field	Description
	• *New* (default value): You can create a new rule chain with this setting. • *<Name of class plan>*: 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* (default value): Allow packet if it matches the filter. • *Allow if filter does not match*: Allow packet if it does not match the filter. • *Deny if filter matches*: Deny packet if it matches the filter. • *Deny if filter does not match*: Deny packet if it does not match the filter. • *Ignore*: Use next rule.

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

13.5.3 Interface Assignment

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

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

13.5.3.1 Edit or New

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

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

Fields in the Interface AssignmentBasic 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. The function is enabled with *Enabled*. The function is activated by default.
Reporting Method	Define whether a syslog message is to be generated if a packet is denied. Possible values: • *No report*: No syslog message. • *Info* (default value): A syslog message is generated with the protocol number, source IP address and source port number. • *Dump*: A syslog message is generated with the contents of the first 64 bytes of the denied packet.

Chapter 14 Routing Protocols

14.1 RIP

The entries in the routing table can be defined statically or the routing table can be updated constantly by dynamic exchange of routing information between several devices. This exchange is controlled by a Routing Protocol, e.g. RIP (Routing Information Protocol). By default, about every 30 seconds (this value can be changed in **Update Timer**), a device sends messages to remote networks using information from its own current routing table. The complete routing table is always exchanged in this process. If triggered RIP is used, information is only exchanged if the routing information has changed. In this case, only the changed information is sent.

Observing the information sent by other devices enables new routes and shorter paths for existing routes to be saved in the routing table. As routes between networks can become unreachable, RIP removes routes that are older than 5 minutes (i.e. routes not verified in the last 300 seconds - **Garbage Collection Timer** + **Route Timeout** -). Routes learnt with triggered RIP are not deleted.

Your device supports both version 1 and version 2 of RIP, either individually or together.

14.1.1 RIP Interfaces

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

14.1.1.1 Edit

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

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

Fields in the RIP Parameters for menu

Field	Description
Send Version	Decide whether routes are to be propagated via RIP and if so, select the RIP version for sending RIP packets over the interface in send direction.

Field	Description
	Possible values: • *None* (default value): RIP is not enabled. • *RIP V1*: Enables sending and receiving of version 1 RIP packets. • *RIP V2*: Enables sending and receiving of version 2 RIP packets. • *RIP V1/V2*: Enables sending and receiving RIP packets of both version 1 and 2. • *RIP V2 Multicast*: For sending RIP V2 messages over the multicast address 224.0.0.9. • *RIP V1 Triggered*: RIP V1 messages are sent, received and processed as per RFC 2091 (triggered RIP). • *RIP V2 Triggered*: RIP V2 messages are sent, received and processed as per RFC 2091 (triggered RIP).
Receive Version	Decide whether routes are to be imported via RIP and if so, select the RIP version for receiving RIP packets over the interface in receive direction. Possible values: • *None* (default value): RIP is not enabled. • *RIP V1*: Enables sending and receiving of version 1 RIP packets. • *RIP V2*: Enables sending and receiving of version 2 RIP packets. • *RIP V1/V2*: Enables sending and receiving RIP packets of both version 1 and 2. • *RIP V1 Triggered*: RIP V1 messages are sent, received and processed as per RFC 2091 (triggered RIP). • *RIP V2 Triggered*: RIP V2 messages are sent, received and processed as per RFC 2091 (triggered RIP).
Route Announce	Select this option if you want to set the time at which any activated routing protocols (e.g. RIP) are to propagate the IP routes defined for this interface. Note: This setting does not affect the interface-specific RIP configuration mentioned above.

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

14.1.2 RIP Filter

In this menu, you can specify exactly which routes are to be exported or imported.

You can use the following strategies for this:

- You explicitly deactivate the import or export of certain routes. The import or export of all other routes that are not listed is still allowed.
- You explicitly activate the import or export of certain routes. In this case, you must also explicitly deactivate the import or export of all other routes. You reach this via a filter for **IP Address / Netmask** = no entry (this corresponds to IP address 0.0.0.0 with netmask 0.0.0.0). To make sure this filter is used last, it must be placed at the lowest position.

You configure a filter for a default route with the following values:

- **IP Address / Netmask** = IP address (this corresponds to IP address 0.0.0.0), for netmasks = 255.255.255.255

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

You can use the button to insert another filter above the list entry. The configuration menu for creating a new window opens.

You can use the button to move the list entry. A dialog box opens, in which you can select the position to which the filter is to be moved.

14.1.2.1 New

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

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

Fields in the RIP FilterBasic Parameters menu

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

14.1.3 RIP Options

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

Fields in the RIP OptionsGlobal RIP Parameters menu

Field	Description
RIP UDP Port	The setting option UDP Port, which is used for sending and re-

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

Fields in the RIP OptionsTimer for RIP V2 (RFC 2453) menu

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

Fields in the RIP OptionsTimer for Triggered RIP (RFC 2091) menu

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

Chapter 15 Multicast

What is multicasting?

Many new communication technologies are based on communication from one sender to several recipients. Therefore, modern telecommunication systems such as voice over IP or video and audio streaming (e.g. IPTV or Webradio) focus on reducing data traffic, e.g. by offering TriplePlay (voice, video, data). Multicast is a cost-effective solution for effective use of bandwidth because the sender of the data packet, which can be received by several recipients, only needs to send the packet once. The packet is sent to a virtual address defined as a multicast group. Interested recipients log in to these groups.

Other areas of use

One classic area in which multicast is used is for conferences (audio/video) with several recipients. The most well-known are probably the MBone Multimedia Audio Tool (VAT), Video Conferencing Tool (VIC) and Whiteboard (WB). VAT can be used to hold audio conferences. All subscribers are displayed in a window and the speaker(s) are indicated by a black box. Other areas of use are of particular interest to companies. Here, multicasting makes it possible to synchronise the databases of several servers, which is valuable for multinationals or even companies with just a few locations.

Address range for multicast

For, IPv4 the IP addresses 224.0.0.0 to 239.255.255.255 (224.0.0.0/4) are reserved for multicast in the class D network. An IP address from this range represents a multicast group to which several recipients can log in. The multicast router then forwards the required packets to all subnets with logged in recipients.

Multicast basics

Multicast is connectionless, which means that any trouble-shooting or flow control needs to be guaranteed at application level.

At transport level, UDP is used almost exclusively, as, in contrast to TCP, it is not based on a point-to-point connection.

At IP level, the main difference is therefore that the destination address does not address a dedicated host, but rather a group, i.e. during the routing of multicast packets, the decisive factor is whether a recipient is in a logged-in subnet.

In the local network, all hosts are required to accept all multicast packets. For Ethernet or FDD, this is based on MAC mapping, where the group address is encoded into the destination MAC address. For routing between several networks, the routers first need to make themselves known to all potential recipients in the subnet. This is achieved by means of Membership Management protocols such as IGMP for IPv4 and MLP for IPv6.

Membership Management protocol

In IPv4, IGMP (Internet Group Management Protocol) is a protocol that hosts can use to provide the router with multicast membership information. IP addresses of the class D address range are used for addressing. An IP address in this class represents a group. A sender (e.g. Internet radio) sends data to this group. The addresses (IP) of the various senders within a group are called the source (addresses). Several senders (with different IP addresses) can therefore transmit to the same multicast group, leading to a 1-to-n relationship between groups and source addresses. This information is forwarded to the router by means of reports. In the case of incoming multicast data traffic, a router can use this information to decide whether a host in its subnet wants to receive it. Your device supports the current version IGMP V3, which is upwardly compatible, which means that both V3 and V1/V2 hosts can be managed.

Your device supports the following multicast mechanisms:

- Forwarding: This relates to static forwarding, i.e. incoming data traffic for a group is passed in all cases. This is a useful option if multicast data traffic is to be permanently passed.
- IGMP: IGMP is used to gather information about the potential recipients in a subnet. In the case of a hop, incoming multicast data traffic can thus be selected.

Tip

With multicast, the focus is on excluding data traffic from unwanted multicast groups. Note that if forwarding is combined with IGMP, the packets can be forwarded to the groups specified in the forwarding request.

15.1 General

15.1.1 General

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

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

Fields in the GeneralBasic Settings menu

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

15.2 IGMP

IGMP (Internet Group Management Protocol, see RFC 3376) is used to signal the information about group (membership) in a subnet. As a result, only the packets explicitly wanted by a host enter the subnet.

Special mechanisms ensure that the requirements of the individual clients are taken into consideration. At the moment there are three versions of IGMP (V1 - V3); most current systems use V3, and less often V2.

Two packet types play a central role in IGMP: queries and reports.

Queries are only transmitted from a router. If several IGMP routers exist in a network, the router with the lowest IP address is the "querier". We differentiate here between a general query (sent to 224.0.0.1), a group-specific query (sent to a group address) and the group-and-source-specific query (sent to a specific group address). Reports are only sent by hosts to respond to queries.

15.2.1 IGMP

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

15.2.1.1 Edit or New

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

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

Fields in the IGMPIGMP Settings menu

Field	Description
Interface	Select the interface on which IGMP is to be enabled, i.e. queries are sent and responses are accepted.
Query Interval	Enter the interval in seconds in which IGMP queries are to be sent. Possible values are `0` to `600`. The default value is `125`.
Maximum Response Time	For the sending of queries, enter the time interval in seconds within which hosts must respond. The hosts randomly select a time delay from this interval before sending the response. This spreads the load in networks with several hosts, improving performance. Possible values are `0` to `100`. The default value is `100`.
Robustness	Select the multiplier for controlling the timer values. A higher value can e.g. compensate for packet loss in a network susceptible to loss. If the value is too high, however, the time between logging off and stopping of the data traffic can be increased (leave latency). Possible values are `2` to `8`. The default value is `2`.
Last Member Query Interval	Define the time after a query for which the router waits for an answer. If you shorten the interval, it will be more quickly detected that the last member has left a group so that no more packets for this group should be forwarded to this interface. Possible values are `0` to `255`. The default value is `10`.

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

IGMP Proxy

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

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

Fields in the Advanced Settings menu

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

15.2.2 Options

In this menu, you can enable and disable IGMP on your system. You can also define whether IGMP is to be used in compatibility mode or only IGMP V3 hosts are to be accepted.

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

Fields in the OptionsBasic Settings menu

Field	Description
IGMP Status	Select the IGMP status. Possible values: • *Auto* (default value): Multicast is activated automatically for hosts if the hosts open applications that use multicast. • *Up*: Multicast is always on. • *Down*: Multicast is always off.
Mode	Only for **IGMP Status** = *Up* or *Auto* Select Multicast Mode. Possible values: • *Compatibility Mode* (default value): The router uses IGMP version 3. If it notices a lower version in the network, it uses the lowest version it could detect. • *Version 3 only*: Only IGMP version 3 is used.
Maximum Groups	Enter the maximum number of groups to be permitted, both internally and in reports.
Maximum Sources	Enter the maximum number of sources that are specified in version 3 reports and the maximum number of internally managed sources per group.
IGMP State Limit	Enter the maximum permitted total number of incoming queries and messages per second. The default value is *0*, i.e. the number of IGMP status messages is not limited.

15.3 Forwarding

15.3.1 Forwarding

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

15.3.1.1 New

Choose the **New** button to create forwarding rules for new multicast groups.

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

Fields in the ForwardingBasic Parameters menu

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

Chapter 16 WAN

This menu offers various options for configuring accesses or connections from your LAN to the WAN. You can also optimise voice transmission here for telephone calls over the Internet.

16.1 Internet + Dialup

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

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

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

Note

Note your provider's instructions.

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

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

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

Possible values for Status

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

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

Default Route

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

Activating NAT

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

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

Connection Idle Timeout

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

Block after Connection Failure

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

Authentication

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

Your device needs the necessary data for this, which you should enter here, for all PPP connections. Establish the type of authentication process that should be performed, then enter a common password and two codes. You get this information, for example, from your Internet Service Provider (ISP) or the system administrator at your head office. If the data you entered on your device is the same as the caller's data, the call is accepted. The call is rejected if the data is not the same.

Callback

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

Channel Bundling

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

Dynamic

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

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

Static

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

16.1.1 PPPoE

In the **WAN**->**Internet + Dialup**->**PPPoE** menu, a list of all PPPoE interfaces is displayed.

PPP over Ethernet (PPPoE) is the use of the Point-to-Point Protocol (PPP) network protocol over an Ethernet connection. Today, PPPoE is used for ADSL connections in Germany. In Austria, the Point To Point Tunnelling Protocol (PPTP) was originally used for ADSL access. However, PPPoE is now offered here too by some providers.

16.1.1.1 New

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

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

Fields in the PPPoEBasic Parameters menu

Field	Description
Description	Enter a name to uniquely identify the PPPoE partner. The first character in this field must not be a number No special characters or umlauts must be used.
PPPoE Mode	Select whether you want to use a standard Internet connection over PPPoE (`Standard`), or whether your Internet access is to be set up over several interfaces (`Multilink`). If you choose `Multilink`, you can combine several DSL connections from a provider over PPP as a static bundle in order to obtain more bandwidth. Each of these DSL connections should use a separate Ethernet connection for this. At the moment, many providers are still in the process of preparing the PPPoE Multilink function. For PPPoE Multilink, we recommend using your device's Ethernet switch in Split-Port mode and to use a separate Ethernet interface e.g. `en1-1`, `en1-2` for each PPPoE connection.
PPPoE Ethernet Interface	Only for **PPPoE Mode** = `Standard` Select the Ethernet interface specified for a standard PPPoE connection. If you want to use an external DSL modem, select the Ethernet port to which the modem is connected. When using the internal DSL modem, select here the EthoA interface configured in **Physical Interfaces**->**ATM**->**Profiles**->**New**
PPPoE Interfaces for Multilink	Only for **PPPoE Mode** = `Multilink` Select the interfaces you want to use for your Internet connection. Click the **Add** button to create new entries.
User Name	Enter the user name.

Field	Description
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the short hold. The default value is *300*. Example: *10* for FTP transmission, *20* for LAN-to-LAN transmission, *90* for Internet connections.

Fields in the PPPoEIP Mode and Routes menu

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

Field	Description
Create NAT Policy	Specify whether Network Address Translation (NAT) is to be activated. The function is enabled with *Enabled*. The function is enabled by default.
Local IP Address	Only if **IP Address Mode** = *Static* Enter the static IP address of the connection partner.
Route Entries	Only if **IP Address Mode** = *Static* Define other routing entries for this connection partner. Add new entries with **Add**. • *Remote IP Address*: IP address of the destination host or network. • *Netmask*: Netmask for **Remote IP Address**. If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (possible values *0*... *15*). The default value is *1*.

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

Fields in the Advanced Settings menu

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

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

16.1.2 PPTP

In the **WAN**->**Internet + Dialup**->**PPTP** menu, a list of all PPTP interfaces is displayed.

In this menu, you configure an Internet connection that uses the Point Tunnelling Protocol (PPTP) to set up a connection, e.g. required in Austria.

16.1.2.1 New

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

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

Fields in the PPTPBasic Parameters menu

Field	Description
Description	Enter a name for uniquely identifying the internet connection. The first character in this field must not be a number No special characters or umlauts must be used.
PPTP Interface	Select the IP interface over which packets are to be transported to the remote PPTP terminal. If you want to use an external DSL modem, select the Ethernet port to which the modem is connected. When using the internal DSL modem, select here the EthoA interface configured in **Physical Interfaces**->**ATM**->**Profiles**->**New** for this connection, e.g. `ethoa50-0`.
User Name	Enter the user name.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with `Enabled`. The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.

Field	Description
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle interval in seconds. This determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the timeout. The default value is *300*. Example: *10* for FTP transmission, *20* for LAN-to-LAN transmission, *90* for Internet connections.

Fields in the PPTPIP Mode and Routes menu

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Get IP Address* (default value): Your device is automatically assigned a temporarily valid IP address from the provider. • *Static*: You enter a static IP address.
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is enabled by default.
Create NAT Policy	Specify whether Network Address Translation (NAT) is to be activated. The function is enabled with *Enabled*. The function is enabled by default.
Local IP Address	Only for **IP Address Mode** = *Static*. Assign an IP address from your LAN to the PPT interface, which is to be used as your device's internal source address.

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

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

Fields in the Advanced Settings menu

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *60*.
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are *0* to *100*. The default value is *5*.
Authentication	Select the authentication protocol for this Internet connection. Select the authentication specified by your provider. Possible values: • *PAP* (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); the password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP*: Primarily run CHAP, on denial then the

Field	Description
	authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) • `MS-CHAPv2`: Run MS-CHAP version 2 only. • `None`: Some providers use no authentication. In this case, select this option.
DNS Negotiation	Select whether your device receives IP addresses for **DNS Server Primary** and **DNS Server Secondary** from the connection partner or sends these to the connection partner. The function is enabled with `Enabled`. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is enabled with `Enabled`. The function is disabled by default.
PPTP Address Mode	Displays the address mode. The value cannot be changed. Possible values: • `Static`: The IP address of the Ethernet port selected in **PPTP Interface** is used.
Local PPTP IP Address	Assign the PPTP interface an IP address that is used as the source address. The default value is `10.0.0.140`.
Remote PPTP IP Address	Enter the IP address of the PPTP partner. The default value is `10.0.0.138`.
LCP Alive Check	Check whether the reachability of the remote terminal is to be checked by sending LCP echo requests or replies. This makes it possible to switch to a backup connection more quickly in the event of line faults. The function is enabled with `Enabled`.

Field	Description
	The function is disabled by default.

16.1.3 PPPoA

In the **WAN**->**Internet + Dialup**->**PPPoA** menu, a list of all PPPoA interfaces is displayed.

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

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

16.1.3.1 New

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

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

Fields in the PPPoABasic Parameters menu

Field	Description
Description	Enter a name for uniquely identifying the connection partner. The first character in this field must not be a number No special characters or umlauts must be used.
ATM PVC	Select an ATM profile created in the **ATM**->**Profiles** menu, indicated by the global identifiers VPI and VCI specified by the provider.
User Name	Enter the user name.
Password	Enter the password for the PPPoA connection.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default. Only activate this option if you have Internet access with a flat-

Field	Description
	rate charge.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are `0` to `3600` (seconds). `0` deactivates the short hold. The default value is `300`. Example: `10` for FTP transmission, `20` for LAN-to-LAN transmission, `90` for Internet connections.

Fields in the PPPoAIP Mode and Routes menu

Field	Description
IP Address Mode	Choose whether your device has a static IP address or is assigned one dynamically. Possible values: • `Get IP Address` (default value): Your device is dynamically assigned an IP address. • `Static`: You enter a static IP address.
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with `Enabled`. The function is enabled by default.
Create NAT Policy	Specify whether Network Address Translation (NAT) is to be activated. The function is enabled with `Enabled`. The function is enabled by default.
Local IP Address	Only for **IP Address Mode** = `Static`.

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

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

Fields in the Advanced Settings menu

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *60*.
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are *0* to *100*. The default value is *5*.
Authentication	Select the authentication protocol for this Internet connection. Select the authentication specified by your provider. Possible values: • *PAP* (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); the password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft

Field	Description
	Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP*: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
DNS Negotiation	Select whether your device receives IP addresses for **DNS Server Primary** and **DNS Server Secondary** from the connection partner or sends these to the connection partner. The function is enabled with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is enabled with *Enabled*. The function is disabled by default.
LCP Alive Check	Check whether the reachability of the remote terminal is to be checked by sending LCP echo requests or replies. This is recommended for leased lines, PPTP and L2TP connections. The function is enabled with *Enabled*. The function is disabled by default.

16.1.4 ISDN

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

In this menu, you configure the following ISDN connections:

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

16.1.4.1 New

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

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

Fields in the ISDNBasic Parameters menu

Field	Description
Description	Enter a name for uniquely identifying the connection partner. The first character in this field must not be a number No special characters or umlauts must be used.
Connection Type	Select which layer 1 protocol your device should use. This setting applies for outgoing connections to the connection partner and only for incoming connections from the connection partner if they could be identified on the basis of the calling party number. Possible values: • `ISDN 64 kbps`: For 64-kbps ISDN data connections. • `ISDN 56 kbps`: For 56-kbps ISDN data connections.
User Name	Enter your device code (local PPP user name).
Remote User (for Dial-in only)	Enter the code of the remote terminal (remote PPP user name).
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with `Enabled`. The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass

Field	Description
	between sending the last traffic data packet and clearing the connection. Possible values are *-1* to *3600* (seconds). A value of *-1* means that the connection is set up again immediately after disconnection and *0* deactivates short hold. The default value is *20*.

Fields in the ISDNIP Mode and Routes menu

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

Field	Description
	Assign the IP address from your LAN to the ISDN interface which is to be used as your device's internal source address.
Route Entries	Only if **IP Address Mode** = *Static* Define other routing entries for this connection partner. • *Remote IP Address*: IP address of the destination host or network. • *Netmask*: Netmask for **Remote IP Address**. If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (possible values *0*... *15*). The default value is *1*.
IP Assignment Pool	Only if **IP Address Mode** = *Provide IP Address* Select IP pools configured in the **WAN**->**Internet + Dialup**->**IP Pools** menu.

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

Fields in the Advanced Settings menu

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *300*.
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are *0* to *100*. The default value is *5*.
Usage Type	If necessary, select a special interface use. Possible values: • *Standard* (default value): No special type is selected. • *Dialin only* : The interface is used for incoming dialup connections and callbacks initiated externally.

Field	Description
	- *Multi-User (Dialin only)* : The interface is defined as multi-user connection partner, i.e. several clients dial in with the same user name and password.
Authentication	Select the authentication protocol for this PPTP partner. Possible values: - *PAP* (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. - *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); the password is transferred encrypted. - *PAP/CHAP*: Primarily run CHAP, otherwise PAP. - *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). - *PAP/CHAP/MS-CHAP*: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) - *MS-CHAPv2*: Run MS-CHAP version 2 only. - *None*: Some providers use no authentication. In this case, select this option.
Encryption	Only for **Authentication** = *MS-CHAPv2* If necessary, select the type of encryption that should be used for data traffic to the connection partner. This is only possible if STAC or MS-STAC compression is not activated for the connection. If **Encryption** is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: - *None* (default value): MPP encryption is not used. - *Enabled*: MPP encryption V2 with 128 bit is used to RFC 3078. - *Windows compatible*: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
Callback Mode	Select the Callback Mode function. Possible values:

Field	Description
	• *None* (default value): Your device does not call back. • *Active*: Select one of the following options: • *No PPP negotiation*: Your device calls the connection partner to request a callback. • *Windows Client Mode*: Your device calls the connection partner to request a callback via CBCP (Callback Control Protocol). Needed for Windows clients. • *Passive*: Select one of the following options: • *PPP Negotiation or CLID*: Your device calls back immediately when requested to do so by the connection partner. • *Windows Server Mode*: Your device calls back after a period of time proposed by the Microsoft client (NT: 10 seconds, new systems: 12 seconds. It uses the call number (**Entries**->**Call Number**) with the **Mode** *Outgoing* or *Both*, entered for the connection partner. If no number is entered, the required number can be reported by the caller in a PPP negotiation. This setting should be avoided where possible for security reasons. Currently cannot be avoided for the connection of mobile Microsoft clients via DCN. • *Delayed, CLID only*: Your device calls back after approx. four seconds if your device is requested to do so by the connection partner. Only makes sense for CLID. • *Windows Server Mode, Callback optional*: Like *Windows Server Mode* with the option of termination. This setting should be avoided for security reasons. The Microsoft client also has the option of aborting callback and maintaining the initial connection to your device without callback. This only applies if no fixed, outgoing number has been configured for the connection partner. This is done by pressing **Cancel** to close the dialog box that appears.

Field in the Advanced SettingsBandwith on Demand Options menu

Field	Description
Channel Bundling	Select whether channel bundling is to be used for ISDN connections with the connection partner, and if so, what type. Your device supports dynamic and static channel bundling for dialup connections. Only one B channel is initially opened when

Field	Description
	a connection is set up. Dynamic channel bundling means that your device connects other ISDN B channels to increase the throughput for connections if this is required, e.g. for large data rates. If the amount of data traffic drops, the additional B-channels are closed again. In static channel bundling, you specify right from the start how many B channels your device is to use, regardless of the transferred data rate. Possible values: • `None` (default value): No channel bundling, only one B channel is ever available for connections. • `Static`: Static channel bundling. • `Dynamic` : Dynamic channel bundling.

Field in the Advanced SettingsDial Numbers menu

Field	Description
Entries	Enter the connection partner's numbers. • **Mode**: Defines whether **Call Number** should be used for incoming or outgoing calls or for both. Possible values: • `Both` (default value): For incoming and outgoing calls. • `Incoming` : For incoming calls, where your connection partner dials in to your device. • `Outgoing`: For outgoing calls, if you wish to dial in to your connection partner. The calling party number of the incoming call is compared with the number entered under **Call Number**. • **Call Number**: Enter the connection partner's number.

Fields in the Advanced SettingsIP Options menu

Field	Description
OSPF Mode	Select whether and how routes are propagated via the interface and/or OSPF protocol packets are sent. Possible values:

Field	Description
	- *Passive* (default value): OSPF is not activated for this interface, i.e. no routes are propagated or OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces. - *Active*: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface. - *Inactive*: OSPF is disabled for this interface.
Proxy ARP Mode	Select whether and how ARP requests from your own LAN are to be responded to for the specified connection partner. Possible values: - *Inactive* (default value): Deactivates Proxy ARP for this connection partner. - *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the connection partner is *Up* or *Dormant*. In the case of *Dormant*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. - *Up only*: Your device responds to an ARP request only if the status of the connection to the connection partner is *Up*, i.e. a connection already exists to the connection partner.
DNS Negotiation	Select whether your device receives IP addresses for **DNS Server Primary** and **Secondary** and **WINS Server Primary** and **Secondary** from the connection partner or sends these to the connection partner. The function is enabled with *Enabled*. The function is enabled by default.

16.1.5 IP Pools

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

Your device can operate as a dynamic IP address server for PPP connections. You can use this function by providing one or more pools of IP addresses. These IP addresses can be assigned to dialling-in connection partners for the duration of the connection.

Any host routes entered always have priority over IP addresses from the address pools. This means if an incoming call has been authenticated, your device first checks whether a host route is entered in the routing table for this caller. If not, your device can allocate an IP address from an address pool (if available). If address pools have more than one IP address, you cannot specify which connection partner receives which address. The addresses are initially assigned in order. If a new dial-in takes place within an interval of one hour, an attempt is made to allocate the same IP address assigned to this partner the last time.

Choose the **Add** button to set up new IP pools.

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

Fields in the OptionsIP Pools menu

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

16.2 ATM

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

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

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

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

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

(VCI); this identifies the virtual connection.

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

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

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

16.2.1 Profiles

A list of all ATM profiles is displayed in the **WAN**->**ATM**->**Profiles** menu.

If the connection for your Internet access is set up using the internal modem, the ATM connection parameters must be set for this. An ATM profile combines a set of parameters for a specific provider.

By default an ATM profile with the description *AUTO-CREATED* is preconfigured. Its values (VPI 1 and VCI 32) are suitable for a Telekom ATM connection, for example.

Note

The ATM encapsulations are described in RFCs 1483 and 2684. You will find the RFCs on the relevant pages of the IETF (*www.ietf.org/rfc.html*).

16.2.1.1 New

Choose the **New** button to set up new ATM profiles.

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

Fields in the ProfilesATM Profiles Parameter menu

Field	Description
Provider	Select one of the preconfigured ATM profiles for your provider from the list or manually define the profile using *-- User-defined --*.

Field	Description
Description	Only for **Provider** = *-- User-defined --* Enter the desired description for the connection.
Type	Only for **Provider** = *-- User-defined --* Select the protocol for the ATM connection. Possible values: • *Ethernet over ATM* (default value): Ethernet over ATM (EthoA) is used for the ATM connection (Permanent Virtual Circuit, PVC). • *Routed Protocols over ATM*: Routed Protocols over ATM (RPoA) is used for the ATM connection (Permanent Virtual Circuit, PVC). • *PPP over ATM*: PPP over ATM (PPPoA) is used for the ATM connection (Permanent Virtual Circuit, PVC).
Virtual Path Identifier (VPI)	Only for **Provider** = *-- User-defined --* Enter the VPI value of the ATM connection. The VPI is the identification number of the virtual path to be used. Note your provider's instructions. Possible values are *0* to *255*. The default value is *8*.
Virtual Channel Identifier (VCI)	Only for **Provider** = *-- User-defined --* Enter the VCI value of the ATM connection. The VCI is the identification number of the virtual channel. A virtual channel is the logical connection for the transport of ATM cells between two or more points. Note your provider's instructions. Possible values are *32* to *65535*. The default value is 32.
Encapsulation	Only for **Provider** = *-- User-defined --* Select the encapsulation to be used. Note your provider's instructions.

Field	Description
	Possible values (in accordance with RFC 2684): • *LLC Bridged no FCS*(Default value for Ethernet over ATM): Is only displayed for **Type** = *Ethernet over ATM*. Bridged Ethernet with LLC/SNAP encapsulation without Frame Check Sequence (checksums). • *LLC Bridged FCS*: Is only displayed for **Type** = *Ethernet over ATM*. Bridged Ethernet with LLC/SNAP encapsulation with Frame Check Sequence (checksums). • *Non ISO* (default value for Routed Protocols over ATM): Is only displayed for **Type** = *Routed Protocols over ATM*. Encapsulation with LLC/SNAP header, suitable for IP routing. • *LLC*: Is only displayed for **Type** = *PPP over ATM*. Encapsulation with LLC header. • *VC Multiplexing*(Default value for PPP over ATM): Bridged Ethernet without additional encapsulation (Null Encapsulation) with Frame Check Sequence (checksums).

Fields in the Ethernet over ATM Settings menu (appears only for Type = Ethernet over ATM)

Field	Description
Default Ethernet for PPPoE Interfaces	Only for **Type** = *Ethernet over ATM* Select whether this Ethernet-over-ATM interface is to be used for all PPPoE connections The function is enabled with *Enabled*. The function is disabled by default.
Address Mode	Only for **Type** = *Ethernet over ATM* Select how an IP address is to be assigned to the interface. Possible values: • *Static* (default value): The interface is assigned a static IP address in **IP Address/Netmask**.

Field	Description
	• *DHCP*: An IP address is assigned to the interface dynamically via DHCP.
IP Address/Netmask	Only for **Address Mode** = *Static* Enter the IP addresses (**IP Address**) and the corresponding netmasks (**Netmask**) of the ATM interfaces. Add new entries with **Add**.
MAC Address	Enter a MAC address for the internal router interface of ATM connection, e.g. *00:a0:f9:06:bf:03*. An entry is only required in special cases. For Internet connections, it is sufficient to select the option **Use built-in** (default setting). The address used is derived from the MAC address of the *en1-0*.
DHCP MAC Address	Only for **Address Mode** = *DHCP*. Enter the MAC address of the internal router interface of ATM connection, e.g. *00:e1:f9:06:bf:03*. If your provider has assigned you a MAC address for DHCP, enter this here. You can also select the **Use built-in** option (default setting) The address used is derived from the MAC address of the *en1-0*.
DHCP Hostname	Only for **Address Mode** = *DHCP*. If necessary, enter the host name registered with the provider to be used by your device for DHCP requests. The maximum length of the entry is 45 characters.

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

Field	Description
IP Address/Netmask	Enter the IP addresses (**IP Address**) and the corresponding netmasks (**Netmask**) of the ATM interface. Add new entries with **Add**.
Prioritize TCP ACK	Select whether the TCP download is to be optimised in the

Field	Description
Packets	event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is enabled with *Enabled*. The function is disabled by default.

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

Field	Description
Client Type	Select whether the PPPoA connection is to be set up permanently or on demand. Possible values: • *On Demand* (default value): The PPPoA is only set up on demand, e.g. for Internet access. You'll find additional information on PPP over ATM under *PPPoA* on page 180.

16.2.2 Service Categories

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

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

Caution

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

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

16.2.2.1 New

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

The menu **WAN**->**ATM**->**Service Categories**->**New** consists of the following fields:

Fields in the Service CategoriesBasic Parameters menu

Field	Description
Virtual Channel Connection (VCC)	Select the already configured ATM connection (displayed by the combination of VPI and VCI) for which the service category is to be defined.
ATM Service Category	Select how the data traffic of the ATM connection is to be controlled. When you select the ATM service category a priority is implicitly assigned: from CBR (highest priority) through VBR.1 /VBR.3 to VBR (lowest priority). Possible settings: • *`Unspecified Bit Rate (UBR)`* (default value): (Unspecified Bit Rate) A particular data rate is not guaranteed for the connection. **Peak Cell Rate (PCR)** specifies the limit above which data is discarded. This category is suitable for non-critical applications. • *`Constant Bit Rate (CBR)`*(Constant Bit Rate) The connection is assigned a guaranteed data rate determined by the **Peak Cell Rate (PCR)** This category is suitable for critical (real-time) applications that require a guaranteed data rate. • *`Variable Bit Rate V.1 (VBR.1)`*: (Variable Bit Rate) The connection is assigned a guaranteed data rate (**Sustained Cell Rate (SCR)**). This may be exceeded by the volume configured in **Maximum Burst Size (MBS)**. Any additional ATM traffic is discarded. **Peak Cell Rate (PCR)**is the maximum possible data rate. This category is suitable for non-critical applications with burst data traffic. • *`Variable Bit Rate V.3 (VBR.3)`*: (Variable Bit Rate) The connection is assigned a guaranteed data rate (**Sustained Cell Rate (SCR)**). This may be exceeded by the volume configured in **Maximum Burst Size (MBS)**. Additional ATM traffic is marked and handled with low priority based on the utilisation of the destination network, i.e. is discarded if necessary. **Peak Cell Rate (PCR)**is the maximum possible data rate. This category is suitable for critical applications with burst data traffic.

Field	Description
Peak Cell Rate (PCR)	Enter a value for the maximum data rate in bits per second. Possible values: *0* to *10000000*. The default value is *0*.
Sustained Cell Rate (SCR)	Only for **ATM Service Category** = *Variable Bit Rate V.1 (VBR.1)* or *Variable Bit Rate V.3 (VBR.3)* Enter a value for the minimum available, guaranteed data rate in bits per second. Possible values: *0* to *10000000*. The default value is *0*.
Maximum Burst Size (MBS)	Only for **ATM Service Category** = *Variable Bit Rate V.1 (VBR.1)* or *Variable Bit Rate V.3 (VBR.3)* Enter a value for the maximum number of bits per second by which the PCR can be exceeded briefly. Possible values: *0* to *100000*. The default value is *0*.

16.2.3 OAM Controlling

OAM is a service for monitoring ATM connections. A total of five hierarchies (flow level F1 to F5) are defined for OAM information flow. The most important information flows for an ATM connection are F4 and F5. The F4 information flow concerns the virtual path (VP) and the F5 information flow the virtual channel (VC). The VP is defined by the VPI value, the VC by VPI and VCI.

Note

Generally, monitoring is not carried out by the terminal but is initiated by the ISP. Your device then only needs to react correctly to the signals received. This is ensured without a specific OAM configuration for both flow level 4 and flow level 5.

Two mechanisms are available for monitoring the ATM connection: Loopback Tests and OAM Continuity Check (OAM CC). These can be configured independently of each other.

Caution

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

In the **WAN**->**ATM**->**OAM Controlling** menu, a list of all monitored OAM flow levels is displayed.

16.2.3.1 New

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

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

Fields in the OAM ControllingOAM Flow Configuration menu

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

Fields in the OAM ControllingLoopback menu

Field	Description
Loopback End-to-End	Select whether you activate the loopback test for the connection between the endpoints of the VCC or VPC.

Field	Description
	The function is enabled with *Enabled*. The function is disabled by default.
End-to-End Send Interval	Only if **Loopback End-to-End** is enabled. Enter the time in seconds after which a loopback cell is to be sent. Possible values are *0* to *999*. The default value is 5.
End-to-End Pending Requests	Only if **Loopback End-to-End** is enabled. Enter the number of directly consecutive loopback cells that may fail to materialise before the connection is regarded as interrupted ("down"). Possible values are *1* to *99*. The default value is *5*.
Loopback Segment	Select whether you want to activate the loopback test for the segment connection (segment = connection of the local endpoint to the next connection point) of the VCC or VPC. The function is enabled with *Enabled*. The function is disabled by default.
Segment Send Interval	Only if **Loopback Segment** is enabled. Enter the time in seconds after which a loopback cell is sent. Possible values are *0* to *999*. The default value is *5*.
Segment Pending Requests	Only if **Loopback Segment** is enabled. Enter the number of directly consecutive loopback cells that may fail to materialise before the connection is regarded as interrupted ("down"). Possible values are *1* to *99*. The default value is *5*.

Fields in the OAM ControllingCC Activation menu

Field	Description
Continuity Check (CC) End-to-End	Select whether you activate the OAM-CC test for the connection between the endpoints of the VCC or VPC. Possible values: • *Passive* (default value): OAM CC requests are responded to after CC negotiation (CC activation negotiation). • *Active* : OAM CC requests are sent after CC negotiation (CC activation negotiation). • *Both* : OAM CC requests are sent and answered after CC negotiation (CC activation negotiation). • *No negotiation* : Depending on the setting in the **Direction** field, OAM CC requests are either sent and/or responded to. There is no CC negotiation. • *Passive*: The function is disabled. Also select whether the test cells of the OAM CC are to be sent or received. Possible values: • *Both* (default value): CC data is both received and generated. • *Sink*: CC data is received. • *Source*: CC data is generated.
Continuity Check (CC) Segment	Select whether you want to activate the OAM-CC test for the segment connection (segment = connection of the local endpoint to the next connection point) of the VCC or VPC. Possible values: • *Passive* (default value): OAM CC requests are responded to after CC negotiation (CC activation negotiation). • *Active* : OAM CC requests are sent after CC negotiation (CC activation negotiation). • *Both* : OAM CC requests are sent and answered after CC negotiation (CC activation negotiation). • *No negotiation*: Depending on the setting in the **Direction** field, OAM CC requests are either sent and/or responded to. There is no CC negotiation.

Field	Description
	- *None*: The function is disabled. Also select whether the test cells of the OAM CC are to be sent or received. Possible settings: - *Both* (default value): CC data is both received and generated. - *Sink*: CC data is received. - *Source*: CC data is generated.

16.3 Real Time Jitter Control

When telephoning over the Internet, voice data packets normally have the highest priority. Nevertheless, if the upstream bandwidth is low, noticeable delays in voice transmission can occur when other packets are routed at the same time.

The real time jitter control function solves this problem. So that the "line" is not blocked for too long for the voice data packets, the size of the other packets can be reduced, if required, during a telephone call.

16.3.1 Controlled Interfaces

In menu **WAN**->**Real Time Jitter Control**->**Controlled Interfaces** a list of interfaces is displayed for which the Real Time Jitter Control function is configured.

16.3.1.1 New

Click the **New** button to optimise voice transmission for other interfaces.

The menu **WAN**->**Real Time Jitter Control**->**Controlled Interfaces**->**New** consists of the following fields:

Fields in the Controlled InterfacesBasic Settings menu

Field	Description
Interface	Define for which interfaces voice transmission is to be optimised.
Control Mode	Select the mode for the optimisation.

Field	Description
	Possible values: • *Controlled RTP Streams only* (default value): By means of the data routed via the media gateway, the system detects voice data traffic and optimises the voice transmission. • *All RTP Streams*: All RTP streams are optimised. • *Inactive*: Voice data transmission is not optimised. • *Always*: Voice data transmission is always optimised.
Maximum Upload Speed	Enter the maximum available upstream bandwidth in kbps for the selected interface.

Chapter 17 VPN

A connection that uses the Internet as a "transport medium" but is not publicly accessible is referred to as a VPN (Virtual Private Network). Only authorised users have access to such a VPN, which is seemingly also referred to as a VPN tunnel. Normally the data transported over a VPN is encrypted.

A VPN allows field staff or staff working from home offices to access data on the company's network. Subsidiaries can also connect to head office over VPN.

Various protocols are available for creating a VPN tunnel, e.g. IPSec or PPTP.

The connection partner is authenticated with a password, using preshared keys or certificates.

With IPSec the data is encrypted using AES or 3DES, for example; with PPTP, you can use MPPE.

17.1 IPSec

IPSec enables secure connections to be set up between two locations (VPN). This enables sensitive business data to be transferred via an unsecure medium such as the Internet. The devices used function here as the endpoints of the VPN tunnel. IPSec involves a number of Internet Engineering Task Force (IETF) standards, which specify mechanisms for the protection and authentication of IP packets. IPSec offers mechanisms for encrypting and decrypting the data transferred in the IP packets. The IPSec implementation can also be smoothly integrated in a Public Key Infrastructure (PKI, see *Certificates* on page 84). The funkwerk IPSec implementation achieves this firstly by using the Authentication Header (AH) protocol and Encapsulated Security Payload (ESP) protocol, and secondly through the use of cryptographic key administration mechanisms like the Internet Key Exchange (IKE) protocol.

17.1.1 IPSec Peers

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

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

Peer Monitoring

The menu for monitoring a peer is called by selecting the 🔍 button for the peer in the peer list. See *Values in the IPSec Tunnels list* on page 340.

17.1.1.1 New

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

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

Fields in the IPSec PeersPeer Parameters menu

Field	Description
Administrative Status	Select the status to which you wish to set the peer after saving the peer configuration. Possible values: • *Up* (default value): The peer is available for setting up a tunnel immediately after saving the configuration. • *Down*: The peer is initially not available after the configuration has been saved.
Description	Enter a description of the peer that identifies it. The maximum length of the entry is 255 characters.
Peer Address	Enter the official IP address of the peer or its resolvable host name. The entry can be omitted in certain configurations, whereby your device then cannot initiate an IPSec connection.
Peer ID	Select the ID type and enter the peer ID. This entry is not necessary in certain configurations. The maximum length of the entry is 255 characters. Possible ID types: • *Fully Qualified Domain Name (FQDN)* • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)*

Field	Description
	On the peer device, this ID corresponds to the **Local ID Value** parameter.
Preshared Key	Enter the password agreed with the peer. The maximum length of the entry is 50 characters. All characters are possible except for *0x* at the start of the entry.

Fields in the IPSec PeersInterface Routes menu

Field	Description
IP Address Assignment	Select the configuration mode of the interface. Possible values: • *Static* (default value): Enter a static IP address. • *IKE Config Mode Client*: Select this option if your gateway receives an IP address from the server as IPSec client. • *IKE Config Mode Server*: Select this option if your gateway assigns an IP address as DHCP server for connecting clients. This is taken from the selected **IP Assignment Pool**.
IP Assignment Pool	Only if **IP Address Assignment** = *IKE Config Mode Server* Select an IP pool configured in the **VPN**->**IP Pools** menu. If an IP pool has not been configured here yet, the message *Not yet defined* appears in this field.
Default Route	Only for **IP Address Assignment** = *Static* and *IKE Config Mode Client*Select whether the route to this IPSec peer is to be defined as the default route. The function is enabled with *Enabled*. The function is disabled by default.
Local IP Address	Only for **IP Address Assignment** = *Static* and *IKE Config Mode Server* Enter the WAN IP address of your IPSec tunnel. This can be the same IP address as the address configured on your router as the LAN IP address.

Field	Description
Route Entries	Only for **IP Address Assignment** = *Static* and *IKE Config Mode Client*Define routing entries for this connection partner. • *Remote IP Address*: IP address of the destination host or LAN. • *Netmask*: Netmask for **Remote IP Address**. • *Metric*: The lower the value, the higher the priority of the route (possible values *0...15*). The default value is *1*.

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

Fields in the Advanced SettingsAdvanced IPSec Options menu

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

Field	Description
XAUTH Profile	Select a profile created in **VPN**->**IPSec**->**XAUTH Profiles** if you wish to use this IPSec peer XAuth for authentication. If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.
Number of Admitted Connections	Choose how many users can connect using this peer profile. Possible values: • *One User* (default value): Only one peer can be connected with the data defined in this profile. • *Multiple Users*: Several peers can be connected with the data defined in this profile. The peer entry is duplicated for each connection request with the data defined in this profile.
Start Mode	Select how the peer is to be switched to the active state. Possible values: • *On Demand* (default value): The peer is switched to the active state by a trigger. • *Always up*: The peer is always active.

Fields in the Advanced SettingsAdvanced IP Options menu

Field	Description
Back Route Verify	Select whether a check on the back route should be activated for the interface to the connection partner. The function is enabled with *Enabled*. The function is disabled by default.
Proxy ARP	Select whether your device is to respond to ARP requests from its own LAN on behalf of the specific connection partner. Possible values: • *Inactive* (default value): Deactivates Proxy ARP for this IPSec peer. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the IPSec peer is *Up*

Field	Description
	(active) or *Dormant*. In the case of *Dormant*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device responds to an ARP request only if the status of the connection to the IPSec peer is *Up* (active), i.e. a connection already exists to the IPSec peer.

IPSec Callback

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

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

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

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

☞ **Note**

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

Transfer of IP Address over ISDN

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

☞ **Note**

To use the IP address transfer over ISDN function, you must obtain a free-of-charge extra licence.

You can obtain the licence data for extra licences via the online licensing pages in the support section at *www.funkwerk-ec.com* . Please follow the online licensing instructions.

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

Method of operation: Various modes are available for transferring your own IP address to the peer: The address can be transferred free in the D channel or in the B channel, but here the call must be accepted by the remote station and therefore incurs costs. If a peer whose IP address has been assigned dynamically wants to arrange for another peer to set up an IPSec tunnel, it can transfer its own IP address as per the settings described in *Fields in the Advanced SettingsIPSec Callback menu* on page 211. Not all transfer modes are supported by all telephone companies. If you are not sure, automatic selection by the device can be used to ensure that all the available possibilities can be used.

Note

The callback configuration on the two devices should be the same so your device of the called peer can identify the IP address information.

The following roles are possible:

- One side takes on the active role, the other the passive role.
- Both sides can take on both roles (both).

The IP address transfer and the start of IKE phase 1 negotiation take place in the following steps:

(1) Peer A (the callback initiator) sets up a connection to the Internet in order to be assigned a dynamic IP address and be reachable for peer B over the Internet.

(2) Your device creates a token with a limited validity and saves it together with the current IP address in the MIB entry belonging to peer B.

(3) Your device sends the initial ISDN call to peer B, which transfers the IP address of peer A and the token as per the callback configuration.

(4) Peer B extracts the IP address of peer A and the token from the ISDN call and assigns them to peer A based on the calling party number configured (the ISDN number used by peer A to send the initial call to peer B).

(5) The IPSec Daemon at peer B's device can use the transferred IP address to initiate phase 1 negotiation with peer A. Here the token is returned to peer A in part of the payload in IKE negotiation.

(6) Peer A is now able to compare the token returned by peer B with the entries in the MIB and so identify the peer without knowing its IP address.

As peer A and peer B can now mutually identify each other, negotiations can also be conducted in the ID Protect mode using preshared keys.

Note

In some countries (e.g. Switzerland), the call in the D channel can also incur costs. An incorrect configuration at the called side can mean that the called side opens the B channel the calling side incurs costs.

The following options are only available on devices with an ISDN connection:

Fields in the Advanced SettingsIPSec Callback menu

Field	Description
Mode	Select the Callback Mode. Possible values: • *Inactive* (default value): IPSec callback is deactivated. The local device neither reacts to incoming ISDN calls nor initiates ISDN calls to the remote device. • *Passive*: The local device only reacts to incoming ISDN calls and, if necessary, initiates setting up an IPSec tunnel to the peer. No ISDN calls are sent to the remote device to cause this to set up an IPSec tunnel. • *Active*: The local device sends an ISDN call to the remote device to cause this to set up an IPSec tunnel. The device does not react to incoming ISDN calls. • *Both*: Your device can react to incoming ISDN calls and send ISDN calls to the remote device. The setting up of an IPSec tunnel is executed (after an incoming ISDN call) and initiated (by an outgoing ISDN call).
Incoming Phone Number	Only for **Mode** = *Passive* or *Both*. Enter the ISDN number from which the remote device calls the local device (calling party number). Wildcards may also be used.
Outgoing Phone Number	Only for **Mode** = *Active* or *Both*. Enter the ISDN number with which the local device calls the remote device calls (called party number). Wildcards may also be used.
Transfer own IP address over ISDN/GSM	Select whether the IP address of your own device is to be transferred over ISDN for IPSec callback. The function is enabled with *Enabled*. The function is disabled by default.
Transfer Mode	Only for **Transfer own IP address over ISDN/GSM** = enabled Select the mode in which your device is to attempt to transfer its IP address to the peer.

Field	Description
	Possible values: • *Autodetect best mode*: Your device automatically determines the most favourable mode. It first tries all D channel modes before switching to the B channel. (Costs are incurred for using the B channel.) • *Autodetect only D Channel Modes*: Your device automatically determines the most favourable D channel mode. The use of the B channel is excluded. • *Use specific D Channel Mode*: Your device tries to transfer the IP address in the mode set in the **Mode** field. • *Try specific D Channel Mode, fall back to B Channel*: Your device tries to transfer the IP address in the mode set in the **Mode** field. If this does not succeed, the IP address is transferred in the B channel. (This incurs costs.) • *Use only B Channel Mode*: Your device transfers the IP address in the B channel. This incurs costs.
D Channel Mode	Only for **Transfer Mode** = *Use specific D Channel Mode* or *Try specific D Channel Mode, fall back to B Channel* Select the D channel mode in which your device tries to transfer the IP address. Possible values: • *LLC* (default value): The IP address is transferred in the "LLC information elements" of the D channel. • *SUBADDR*: The IP address is transferred in the subaddress "information elements" of the D channel. • *LLC and SUBADDR*:The IP address is transferred in both the "LLC" and "subaddress information elements".

17.1.2 Phase-1 Profiles

In the **VPN**->**IPSec**->**Phase-1 Profiles**menu, a list of all configured IPSec phase 1 profiles is displayed.

In the **Default** column, you can mark the profile to be used as the default profile.

17.1.2.1 New

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

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

Fields in the Phase-1 ProfilesPhase-1 (IKE) Parameters menu

Field	Description
Description	Enter a description that uniquely defines the type of rule.
Proposals	In this field, you can select any combination of encryption and message hash algorithms for IKE phase 1 on your device. The combination of six encryption algorithms and four message hash algorithms gives 24 possible values in this field. At least one proposal must exist. Therefore the first line of the table cannot be deactivated. Encryption algorithms (**Encryption**): • `3DES` (default value): 3DES is an extension of the DES algorithm with an effective key length of 112 bits, which is rated as secure. It is the slowest algorithm currently supported. • `Twofish`: Twofish was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower. • `Blowfish`: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish. • `CAST`: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES. • `DES`: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits. • `AES`: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. • `AES-128`: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 128 bits. • `AES-192`: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of secur-

Field	Description
	ity against attacks and general speed. Here, it is used with a key length of 192 bits. • *AES-256*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 256 bits. Hash algorithms (**Authentication**): • *MD5* (default value): MD 5 (Message Digest #5) is an older hash algorithm. It is used with a 96 bit digest length for IPSec. • *SHA1*: SHA1 (Secure Hash Algorithm #1) is a hash algorithm developed by the NSA (United States National Security Association). It is rated as secure, but is slower than MD5. It is used with a 96 bit digest length for IPSec. • *RipeMD 160*: RipeMD 160 is a 160 bit hash algorithm. It is used as a secure replacement for MD5 and RipeMD. • *Tiger192*: Tiger 192 is a relatively new and very fast algorithm. Please note that the description of the encryption and authentication or the hash algorithms is based on the author's knowledge and opinion at the time of creating this User Guide. In particular, the quality of the algorithms is subject to relative aspects and may change due to mathematical or cryptographic developments.
DH Group	The Diffie-Hellman group defines the parameter set used as the basis for the key calculation during phase 1. "MODP" as supported by **bintec** devices stands for "modular exponentiation". Possible values: • *1 (768 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 768 bits is used to create the encryption material. • *2 (1024 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 1024 bits is used to create the encryption material. • *5 (1536 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 1536 bits is used to create the encryption material.

Field	Description
Lifetime	Create a lifetime for phase 1 keys. As for RFC 2407, the default value is eight hours, which means the key must be renewed once eight hours have elapsed. The following options are available for defining the lifetime: Input in **Seconds**: Enter the lifetime for phase 1 key in seconds. The value can be a whole number from 0 to 2147483647. The default value is *14400*. Input in **kBytes**: Enter the lifetime for phase 1 keys as amount of data processed in kBytes. The value can be a whole number from 0 to 2147483647. The default value is *0*. The standard value as per RFC is used *0* seconds and *0* Kbytes are entered.
Authentication Method	Select the authentication method. Possible values: • *Preshared Keys* (default value): If you do not use certificates for the authentication, you can select Preshared Keys. These are configured during peer configuration in the **IPSec Peers** menu. The preshared key is the shared password. • *DSA Signature*: Phase 1 key calculations are authenticated using the DSA algorithm. • *RSA Signature*: Phase 1 key calculations are authenticated using the RSA algorithm. • *RSA Encryption*: In RSA encryption the ID payload is also encrypted for additional security.
Local Certificate	Only for **Authentication Method** = *DSA Signature* , *RSA Signature* or *RSA Encryption* This field enables you to select one of your own certificates for authentication. It shows the index number of this certificate and the name under which it is saved. This field is only shown for authentication settings based on certificates and indicates that a certificate is essential.
Mode	Select the phase 1 mode.

Field	Description
	Possible values: • *Aggressive* (default value): The Aggressive Mode is necessary if one of the peers does not have a static IP address and preshared keys are used for authentication; it requires only three messages for configuring a secure channel. • *Main Mode (ID Protect)*: This mode (also designated Main Mode) requires six messages for a Diffie-Hellman key calculation and thus for configuring a secure channel, over which the IPSec SAs can be negotiated. A condition is that both peers have static IP addresses if preshared keys are used for authentication. Also define whether the selected mode is used exclusively (**Strict**), or the peer can also propose another mode.
Local ID Type	Select the local ID type. Possible values: • *Fully Qualified Domain Name (FQDN)* • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)*
Local ID Value	Enter the ID of your device. For **Authentication Method** = *DSA Signature*, *RSA Signature* or *RSA Encryption* the option **Use Subject Name from certificate**is displayed. When you initially enable the **Use Subject Name from certificate** option, the first alternative subject name indicated in the certificate is used, or, if none is specified, the subject name of the certificate is used. Note: If you use certificates for authentication and your certificate contains alternative subject names (see *Certificates* on page 84), you must make sure your device selects the first alternative subject name by default. Make sure you and your peer both use the same name, i.e. that your local ID and the peer ID your partner configures for you are identical.

Alive Check

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

Two methods are available: Heartbeats and Dead Peer Detection.

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

Fields in the Advanced Settings menu

Field	Description
Alive Check	Select the method to be used to check the functionality of the IPSec connection. In addition to the default method Dead Peer Detection (DPD), the (proprietary) Heartbeat method is implemented. This sends and receives signals every 5 seconds, depending on the configuration. If these signals are not received after 20 seconds, the SA is discarded as invalid. Possible values: • *Autodetect* (default value): Your device detects and uses the mode supported by the remote terminal. • *Inactive*: Your device neither sends nor expects a heartbeat. Set this option if you use devices from other manufacturers. • *Heartbeats (Expect only)*: Your device expects a heartbeat from the peer, but does not send one itself. • *Send*: Your device expects no heartbeat from the peer, but sends one itself. • *Heartbeats (Send &Expect)*: Your device expects a heartbeat from the peer and sends one itself. • *Dead Peer Detection*: Use DPD (dead peer detection) in accordance with RFC 3706. DPD uses a request-reply protocol to check the availability of the remote terminal and can be configured independently on both sides. This option only checks the availability of the peer if data is to be sent to it.

Field	Description
	• *Dead Peer Detection (Idle)*: Use DPD (dead peer detection) in accordance with RFC 3706. DPD uses a request-reply protocol to check the availability of the remote terminal and can be configured independently on both sides. This option is used to carry out a check at certain intervals depending on forthcoming data transfers.
Block Time	Define how long a peer is blocked for tunnel setups after a phase 1 tunnel setup has failed. This only affects locally initiated setup attempts. Possible values are *-1* to *86400* (seconds); *-1* means the value in the default profile is used and *0* means that the peer is never blocked. The default value is *30*.
NAT Traversal	NAT Traversal (NAT-T) also enables IPSec tunnels to be opened via one or more devices on which network address translation (NAT) is activated. Without NAT-T, incompatibilities may arise between IPSec and NAT (see RFC 3715, section 2). These primarily prevent the setup of an IPSec tunnel from a host within a LANs and behind a NAT device to another host or device. NAT-T enables these kinds of tunnels without conflicts with NAT device, activated NAT is automatically detected by the IPSec Daemon and NAT-T is used. The function is enabled with *Enabled*. The function is enabled by default.
CA Certificates	Only for **Authentication Method** = *DSA Signature* , *RSA Signature* or *RSA Encryption* If you enable option **Trust the following CA certificates** , you can select up to three CA certificates that are accepted for this profile. This option can only be configured if certificates are loaded.

17.1.3 Phase-2 Profiles

You can define profiles for phase 2 of the tunnel setup just as for phase 1.

In the **VPN**->**IPSec**->**Phase-2 Profiles**menu, a list of all configured IPSec phase 2 profiles is displayed.

In the **Default** column, you can mark the profile to be used as the default profile.

17.1.3.1 New

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

The menu **VPN**->**IPSec**->**Phase-2 Profiles**->**New** consists of the following fields:

Fields in the Phase-2 ProfilesPhase-2 (IPSEC) Parameters menu

Field	Description
Description	Enter a description that uniquely identifies the profile. The maximum length of the entry is 255 characters.
Proposals	In this field, you can select any combination of encryption and message hash algorithms for IKE phase 2 on your default. The combination of six encryption algorithms and two message hash algorithms gives 12 possible values in this field. Encryption algorithms (**Encryption**): • *3DES* (default value): 3DES is an extension of the DES algorithm with an effective key length of 112 bits, which is rated as secure. It is the slowest algorithm currently supported. • *-- ALL --*: All options can be used. • *AES-128*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 128 bits. • *AES-192*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 192 bits. • *AES-256*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of secur-

Field	Description
	ity against attacks and general speed. Here, it is used with a key length of 256 bits. • *Twofish*: Twofish was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower. • *Blowfish*: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish. • *CAST*: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES. • *DES*: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits. Hash algorithms (**Authentication**): • *MD5* (default value): MD 5 (Message Digest #5) is an older hash algorithm. It is used with a 96 bit digest length for IPSec. • *-- ALL --*: All options can be used. • *SHA1*: SHA1 (Secure Hash Algorithm #1) is a hash algorithm developed by the NSA (United States National Security Association). It is rated as secure, but is slower than MD5. It is used with a 96 bit digest length for IPSec. Note that RipeMD 160 and Tiger 192 are not available for message hashing in phase 2.
Use PFS Group	As PFS (Perfect Forward Secrecy) requires another Diffie-Hellman key calculation to create new encryption material, you must select the exponentiation features. If you activate PFS (**Enabled**), the options are the same as for the configuration in **Phase-1 ProfilesDH Group**. PFS is used to protect the keys of a renewed phase 2 SA, even if the keys of the phase 1 SA have become known. The field has the following options: • *1 (768 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 768 bits is used to create the encryption material. • *2 (1024 Bit)* (default value): During the Diffie-Hellman key calculation, modular exponentiation at 1024 bits is used to create the encryption material. • *5 (1536 Bit)*: During the Diffie-Hellman key calculation,

Field	Description
	modular exponentiation at 1536 bits is used to create the encryption material.
Lifetime	Define how the lifetime is defined that will expire before phase 2 SAs need to be renewed. The new SAs are negotiated shortly before expiry of the current SAs. As for RFC 2407, the default value is eight hours, which means the key must be renewed once eight hours have elapsed. The following options are available for defining the lifetime: Input in *Seconds*: Enter the lifetime for phase 2 key in seconds. The value can be a whole number from *0* to *2147483647* . The default value is *7200*. Input in *kBytes*: Enter the lifetime for phase 2 keys as amount of data processed in Kbytes. The value can be a whole number from *0* to *2147483647* . The default value is *0*.

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

Fields in the Advanced Settings menu

Field	Description
IP Compression	Select whether compression is to be activated before data encryption. If data is compressed effectively, this can result in higher performance and a lower volume of data to be transferred. In the case of fast lines or data that cannot be compressed, you are advised against using this option as the performance can be significantly affected by the increased effort during compression. The function is enabled with *Enabled*. The function is disabled by default.
Alive Check	Select whether and how IPSec heartbeats are used. A **bintec** IPSec heartbeat is implemented to determine whether or not a Security Association (SA) is still valid. This function sends and receives signals every 5 seconds, depending on the configuration. If these signals are not received after 20 seconds, the SA is discarded as invalid.

Field	Description
	Possible values: • *Inactive*: Your device neither sends nor expects a heartbeat. Set this option if you use devices from other manufacturers. • *Heartbeats (Expect only)*: Your device expects a heartbeat from the peer, but does not send one itself. • *Send*: Your device expects no heartbeat from the peer, but sends one itself. • *Heartbeats (Send &Expect)*: Your device expects a heartbeat from the peer and sends one itself. • *Autodetect*: Automatic detection of whether the remote terminal is a **bintec** device. If it is, Heartbeat Both (for a remote terminal with **bintec**) or None (for a remote terminal without **bintec**) is set.
Propagate PMTU	Select whether the PMTU (Path Maximum Transfer Unit) is to be propagated during phase 2. The function is enabled with *Enabled*. The function is enabled by default.

17.1.4 XAUTH Profiles

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

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

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

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

In server mode multiple users can obtain authentication via XAuth, e.g. users of Apple iPhones. Authorisation is verified either on the basis of a list or via a Radius Server. If using a one time password (OTP), the password check can be carried out by a token server (e.g. SecOVID from Kobil), which is installed behind the Radius Server. If a company's headquarters is connected to several branches via IPSec, several peers can be configured. A specific user can then use the IPSec tunnel over various peers depending on the assignment of various profiles. This is useful, for example, if an employee works alternately in different branches, if each peer represents a branch and if the employee wishes to have on-site access to the tunnel.

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

If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.

17.1.4.1 New

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

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

Fields in the XAUTH ProfilesBasic Parameters menu

Field	Description
Description	Enter a description for this XAuth profile.
Role	Select the role of the gateway for XAuth authentication. Possible values: • `Server` (default value): The gateway requires a proof of authorisation. • `Client`: The gateway provides proof of authorisation.
Mode	Only for **Role** = `Server` Select how authentication is carried out. Possible values: • `RADIUS` (default value): Authentication is carried out via a Radius server. It is configured in the **System Management**->**Remote Authentication**->**RADIUS** menu and selected in the **RADIUS Server Group ID** field. • `Local`: Authentication is carried out via a local list.
Name	Only for **Role** = `Client` Enter the authentication name of the client.

Field	Description
Password	Only for **Role** = `Client` Enter the authentication password.
RADIUS Server Group ID	Only for **Role** = `Server` Select the desired **System Management**->**Remote Authentication**->**RADIUS** configured RADIUS group.
Users	Only for **Role** = `Server` and **Mode** = `Local` If your gateway is configured as an XAuth server, the clients can be authenticated via a locally configured user list. Define the members of the user group of this XAUTH profile here by entering the authentication name of the client (**Name**) and the authentication password (**Password**). Add new members with **Add**.

17.1.5 IP Pools

In the **IP Pools** menu, a list of all IP pools for your configured IPSec connections is displayed.

If you have set **IP Address Assignment** `IKE Config Mode Server` for an IPSec peer, here, you must define the IP pools from which the IP addresses are assigned.

Choose the **Add** button to set up new IP pools.

The **VPN**->**IPSec**->**IP Pools**->**Add** menu consists of the following fields:

Fields in the OptionsIP Pools menu

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

17.1.6 Options

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

Fields in the OptionsGlobal Options menu

Field	Description
Enable IPSec	Select whether you want to activate IPSec. The function is enabled with *Enabled*. The function is active as soon as an IPSec Peer is configured.
Delete complete IPSec configuration	If you click the 🗑 icon, delete the complete IPSec configuration of your device. This cancels all settings made during the IPSec configuration. Once the configuration is deleted, you can start with a completely new IPSec configuration. You can only delete the configuration with **Enable IPSec** = Not activated..
IPSec Debug Level	Select the priority of the syslog messages of the IPSec subsystem to be recorded internally. Possible values: • *Emergency* (highest priority) • *Alert* • *Critical* • *Error* • *Warning* • *Notice* • *Information* • *Debug* (default value, lowest priority) Syslog messages are only recorded internally if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level debug.

The **Advanced Settings** menu is for adapting certain functions and features to the special requirements of your environment, i.e. mostly interoperability flags are set. The default values are globally valid and enable your system to work correctly to other **bintec** devices, so that you only need to change these values if the remote terminal is a third-party product or you know special settings are necessary. These may be needed, for example, if the remote end operates with older IPSec implementations.

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

Fields in the OptionsAdvanced Settings menu

Field	Description
Send Initial Contact Message	Select whether IKE Initial Contact messages are to be sent during IKE (phase 1) if no SAs with a peer exist. The function is enabled with *Enabled*. The function is enabled by default.
Sync SAs with ISP interface state	Select whether all SAs are to be deleted whose data traffic was routed via an interface on which the status has changed from *Up*to *Down*, *Dormant* or *Blocked*. The function is enabled with *Enabled*. The function is disabled by default.
Use Zero Cookies	Select whether zeroed ISAKMP Cookies are to be sent. These are equivalent to the SPI (Security Parameter Index) in IKE proposals; as they are redundant, they are normally set to the value of the negotiation currently in progress. Alternatively, your device can use zeroes for all values of the cookie. In this case, select *Enabled*.
Zero Cookie Size	Only for **Use Zero Cookies** = enabled. Enter the length in bytes of the zeroed SPI used in IKE proposals. The default value is *32*.
Dynamic RADIUS Authentication	Select whether RADIUS authentication is to be activated via IPSec. The function is enabled with *Enabled*. The function is disabled by default.

Fields in the Advanced SettingsPKI Handling Options menu

Field	Description
Ignore Certificate Re-	Select whether certificate requests received from the remote

Field	Description
quest Payloads	end during IKE (phase 1) are to be ignored. The function is enabled with *Enabled*. The function is disabled by default.
Send Certificate Request Payloads	Select whether certificate requests are to be sent during IKE (phase 1). The function is enabled with *Enabled*. The function is enabled by default.
Send Certificate Chains	Select whether complete certificate chains are to be sent during IKE (phase 1). The function is enabled with *Enabled*. The function is enabled by default. Deactivate this function if you do not wish to send the peer the certificates of all levels (from your level to the CA level).
Send CRLs	Select whether CRLs are to be sent during IKE (phase 1). The function is enabled with *Enabled*. The function is disabled by default.
Send Key Hash Payloads	Select whether key hash payloads are to be sent during IKE (phase 1). In the default setting, the public key hash of the remote end is sent together with the other authentication data. Only applies to RSA encryption; activate this function with *Enabled* to suppress this behaviour.

17.2 L2TP

The layer 2 tunnel protocol (L2TP) enables PPP connections to be tunnelled via a UDP connection.

Your **bintec** device supports the following two modes:

- L2TP LNS Mode (L2TP Network Server): for incoming connections only
- L2TP LAC Mode (L2TP Access Concentrator): for outgoing connections only

Note the following when configuring the server and client: An L2TP tunnel profile must be created on each of the two sides (LAC and LNS). The corresponding L2TP tunnel profile is used on the initiator side (LAC) to set up the connection. The L2TP tunnel profile is needed on the responder side (LNS) to accept the connection.

17.2.1 Tunnel Profiles

A list of all configured tunnel profiles is displayed in the **VPN**->**L2TP**->**Tunnel Profiles** menu.

17.2.1.1 New

Choose the **New** button to create additional tunnel profiles.

The menu **VPN**->**L2TP**->**Tunnel Profiles** ->**New** consists of the following fields:

Fields in the Tunnel ProfilesBasic Parameters menu

Field	Description
Description	Enter a description for the current profile. The device automatically names the profiles `L2TP` and numbers them, but the value can be changed.
Local Hostname	Enter the host name for LNS or LAC. • LAC: The **Local Hostname** is used in outgoing tunnel set-up messages to identify this device and is associated with the **Remote Hostname** of a tunnel profile configured on the LNS. These tunnel setup messages are SCCRQs (Start Control Connection Request) sent from the LAC and SCCRPs (Start Control Connection Reply) sent from the LNS. • LNS: Is the same as the value for **Remote Hostname** of the incoming tunnel setup message from the LAC.
Remote Hostname	Enter the host name of the LNS or LAC. • LAC: Defines the value for **Local Hostname** of the LNS (contained in the SCCRQs received from the LNS and the SCCRPs received from the LAC). The **Local Hostname** configured in LAC must match **Remote Hostname** configured for the intended profile in LNS, and vice-versa.

Field	Description
	• LNS: Defines the **Local Hostname** of the LAC. If the **Remote Hostname** field remains empty on the LNS, the related profile qualifies as the standard entry and is used for all incoming calls for which no profile with a matching **Remote Hostname** can be found.
Password	Enter the password to be used for tunnel authentication. Authentication between LAC and LNS takes place in both directions, i.e. the LNS checks the **Local Hostname** and the **Password** contained in the SCCRQ of the LAC and compares them with those specified in the relevant profile. The LAC does the same with the fields of the SCCRP of the LNS. If this field remains empty, authentication data in the tunnel setup messages are not sent and are ignored.

Fields in the Tunnel ProfilesLAC Mode Parameters menu

Field	Description
Remote IP Address	Enter the fixed IP address of the LNS used as the destination address for connections based on this profile. The destination must be a device that can behave like an LNS.
UDP Source Port	Enter how the port number to be used as the source port for all outgoing L2TP connections based on this profile is to be determined. By default, the **Fixed**option is disabled, which means that ports are dynamically assigned to the connections that use this profile. If you want to enter a fixed port, activate the option **Fixed**. Select this option if you encounter problems with the firewall or NAT. The available values are *0* to *65535*.
UDP Destination Port	Enter the destination port number to be used for all calls based on this profile. The remote LNS that receives the call must monitor this port on L2TP connections. Possible values are *0* ... *65535*.

Field	Description
	The default value is *1701* (RFC 2661).

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

Fields in the Advanced Settings menu

Field	Description
Local IP Address	Enter the IP address to be used as the source address for all L2TP connections based on this profile. If this field is left empty, your device uses the IP address of the interface over which the L2TP tunnel reaches **Remote IP Address**.
Hello Intervall	Enter the interval (in seconds) between the sending of two L2TP HELLO messages. These messages are used to keep the tunnel open. The available values are *0* to *255*, the default value is *30*. The value *0* means that no L2TP HELLO messages are sent.
Minimum Time between Retries	Enter the minimum time (in seconds) that your device waits before resending a L2TP control packet for which it received no response. The wait time is dynamically extended until it reaches the **Maximum Time between Retries**. The available values are *1* to *255*, the default value is *1*.
Maximum Time between Retries	Enter the maximum time (in seconds) that your device waits before resending a L2TP control packet for which it received no response. The available values are *8* to *255*, the default value is *16*.
Maximum Retries	Enter the maximum number of times your device is to try to resend the L2TP control packet for which is received no response. The available values are *8* to *255*, the default value is *5*.
Data Packets Sequence Numbers	Select whether your device is to use sequence numbers for data packets sent through a tunnel on the basis of this profile. The function is not currently used.

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

17.2.2 Users

A list of all configured L2TP partner is displayed in the **VPN**->**L2TP**->**Users** menu.

17.2.2.1 New

Choose the **New** button to set up new L2TP partners.

The menu **VPN**->**L2TP**->**Users**->**New** consists of the following fields:

Fields in the UsersBasic Parameters menu

Field	Description
Description	Enter a name for uniquely identifying the L2TP partner. The first character in this field must not be a number No special characters or umlauts must be used. The maximum length of the entry is 25 characters.
Connection Type	Select whether the L2TP partner is to take on the role of the L2TP network server (LNS) or the functions of a L2TP access concentrator client (LAC client). Possible values: • *LNS* (default value): If you select this option, the L2TP partner is configured so that it accepts L2TP tunnels and restores the encapsulated PPP traffic flow. • *LAC*: If you select this option, the L2TP partner is configured so that it encapsulates a PPP traffic flow in L2TP and sets up a L2TP tunnel to a remote LNS.
Tunnel Profile	Only for **Connection Type** = *LAC* Select a profile created in the **Tunnel Profile** menu for the connection to this L2TP partner.
User Name	Enter the code of your device.

Field	Description
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the short hold. The default value is *300*.

Fields in the UsersIP Mode and Routes menu

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

Field	Description
Create NAT Policy	Only for **IP Address Mode** = *Get IP Address* and *Static* Specify whether Network Address Translation (NAT) is to be activated for this connection. The function is enabled with *Enabled*. The function is disabled by default.
IP Assignment Pool (IPCP)	Only for **IP Address Mode** = *Provide IP Address* Select IP pools configured in the **WAN**->**Internet + Dialup**->**IP Pools** menu.
Local IP Address	Only for **IP Address Mode** = *Static*. Enter the WAN IP address of your device.
Route Entries	Only for **IP Address Mode** = *Static*. Enter the **Remote IP Address** and **Netmask** for the LAN of the L2TP partner and the attendant **Metric**. Add new entries with **Add**.

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

Fields in the Advanced Settings menu

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *300*.
Authentication	Select the authentication protocol for this L2TP partner. Possible values: • *PAP/CHAP/MS-CHAP* (default value): Primarily run CHAP, on denial, the authentication protocol required by the PPTP partner. (MSCHAP version 1 or 2 possible.) • *PAP*: Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.

Field	Description
	- *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); the password is transferred encrypted. - *PAP/CHAP*: Primarily run CHAP, otherwise PAP. - *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). - *MS-CHAPv2*: Run MS-CHAP version 2 only. - *None*: Some providers use no authentication. In this case, select this option.
Encryption	If necessary, select the type of encryption that should be used for data traffic to the L2TP partner. This is only possible if STAC or MS-STAC compression is not activated for the connection. If **Encryption** is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: - *None*: MPP encryption is not used. - *Enabled* (default value): MPP encryption V2 with 128 bit is used to RFC 3078. - *Windows compatible*: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
LCP Alive Check	Check whether the reachability of the remote terminal is to be checked by sending LCP echo requests or replies. This is recommended for leased lines, PPTP and L2TP connections. The function is enabled with *Enabled*. The function is disabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is enabled with *Enabled*. The function is disabled by default.

Fields in the Advanced SettingsIP Options menu

Field	Description
OSPF Mode	Select whether and how routes are propagated via the interface and/or OSPF protocol packets are to be sent. Possible values: • *Passive* (default value): OSPF is not activated for this interface, i.e. no routes are propagated or OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces. • *Active*: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface. • *Inactive*: OSPF is disabled for this interface.
Proxy ARP Mode	Select whether your device is to respond to ARP requests from its own LAN on behalf of the specific L2TP partner. Possible values: • *Inactive* (default value): Deactivates Proxy ARP for this L2TP partner. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the L2TP partner is *Up* (active) or *Dormant*. In the case of *Idle*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device responds to an ARP request only if the status of the connection to the L2TP partner is *Up* (active), i.e. a connection already exists to the L2TP partner.
DNS Negotiation	Select whether your device shall receive IP addresses for **DNS Server Primary** and **Secondary** and **WINS Server Primary** and **Secondary** from the L2TP partner or send these to the L2TP partner. The function is enabled with *Enabled*. The function is enabled by default.

17.2.3 Options

The menu **VPN**->**L2TP**->**Options** consists of the following fields:

Fields in the OptionsGlobal Options menu

Field	Description
UDP Destination Port	Enter the port to be monitored by the LNS on incoming L2TP tunnel connections. Available values are all whole numbers from *1* to *65535*, the default value is *1701,* as specified in RFC 2661.
UDP Source Port Selection	Select whether the LNS should only use the monitored port (**UDP Destination Port**) as the local source port for the L2TP connection. The function is enabled with *Fixed*. The function is disabled by default.

17.3 PPTP

The Point-to-Point Tunnelling Protocol (=PPTP) can be used to set up an encrypted PPTP tunnel to provide security for data traffic over an existing IP connection.

First a connection to an ISP (=Internet Service Provider) is set up at both sites. Once these connections are available, a tunnel is set up to the PPTP partner over the Internet using PPTP.

The PPTP subsystem sets up a control connection between the endpoints of the tunnel. This is used to send control data to set up, keep alive and terminate the connection between the two PPTP tunnel end-points. As soon as this control connection is set up, the PPTP transfers the traffic data packed in GRE packets (GRE = Generic Routing Encapsulation).

17.3.1 PPTP Tunnels

In the **PPTP Tunnels** menu, a list of all PPTP tunnels is displayed.

17.3.1.1 New

Click on **New** to set up further PPTP partners.

The **VPN**->**PPTP**->**PPTP Tunnels**->**New** menu consists of the following fields:

Fields in the PPTP TunnelsPPTP Partner Parameters menu

Field	Description
Description	Enter a unique name for the tunnel. The first character in this field must not be a number No special characters or umlauts must be used.
PPTP Mode	Enter the role to be assigned to the PPTP interface. Possible values: • *PNS* (default value): this assigns the PPTP interface the role of PPTP server. • *Windows Client Mode*: This assigns the PPTP interface the role of PPTP client.
User Name	Enter the user name.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle interval in seconds. This determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the timeout. The default value is *300*. Example: *10* for FTP transmission, *20* for LAN-to-LAN transmission, *90* for Internet connections.
Remote PPTP IP Address	**PPTP Mode** = *PNS*Enter the IP address of the PPTP partner.
Remote PPTP IP AddressHostname	**PPTP Mode** = *Windows Client Mode*Enter the IP address of the PPTP partner.

Fields in the PPTP TunnelsIP Mode and Routes menu

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Static* (default value): You enter a static IP address. • *Provide IP Address*: Only for **PPTP Mode** = *PNS*IYour device dynamically assigns an IP address to the remote terminal. • *Get IP Address*: Only for **PPTP Mode** = *Windows Client Mode*Your device is dynamically assigned an IP address.
Default Route	Only if **IP Address Mode** = *Static* Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is disabled by default.
Create NAT Policy	Only if **IP Address Mode** = *Static* When you configure an ISDN connection, specify whether Network Address Translation (NAT) is to be enabled. The function is enabled with *Enabled*. The function is disabled by default.
Local IP Address	Only for **IP Address Mode** = *Static* Assign the IP address from your LAN to the ISDN interface which is to be used as your device's internal source address.
Route Entries	Only if **IP Address Mode** = *Static* Define routing entries for this connection partner. • *Remote IP Address*: IP address of the destination host or LAN. • *Netmask*: Netmask for **Remote IP Address**. • *Metric*: The lower the value, the higher the priority of the route (possible values *0...15*). The default value is *1*.

Field	Description
IP Assignment Pool (IPCP)	Only if **IP Address Mode** = *Provide IP Address* Select IP pools configured in the **WAN**->**Internet + Dialup**->**IP Pools** menu. If an IP pool has not been configured here yet, the message *Not yet defined* appears in this field.

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

Fields in the Advanced Settings menu

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *300*.
Authentication	Select the authentication protocol for this PPTP partner. Possible values: • *PAP*: Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); the password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP*: Primarily run CHAP, on denial, the authentication protocol required by the PPTP partner. (MSCHAP version 1 or 2 possible.) • *MS-CHAPv2* (default value): Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
Encryption	If necessary, select the type of encryption that should be used for data traffic to the connection partner. If **Encryption** is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values:

Field	Description
	• *None*: MPP encryption is not used. • *Enabled* (default value): MPP encryption V2 with 128 bit is used to RFC 3078. • *Windows compatible*: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
Compression	If necessary, select the type of encryption that should be used for data traffic to the connection partner. If encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: • *None* (default value): Encryption is not used. • *STAC* • *MS-STAC* • *MPPC*: Microsoft Point-to-Point Compression
LCP Alive Check	Check whether the reachability of the remote terminal is to be checked by sending LCP echo requests or replies. This is recommended for leased lines, PPTP and L2TP connections. The function is enabled with *Enabled*. The function is enabled by default.

Fields in the Advanced SettingsIP Options menu

Field	Description
OSPF Mode	Select whether and how routes are propagated via the interface and/or OSPF protocol packets are to be sent. Possible values: • *Passive* (default value): OSPF is not activated for this interface, i.e. no routes are propagated or OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces. • *Active*: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface. • *Inactive*: OSPF is disabled for this interface.

Field	Description
Proxy ARP Mode	Select whether your device is to answer APR requests from your LAN on behalf of the specific PPTP partner. Possible values: • *Inactive* (default value): Disables Proxy-ARP (Address Resolution Protocol) for this PPTP partner. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the PPTP partner is *Up* (active) or *Dormant*. In the case of *Idle*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device answers an APR request only if the status of the connection to the PPTP partner is *Active*, i.e. if a connection to the PPTP partner has already been established.
DNS Negotiation	Select whether your device shall receive IP addresses for **DNS Server Primary** und **DNS Server Secondary** from the PPTP partner or send these to the PPTP partner. The function is enabled with *Enabled*. The function is enabled by default.

The following options are only available on devices with an ISDN connection:

Fields in the Advanced SettingsPPTP Callback menu

Field	Description
Callback	Enables a PPTP tunnel through the Internet to be set up with a PPTP partner, even if the partner is currently inaccessible. As a rule, the PPTP partner will be requested by means of an ISDN call to go online and set up a PPTP connection. The function is enabled with *Enabled*. The function is disabled by default. Note that you must activate the relevant option on the gateways of both partners. An ISDN connection is usually required for this function. Without ISDN, callback is only to be activated in special applications.

Field	Description
Incoming ISDN Number	Only if **Callback** is enabled. Enter the ISDN number from which the remote device calls the local device (calling party number).
Outgoing ISDN Number	Only if **Callback** is enabled. Enter the ISDN number with which the local device calls the remote device calls (called party number).

17.3.2 Options

In this menu, you can make general settings of the global PPTP profile.

The **VPN**->**PPTP**->**Options** menu includes the following fields:

Fields in the OptionsGlobal Options menu

Field	Description
GRE Window Adaption	Select whether the GRE Window Adaptation is to be enabled. This adaptation only becomes necessary if you have downloaded service pack 1 from the Microsoft Windows XP page and installed it. Since, in SP 1, Microsoft has changed the confirmation algorithm in the GRE protocol, the automatic window adaptation for GRE must be turned off on the funkwerk side. The function is enabled with `Enabled`. The function is enabled by default.
GRE Window Size	Enter the maximum number of GRE packets that can be sent without confirmation. Windows XP uses a higher initial reception window in the GRE, which is why the maximum send window size on the funkwerk side must be adjusted here via the value **GRE Window Size**. Possible values are `0` to `256`. The default value is `0`.
Max. incomming control connections per remote IP Address	Enter the maximum number of control connections.

17.3.3 IP Pools

In the **IP PoolsI** menu, a list of all IP pools for PPTP connections is displayed.

Your device can operate as a dynamic IP address server for PPTP connections. You can use this function by providing one or more pools of IP addresses. These IP addresses can be assigned to dialling-in connection partners for the duration of the connection.

Any host routes entered always have priority over IP addresses from the address pools. This means if an incoming call has been authenticated, your device first checks whether a host route is entered in the routing table for this caller. If not, your device can allocate an IP address from an address pool (if available). If address pools have more than one IP address, you cannot specify which connection partner receives which address. The addresses are initially assigned in order. If a new dial-in takes place within an interval of one hour, an attempt is made to allocate the same IP address assigned to this partner the last time.

Choose the **Add** button to set up new IP pools.

The **VPN**->**PPTP**->**IP Pools**->**Add** menu consists of the following fields:

Fields in the OptionsIP Pools menu

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

17.4 GRE

Generic Routing Encapsulation (GRE) is a network protocol that encapsulates other protocols and transports them in the form of IP tunnels to the specified recipients.

The specification of the GRE protocol is available in two versions:

- GRE V.1 for use in PPTP connections (RFC 2637, configuration in the **PPTP** menu)
- GRE V.0 (RFC 2784) for general encapsulation using GRE

In this menu you can configure a virtual interface for using GRE V.0. The data traffic routed over this interface is then encapsulated using GRE and sent to the specified recipient.

17.4.1 GRE Tunnels

A list of all configured GRE tunnels is displayed in the **VPN**->**GRE**->**GRE Tunnels** menu.

17.4.1.1 New

Choose the **New** button to set up new GRE tunnels.

The **VPN**->**GRE**->**GRE Tunnels** menu includes the following fields:

Fields in the GRE TunnelsBasic Parameters menu

Field	Description
Description	Enter a description for the GRE tunnel.
Local GRE IP Address	Enter the source IP address of the GRE packets to the GRE partner. If no IP address is given (this corresponds to IP address 0.0.0.0), the source IP address of the GRE packets is selected automatically from one of the addresses of the interface via which the GRE partner is reached.
Remote GRE IP Address	Specify the destination IP address of the GRE packets to the GRE partner.
Default Route	If you enable the **Default Route**, all data is automatically routed to one connection. The function is disabled by default.
Local IP Address	Enter the (LAN) IP address to be used as the source address of your device for sending own packets through the GRE tunnel.
Route Entries	Define other routing entries for this connection partner. Add new entries with **Add**. • `Remote IP Address`: IP address of the destination host or network. • `Netmask`: Netmask for **Remote IP Address**. If no entry is made, your device uses a default netmask. • `Metric`: The lower the value, the higher the priority of the route (possible values `0`... `15`). The default value is `1`.

Field	Description
MTU	Enter the maximum packet size (Maximum Transfer Unit, MTU) in bytes that is allowed for the GRE connection between the partners. Possible values are *1* to *8192*. The default value is *1500*.
Use key	Enable the key input for the GRE connection, which makes it possible to distinguish between several parallel GRE connections between two GRE partners (see RFC 1701). The code is activated with *Enabled* The function is disabled by default.
Key Value	Only if **Use key** is enabled. Enter the GRE connection key. Possible values are *0* to *2147483647*. The default value is *0*.

Chapter 18 Firewall

The Stateful Inspection Firewall (SIF) provided for **bintec** 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

bintec's Stateful Inspection Firewall fits into the existing security architecture of **bintec** devices. 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).

18.1 Policies

18.1.1 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.

A list of all configured filter rules is displayed in the **Firewall**->**Policies**->**Filter Rules** menu.

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.

18.1.1.1 New

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

The menu **Firewall**->**Policies**->**Filter Rules**->**New** consists of the following fields:

Fields in the Filter RulesBasic 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**) are available. The value *Any* means that neither the destination interface nor the destination address is checked.

Field	Description
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**. 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.
Apply QoS	Only for **Action** = *Access* Select whether you want to enable QoS for this policy with the priority selected in **Priority**. The function is enabled with *Enabled*. The option is deactivated by default. If QoS is not activated for this policy, bear in mind that the data cannot be prioritised on the sender side either.

Field	Description
	A policy for which QoS has been enabled is also set for the firewall. Make sure therefore that data traffic that has not been expressly authorised if blocked by the firewall!
Priority	Only for **Apply QoS** = *Enabled* Select the priority with which the data specified by the policy is handled on the send side. Possible values: • *None* (default value): No priority. • *Low Latency*: Low Latency Transmission (LTT), i.e. handling of data with the lowest possible latency, e.g. suitable for VoIP data. • *High* • *Medium* • *Low*

18.1.2 QoS

More and more applications need increasingly larger bandwidths, which are not always available. Quality of Service (QoS) makes it possible to distribute the available bandwidths effectively and intelligently. Certain applications can be given preference and bandwidth reserved for them.

A list of all QoS rules is displayed in the **Firewall**->**Policies**->**QoS** menu.

18.1.2.1 New

Choose the **New** button to set up new QoS rules.

The **Firewall**->**Policies**->**QoS**->**New** menu consists of the following fields:

Fields in the QoSConfigure QoS Interface menu

Field	Description
Interface	Select the interface on which bandwidth management is to be carried out.
Traffic Shaping	Select whether you want to activate bandwidth management for

Field	Description
	the selected interface. The function is enabled with *Enabled*. The function is disabled by default.
Specify bandwidth	Only for **Traffic Shaping** = *Enabled*. Enter the maximum available bandwidth in kbps for the selected interface.
Filter Rules	This field contains a list of all configured firewall policies for which QoS was activated (**Apply QoS** = *Enabled*). The following options are available for each list entry: • **Use**: Select whether this entry should be assigned to the QoS interface. The option is deactivated by default. • **Bandwidth**: Enter the maximum available bandwidth in Bit/s for the service specified under **Service**. *0* is entered by default. • **Bounded**: Select whether the bandwidth defined in **Bandwidth** can be exceeded in the longer term. By activating this field, you specify that it cannot be exceeded. If the option is deactivated, the bandwidth can be exceeded and the excess data rate is handled in accordance with the priority defined in the firewall policy. The option is deactivated by default.

18.1.3 Options

In this menu, you can disable or enable the firewall and can log its activities. In addition, you can define after how many seconds of inactivity a session shall be ended.

The menu **Firewall**->**Policies**->**Options** consists of the following fields:

Fields in the OptionsGlobal Firewall Options menu

Field	Description
Firewall Status	Enable or disable the firewall function. The function is enabled with *Enabled* The function is enabled by default.

Field	Description
Logged Actions	Select the firewall syslog level. The messages are output together with messages from other subsystems. Possible values: • *All* (default value): All firewall activities are displayed. • *Deny* : Only reject and deny events are shown, see "Action". • *Accept* : Only accept events are shown. • *None* : Syslog messages are not generated.
Full Filtering	Here you specify if only such packets are to be filtered that are being sent to an interface that is different from the one that has initiated the connection. With the option *Enabled*(default value) all packets will be filtered.

Fields in the OptionsSession Timer menu

Field	Description
UDP Inactivity	Enter the inactivity time after which a UDP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *180*.
TCP Inactivity	Enter the inactivity time after which a TCP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *3600*.
PPTP Inactivity	Enter the inactivity time after which a PPTP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *86400*.
Other Inactivity	Enter the inactivity time after which a session of another type is to be regarded as expired (in seconds).

Field	Description
	Possible values are *30* to *86400*. The default value is *30*.

18.2 Interfaces

18.2.1 Groups

A list of all configured interface routes is displayed in the **Firewall**->**Interfaces**->**Groups** menu.

You can group together the interfaces of your device. This makes it easier to configure firewall rules.

18.2.1.1 New

Choose the **New** button to set up new interface groups.

The menu **Firewall**->**Interfaces**->**Groups**->**New** consists of the following fields:

Fields in the GroupsBasic Parameters menu

Field	Description
Description	Enter the desired description of the interface group.
Members	Select the members of the group from the available interfaces. To do this, activate the field in the **Members** column.

18.3 Addresses

18.3.1 Address List

A list of all configured addresses is displayed in the **Firewall**->**Addresses**->**Address List** menu.

18.3.1.1 New

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

The menu **Firewall**->**Addresses**->**Address List**->**New** consists of the following fields:

Fields in the Address ListBasic Parameters menu

Field	Description
Description	Enter the desired description of the address.
Address Type	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 **Address Type** = *Address / Subnet* Enter the IP address of the host or a network address and the related netmask. The default value is *0.0.0.0*.
Address Range	Only for **Address Type** = *Address Range* Enter the start and end IP address of the range.

18.3.2 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.

18.3.2.1 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 GroupsBasic Parameters menu

Field	Description
Description	Enter the desired description of the address group.
Selection	Select the members of the group from the available **Addresses**. To do this, activate the field in the **Selection** column.

18.4 Services

18.4.1 Service List

In the **Firewall**->**Services**->**Service List** menu, a list of all available services is displayed.

18.4.1.1 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 Service ListBasic 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 applic-

Field	Description
	able. If a port number range is specified, in the second field enter the last port of the port range. By default the field does not contain an entry. If a value is displayed, this means that the previously specified port number is verified. If a port range is to be checked, enter the upper limit here. Possible values are *1* to *65535*.
Type	Only for **Protocol** = *ICMP* The **Type** field shows the class of ICMP messages, the **Code** field specifies the type of message in greater detail. Possible values: • *Any* (default value) • *Echo reply* • *Destination Unreachable* • *Source quench* • *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*

Field	Description
	• *Protocol Unreachable* • *Port Unreachable* • *Fragmentation Needed* • *Communication with Destination Network is Administratively Prohibited* • *Communication with Destination Host is Administratively Prohibited*

18.4.2 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.

18.4.2.1 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 GroupsBasic Parameters menu

Field	Description
Description	Enter the desired description of the service group.
Members	Select the members of the group from the available service aliases. To do this, activate the field in the **Members** column.

Chapter 19 VoIP

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

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

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

19.1 SIP

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

19.1.1 Options

In the **VoIP**->**SIP**->**Options** menu you can perform global settings for the SIP.

The **VoIP**->**SIP**->**Options** menu includes the following fields:

Fields in the OptionsBasic Parameters menu

Field	Description
SIP Proxy	Select whether you want to activate the SIP proxy. The function is enabled with *Enabled*. The function is disabled by default.
SIP Port	Enter the port to be supervised by the proxy. or each destination port to which VoIP clients from the LAN can connect, you must configure a proxy. The ports can be provider-specific. The default value is *5060*.
Prioritize SIP Calls	Select whether you want to activate Prioritize SIP Calls.

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

19.2 RTSP

In this menu, you configure the use of the RealTime Streaming protocol (RTSP).

RTSP is a network protocol for controlling multimedia traffic flows in IP-based networks. Payload data is not transferred using RTSP. Rather, it is used to control a multimedia session between sender and recipient.

If you want to use RTSP, the firewall and NAT must be configured accordingly. In the **VoIP**->**RTSP** menu, you can activate the RTSP proxy to enable requested RTSP sessions over the defined port if required.

19.2.1 RTSP Proxy

In the **VoIP**->**RTSP**->**RTSP Proxy** menu, you configure the use of the RealTime Streaming protocol.

The **VoIP**->**RTSP**->**RTSP Proxy** menu consists of the following fields:

Fields in the RTSP ProxyBasic Parameters menu

Field	Description
RTSP Proxy	Select whether you want to permit RTSP sessions. The function is activated by selecting *Enabled*. The function is disabled by default.
RTSP Port	Select the port over which the RTSP messages are to come in and go out. Possible values are *0* to *65535*. The default value is *554*.

Chapter 20 Local Services

This menu offers services for the following application areas:

- Name resolution (DNS)
- Configuration via web browser (HTTPS)
- Locating of dynamic IP addresses using a DynDNS provider
- Configuration of gateway as a DHCP server (assignment of IP addresses)
- Access restriction on the Internet (web filter)
- Assignment of incoming and outgoing data and voice calls to authorised users (CAPI server)
- Automation of tasks according to schedule (scheduling)
- Alive checks for hosts or interfaces, ping tests
- User LAN protection (theft protection)
- Automatic detection and configuration of **bintec** devices
- Realtime video/audio conferences (Messenger services, universal plug & play)
- Provision of public Internet accesses (hotspot).
- Use of a redundant gateway (BRRP)

20.1 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, for providing an overview of DNS requests on your device.

Global Name Server

Under **Local Services**->**DNS**->**Global Settings**->**Basic Parameters** you enter the IP addresses of global name servers that are asked if your device cannot answer requests itself or by forwarding entries.

For local applications, the IP address of your device or the general loopback address (127.0.0.1) can be entered as the global name server.

Your device can also receive the global name servers dynamically 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 global name servers are entered, the primary DNS server then the secondary DNS server are asked. If the IP address of your device or the loopback address is entered for local applications, these are ignored here. 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 (**DNS Server Configuration** = *`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. If name server negotiation is successful, these are entered as global name servers and are therefore available for further requests.

(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.

20.1.1 Global Settings

The menu **Local Services**->**DNS**->**Global Settings** consists of the following fields:

Fields in the Global SettingsBasic Parameters menu

Field	Description
Domain Name	Enter the standard domain name of your device.
DNS Server Configuration	Select whether the addresses of the global name server on your device can be overwritten by transferred name server addresses. Possible values: • *Dynamic* (default value): The name server addresses can be automatically overwritten. • *Static* : The name server addresses are not overwritten.
DNS Server **Primary** **Secondary**	Only for **DNS Server Configuration** = *Static* Enter the IP address of the first and, if necessary, second global DNS server.
WINS Server **Primary** **Secondary**	Enter the IP address of the first and, if necessary, alternative global Windows Internet Name Server (=WINS) or NetBIOS Name Server (=NBNS).

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

Fields in the Advanced Settings menu

Field	Description
Positive Cache	Select whether the positive dynamic cache is to be activated, i.e. successfully resolved names and IP addresses are to be stored in the cache. The function is activated by selecting *Enabled*. The function is enabled by default.

Field	Description
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. Static 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*.
Fallback interface to get DNS server	Only for **DNS Server Configuration** = *Dynamic* 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.
IP address to use for DNS/WINS server assignment	**As DHCP Server** Select which name server addresses are sent to the DHCP client if your device is used as DHCP server.

Field	Description
	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. • *Global 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. • *Global DNS Setting* (default value): The addresses of the global name servers entered on your device are sent.

20.1.2 Static Hosts

A list of all configured static hosts is displayed in the **Local Services**->**DNS**->**Static Hosts** menu.

20.1.2.1 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 Static HostsBasic Parameters menu

Field	Description
DNS Hostname	Enter the host name to which the **IP Address** defined in this menu is to be assigned if a positive response is received to a DNS request. If a negative response is received to a DNS request, no address is specified. The entry can also start with the wildcard *, e.g. *.funkwerk.de.

Field	Description
	If a name is entered without a dot, this is completed with **OK** "<**Name**.> " after confirmation. 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.
IP Address	Only if **Response** = *Positive* Enter the IP address assigned to **DNS Hostname**.
TTL	Enter the validity period of the assignment from **DNS Hostname** to **IP Address** in seconds (only relevant for **Response** = *Positive*) transmitted to requesting hosts. The default value is *86400* (= 24 h).

20.1.3 Domain Forwarding

In the **Local Services**->**DNS**->**Domain Forwarding**menu, a list of all configured forwardings for defined domains is displayed.

20.1.3.1 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 Domain ForwardingForwarding Parameters menu

Field	Description
Forward	Select whether a host or domain is to be forwarded.

Field	Description
	Possible values: • *Host* (default value) • *Domain*
Host	Only for **Forwarding** = *Host* Enter the name of the host to be forwarded. The entry can also start with the wildcard *, e.g. *.funkwerk.com. If a name is entered without a full stop, you complete with **OK** " **<Default Domain>.** " after confirmation.
Domain	Only for **Forwarding** = *Domain* Enter the name of the domain to be forwarded. The entry can also start with the wildcard *, e.g. *.funkwerk.com. If a name is entered without a full stop, you complete with **OK** " **<Default Domain>.** " after confirmation.
Forward to	Select the forwarding destination requests to the name defined in **Host** or **Domain**. Possible values: • *Interface* (default value): The request is forwarded to the defined **Interface**. • *DNS Server*: The request is forwarded to the defined **DNS Server**.
Interface	Only for **Forward to** = *Interface* Select the interface via which the requests for the defined **Domain** are to be received and forwarded to the DNS server.
DNS Server	Only for **Forward to** = *DNS Server* Enter the IP address of the primary and secondary DNS server.

20.1.4 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 entry then disappears from the list and is thus included in the list in the **Static Hosts** menu. The TTL is transferred in this operation.

20.1.5 Statistics

In the**Local Services**->**DNS**->**Statistics**menu, the following statistical values are displayed::

Fields in the StatisticsDNS Statistics menu

Field	Description
Received DNS Packets	Shows the number of received DNS packets addressed direct to your device, including the response packets for forwarded requests.
Invalid DNS Packets	Shows the number of invalid DNS packets received and addressed direct to your device.
DNS Requests	Shows the number of valid DNS requests received and addressed direct to your device.
Cache Hits	Shows the number of requests that were answered with static or dynamic entries from the cache.
Forwarded Requests	Shows the number of requests forwarded to other name servers.
Cache Hitrate (%)	Indicates the number of **Cache Hits** per **DNS Requests** in percentage.
Successfully Answered Queries	Shows the number of successfully answered requests (positive and negative).
Server Failures	Shows the number of requests that were not answered by any name server (either positively or negatively).

20.2 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.

20.2.1 HTTPS Server

In the **Local Services**->**HTTPS**->**HTTPS Server** menu, you configure the parameters of the secured configuration connection over HTTPS.

The **Local Services**->**HTTPS**->**HTTPS Server** menu includes the following fields:

Fields in the HTTPS ServerHTTPS 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>`: Select a certificate entered under **System Management**->**Certificates**->**Certificate List**.

20.3 DynDNS Client

The use of dynamic IP addresses has the disadvantage that a host in the network can no longer be found once its IP address has changed. DynDNS ensures that your device can still be reached after a change to the IP address.

The following configuration steps are necessary:

- Registration of a host name at a DynDNS provider
- Configuration of your device

Registration

The registration of a host name means that you define an individual user name for the DynDNS service, e.g. *dyn_client*. The service providers offer various domain names for this, so that a unique host name results for your device , e.g. *dyn_client.provider.com*. The DynDNS provider relieves you of the task of answering all DNS requests concerning the host *dyn_client.provider.com* with the dynamic IP address of your device.

To ensure that the provider always knows the current IP address of your device, your device contacts the provider when setting up a new connection and propagates its present IP address.

20.3.1 DynDNS Update

In the **Local Services**->**DynDNS Client**->**DynDNS Update** menu, a list of all configured DynDNS registrations for updating is displayed.

20.3.1.1 New

Choose the **New** button to set up further DynDNS registrations to be updated.

The menu **Local Services**->**DynDNS Client**->**DynDNS Update**->**New** consists of the following fields:

Fields in the DynDNS UpdateBasic Parameters menu

Field	Description
Host Name	Enter the complete host name as registered with the DynDNS provider.
Interface	Select the WAN interface whose IP address is to be propagated over the DynDNS service (e.g. the interface of the Internet Service Provider).
User Name	Enter the user name as registered with the DynDNS provider.
Password	Enter the password as registered with the DynDNS provider.

Field	Description
Provider	Select the DynDNS provider with which the above data is registered. A choice of DynDNS providers is already available in the unconfigured state and their protocols are supported. Other DynDNS providers can be configured in the **Local Services**->**DynDNS Client**->**DynDNS Provider** menu. The default value is `DynDNS`.
Enable update	Select whether the DynDNS entry configured here is to be activated. The function is activated by selecting `Enabled`. The function is disabled by default.

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

Fields in the Advanced Settings menu

Field	Description
Mail Exchanger (MX)	Enter the full host name of a mail server to which e-mails are to be forwarded if the host currently configured is not to receive mail. Ask your provider about this forwarding service and make sure e-mails can be received from the host entered as MX.
Wildcard	Select whether the forwarding of all subdomains of the **Host Name** should be enabled for the current IP address of the **Interface** (advanced name resolution). The function is activated by selecting `Enabled`. The function is disabled by default.

20.3.2 DynDNS Provider

A list of all configured DynDNS providers is displayed in the **Local Services**->**DynDNS Client**->**DynDNS Provider** menu.

20.3.2.1 New

Choose the **New** button to set up new DynDNS providers.

The menu **Local Services**->**DynDNS Client**->**DynDNS Provider**->**New** consists of the following fields:

Fields in the DynDNS ProviderBasic Parameters menu

Field	Description
Provider Name	Enter a name for this entry.
Server	Enter the host name or IP address of the server on which the provider's DynDNS service runs.
Update Path	Enter the path on the provider's server that contains the script for managing the IP address of your device. Ask your provider for the path to be used.
Port	Enter the port at which your device is to reach your provider's server. Ask your provider for the relevant port. The default value is *80*.
Protocol	Select one of the protocols implemented. Possible values: • *DynDNS* (default value) • *Static DynDNS* • *ODS* • *HN* • *DYNS* • *GnuDIP-HTML* • *GnuDIP-TCP* • *Custom DynDNS* • *DnsExit*
Update Interval	Enter the minimum time (in seconds) that your device must wait

Field	Description
	before it is allowed to propagate its current IP address to the DynDNS provider again. The default value is `300` seconds.

20.4 DHCP Server

You can configure your device as a DHCP (Dynamic Host Configuration Protocol) server.

Your device and each PC in your LAN requires its own IP address. One option for allocating IP addresses in your LAN is the Dynamic Host Configuration Protocol (DHCP). If you configure your device as a DHCP server, the device automatically assigns IP addresses to requesting PCs in the LAN from a predefined IP address pool. A PC sends out an ARP request and in turn receives its IP address assigned by your device. 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.

20.4.1 DHCP Pool

To activate your device as a DHCP server, you must first define IP address pools from which the IP addresses are distributed to the requesting clients.

A list of all configured IP address pools is displayed in the **Local Services**->**DHCP Server**->**DHCP Pool** 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.

20.4.1.1 Edit or New

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

The menu **Local Services**->**DHCP Server**->**DHCP Pool**->**New** consists of the following fields:

Fields in the DHCP PoolBasic Parameters menu

Field	Description
Interface	Select the interface over which the addresses defined in **IP Address Range** 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 Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
Pool Usage	Specify whether the IP pool is used for DHCP requests in the same subnet or for DHCP requests that have been forwarded to your device from another subnet. In this case it is possible to define IP addresses from another network. Possible values: • *Local* (default value): The DHCP pool is only used for DHCP requests in the same subnet. • *Local/Relay*: The DHCP pool is used for DHCP requests in the same subnet and from other subnets. • *Relay*: The DHCP pool is only used for DHCP requests forwarded from other subnets.

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

Fields in the Advanced Settings menu

Field	Description
Gateway	Select which IP address is to be transferred to the DHCP client as gateway. Possible values: • *No gateway* (default value): No IP address is sent. • *Use router as gateway*: Here, the IP address defined for the **Interface** is transferred. • *Specify*: Enter the corresponding IP address.

Field	Description
Lease Time	Enter the length of time (in minutes) for which an address from the pool is to be assigned to a host. After the **Lease Time** expires, the address can be reassigned by the server. The default value is *120*.
DHCP Options	Specify which additional data is forwarded to the DHCP client. Possible values for **Option**: • *Time Server* (default value): Enter the IP address of the time server to be sent to the client. • *DNS Server*: Enter the IP address of the DNS server to be sent to the client. • *DNS Domain Name*: Enter the DNS domain to be sent to the client. • *WINS/NBNS Server*: Enter the IP address of the WINS/ NBNS server to be sent to the client. • *WINS/NBT Node Type*: Enter 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. Several entries are possible. Add additional entries with the **Add** button.

20.4.2 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 now 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**.

20.4.2.1 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 IP/MAC BindingBasic 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.

20.4.3 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 DHCP Relay SettingsBasic Parameters menu

Field	Description
Primary DHCP Server	Enter the IP address of a server to which BootP or DHCP requests are to be forwarded.

Field	Description
Secondary DHCP Server	Enter the IP address of an alternative BootP or DHCP server.

20.5 Web Filter

In the **Local Services**->**Web Filter** menu, you can configure a URL-based Web Filter service, which accesses the Proventia Web Filter from the company Internet Security Systems (*www.iss.net*) and checks how a requested Internet page is categorised by the Proventia Web Filter. The action resulting from the classification is configured on your device.

20.5.1 General

This menu contains the configuration of basic parameters for using the Proventia Web Filter.

The **Local Services**->**Web Filter**+**General**menu consists of the following fields:

Fields in the GeneralWeb Filter Options menu

Field	Description
Web Filter Status	Activate or deactivate the filter. The function is activated by selecting *Enabled*. The function is disabled by default.
Filtered Input Interface(s)	Select for which of the existing Ethernet and WLAN interfaces web filtering is to be activated. Press the **Add** button to add more interfaces. The requests from http Internet pages that reach your device via these interfaces are then monitored by web filtering.
Maximum Number of History Entries	Define the number of entries to be saved in the web filtering history (**History** menu). Possible values are *1* to *512*. The default value is *64*.
URL Path Depth	Select the path length to which a URL is to be checked by the Cobion Orange Filter.

Field	Description
Action if server not reachable	Select which is to be done with URL requests if the web filtering server cannot be reached. Possible values: • *Allow all* (default value): The download is permitted. • *Block all*:The download of the requested page is blocked. • *Log all*: The call is permitted, but logged.
Action if license not registered	Select what is to be done with URL requests if the licence key status is *Not Valid*. Possible values: • *Allow all* (default value): The download is permitted. • *Block all*:The download of the requested page is blocked. • *Log all*: The call is permitted, but logged.

The menu **License Information** consists of the following fields:

Fields in the GeneralLicense Information menu

Field	Description
Licence Key	Enter the number of your Proventia Web Filter licence. The preset code assigned by ISS designates the device type. In the ex works state, you can activate a 30-day demo version of the Proventia Web Filter. To do this, click the **Activate 30 days demo licence** link
Licence Status	Shows the result of the last validity check of the licence. The validity of the licence is checked every 23 hours.
License valid until	This shows the expiry date of the licence (relative to the time set on your device) and cannot be edited.

20.5.2 Filter List

In the **Local Services**->**Web Filter**->**Filter List** menu, you configure how the various categories of Internet pages are to be handled.

You configure the relevant filters for this purpose. A list of filters already configured is displayed.

There are basically different approaches for configuring the filters:

- First a filter list can be created that only contains entries for those addresses that are to be blocked. In this case it is necessary to make an entry at the end of the filter list that allows all accesses that do not match a filter. (Setting for this: **Category** = *Default behaviour*, **Action** = *Allow* or *Allow and Log*)
- If you only create entries for those addresses that are to be allowed or logged, it is not necessary to change the default behaviour (= all other calls are blocked).

20.5.2.1 New

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

The **Local Services**->**Web Filter**->**Filter List**->**New**menu consists of the following fields:

Fields in the Filter ListFilter Parameters menu

Field	Description
Category	Select which category of addresses/URLs the filter is to be used on. The options are first the standard categories of the Proventia Web Filter (default value: *Anonymous Proxies*). Actions can also be defined for the following special cases, e.g.: • *Default behaviour*: This category applies to all Internet addresses. • *Other Category*: Some addresses are already known to the Proventia Web Filter, but not yet classified. The action associated with this category is used for such addresses. • *Unknown URL*: If an address is not known to the Proventia Web Filter, the action associated with this category is used.
Day	Select the days on which the filter is to be active. Possible settings: • *Everyday* (default value): The filter is used every day of the week. • *<Weekday>*: The filter is used on a certain day of the week. Only one day can be selected per filter; several filters must be configured if several individual days are to be covered.

Field	Description
	• *Monday-Friday*: The filter is used from Monday to Friday. The default value is *Everyday*.
Schedule (Start / Stop Time)	In **From**, enter from which time the filter is to be activated. The time is entered in the form hh:mm. Enter the time at which the filter is to be deactivated in the field after the **to**. The time is entered in the form hh:mm. The default value is 00:00 to 23:59.
Action	Select the action to be executed if the filter matches a call. Possible values: • *Block and Log* (default value): The call of the requested page is prevented and logged. • *Allow and Log*: The call is permitted, but logged. You can view the logged events in the **Local Services**->**Web Filter**->**Filter List**. • *Allow*: The call is allowed and not logged.

20.5.3 Black / White List

The menu **Local Services**->**Web Filter**->**Black / White List** includes a list with URLs or IP addresses. Addresses **on the White List** can even be called up if they were blocked because of filter configuration and classification in the Proventia Web Filter . Addresses **on the Black List** remain blocked if they can be called up because of filter configuration and classification in the Proventia Web Filter . Neither list contains entries in standard configuration.

20.5.3.1 Add

Use the **Add** button to add further URLs or IP addresses to the list.

The **Local Services**->**Web Filter**->**Black / White List**->**Add**menu consists of the following fields:

Fields in the Black / White List menu

Field	Description
URL / IP Address	You enter a URL or IP address. The length of the entry is limited to 60 characters.

Field	Description
Blacklisted **Whitelisted**	You can select whether a URL or an IP address can always (*Whitelisted*) or never (*Blacklisted*) be called up. *Whitelisted*is active by default. Addresses listed in the White List are allowed automatically. It is not necessary to configure a suitable filter.

20.5.4 History

In the **Local Services**->**Web Filter**->**History** menu, you can view the recorded history of the web filter. The history logs all requests that are marked for logging by a relevant filter (**Action** = *Allow and Log* oder *Block and Log*), likewise all rejected requests.

20.6 CAPI Server

You can use the CAPI Server function to assign user names and passwords to users of the CAPI applications on your device. This makes sure that only authorised users can receive incoming calls and make outgoing calls via CAPI.

The CAPI service allows connection of incoming and outgoing data and voice calls to communications applications on hosts in the LAN that access the Remote CAPI interface of your device. This enables, for example, hosts connected to your device to receive and send faxes.

Note

All incoming calls to the CAPI are offered to all registered and "eavesdropping" CAPI applications in the LAN.

Ex works, a user with the user name *default* and no password is always entered for the CAPI subsystem.

Once you've created your intended user with password, delete the *default* user without password.

20.6.1 User

A list of all configured CAPI users is displayed in the **Local Services**->**CAPI Server**->**User** menu.

20.6.1.1 New

Choose the **New** button to set up new CAPI users.

The menu **Local Services**->**CAPI Server**->**User**->**New** consists of the following fields:

Fields in the UserBasic Parametersmenu

Field	Description
User Name	Enter the user name for which access to the CAPI service is to be allowed or denied.
Password	Enter the password which user **User Name** shall employ for identification to gain access to the CAPI service.
Access	Select whether access to the CAPI service is to be permitted or denied for the user. The function is activated by selecting *Enabled*. The function is enabled by default.

20.6.2 Options

The menu **Local Services**->**CAPI Server**->**Options** consists of the following fields:

Fields in the OptionsBasic Parameters menu

Field	Description
Enable server	Select whether your device is to be enabled as a CAPI server. The function is activated by selecting *Enabled*. The function is enabled by default.
CAPI Server TCP Port	The field can only be edited if **Enable server** is enabled.

Field	Description
	Enter the TCP port number for remote CAPI connections. The default value is *2662*.

20.7 Scheduling

Your device has a event scheduler, which enables certain standard actions (activation or deactivation of interfaces) to be carried out on a time-dependent basis.

Note

To run the event scheduler, the date configured on your device must be 1.1.2000 or later.

20.7.1 Trigger

A list of all planned tasks is displayed in the **Local Services**->**Scheduling**+**Trigger** menu.

20.7.1.1 New

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

The menu **Local Services**->**Scheduling**+**Trigger**->**New** consists of the following fields:

Fields in the TriggerBasic Parameters menu

Field	Description
Event List	Indicate the desired index for this initiator. The configured initiators can be summarised via assignment to an index to the events list, so that complex conditions for initiating an action may also be created. The initiators within an events list are then processed in the listed order. If you wish to add a new events list, select *New* (default value). If a single event is to be configured as an initiator, it also receives an index.
Description	Enter the desired name for the scheduled task.

Field	Description
Event Type	Select the initiator type. Possible values: • *Time* (default value): The operations configured and assigned in **Actions** are triggered at specific points in time. • *MIB/SNMP*: The actions configured and assigned in **Actions** are triggered if the defined MIB variables assume the specified values.. • *Interface Status*: The actions configured and assigned in **Actions** are triggered if the defined interfaces take on a specified status. • *Interface Traffic*: The operations configured and assigned in **Actions** are triggered if the data traffic on the specified interfaces falls below or exceeds the defined value. • *Ping Test*: The operations configured and assigned in **Actions** are triggered if the defined interfaces are accessible or not accessible. Interface status is checked via ping test. • *Certificate Lifetime*: The operations configured and assigned in **Actions** are triggered when the specified validity period is reached.
Monitored Variable	Only for **Event Type** *MIB/SNMP* Select the MIB variables whose defined value is to be configured as initiator. First select the **System** on which the MIB variable is saved, then the **MIB Table** and finally the **MIB Variable** itself. Only MIB tables and MIB variables existing in the relevant area are displayed.
Compare Condition	Only for **Event Type** *MIB/SNMP* Select whether the MIB variable must be *Greater* (default value), *Equal*, *Less*, *Not Equal* to the value specified in *Compare Value*, or lie within a *Range* in order to trigger 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*

Field	Description
	Where required, select MIB variables to be used as "index" in order to uniquely identify a specific data set in **MIB Table**, e.g. *ConnIfIndex*. The combination of **Index Variable** and **Index Value** yields unique identification of a specific table entry.
Monitored Interface	Only for **Event Type** *Interface Status* and *Interface Traffic* Select the interface whose defined status shall trigger an operation.
Interface Status	Only for **Event Type** *Interface Status* Select the status that the interface must assume in order to trigger the intended operation. Possible values: • *Up* (default value): The interface is active. • *Down*: The interface is inactive.
Traffic Direction	Only for **Event Type** *Interface Traffic* Select the direction of the data traffic whose values should be monitored as initiator for an action. Possible values: • *RX* (default value): Incoming data traffic is monitored. • *TX*: Outgoing data traffic is monitored.
Monitored Variable	Only for **Event Type** *MIB/SNMP* Select the MIB variables whose defined value is to be configured as initiator. First select the **System** on which the MIB variable is saved, then the **MIB Table** and finally the **MIB Variable** itself. Only MIB tables and MIB variables existing in the relevant area are displayed.
Compare Condition	Only for **Event Type** *MIB/SNMP* Select whether the MIB variable must be *Greater* (default value), *Equal*, *Less*, *Not Equal* to the value specified in *Compare Value*, or lie within a *Range* in order to trigger the

Field	Description
	operation.
Compare Value	Only for **Event Type** *MIB/SNMP* Enter the value of the MIB variable.
Index Variables	Only for **Event Type** *MIB/SNMP* Where required, select MIB variables to be used as "index" in order to uniquely identify a specific data set in **MIB Table**, e.g. *ConnIfIndex*. The combination of **Index Variable** and **Index Value** yields unique identification of a specific table entry.
Monitored Interface	Only for **Event Type** *Interface Status* and *Interface Traffic* Select the interface whose defined status shall trigger an operation.
Interface Status	Only for **Event Type** *Interface Status* Select the status that the interface must assume in order to trigger the intended operation. Possible values: • *Up* (default value): The interface is active. • *Down*: The interface is inactive.
Traffic Direction	Only for **Event Type** *Interface Traffic* Select the direction of the data traffic whose values should be monitored as initiator for an action. Possible values: • *RX* (default value): Incoming data traffic is monitored. • *TX*: Outgoing data traffic is monitored.
Monitored Certificate	Only for **Event Type** *Certificate Lifetime* Select the certificate whose validity should checked.
Remaining Validity	Only for **Event Type** *Certificate Lifetime*

Field	Description
	Indicate the remaining validity of the certificate as a percentage.

Fields in the TriggerSelect time interval menu

Field	Description
Time Condition	First select the type of time entry in **Condition Type**. Possible values: • *Weekday* : Select a weekday in **Condition Settings**. • *Periods* (default value): In **Condition Settings**, select a particular period. • *Day of Month*: Select a specific day of the month in **Condition Settings**. Possible values for **Condition Settings** in **Condition Type** = *Weekday*: *Monday* (default value) ... *Sunday*. Possible values for **Condition Settings** in **Condition Type** = *Periods*: • *Daily* : The initiator becomes active daily (default value). • *Monday-Friday* : The initiator becomes active daily from Monday to Friday. • *Monday - Saturday* : The initiator becomes active daily from Monday to Saturday. • *Saturday - Sunday* : The initiator becomes active on Saturdays and Sundays. Possible values for **Condition Settings** in **Condition Type** = *Day of Month*: *1* ... *31*.
Start Time	Enter the time from which the initiator is to be activated. Activation is carried on the next scheduling interval. the default value of this interval is 55 seconds.
Stop Time	Enter the time from which the initiator is to be deactivated. De-

Field	Description
	activation is carried on the next scheduling interval. If you do not enter a **Stop Time** or set **Stop Time** = **Start Time**, the initiator is activated and deactivated after 10 seconds.

20.7.2 Actions

In the **Local Services**->**Scheduling**+**Actions**menu a list of all operations to be triggered by events or event chains configured in **Local Services**->**Scheduling**->**Trigger** is displayed.

20.7.2.1 New

Choose the **New** button to configure additional operations.

The menu **Local Services**->**Scheduling**+**Actions**->**New** consists of the following fields:

Fields in the ActionsBasic Parameters menu

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. • *Software Update*: A software update is initiated. • *Configuration Management*: A configuration file is loaded onto your device or backed up by your device. • *Ping Test*: Accessibility of an IP address is checked. • *Certificate Management*: A certificate is to be renewed, deleted or entered. • *WLC: New Neighbor Scan*: A Neighbor Scan is launched in a WLAN network controlled by the WLAN controller. • *WLC: VSS State*: The status of a wireless network is modified.

Field	Description
Event List	Select the index of events or event chain configured in **Local Services**->**Scheduling**->**Trigger**->**Event List**.
Event List Condition	For event chains, select how many of the configured events must occur for the operation to be triggered. Possible values: • *all* (default value): The operation is triggered if all events occur. • *one*: The operation is triggered if one 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* Indicate a timespan in seconds that must pass before 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 is to be modified is saved. First select the **System**, then the **MIB Table**. Only MIB tables present in the relevant area are displayed.
Command Mode	Only if **Command Type** = *MIB/SNMP* Select how the MIB entry is to be modified. Possible settings: • *Change existing entry* (default value): An existing entry must be modified. • *Create new MIB entry*: A new entry must be created.
Index Variables	Only if **Command Type** = *MIB/SNMP* Where required, select MIB variables to be used as "index" in order to uniquely identify a specific data set in **MIB Table**, e.g. *ConnIfIndex*. The combination of **Index Variable** and **Index**

Field	Description
	Value yields unique identification of a specific table entry. Use **Index Variables** to create**Add**.
Trigger Status	Only if **Command Type** = *MIB/SNMP* Select the 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 active. • *Both* : The value of the MIB variable is differentially modified as the initiator status evolves.
MIB Variables	Only if **Command Type** = *MIB/SNMP* Select the MIB variables whose value, dependent on the initiator status, is to be modified. If the initiator is active (**Trigger Status** *Active*), the MIB variable with the value entered in **Active Value** is described. If the initiator is inactive (**Trigger Status** *Inactive*), the MIB variable with the value entered in **Inactive Variable** is described. 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 entered in **Inactive Variable**. 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.

Field	Description
	Possible values: - *Up* (default value) - *Down* - *Reset*
Source Location	Only if **Command Type** = *Software Update* Select the source for the software update. Possible values: - *Current Software from Funkwerk Server* (default value): The latest software will be downloaded from the Funkwerk server. - *HTTP Server*: The latest software will be downloaded from an HTTP server that you define in *Server URL*. - *HTTPS Server*: The latest software will be downloaded from an HTTP server that you define in *Server URL*. - *TFTP Server*: The latest software will be downloaded from an HTTP server that you define in *Server URL*.
Server URL	For **Command Type** = *Software Update* if **Source Location** not *Current Software from Funkwerk Server* Enter the URL of the server from which the desired software version is to be drawn. For **Command Type** = *Configuration Management* with **Action** = *Import configuration* or *Export configuration* Enter the URL of the server from which a configuration file will be obtained, 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. For **Command Type** = *Certificate Management* with **Action** = *Import certificate*

Field	Description
	Enter the file name of the certificate file.
Action	For **Command Type** = *Configuration Management* Select which operation you wish to perform on a configuration file. Possible values: • *Import configuration* (default value) • *Export configuration* • *Rename configuration* • *Delete configuration* • *Copy configuration* For **Command Type** = *Certificate Management* Select which operation you wish to perform on a certificate file. Possible values: • *Import certificate* (default value) • *Delete certificate* • *SCEP*
Protocol	Only for **Command Type** = *Certificate Management* and *Configuration Management* if **Action** = *Import configuration* Select the protocol for the data transfer. Possible values: • *HTTP* (default value) • *HTTPS* • *TFTP*
CSV File Format	Only for **Command Type** = *Configuration Management* and **Action** = *Import configuration* or *Export configuration* Select whether to transfer the file in CSV format, which can easily be read and modified. In addition, you can view the corres-

Field	Description
	ponding 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 name of the file under which to save it on the server on which it is to be saved.
Local File Name	Only for **Command Type** = *Configuration Management* and **Action** = *Import configuration*, *Rename configuration* or *Copy configuration* When importing, renaming or copying, assign a name to the configuration file under which it can be saved locally on the device.
File Name in Flash	For **Command Type** = *Configuration Management* and **Action** = *Export configuration* Select the source file to be exported. For **Command Type** = *Configuration Management* and **Action** = *Rename configuration* Select the file to be renamed. For **Command Type** = *Configuration Management* and **Action** = *Delete configuration* Select the file to be deleted. For **Command Type** = *Configuration Management* and **Action** = *Copy configuration* Select the file to be copied.
Configuration contains certificates/keys	Only for **Command Type** = *Configuration Management* and **Action** = *Import configuration* or *Export config-*

Field	Description
	uration 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 for **Command Type** = *Configuration Management* and **Action** = *Import configuration* or *Export configuration* Define whether the data of the selected **Action** are to be encrypted.. The function is disabled by default.
Reboot after execution	Only if **Command Type** = *Configuration Management* Select whether to restart your device after the desired **Action**. The function is disabled by default.
Version Check	Only for **Command Type** = *Configuration Management* and **Action** = *Import configuration* Select whether, when importing a configuration file, there should be a check for the existence on the server of a newer version of the already loaded configuration. If not, the file import is aborted. The function is disabled by default.
Destination IP Address	Only if **Command Type** = *Ping Test* Enter the IP address to be checked for accessibility.
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.

Field	Description
	• *Specific*: Enter the desired IP address in the entry field.
Interval	Only if **Command Type** = *Ping Test* Enter the time in **Seconds** after which to send a new ping. 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 to be considered unreachable. The default value is *3*.
Server Address	Only for **Command Type** = *Certificate Management* and **Action** = *Import certificate* Enter the URL of the server from which a certificate file is to be obtained.
Local Certificate Description	For **Command Type** = *Certificate Management* and **Action** = *Import certificate* Enter a description for the certificate under which to save it on the device. For **Command Type** = *Certificate Management* and **Action** = *Delete certificate* Select the certificate to be deleted.
Password for protected Certificate	Only for **Command Type** = *Certificate Management* and **Action** = *Import certificate* Select whether to use a secure certificate requiring a password, and enter into the entry field. The function is disabled by default.
Overwrite similar certificate	Only for **Command Type** = *Certificate Management* and **Action** = *Import certificate* Select whether to overwrite a certificate already present on your device with a new one.

Field	Description
	The function is disabled by default.
Write certificate in configuration	Only for **Command Type** = *Certificate Management* and **Action** = *Import certificate* Choose whether to integrate the certificate into a configuration file, and select the desired configuration file. The function is disabled by default.
Certificate Request Description	Only for **Command Type** = *Certificate Management* and **Action** = *SCEP* Enter a description under which to save the SCEP certificate on your device.
URL SCEP Server URL	Only for **Command Type** = *Certificate Management* and **Action** = *SCEP* Enter the URL of the SCEP server, e.g. *http://scep.funkwerk.de:8080/scep/scep.dll* Your CA administrator can provide you with the necessary data.
Subject Name	Only for **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 for **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 for **Command Type** = *Certificate Management* and **Action** = *SCEP* You may need a password from the certification authority to ob-

Field	Description
	tain certificates. Enter the password you received from the certification authority here.
Key Size	Only for **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 for **Command Type** = *Certificate Management* and **Action** = *SCEP* Select whether your device automatically stores the various steps of the enrolment internally. This is an advantage if enrolment cannot be concluded immediately. If the status has not been saved, the incomplete registration cannot be completed. As soon as the enrolment is completed and the certificate has been downloaded from the CA server, it is automatically saved in the device configuration. The function is enabled by default.
Use CRL	Only for **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): If the CA certificate contains an entry for a CDP, CRL Distribution Point, it should be evaluated in addition to the CRLs already globally configured on the device. • *Yes*: CRLs are always checked. • *No*: No CRL check.
WLC SSID	Only if **Command Type** = *WLC: VSS State* Select the wireless network administered via the WLAN controller whose status should be changed.
Set status	Only if **Command Type** = *WLC: VSS State*

Field	Description
	Select the status for the selected wireless network. Possible values: • *Activate* (default value) • *Deactivate*

20.7.3 Options

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

The **Local Services**->**Scheduling**->**Options** menu includes the following fields:

Fields in the OptionsScheduling Options menu

Field	Description
Schedule Interval	Select whether the schedule interval is to be enabled for the interface. Enter the interval in seconds during which the system checks whether there are planned tasks. Possible values are *0* to *65535*. The value *300* is recommended (5 minute accuracy). Values lower than 60 are generally pointless and are an unnecessary use of system resources.

20.8 Surveillance

In this menu, you can configure an automatic availability check for hosts or interfaces and automatic ping tests.

Note

This function cannot be configured on your device for connections that are authenticated via a RADIUS server.

20.8.1 Hosts

In the **Local Services**->**Surveillance**->**Hosts** menu, a list of all monitored hosts is displayed.

20.8.1.1 Edit or New

Choose the 🔧 icon to edit existing entries. Choose the **New** button to create additional monitoring tasks.

The menu **Local Services**->**Surveillance**->**Hosts**->**New** consists of the following fields:

Field in the HostsHost Parameters menu

Field	Description
Group ID	Select an ID for the group of hosts whose availability is to be monitored by your device. The group IDs are automatically created from *0* to *255*. If an entry has not yet been created, a new group is created using the *New ID* option. If entries have been created, you can select one from the list of created groups. Each host to be monitored must be assigned to a group. The operation configured in **Interface Action** is only executed if no other group member can be reached.

Fields in the HostsTrigger menu

Field	Description
Monitored IP Address	Enter the IP address of the host to be monitored.
Source IP Address	Select how the IP address is to be determined that your device uses as the source address of the packet sent to the host to be monitored. Possible values: • *Automatic* (default value): The IP address is determined automatically. • *Specific*: Enter the IP address in the adjacent input field.

Field	Description
Interval	Enter the time interval (in seconds) to be used for checking availability of the host. Possible values are *1* to *65536*. The default value is *10*. The smallest **Interval** of the group members is used within a group.
Trials	Enter the number of pings that must remain unanswered for the host to be regarded as unavailable. Possible values are *1* to *65536*. The default value is *3*.
Controlled Interfaces	Select the interface(s) for which the action defined in **Interface Action** is to be performed. All physical and virtual interfaces can be selected. Select whether each interface is to be enabled (*Enable*) disabled (*Disable*default value), set back (*Reset*) or the connection restored (*Redial*).

20.8.2 Interfaces

In the **Local Services**->**Surveillance**->**Interfaces** menu, a list of all monitored interfaces is displayed.

20.8.2.1 Edit or New

Choose the icon to edit existing entries. Choose the **New** button to set up monitoring for other interfaces.

The menu **Local Services**->**Surveillance**->**Interfaces**->**New** consists of the following fields:

Fields in the InterfaceBasic Parameters menu

Field	Description
Monitored Interface	Select the interface on your device that is to be monitored.

Field	Description
Trigger	Select the status or status transition of **Monitored Interface** that is to trigger a particular **Interface Action**. Possible values: • *Interface goes up* (default value) • *Interface goes down*
Interface Action	Select the action that is to follow the status or status transition defined in **Trigger**. The action is applied to the interface(s) selected in **Interface**. Possible values: • *Enable* (default value): Activation of interface(s) • *Disable*: Deactivation of interface(s)
Interface	Select the interface(s) for which the action defined in **Interface** is to be performed. All physical and virtual interfaces can be selected, along with the *All PPP Interfaces* and *All IPSec Interfaces* options .

20.8.3 Ping Generator

In the **Local Services**->**Surveillance**->**Ping Generator** menu, a list of all configured, automatically generated pings is displayed.

20.8.3.1 Edit or New

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

The menu **Local Services**->**Surveillance**->**Ping Generator**->**New** consists of the following fields:

Fields in the Ping GeneratorBasic Parameters menu

Field	Description
Destination IP Address	Enter the IP address to which the ping is automatically sent.

Field	Description
Source IP Address	Enter the source IP address of the outgoing ICMP echo request packets. Possible values: • *Automatic*: The IP address is determined automatically. • *Specific* (default value): Enter the IP address in the adjacent input field e.g. to test a particular extended route.
Interval	Enter the interval in seconds during which the ping is sent to the address specified in **Remote IP Address**. Possible values are *1* to *65536*. The default value is *10*.
Trials	Enter the number of ping tests to be performed until **Destination IP Address** is to be considered *Unreacheable*. The default value is *3*.

20.9 ISDN Theft Protection

With the ISDN theft protection function, you can prevent a thief who has stolen a gateway from gaining access to the gateway owner's LAN. (Without theft protection, he could dial into the LAN by ISDN if the field setting **WAN**->**Internet + Dialup**->**ISDN**->🔧-1**Always on** is enabled.)

20.9.1 Options

All interfaces for which the theft protection is enabled are administratively set to "down" when the gateway boots.

The gateway then calls itself by ISDN and checks its location. If the configured ISDN call numbers differ from the numbers dialled, the interfaces remain disabled.

If the numbers agree, the device assumes that it is at the original location and the interfaces are administratively set to "up".

To reduce cost, the function uses the ISDN D channel.

Note

Note that the ISDN theft protection function is not available for Ethernet interfaces.

The menu **Local Services**->**ISDN Theft Protection**->**Options** consists of the following fields:

Fields in the OptionsBasic Parameters menu

Field	Description
ISDN Theft Protection Service	Enable or disable the ISDN theft protection function. The function is enabled with *Enabled*. The function is disabled by default.
Dialling Number	Only if **ISDN Theft Protection Service** is enabled. Enter the subscriber number that the gateway dials to call itself.
Incoming Number	Only if **ISDN Theft Protection Service** is enabled. Enter the subscriber number to be compared with the current calling party number.
Outgoing Number	Only if **ISDN Theft Protection Service** is enabled. Enter the subscriber number to be set as calling party number.
Monitored Interfaces	Only if **ISDN Theft Protection Service** is enabled. Use **Add** to add a new interface to the list. Select from the available interfaces those to which the ISDN theft protection function is to be applied.

Fields in the OptionsAdvanced Settings menu

Field	Description
Number of Dialling Retries	Enter the number of dial attempts that the gateway is to make to call itself by ISDN after a reboot. Possible values are *1* to *255*.

Field	Description
	The default value is *3*.
Timeout	Enter the time in seconds that the gateway is to wait before trying again after an unsuccessful attempt to call itself. Possible values are *2* to *20*. The default value is *5*.

20.10 Funkwerk Discovery

20.10.1 Device Discovery

The funkwerk Discovery protocol is used to identify and configure **bintec** devices that are in the same wired network as your device. Once a **bintec** device has been discovered, certain basic parameters (node name, IP address, netmask, and device address) can be configured on the access point (provided you know the administrator password).

☞ **Note**

Any **bintec** devices that exist are determined by means of a multicast. The IP address of the device is therefore irrelevant.

Please note that the discovered **bintec** devices are not stored in the flash, which means discovery must be repeated after you reboot your device.

In the **Local Services**->**Funkwerk Discovery**->**Device Discovery** menu, a list of all discovered access points in the network is displayed under **Results**. In the **Interface** field, select the interface of your device via which access point discovery is to be carried out. You use the *-All-* option to query all interfaces.

The current discovery status is displayed for each individual interface under Discovery Status. Here, *None* means that no discovery is active. *Discovery* is displayed if a discovery is currently performed.

This discovery function also enables your device to be discovered and configured by other access points with a discovery function. You configure this in the **Options** submenu.

20.10.1.1 Discover

Click the **Discover** button to launch the **bintec** access point discovery.

If access points were discovered in the network, they are displayed in the list. You use the 🔧 button to go to the configuration menu for the access point.

The menu **Local Services**->**Funkwerk Discovery** ->**Device Discovery**->🔧 consists of the following fields:

Fields in the Device DiscoveryBasic Parameters menu

Field	Description
Interface	The value of this field can only be read. Shows the interface of your device on which discovery is carried out.
MAC Address	The value of this field can only be read. Shows the MAC address of the discovered access point.
Node Name	You can change the name of the discovered access point.
IP Address	You can change the IP address of the discovered access point.
Netmask	You can change the related netmask.
Gateway	You can change the gateway address of the discovered access point.
Authentication Password	You must enter the administrator password for the access point, The configuration operation cannot be performed without a password.
Last Write Result	The value of this field can only be read. Displays the result of the last configuration operation. Possible values: • *No error*: The access point reported a successful operation, or a configuration change has not yet been performed with

Field	Description
	OK . - *Timeout*: The access point has not responded. - *Access denied*: The access point reported an authorisation error. Check the authentication password. - *Invalid IP Parameters*: There is a problem with the intended IP parameters (IP address, netmask, or gateway address). - *Destination Unreachable*: The access point cannot be reached for internal reasons (e.g. the interface to which the access point is connected is down). A configuration request cannot be sent to the access point. - *Other Error*: The access point responds to the configuration request with an unexpected or non-specific error. - *Internal Error*: An internal device problem prevented the configuration option from being carried out.

20.10.2 Options

In this menu, you can grant permission for your device to be discovered by other **bintec** devices using the funkwerk Discovery protocol and to be configured by means of this.

The **Local Services**->**Funkwerk Discovery** ->**Options**menu consists of the following fields:

Fields in the OptionsDiscovery Server Options menu

Field	Description
Enable Discovery Server	Select whether your device is to be discovered and configured by other **bintec** devices in the network. The function is enabled with *Enabled*. The function is disabled by default.

20.11 UPnP

Universal Plug and Play (UPnP) makes it possible to use current messenger services (e.g. real time video/audio conferencing) as peer-to-peer communication where one of the peers lies behind a NAT-enabled gateway.

UPnP enables (mostly) Windows-based operating systems to take control of other devices with UPnP functionality on the local network. These include gateways, access points and print servers. No special device drivers are needed as known common protocols are used, such as TCP/IP, HTTP and XML.

Your gateway makes it possible to use the subsystem of the Internet Gateway Device (IGD) from the UPnP function range.

In a network behind a NAT-enabled gateway, the UPnP-configured computers act as LAN UPnP clients. To do this, the UPnP function on the PC must be enabled.

The pre-configured port used for UPnP communication between LAN UPnP clients and the gateway is *5678*. The LAN UPnP client acts as a so-called service control point, i.e. it recognizes and controls the UPnP devices on the network.

The ports assigned dynamically by, for example, MSN Messenger, lie in the range from *5004* to *65535*. The ports are released internally to the gateway on demand, i.e. when an audio/video transfer is started in Messenger. When the application is closed, the ports are immediately closed again.

The peer-to-peer-communication is initiated via public SIP servers with only the information from the two clients being forwarded. The clients then communicate directly with one another.

For further information about UPnP, see *www.upnp.org* .

20.11.1 Interfaces

In this menu, you configure the UPnP settings individually for each interface of your gateway.

You can determine whether UPnP requests from clients are accepted by each interface (for requests from the local network) and/or whether the interface can be controlled via UPnP requests.

The **Local Services**->**UPnP**->**Interfaces**menu consists of the following fields:

Fields in the Interfaces menu

Field	Description
Interface	Shows the name of the interface for which the UPnP settings are to be made. The entry cannot be changed.
Answer to client request	Determine whether UPnP requests from clients are to be answered via the particular interface (from the local network).

Field	Description
	The function is enabled with *Enabled*. The function is disabled by default.
Interface is UPnP controlled	Determine whether the NAT configuration of this interface is controlled by UPnP. The function is enabled with *Enabled*. The function is enabled by default.

20.11.2 General

In this menu, you make the basic UPnP settings.

The **Local Services**->**UPnP**+**General**menu consists of the following fields:

Fields in the General menu

Field	Description
UPnP Status	Decide how the gateway processes UPnP requests from the LAN. The function is enabled with *Enabled*. The gateway proceeds with UPnP releases in accordance with the parameters contained in the request from the LAN UPnP client, independently of the IP address of the requesting LAN UPnP client. The function is disabled by default. The gateway rejects UPnP requests, NAT releases are not made.
UPnP TCP Port	Enter the number of the port on which the gateway listens for UPnP requests. The possible values are *1* to *65535*, the default value is *5678*.

20.12 HotSpot Gateway

The **bintec HotSpot Solution** allows provision of public Internet accesses (using WLAN or wired Ethernet). The solution is adapted to setup of smaller and larger Hotspot solutions for cafes, hotels, companies, communal residences, campgrounds, etc.

The **bintec HotSpot Solution** consists of a bintec gateway installed onsite (with its own WLAN access point or additional connected WLAN device or wired LAN) and of the Hotspot server, centrally located at a computing centre. The operator account is administered on the server via an administration terminal (e.g., a hotel reception PC); this includes functions such as registration entry, generating tickets, statistical analysis, etc.

Login sequence at the Hotspot server

- When a new user connects with the Hotspot, he/she is automatically assigned an IP address via DHCP.
- As soon as he attempts to access any Internet site with a browser, the user is redirected to the home/login page.
- After the user has entered the registration data (user/password), these are sent to the central RADIUS server (Hotspot server) as RADIUS registration.
- Following successful registration, the gateway opens Internet access.
- For each user, the gateway sends regular additional information to the RADIUS server for recording accounting data.
- When the ticket expires, the user is automatically logged off and again redirected to the home/login page.

Requirements

To operate a Hotspot, the customer requires:

- a bintec device as hotspot gateway with an active Internet access and configured hotspot server entries for login and accounting (see menu**System Management**->**Remote Authentication**->**RADIUS**->**New** with **Group Description** *Default group 0*)
- bintec Hotspot hosting (article number 5510000198)
- Access data
- Documentation
- Software licensing

  Please note that you must first activate the licence.

  - Go to *www.funkwerk-ec.com* then **Service/Support** -> **Services** -> **Online Services**.

  - Enter the required data (please note the relevant explanations on the license sheet), and follow the instructions of the online licensing.

  - You then receive the Hotspot server's login data.

Note

Activation may require 2-3 business days.

Access data for gateway configuration

RADIUS Server IP	62.245.165.180
RADIUS Server Password	Set by Funkwerk Enterprise Communications GmbH
Domain	Individually set for customers by customer/dealer
Walled Garden Network	Individually set for customers by customer/dealer
Walled Garden Server URL	Individually set for customers by customer/dealer
Terms & Conditions URL	Individually set for customers by customer/dealer

Access data for configuration of the Hotspot server

Admin URL	https://hotspot.funkwerk-ec.com/
Username	Individually set by FEC
Password	Individually set by FEC

Note

Also refer to the WLAN Hotspot Workshop that is available to download from *www.funkwerk-ec.com* .

20.12.1 HotSpot Gateway

In the **HotSpot Gateway** menu, you configure the bintec gateway installed onsite for the **bintec Hotspot Solution**.

A list of all configured hotspot networks is displayed in the **Local Services**->**HotSpot Gateway**->**HotSpot Gateway** menu.

You can use the **Enabled** option to enable or disable the corresponding entry.

20.12.1.1 Edit or New

In the **Local Services**->**HotSpot Gateway**->**HotSpot Gateway**->🔧 menu, you configure the hotspot network. Choose the **New** button to set up additional Hotspot networks.

The **Local Services**->**HotSpot Gateway**->**HotSpot Gateway**->🔧 menu includes the following fields:

Fields in the HotSpot GatewayBasic Parameters menu

Field	Description
Interface	Choose the interface to which the Hotspot LAN or WLAN is connected. When operating over LAN, enter the Ethernet interface here (e.g. en1-0). If operating over WLAN, the WLAN interface to which the access point is connected must be selected.
⚠	**Caution** For security reasons you cannot configure your device over an interface that is configured for the Hotspot. Therefore take care when selecting the interface you want to use for the Hotspot. If you select the interface over which the current configuration session is running, the current connection will be lost. You must then log in again over a reachable interface that is not configured for the Hotspot to configure your device.
Domain at the HotSpot Server	Enter the domain name that you used when setting up the HotSpot server for this customer. The domain name is required so that the Hotspot server can distinguish between the different clients (customers).
Walled Garden	Enable this function if you want to define a limited and free area of websites (intranet). The function is not activated by default.
Walled Network / Netmask	Only if **Walled Garden** is enabled. Enter the network address of the **Walled Network**, the corresponding **Netmask** of the intranet server.

Field	Description
	For the address range resulting from **Walled NetworkNetmask**, clients require no authentication. Example: Enter 192.168.0.0 / 255.255.255.0, if all IP addresses from 192.168.0.0 to 19.168.0.255 are free. Enter 192.168.0.1 / 255.255.255.255, if only the IP address 192.168.0.1 is free.
Walled Garden URL	Only if **Walled Garden** is enabled. Enter the **Walled Garden URL** of the intranet server. Freely accessible websites must be reachable over this address.
Terms &Conditions	Only if **Walled Garden** is enabled. In the **Terms &Conditions** input field, enter the address of the general terms and conditions on the intranet server, or public server, e.g., http://www.webserver.de/agb.htm. The page must lie within the address range of the walled garden network.
Language for login window	Here you can choose the language for the start/login page. The following languages are supported: `English`, `Deutsch`, `Italiano`, `Français`, `Español`, `Português` and `Nederlands` . The language can be changed on the start/login page at any time.

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

Fields in the Advanced Settings menu

Field	Description
Ticket Type	Select the ticket type. Possible values: • `Voucher`: Only the user name must be entered. Define a default password in the input field. • `Username/Password` (default value): User name and password must be entered.
Allowed HotSpot Client	Here you can define which type of users can log in to the Hotspot.

Field	Description
	Possible values: • *All*: All clients are approved. • *DHCP Client*: Prevents users who have not received an IP address from DHCP from logging in.

20.12.1.2 Options

In the **Local Services**->**HotSpot Gateway**->**Options** menu, general settings for the hotspot are performed.

The **Local Services**->**HotSpot Gateway**->**Options** menu includes the following fields:

Fields in the OptionsBasic Parameters menu

Field	Description
Host for multiple locations	If several locations (branches) are set up on the Hotspot server, enter the value of the NAS identifier (RADIUS server parameter) that has been registered for this location on the Hotspot server.

20.13 BRRP

In the **BRRP** menu you can configure the redundancy of your gateway.

Note

You require a licence for devices in the R23x series and RS series.

BRRP (Bintec Router Redundancy Protocol) is a Bintec-specific implementation of the VRRP (Virtual Router Redundancy Protocol). A router redundancy procedure is used mainly to safeguard the availability of a physical gateway in a LAN or WAN.

Terms and Definitions

A number of special terms are used to describe the functionality. The following terms are defined in the relevant RFC and in the Internet draft.

BRRP terms

Field	Description
VRRP router	“A router that uses the Virtual Router Redundancy Protocol. It can be integrated into one or more “virtual routers”.”
Virtual Router	“An abstract object controlled by the VRRP, which is used as default router for the hosts of a LAN. It comprises a Virtual Router Identifier (**Virtual Router ID**) and an IP address, or a group of associated IP addresses in a common LAN. A VRRP router can protect the data traffic of one or more virtual routers.”
IP Address Owner	“The VRRP router that possesses the IP address(es) of the virtual router as real interface address(es). This is the router which – if active - answers packets for ICMP pings, TCP connections, etc. to one of these IP addresses.”
Primary IP Address	“An IP address that is selected from the group of real interface addresses. A possible algorithm option is the selection of the first address. VRRP advertisements are always sent with the primary IP address as source of the IP packet.”
VRRP Advertisement	A keepalive that sends the master to the backup gateway to indicate his reachability.
Virtual Router Master	“The VRRP router that takes over forwarding the packets that have been sent to the IP addresses associated with the “virtual router”. It is also responsible for answering ARP (Address Resolution Protocol) requests for these IP addresses."
Virtual Router Backup	“The group of VRRP routers that take over responsibility for forwarding the packets if the master fails.” In backup status these VRRP routers are inactive, i.e. they do not respond to any ARP requests."

20.13.1 Virtual Routers

When using a route redundancy protocol, multiple routers are combined into a logical unit. The router redundancy protocol BRRP manages the routes involved and organises these as follows:

It ensures that only one routers within the logical connection is active.

It guarantees that if the active route fails, another router takes over the function of the failed device. The time that each router is active is determined by the priority assigned to the router.

Let us take the example of a simple scenario, in which gateway A provides Internet access for the hosts in a LAN. If this gateway fails, all hosts cannot access the Internet and their routes are configured statically. To allow the hosts continued access to the Internet, gateway B offers all hosts in the LAN the service that gateway A previously performed. All the tasks of a "virtual router" and the switching of services from one gateway to the other are controlled by the BRRP redundancy procedure.

The BRRP conforms to the specifications in RFC 2338 and the relevant Internet draft (see *www.ietf.org*).

The configuration of the router redundancy procedure is carried out in the following steps:

- Configuration of the interface via which the BRRP advertisement data packets are sent.

Note

This interface is used to transmit the BRRP advertisement data packets and possibly to transmit keepalive monitoring data packets. Another interface must be configured in the next step to transmit the usage data.

Configuration of the advertisement interface is performed in the **Local Services**->**BRRP**->**Virtual Router**->**New**->**BRRP Advertisement Interface** menu.

Only the active router in the router group sends advertisement data packets. The IPv4 multicast address 224.0.0.18 is used as the destination address for all routers in the group. All passive routers in the group must monitor this address so that if the advertisement data packets are not received that can react according to their priority and BRRP configuration.

- Configuration of the interface for transmitting usage data (configuration of the virtual interface).

  A virtual interface is activated and deactivated by assigning it to a virtual router over the BRRP router redundancy protocol.

  Configuration is performed in the **Local Services**->**BRRP**->**Virtual Router**->**New**->**Ethernet Interface** menu.

  In this step, you configure the IP address settings and assign the interface to a virtual router. The properties of the virtual router (e.g. the priority) are also defined here.

Note

The system automatically assigns the MAC address of the virtual interface according to the following model: 00:00:5E:00:01:<ID of the virtual router>. The ID of the virtual router therefore determines the MAC address of the interface, which is used to transmit the usage data.

The configuration of the virtual interface (MAC address, IP address) and configuration of the virtual router (sending interval for advertisement, master down trials) must be identical on all routers with the same virtual router ID within the logical group.

You must use IP addresses from different subnets for the advertisement interface and for the virtual interface.

All virtual interfaces on a physical router should normally have the same priority.

- Configuration of the synchronisation between the virtual router and configuration of the events, which result in a switching of the operating status of the virtual router.

  Controlling the operating status of a virtual router implicitly also controls the operating status of the interface to which the virtual router is linked. If an error occurs, all interfaces on a device have to be deactivated. Consequently, the operating status of all interfaces on a device must be synchronised. This synchronisation is required if multiple interfaces are monitored on a single device. This configuration is performed in the **Local Services**->**BRRP**->**VR Synchronisation**->**New** menu.
- Switching on the redundancy procedure. This configuration is performed in the **Local Services**->**BRRP**->**Options** menu.

You configure the advertisement interface and the virtual interface(s) in the **Local Services**->**BRRP**->**Virtual Router**->**New** menu. You must configure the same virtual routers with the same interfaces on all physical routers involved in the redundancy procedure. (However, the virtual routers have different priorities on the various physical routers.)

20.13.1.1 New

Choose the **New** button to configure other virtual routers.

The **Local Services**->**BRRP**->**Virtual Routers**->**New** menu consists of the following fields:

Fields in the Virtual RoutersBRRP Advertisement Interface menu

Field	Description
Ethernet Interface	Choose the interface via which BRRP advertisement packets are sent and expected.

Field	Description
	If you edit a Virtual Router, the Ethernet interface is displayed and cannot be changed. Note: The Ethernet interface for sending the advertisements is always up and running and cannot therefore be used as the **Virtual Router Interface**.
IP Address	Shows the IP address(es) of the interface via which BRRP advertisement packets are sent and expected.

Fields in the Virtual RoutersBRRP Monitored Interface menu

Field	Description
Virtual Router Interface	Indicates on which physical interface the virtual interface is based, if a new virtual interface is created. The name of the virtual interface is assigned automatically when it is created. Shows the name of the virtual interface, if a virtual interface that has already been created is edited.
Virtual Router IP Address	Enter the IP address and the netmask of the virtual router. Here enter the IP address that you want to use in the local network as the actual gateway IP address. **Note** To avoid problems in the LAN, the **IP Address** for advertisements and the **Virtual Router IP Address** cannot originate from the same subnet.
Virtual Router ID	Select the ID of the virtual router. This ID identifies the “virtual router” in the LAN and is part of every BRRP advertisement packet that is sent by the current master. Possible values are whole numbers between 1 and 255.
Virtual Router Priority	Define the logical priority of the virtual router. Possible values are between 1 and 255. The higher the value, the higher the priority. The value 255 defines that this virtual router always functions as master as soon as it is active.

Field	Description
	The default value is *100*. The virtual router with the highest priority normally takes over the master role. After occurence of a backup case, the ensuing master-slave role distribution is determined by the parameters **Virtual Router Priority** and **Pre-empt mode (go back into master state)**.

In the **Advanced Settings** menu you must configure all of the parameters for all virtual routers identically on all devices in the group. We recommend leaving the preset values.

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

Fields in the Advanced Settings menu

Field	Description
Advertisement send interval	Determine how often a BRRP advertisement packet is sent if the virtual router is defined as master. Only the current master sends via multicast BRRP advertisements, which also contain the ID and the priority of the master. Possible values are whole numbers between *1* and *255*. The value is indicated in seconds, the default value is 1. *1*. An advertisement timer based on the sending interval for advertisements runs in the router and an advertisement packet is sent when the timer expires.
Master down trials	Define the number of BRRP advertisements that must fail before the backup router with the lowest priority assumes that the master is inactive and takes over the role of master. A master down timer based on the **Master down trials** parameter runs in the router; when this timer expires, the backup assumes that the master is not reachable if no advertisement has been received. The effective master down interval is the time calculated from the number of expected but omitted BRRP advertisements, the advertisement interval and the skew time, which adds a minimum period depending on the priority. The higher the priority, the shorter the time added. Consequently, a backup router with a higher priority responds more quickly than a router with lower priority).

Field	Description
	Possible values are whole numbers between *1* and *255* and the default value is *10*.
Pre-empt mode (go back into master state)	Define whether a backup router with higher priority has priority over a master router with low priority. Pre-empt mode is used to prevent unnecessary switching. The function is enabled with *Enabled* The router having the higher priority always takes precedence, i.e. as soon as the original master router becomes available again, it also becomes active. If the function remains disabled, the currently active backup router remains active even after the original master router has become available again, independently of the master router having higher priority than the currently active backup router. The function is enabled by default. Note the following exception: If **Virtual Router Priority** *255* is selected, the gateway with this priority certainly takes over the master role, i.e. the setting in **Pre-empt mode (go back into master state)** is not considered. You should therefore select a **Virtual Router Priority** lower than *255255*if you wish to use Pre-empt Mode.
Enable authentication	Enable or disable authentication. The function is enabled with *Enabled*. If the function is active, an input field is displayed. Enter the authentication key here. Note: Note that the authentication key must be the same for all virtual routers in the group. The function is disabled by default.

20.13.2 VR Synchronisation

The watchdog daemon is configured in the **Local Services**->**BRRP**->**VR Synchronisation** menu, i.e. you define how status changes are handled.

After opening the menu **Local Services**->**BRRP**->**VR Synchronisation**, a list of all synchronisations is displayed. You can either synchronise virtual interfaces or interfaces. New synchronisations can be added in the **New** menu.

For example, you can synchronise both virtual routers R1 and R2 over BRRP. To do this, you must create two entries. For the first entry, as **Monitoring VR / Interface** R1 and as **Synchronisation VR / Interface** you must use R2. For the second entry, as **Monitoring VR / Interface** R2 and as **Synchronisation VR / Interface** you must use R1.

20.13.2.1 New

Select the **New** button to create new synchronisations.

The **Local Services**->**BRRP**->**VR Synchronisation**->**New** menu consists of the following fields:

Fields in the VR SynchronisationMonitoring VR / Interface menu

Field	Description
Monitoring Mode	Shows which mechanism is used for monitoring a virtual router. Possible values: • *BRRP*:The BRRP-specific status advertisements are used for determining the status of the master. (The master sends advertisements as per its configuration in the **Local Services**->**BRRP**->**Virtual Routers**->**New**->**Advanced Settings** menu.)
Virtual Router ID	Select a virtual router using the **Virtual Router ID** and define which interface is to be checked. You can choose previously defined IDs (see **Virtual Router ID** in menu **Local Services**->**BRRP**->**Virtual Router**->**New**->**BRRP Monitored Interface**). The watchdog daemon requests detailed information entered in the **Virtual Router**.

Fields in the VR SynchronisationSynchronisation VR / Interface menu

Field	Description
Synchronisation Mode	Indicates the mechanism with which virtual routers or interfaces are synchronised: Possible values: • *BRRP* : BRRP is used to synchronise the virtual router.

Field	Description
Virtual Router ID	Select the ID of the virtual router to be synchronised. Synchronising the virtual router implicitly synchronises the virtual interface associated with the virtual router.

20.13.3 Options

In the **Local Services**->**BRRP**->**Options** menu, you can enable or disable the BRRP function.

The **Local Services**->**BRRP**->**Options** menu includes the following fields:

Fields in the OptionsBasic Parameters menu

Field	Description
Enable BRRP	Enable or disable the BRRP function. The function is enabled with *Enabled*. The function is disabled by default.

Chapter 21 Maintenance

This menu provides you with numerous functions for maintaining your device. It firstly provides a menu for testing availability within the network. You can manage your system configuration files. If more recent system software is available, you can use this menu to install it. If you need other languages for the configuration interface, you can import these. You can also trigger a system reboot in this menu.

21.1 Diagnostics

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

21.1.1 Ping Test

You can use the ping test to check whether a certain host in the LAN or an internet address can be reached. The **Output**field displays the ping test messages. The ping test is launched by entering the IP address to be tested in **Test Ping Address** and clicking the **Go** button.

21.1.2 DNS Test

The DNS test is used to check whether the domain name of a particular host is correctly resolved. The **Output**field displays the DSN test messages. The DSN test is launched by entering the domain name to be tested in **DNS Address** and clicking the **Go** button.

21.1.3 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. The **Output**field displays the traceroute test messages. The traceroute test is launched by entering the address to be tested in **Traceroute Address** and clicking the **Go** button.

21.2 Software &Configuration

21.2.1 Options

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

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.funkwerk-ec.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 Funkwerk Enterprise Communications 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: **Save configuration** button via the **Funkwerk Configuration Interface** navigation area. 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.

Operations

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 menu **Maintenance**->**Software &Configuration**->**Options** consists of the following fields:

Fields in the OptionsCurrently 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.
ADSL Logic	Shows the current version of the ADSL logic loaded on your device.

Fields in the OptionsSoftware 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.

Field	Description
	Possible values: • *No Action* (default value): • *Import configuration*: Under **Filename** select a configuration file you want to import. 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. Note: The files to be imported must be in CSV format! • *Import language*: You can import additional language versions of the **Funkwerk Configuration Interface** into your device. You can download the files to your PC from the download area at *www.funkwerk-ec.com* and from there import them to your device. • *Update system software*: You can launch an update of the system software, the ADSL logic and the BOOTmonitor. • *Export configuration*: The configuration file **Current File Name in Flash** is transferred to your local host. If you press 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. • *Export configuration with state information*: The active configuration from the RAM is transferred to your local host. If you press 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. • *Restore backup*: Only if, under **Save configuration** with the setting *Save configuration and back up previous boot configuration*, the current configuration was saved as boot configuration and the previous boot configuration was also archived. You can load the archived boot configuration again. • *Copy*: The configuration file in the **Source File Name** field is saved as**Destination File Name**. • *Rename*: The configuration file in the **Select file** field is renamed to **New File Name**. • *Delete configuration*: The configuration in the **Select file** field is deleted. • *Delete file*: The file in the **Select file** field is deleted.

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 Location	Only for **Action** = *Update system software* Select the source for the update. Possible values: • *Local File* (default value): The system software file is stored locally on your PC. • *HTTP Server*: The file is stored on a remote server specified in the **URL**. • *Current Software from Funkwerk Server*: The file is on the official Funkwerk update server.
URL	Only for **Source Location** = *HTTP Server* Enter the URL of the update server from which the system software file is loaded.
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** shall also apply to certificates and keys. The function is activated by selecting *Enabled*. The function is enabled by default.

Field	Description
Source File Name	Only for **Action** = *Copy* select the source file to be copied.
Destination File Name	Only for **Action** = *Copy* Enter the name of the copy.
Select file	Only for **Action** = *Rename* , *Delete configuration* or *Delete file* select the file or configuration to be renamed or deleted.
New File Name	Only for **Action** = *Rename* Enter the new name of the configuration file.

21.3 Reboot

21.3.1 System Reboot

In this menu, you can trigger an immediate reboot of your device. Once your system has restarted, you must call the **Funkwerk Configuration Interface** 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 on the **OK** button. The device will reboot.

Chapter 22 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. Moreover, you can prepare your device for monitoring with the activity monitor.

22.1 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.funkwerk-ec.com*).

22.1.1 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.

22.1.1.1 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 Syslog ServersBasic 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*

22.2 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).

22.2.1 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.

22.2.2 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]`*

22.3 E-mail Alert

Depending on the configuration, E-mails are sent to the administrator as soon as relevant syslog messages occur.

22.3.1 E-mail Alert Server

The menu **E-mail Alert Server** consists of the following fields:

The menu **External Reporting**->**E-mail Alert**->**E-mail Alert Server** consists of the following fields:

Fields in the E-mail Alert ServerBasic Parameters menu

Field	Description
Alert Service	Enable or disable the function.
Sender E-Mail Address	Enter the mail address to be entered in the sender field of the E-mail.
Maximum Messages 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 Alert ServerSMTP Settings menu

Field	Description
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 Authentication	Authentication expected by the SMTP server. Possible values: • *None* (default value): The server accepts and send emails without further authentication. • *ESMTP*: The server only accepts e-mails if the router logs in with the correct user name and password. • *SMTP after POP*: The server requires that e-mails are called via POP3 by the sending IP with the correct POP3 user name and password before sending an e-mail.
User Name	Only if **SMTP Authentication** = *ESMTP* or *SMTP after POP*.

Field	Description
	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.

22.3.2 E-mail Alert Recipient

In the **E-mail Alert Recipient** menu, a list of Syslog messages is displayed.

22.3.2.1 New

Choose the **New** button to create additional e-mail alert recipients.

The menu **External Reporting**->**E-mail Alert**->**E-mail Alert Recipient** consists of the following fields:

Fields in the E-mail Alert RecipientAdd / Edit E-mail Alert Recipient menu

Field	Description
Recipient	Enter the E-mail address of the recipient. The entry is limited to 40 characters.
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 "*".

Field	Description
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*
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.
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*.
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.

Fields in the E-mail Alert RecipientMonitored Subsystems menu

Field	Description
Subsystem	Select the subsystems to be monitored. Add new subsystems with **Add**.

22.4 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

22.4.1 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 SNMP Trap OptionsBasic 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. 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

Field	Description
	device. A character string of between *0* and *255* characters is possible here. The default value is *SNMP Trap*.

22.4.2 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.

22.4.2.1 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 SNMP Trap HostsBasic Parameters menu

Field	Description
IP Address	Enter the IP address of the SNMP trap host.

22.5 Activity Monitor

This menu contains the settings needed to monitor your device with the Windows tool **Activity Monitor** (part of **BRICKware** for Windows).

Purpose

The **Activity Monitor** enables Windows users to monitor the activities of your device. Important information about the status of physical interfaces (e.g. ISDN line) and virtual interfaces is easily obtained with one tool. A permanent overview of the utilisation of your device is possible.

Method of operation

A Status Daemon collects information about your device and transfers it as UDP packets to the broadcast address of the first LAN interface (default setting) or to an explicitly entered IP address. One packet is sent per time interval, which can be adjusted individually to values from 1 - 60 seconds. Up to 100 physical and virtual interfaces can be monitored, provided the packet size of 4096 bytes is not exceeded. The **Activity Monitor** on your PC receives the packets and can display the information contained in them in various ways according to the configuration.

Activate the **Activity Monitor** as follows:

- configure the relevant device(s) to be monitored.
- Start and configure the Windows application on your PC (you can download **BRICKware** for Windows to your PC from the download area at *www.funkwerk-ec.com* and from there import it to your device).

22.5.1 Options

The menu **External Reporting**->**Activity Monitor**->**Options** consists of the following fields:

Fields in the OptionsBasic Parameters menu

Field	Description
Monitored Interfaces	Select the type of information to be sent in the UDP packets to the Windows application. Possible values: • *None* (default value): Deactivates the sending of information to the **Activity Monitor**. • *Physical*: Only information about the physical interfaces is sent. • *Physical/WAN/VPN*: Information about physical and virtual interfaces is sent
Send information to	Select where your device sends the UDP packets. Possible values: • *All IP Addresses (Broadcast)* (default value): The default value *255.255.255.255* means that the broadcast address of the first LAN interface is used. • *Single Host*: The UDP packets are sent to the IP address

Field	Description
	entered in the adjacent input field.
Update Interval	Enter the update interval (in seconds). Possible values are *0* to *60*. The default value is *5*.
UDP Destination Port	Enter the port number for the Windows application **Activity Monitor**. The default value is *2107* (registered by IANA - Internet Assigned Numbers Authority).
Password	Enter the password for the **Activity Monitor**.

Chapter 23 Monitoring

This menu contains information that enable you to locate problems in your network and monitor activities, e.g. at your device's WAN interface.

23.1 Internal Log

23.1.1 System Messages

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

Values in the System Messages list

Field	Description
No.	Displays the serial number of the system message.
Date	Displays the date of the record.
Time	Displays the time of the record.
Level	Displays the hierarchy level of the message.
Subsystem	Displays which subsystem of the device generated the message.
Message	Displays the message text.

23.2 IPSec

23.2.1 IPSec Tunnels

A list of all configured IPSec tunnels is displayed in the **Monitoring**->**IPSec**->**IPSec Tunnels** menu.

Values in the IPSec Tunnels list

Field	Description
Description	Displays the name of the IPSec tunnel.

Field	Description
Remote IP	Displays the IP address of the remote IPSec Peers.
Remote Networks	Displays the currently negotiated subnets of the remote terminal.
Security Algorithm	Displays the encryption algorithm of the IPSec tunnel.
Status	Displays the operating status of the IPSec tunnel.
Action	Enables you to change the status of the IPSec tunnel as displayed.
Details	Opens a detailed statistics window.

You change the status of the IPSec tunnel by pressing the ⬆ button or ⬇ button in the **Action** column.

By pressing the 🔍 button, you display detailed statistics on the IPSec connection.

Values in the IPSec Tunnels list

Field	Description
Description	Shows the description of the peer.
Local IP Address	Shows the WAN IP address of your device.
Remote IP Address	Shows the WAN IP address of the connection partner.
Local ID	Shows the ID of your device for this IPSec tunnel.
Remote ID	Shows the ID of the peer.
Negotiation Type	Shows the exchange type.
Authentication Method	Shows the authentication method.
MTU	Shows the current MTU (Maximum Transfer Unit).
Alive Check	Shows the method for checking that the peer is reachable.
NAT Detection	Displays the NAT detection method.
Local Port	Shows the local port.
Remote Port	Shows the remote port.
Packets	Shows the total number of incoming and outgoing packets.
Bytes	Shows the total number of incoming and outgoing bytes.
Errors	Shows the total number of errors.
IKE (Phase-1) SAs (x) **Role** / **Algorithm** / **Lifetime remaining** / **Status**	The parameters of the IKE (Phase 1) SAs are displayed here.

Field	Description
IPSec (Phase-2) SAs (x) **Role** / **Algorithm** / **Lifetime remaining** / **Status**	Shows the parameters of the IPSec (Phase 2) SAs.
Messages	The system messages for this IPSec tunnel are displayed here.

23.2.2 IPSec Statistics

In the **Monitoring**->**IPSec**->**IPSec Statistics** menu, statistical values for all IPSec connections are displayed.

The **Monitoring**->**IPSec**->**IPSec Statistics** menu consists of the following fields:

Field in the IPSec StatisticsLicences menu

Field	Description
IPSec Tunnels	Shows the IPSec licences currently in use (**In Use**) and the maximum number of licences usable (**Maximum**).

Field in the IPSec StatisticsPeers menu

Field	Description
Status	Displays the number of IPSec tunnels by their current status. • **Up**: Currently active IPSec tunnels. • **Going up**: IPSec tunnels currently in the tunnel setup phase. • **Blocked**: IPSec tunnels that are blocked. • **Dormant**: Currently inactive IPSec tunnels. • **Configured**: Configured IPSec tunnels.

Fields in the IPSec StatisticsSAs menu

Field	Description
IKE (Phase-1)	Shows the number of active phase 1 SAs (**Established**) from the total number of phase 1 SAs (**Total**).
IPSec (Phase-2)	Shows the number of active phase 2 SAs (**Established**) from the total number of phase 2 SAs (**Total**).

Fields in the IPSec StatisticsPacket Statistics menu

Field	Description
Total	Shows the number of all processed incoming (**In**) or outgoing (**Out**) packets.
Passed	Shows the number of incoming (**In**) or outgoing (**Out**) packets forwarded in plain text.
Dropped	Shows the number of all rejected incoming (**In**) or outgoing (**Out**) packets.
Encrypted	Shows the number of IPSec-protected incoming (**In**) or outgoing (**Out**) packets.
Errors	Shows the number of incoming (**In**) or outgoing (**Out**) packets for which processing led to errors.

23.3 ISDN/Modem

23.3.1 Current Calls

In menu **Monitoring**->**ISDN/Modem**->**Current Calls** a list of the existing ISDN connections (incoming and outgoing calls) is displayed.

Values in the Current Calls list

Field	Description
Service	Displays the service to or from which the call is connected: *PPP*, *IPSec*, *X.25*, *POTS*.
Remote Number	Displays the number that was dialled (in the case of outgoing calls) or from which the call was made (in the case of incoming calls).
Interface	Displays additional information for PPP connections.
Direction	Displays the send direction: *Incoming*, *Outgoing*.
Charge	Displays the costs of the current connection.
Duration	Displays the duration of the current connection.
Stack	Displays the related ISDN port (STACK).
Channel	Displays the number of the ISDN B channel.
Status	Displays the state of the connection: *null*, *c-initiated*, *ovl-send*, *oc-procd*, *c-deliverd*, *c-present*, *c-recvd*, *ic-procd*, *up*, *discon-req*, *discon-ind*, *suspd-req*, *resum-req*, *ovl-recv*.

23.3.2 Call History

In the **Monitoring**->**ISDN/Modem**->**Call History** menu, a list of the last 20 ISDN calls (incoming and outgoing) completed since the last system start is displayed.

Values in the Call History list

Field	Description
Service	Displays the service to or from which the call was connected: *PPP*, *IPSec*, *X.25*, *POTS*.
Remote Number	Displays the number that was dialled (in the case of outgoing calls) or from which the call was made (in the case of incoming calls).
Interface	Displays additional information for PPP connections.
Direction	Displays the send direction: *Incoming*, *Outgoing*.
Charge	Displays the costs of the connection.
Start Time	Displays the time at which the call was made or received.
Duration	Displays the duration of the connection.

23.4 Interfaces

23.4.1 Statistics

In the **Monitoring**->**Interfaces**->**Statistics** menu, current values and activities of all device interfaces are displayed.

Change the status of the interface by pressing the ⬆ button or ⬇ button in the **Action** column. Press the 🔍 button to display the statistical data for the individual interfaces in detail.

Values in the Statistics list

Field	Description
No.	Shows the serial number of the interface.
Description	Displays the name of the interface.
Type	Displays the interface text.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.

Field	Description
Tx Errors	Shows the total number of errors sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.
Rx Errors	Shows the total number of errors received.
Status	Shows the operating status of the selected interface.
Unchanged for	Shows the length of time for which the operating status of the interface has not changed.
Action	Enables you to change the status of the interface as displayed.

23.5 WLAN

23.5.1 WLAN1

In the **Monitoring**->**WLAN**->**WLAN** menu, current values and activities of the WLAN interfaces are displayed.

Values in the WLAN list

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

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

Values in the Advanced list

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

Meaning of the list entries

Description	Meaning
Unicast MSDUs transmitted successfully	Displays the number of MSDUs successfully sent to unicast addresses since the last reset. An acknowledgement was received for each of these packets.

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

23.5.2 VSS

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

Values in the VSS list

Field	Description
MAC Address	Shows the MAC address of the associated client.
IP Address	Shows the IP address of the client.
Up Time	Shows the time in hours, minutes and seconds for which the client is logged in.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.

Field	Description
Signal dBm (RSSI1, RSSI2, RSSI3)	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
Data Rate mbps	Shows the current transmission rate of data received by this client in mbps. The following clock rates are possible: IEEE 802.11b: 11, 5.5, 2 and 1 mbps; IEEE 802.11g/a: 54, 48, 36, 24, 18, 12, 9, 6 mbps. If the 5 GHz frequency band is used, the indication of 11, 5.5, 2 and 1 mbps is suppressed for IEEE 802.11b.

VSS - Details for Connected Clients

In the **Monitoring**->**WLAN**->**VSS**->**<Connected client>**->🔍 menu, the current values and activities of a connected client are shown.

Values in the VSS <connected client> list

Field	Description
Client MAC Address	Shows the MAC address of the associated client.
IP Address	Shows the IP address of the client.
Up Time	Shows the time in hours, minutes and seconds for which the client is logged in.
Signal dBm (RSSI1, RSSI2, RSSI3)	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
SNR dB	Signal-to-Noise Ratio in dB is an indicator of the quality of the wireless connection. Values: • > 25 dB excellent • 15 – 25 dB good • 2 – 15 dB borderline • 0 – 2 dB bad.
Data Rate mbps	Shows the current transmission rate of data received by this client in mbps. The following clock rates are possible: IEEE 802.11b: 11, 5.5, 2 and 1 mbps; IEEE 802.11g/a: 54, 48, 36, 24,

Field	Description
	18, 12, 9.6 Mbps. If the 5 GHz frequency band is used, the indication of 11, 5.5, 2 and 1 Mbps is suppressed for IEEE 802.11b.
Rate	Displays the possible data rates on the wireless module.
Tx Packets	Shows the number of sent packets for the data rate.
Rx Packets	Shows the number of received packets for the data rate.

23.6 Bridges

23.6.1 br<x>

In the **Monitoring**->**Bridges**-> **br<x>** menu, the current values of the configured bridges are shown.

Values in the br<x> list

Field	Description
MAC Address	Shows the MAC addresses of the associated bridge.
Port	Shows the port on which the bridge is active.

23.7 HotSpot Gateway

23.7.1 HotSpot Gateway

In the **Monitoring**->**HotSpot Gateway**->**HotSpot Gateway** menu, a list of all connected hosts is displayed.

Values in the HotSpot Gateway list

Field	Description
User Name	Displays the user's name.
IP Address	Shows the IP address of the user.
Physical Address	Shows the physical address of the user.
Logon	Shows the login time.

Field	Description
Interface	Shows the interface used.

23.8 QoS

In the **Monitoring**->**QoS** menu, statistics are displayed for all interfaces for which QoS has been configured.

23.8.1 QoS

In the **Monitoring**->**QoS**->**QoS** menu, a list of all interfaces configured for QoS is displayed.

Values in the QoS list

Field	Description
Interface	Shows the interface for which QoS has been configured.
QoS Queue	Shows the QoS queue, which has been configured for this interface.
Send	Shows the number of sent packets with the corresponding packet class.
Dropped	Shows the number of rejected packets with the corresponding packet class in case of overloading.
Queued	Shows the number of waiting packets with the corresponding packet class in case of overloading.

Glossary

Announcement If you want to call your employees or family members to a meeting or the dinner table, you could call each one of them individually or simply use the announcement function. With just one call, you reach all the announcement-enabled telephones without the subscribers having to pick up the receiver.

Announcement function Performance feature of a PBX. On suitable telephones (e.g. system telephones), announcements can be made as on an intercom.

Bit Binary digit. Smallest unit of information in computer technology. Signals are represented in the logical states "0" and "1".

Bundle The external connections of larger PBXs can be grouped into bundles. When an external call is initiated by the exchange code or in the event of automatic external line access a bundle released for this subscriber is used to establish the connection. If a subscriber has authorisation for several bundles, the connection is established using the first released bundle. If one bundle is occupied, the next released bundle is used. If all the released bundles are occupied, the subscriber hears the engaged tone.

Busy On Busy Call to engaged team subscriber. If one subscriber in a team has taken the receiver off the hook or is on the telephone, you can decide whether other calls are to be signalled for this team. The setting for reaching a subscriber can be toggled between "Standard" and "Busy On Busy". In the basic configuration, it is set to Standard. If Busy on Busy is set for a team, other callers hear the engaged tone.

DECT Digital European Cordless Telecommunication. European standard for wireless telephones and wireless PBXs. Internal calls can be made free of charge between several handheld units. Another advantage is the higher degree of interception protection (GAP).

Digital exchange Allows computer-controlled crossbar switches to set up a connection quickly, and special features such as inquiries, call waiting, three-party conference and call forwarding to be activated. All T-Com exchanges have been digital since January 1998.

Digital voice transmission As a result of the internationally standardised Pulse Code Modulation (PCM), analogue voice signals are converted to a digital pulse flow of 64 kbps. Advantages: Better voice quality and less susceptibility to faults during analogue voice transmission.

Direct Call

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). As you can set up the Direct Call function for one or more telephones, the receiver of the telephone simply needs to be lifted. After five seconds, the PBX automatically calls the defined direct call number, if you do not start dialling another number first. You can enter up to 12 destination numbers when you configure Direct Call. A direct call number can only be used by one subscriber. If you want to change an entered direct call number, you can simply enter the new direct call number without having to delete the old direct call number. The old number is automatically overwritten when the new configuration is transferred to the PBX.

DISA

Direct Inward System Access

Download

Data transfer during online connections, where files are "loaded" from a PC or data network server to the user's own PC, PBX or terminal, so that they can be used there.

DSL and ISDN connections

Data is transferred between the Internet and your PBX over ISDN or T-DSL. The PBX determines the remote terminal to which a data packet is to be sent. For a connection to be selected and set up, parameters must be defined for all the required connections. These parameters are stored in lists which together permit the right connection to be set up. The PBX uses the PPP (Point-to-Point Protocol) for ISDN access, and PPPoE (Point-to-Point Protocol over Ethernet) for access over T-DSL. The traffic on these two Internet connections is monitored separately by the PBX.

DSL modem

Special modem for data transmission using DSL access technology.

DSL splitter

A DSL splitter is a device that splits the data or frequencies of various applications that run via a subscriber line or distribution point, and provides this via separate connections.

Services

Euro ISDN contains service indicates with defined names. Some of these have only historical meaning. In general, you should choose the "Telephony" service for "real" telephone calls. If this selection does not work (depends on network operator), you can try "speech", "audio 3k1Hz" or "telephony 3k1Hz". The same applies for faxing. Here, too, there is the collective term "Fax" plus a couple of more specific cases. From a purely technical point of view, the services are bits in a data word evaluated by means of a mask. If you include several bits in the mask, all these services are approved for activation, while in the case of just one bit, it is just the one selected service.

Three-party conference A three-way telephone call. Performance feature in T-Net, T-ISDN and your PBX.

10 Base 2 Thin Ethernet connection. Network connection for 10-mbps networks with BNC connector. T-connectors are used for the connection of equipment with BNC sockets.

100Base-T Twisted pair connection, Fast Ethernet. Network connection for 100-mbps networks.

10Base-T Twisted pair connection. Network connection for 10-mbps networks with RJ45 connector.

1TR6 D channel protocol used in the German ISDN. Today the more common protocol is DSS1.

3DES (Triple DES) See DES.

802.11a/g Specified data rates of 54, 48, 36, 24, 18, 12, 9 and 6 mbps and a working frequency in the range of 5 GHz (for IEEE802.11a) or 2.4 GHz (for IEEE802.11g). IEEE802.11 g can be configured to run in compliance with 11b or 11b and 11 as well.

802.11b/g One of the IEEE standards for wireless network hardware. Products that meet the same IEEE standard can communicate with each other, even if they come from different hardware manufacturers. The IEEE802.11b standard specifies the data rates of 1, 2, 5.5 and 11 mbps, a working frequency in the range of 2.4 to 2.4835 GHz and WEP encryption. IEEE802.11 wireless networks are also known as Wi-Fi networks.

A-subscriber The A-subscriber is the caller.

a/b interface For connection of an analogue terminal. In the case of an ISDN terminal (terminal adapter) with a/b interface, the connected analogue terminal is able to use the supported T-ISDN performance features.

AAA Authentication, Authorisation, Accounting

Access code PIN or password

Access list A rule that defines a set of packets that should or should not be transmitted by the device.

Access point An active component of a network consisting of wireless parts and optionally also of wired parts. Several WLAN clients (terminals) can log in to an access point (AP) and communicate via the AP data. If the optional wired Ethernet is connected, the signals between the two physical media, the wireless interface and wired interface, are bridged (bridging).

Access protection Filters can be used to prevent external persons from accessing the data on the computers in your LAN. These filters are a basic function of a firewall.

Accounting Recording of connection data, e.g. date, time, connection duration, charging information and number of data packets transferred.

Active probing Active probing takes advantage of the fact that as standard, access points are to respond to client requests. Clients therefore send "probe requests" on all channels and wait for responses from an access point in the vicinity. The response packet then contains the SSID of the wireless LAN and information on whether WEP encryption is used.

Ad hoc network An ad hoc network refers to a number of computers that form an independent 802.11 WLAN each with a wireless adapter. Ad hoc networks work independently without an access point on a peer-to-peer basis. Ad hoc mode is also known as IBSS mode (Independent Basic Service Set) and makes sense for the smallest networks, e.g. if two notebooks are to be linked to each other without an access point.

ADSL Asymmetric digital subscriber line

AH Authentication header

Alphanumeric display Display unit e.g. for T-Concept PX722 system telephone, able to display letters and other characters as well as digits.

Analogue connections For the connection of analogue terminals such as telephone, fax and answering machine.

Analogue terminals Terminals that transmit voice and other information analogously, e.g. telephone, fax machine, answering machine and modem.

Analogue voice transmission To transmit voice via the telephone, acoustic oscillations are converted to continuous electrical signals, which are transmitted via a network of lines (digital voice transmission).

Answering machine You configure an analogue answering machine under "Terminal Type".

AOC-D Display during and at end of connection.

AOC-D/E Advice of charge-during/end.

AOC-E Display only at end of connection.

ARP Address Resolution Protocol

Assignment An external call can be signalled to internal subscribers. The entries in the "Day" option and "Night" option can be different.

Asynchronous A method of data transmission in which the time intervals between transmitted characters can vary in length. This allows computers and peripheral devices to intercommunicate without being synchronised by clock signals. The beginning and end of the transmitted characters must be marked by start and stop bits – in contrast to synchronous transmission.

ATM Asynchronous transfer mode

Attention tone Superimposing of an acoustic signal during a telephone call e.g. for call waiting.

Authentication Check on the user's identify.

Authorisation Based on the identity (authentication), the user can access certain services and resources.

Automatic callback Special feature on telephones: By pressing a key or code, the caller requests a call back from the engaged terminal. If the subscriber you want is not at their desk or cannot take the call, they are automatically connected with the caller as soon as they have used the telephone again and replaced the receiver.

Automatic callback on busy This function can only be used on telephones that permit suffix dialling. An automatic callback from an inquiry connection is not possible.

Automatic callback on busy (CCBS) You urgently need to contact a business partner or internal subscriber. However, when you call, you always hear the engaged tone. If you were to receive notification that the subscriber had ended the call, your chance of reaching them would be very good. With "Callback on Busy" you can reach the engaged subscriber once they have replaced the receiver at the end of the call. Your telephone rings. When you lift the receiver, a connection to the required subscriber is set up automatically. An internal "Callback on Busy" is deleted automatically after 30 minutes. The external "Callback on

Busy" is deleted after a period specified by the exchange (approx. 45 minutes). Manual deletion before this period has elapsed is also possible.

Automatic callback on no reply (CCBS) You urgently need to contact a business partner or internal subscriber. When you call them, you always hear the ringing tone, but your business partner is not close to the telephone and does not pick up. With "Callback on no reply", you can reach the subscriber as soon as they have completed a call or lifted and replaced the receiver of their telephone. Your telephone rings. When you lift the receiver, a connection to the required subscriber is established automatically.

Automatic clearing of Internet connection (ShortHold) You can activate ShortHold. When you do so, you define the time after which an existing connection is cleared if data transfer is no longer taking place. If you enter a time of 0, ShortHold is deactivated.

Automatic outside line After the receiver of a telephone is lifted, the telephone number of the external subscriber can be dialled immediately.

Automatic redialling Performance feature of a terminal. If the line is busy, several redial attempts are made.

B channel Corresponds to a telephone line in T-Net. In T-ISDN, the basic connection contains two B channels, each with a data transmission rate of 64 kbps.

B channel Bearer channel of an ISDN Basic Rate Interface or a Primary Rate Interface for the transmission of traffic (voice, data). An ISDN Basic Rate Interface consists of two B channels and one D channel. A B channel has a data transmission rate of 64 kbps. The data transmission rate of an ISDN Basic Rate Interface with your gateway can be increased to up to 128 kbps using channel bundling.

BACP/BAP Bandwidth Allocation Control Protocols (BACP/BAP in accordance with RFC 2125)

Base station Central unit of wireless telephone devices. There are two different types: The simple base station is used to charge the handheld unit. For special-feature telephones, the base station can also be used as a telephone, the handheld unit is charged using separate charging stations.

Basic Rate Interface ISDN connection that includes two basic channels (B channels) each with 64 kbps and one control and signalling channel (D channel) with 16 kbps. The two basic channels can be used independently of each other for each service offered in the T-ISDN. You can therefore telephone and fax at the same time. T-Com offers the Basic Rate Interface as a point-to-multipoint or point-to-point connection.

Blacklist (dialling ranges) You can define a restriction on external dialling for individual subscribers. The telephone numbers entered in the blacklist table cannot be called by the terminals subject to dialling control, e.g. entry 0190 would block all connections to expensive service providers.

Block Cipher Modes Block-based encryption algorithm

Blowfish An algorithm developed by Bruce Schneier. It relates to a block cipher with a block size of 64 bit and a key of variable length (up to 448 bits).

Bluetooth Bluetooth is a wireless transfer technology that can connect up different devices. Bluetooth replaces cables to connect various devices e.g. Notebook, PC, PDA, etc. Thanks to Bluetooth, these devices can exchange data with each other without a fixed connection. For example, PCs, notebooks or a PDA can access the Internet or a local network. The appointments on a PDA can be synchronised with the appointments on the PC without the need for a cable connection. Because of the many different application areas for the Bluetooth technology, the different types of connections between the devices are divided into profiles. A profile determines the service (function) that the individual Bluetooth clients can use among each other.

BOD Bandwidth on Demand

BootP Bootstrap protocol

Bps Bits per second. A unit of measure for the transmission rate.

Break-in In a PBX, the option of breaking in to an existing call. This is signalled acoustically by an attention tone.

BRI Basic Rate Interface

Bridge Network component for connecting homogeneous networks. As opposed to a gateway, bridges operate at layer 2 of the OSI model, are independent of higher-level protocols and transmit data packets using MAC addresses. Data transmission is transparent, which means the information contained in the data packets is not interpreted.

Broadcast Broadcasts (data packages) are sent to all devices in a network in order to exchange information. Generally, there is a certain address (broadcast address) in the network that allows all devices to interpret a message as a broadcast.

Brokering Brokering makes it possible to switch between two external or internal subscribers without the waiting subscriber being able to hear the other conversation.

Browser Program for displaying content on the Internet or World Wide Web.

Bus A data transmission medium for use by all the devices connected to a network. Data is forwarded over the entire bus and received by all devices on the bus.

CA Certificate Authority

Calendar By allocating a calendar, you switch between Day and Night call assignment. For each day of the week, you can select any day/night switching time. A calendar has four switch times, which can be specifically assigned to each individual day of the week.

Call allocation In a PBX, calls can be assigned to certain terminals.

Call costs account You can set up a "call costs account" for a subscriber here. The maximum available number of units, in the form of a limit, can be assigned to each subscriber on their personal "call costs account". The "cost limit" is to be activated so that units can be booked. Once the units have been used up, no further external calls are possible. Internal calls can still be made at any time. The units are booked to the account each time a call is ended.

Call diversion Also known as call forwarding. An incoming call is diverted to a specified telephone, Internet or wireless connection.

Call filter Performance feature e.g. of the T-Concept PX722 system telephone, special-feature telephones or answering machines. The call is only signalled in the case of certain previously defined telephone numbers.

Call forwarding in the exchange You can only use the options of call forwarding in the exchange via the keypad if certain services are activated for your connection. You can receive more information on this from your T-Com advisor. The exchange connects the calling subscriber with an external subscriber you have specified.

Call forwarding in the PBX The call forwarding (CF) performance feature of the PBX enables you to be reached even if you are not in the vicinity of your telephone. You achieve this by automatically forwarding your calls to the required internal or external telephone number. You can use the configuration program to define whether call forwarding should be carried out in the PBX or the exchange. You should use call forwarding in the exchange if certain services are activated for your connection. You can receive more information on this from your T-Com advisor.

Call option day/night Option of changing the call allocation on a PBX using a calendar. Calls received after office hours are forwarded to a telephone still manned, or to the answering machine or fax.

Call pickup Performance feature of a PBX. Calls can be received on an internal terminal that is not part of active call allocation.

Call pickup An external call is only signalled for your colleague. As you belong to several different teams, this is not surprising. You can now form various groups of subscribers in which call pickup is possible. A call can only be picked up by subscribers/terminals in the same pickup group. The assignment of subscribers in pickup groups is not dependent on the settings in the Day and Night team call assignment.

Call Relay on Busy Reject

Call Through Call Through is a dial-in via an external connection to the PBX with the call put through from the PBX via another external connection.

Call to engaged subscriber Busy on busy

Call waiting The "Call Waiting" performance feature means that other people can contact you during a telephone call. If another subscriber calls while you are on the telephone, you hear your telephone's call waiting tone. You can then decide whether to continue with your first call or speak to the person whose call is waiting.

Call waiting protection If you do not want to use the call waiting feature, you switch on call waiting protection. If you are taking a call, a second caller hears the engaged tone.

Callback on Busy Performance feature in T-ISDN, PBXs and T-Net. A connection is set up automatically as soon as the Busy status on the destination connection ends. When the connection is free, this is signalled to the caller. As soon as the caller lifts the receiver, the connection is set up automatically. However, Callback must first be activated by the caller on his or her terminal.

Callback on no reply You call a subscriber, who does not pick up. With "Callback on no reply", this is not a problem for you, because with this special feature, you can set up the connection without having to redial. If you are not on the telephone yourself, a new connection with the subscriber is set up - for a maximum of 180 minutes.

Called party number Number of the terminal called.

Caller list Special-feature telephones such as the T-Concept PX722 system telephone enable call requests to be stored during absence.

Calling party number Number of the calling terminal.

CAPI Common ISDN Application Programming Interface

CAST A 128-bit encryption algorithm with similar functionality to DES. See Block Cipher Modes.

CBC Cipher Block Chaining

CCITT Consultative Committee for International Telegraphy and Telephony

CD (Call Deflection) The forwarding of calls. This performance feature enables you to forward a call without having to take it yourself. If you forward a call to an external subscriber, you bear any connection costs from your connection to the destination of the forwarded call. This feature can therefore be used by system telephones and ISDN telephones that support this function (see user's guide for terminals). For more information on using this performance feature with the telephone, please see the user's guide.

Central speeddial memory Performance feature of a PBX. Telephone numbers are stored in a PBX and can be called from every connected telephone using a key combination.

Certificate Certificate

Channel Bundling Channel bundling

CHAP Challenge Handshake Authentication Protocol

Checksum field Frame Check Sequence (FCS)

CLID Calling Line Identification

Client A client uses the services provided by a server. Clients are usually workstations.

CLIP Abbreviation for Calling Line Identification Presentation. Telephone number display of calling party.

CLIR Abbreviation for Calling Line Identification Restriction. Temporary suppression of the transmission of the calling party's telephone number.

COLR Connected Line Identification Restriction (suppress B telephone number). This performance feature permits or suppresses the display of the called subscriber's telephone number. If display of the B telephone number is suppressed, your telephone number is not transmitted to the caller when you take a call. Example: You have set up call diversion to another terminal. If this terminal has activated suppression of the B telephone number, the calling party does not see a telephone number on the terminal display.

Combination device If an analogue terminal connection of the PBX is set up as a "multifunctional port" for combination devices, all calls are received, regardless of the service. In the case of trunk prefixes using codes, the service ID "Analogue Telephony" or "Telefax Group 3" can also be transmitted, regardless of the configuration of the analogue connection. If 0 is dialled, the service ID "Analogue Telephony" is also transmitted.

Conference call Performance feature of a PBX: Several internal subscribers can telephone simultaneously. Three-party conferences are also possible with external subscribers.

Configuration Manager Windows application (similar to the Windows Explorer), which uses SNMP commands to request and carry out the settings of your gateway. The application was called the DIME Browser before BRICKware version 5.1.3.

Configuration of the PBX with the PC One important prerequisite for the transfer of your configuration to the PBX is that you have set up a connection between the PC and PBX. You can do this using the LAN Ethernet connection.

Configuration of the PBX with the telephone With some restrictions, you can also program your PBX using the telephone. For information on programming your PBX using the telephone, please see the accompanying user's guide.

Connection of analogue terminals The performance features for analogue terminals can only be used with terminals that use the MFC dialling method and that have an R or flash key.

Connection of ISDN terminals
The internal telephone number of the connection, and not the external number (multiple subscriber number) must be entered as the MSN in the ISDN terminal connected to the internal ISDN bus. See the user's guide for the ISDN terminals: Enter MSN. Please note that not all the ISDN terminals available on the market can use the performance features provided by the PBX via their key interface.

CRC
Cyclic Redundancy Check

CTI
Computer Telephony Integration. Term for connection between a PBX and server. CTI enables PBX functions to be controlled and evaluated by a PC.

D channel
Control and signalling channel of an ISDN Basic Rate Interface or Primary Rate Interface. The D channel has a data transmission rate of 16 kbps. In addition to the D channel, each ISDN BRI has two B channels.

Data compression
A process for reducing the amount of data transmitted. This enables higher throughput to be achieved in the same transmission time. Examples of this technique include STAC, VJHC and MPPC.

Data Link Layer
(DLL)

Data packet
A data packet is used for information transfer. Each data packet contains a prescribed number of characters (information and control characters).

Data transmission rate
The data transmission rate specifies the number of information units for each time interval transferred between sender and recipient.

Datagram
A self-contained data packet that is forwarded in the network with minimum protocol overhead and without an acknowledgement mechanism.

Datex-J
Abbreviation for Data Exchange Jedermann, the T-Online access platform. Local dial-in node in every local network. Some German cities offer additional high-speed access over T-Net/T-Net-ISDN.

Day/Night option
If you want to transfer important calls made after office hours to your home office to an answering machine, so that you are not disturbed, you can use call assignment. You can allocate each subscriber two different call allocations (call assignment Day and call assignment Night). With call assignments, it is also possible to forward the call to an external subscriber, so that you can be contacted at all times.

With call assignment Day/Night, therefore, you define which internal terminals are to ring in the event of an external call. Call assignment Day/Night is achieved using a table in which all the incoming calls are assigned to internal subscribers.

Day/Night/Calendar You define switching of call variant Day/Night.

DCE Data Circuit-Terminating Equipment

DCN Data communications network

Default gateway Describes the address of the gateway to which all traffic not destined for its own network is sent.

Denial-Of-Service Attack A Denial-of-Service (DoS) attack is an attempt to flood a gateway or host in a LAN with fake requests so that it is completely overloaded. This means the system or a certain service can no longer be run.

DES Data Encryption Standard

Destination number memory Speeddial memory

DHCP Dynamic Host Configuration Protocol

Dial preparation On some telephones with a display, you can first enter a telephone, check it first, and then dial it.

Dial-in parameters Define the dial-in parameters i.e. you enter the provider's dial-in number and specify:

Dialling control In the configuration for certain terminals, you can define restrictions for external dialling.

Dialup connection A connection is set up when required by dialling an extension number, in contrast to a leased line.

DIME Desktop Internetworking Management Environment

DIME Browser Old name for Configuration Manager.

Direct dial-in Performance feature of larger PBXs at the point-to-point connection: The extensions can be called directly from outside.

Direct dialling range See Extension numbers range

Display and output of connection data In the configuration, it is possible to define storage of data records for specific terminals or all terminals. In the ex works setting, all incoming external connections and all external calls you make are stored.

Display of caller's number A suitable telephone is a prerequisite for this feature. Transmission of the telephone number must be permitted by the caller.

DLCI In a Frame Relay network, a DLCI uniquely describes a virtual connection. Note that a DLCI is only relevant for the local end of the point-to-point connection.

DMZ Demilitarised Zone

DNS Domain Name System

Do not disturb Station guarding

DOI Domain of Interpretation

Domain A domain refers to a logical group of devices in a network. On the Internet, this is part of a naming hierarchy (e.g. bintec.de).

Door intercom Door intercom device. It can be connected to various PBXs. A telephone can be used to take an intercom call and open the door.

Door intercom on analogue connection An analogue connection can be set up for connected of function module M06 to connect a DoorLine intercom system.

Door terminal adapter The function module can be installed on an analogue connection of your PBX. If a door intercom (DoorLine) is connected to your PBX via a function module, you can speak with a visitor at the door via 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.

Dotted Decimal Notation The syntactic representation of a 32-bit whole number, written in four 8-bit numbers in decimal form and subdivided by a point. It is used to represent IP addresses on the Internet, e.g. 192.67.67.20

Downstream Data transmission rate from the ISP to the customer.

DSA (DSS) Digital Signature Algorithm (Digital Signature Standard).

DSL/xDSL Digital Subscriber Line

DSS1 Digital Subscriber Signalling System

DSSS Direct Sequence Spread Spectrum is a wireless technology that was originally developed for the military and offers a high level of protection against faults because the wanted signal is spread over a wide area. The signal is spread by means of a spread sequence or chipping code consisting of 11 chips across 22 MHz. Even if there is a fault on one or more of the chips during transfer, the information can still be obtained reliably from the remaining chips.

DTE Data Terminal Equipment

DTMF Dual Tone Multi Frequency (tone dialling system)

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.

E1/T1 E1: European variant of the 2.048 mbps ISDN Primary Rate Interface, which is also called the E1 system.

ECB Electronic Code Book mode

ECT Explicit Call Transfer. This performance feature allows two external connections to be transferred without blocking the two B channels of the exchange connection.

Email Electronic mail

Emergency numbers You urgently need to contact the policy, fire brigade or another telephone number. To make things worse, all the connections are busy. However, you have informed your PBX of the telephone numbers that need to be contactable in an emergency. If you now dial one of these numbers, it is recognised by the PBX and a B channel of the T-ISDN is automatically freed up for your emergency call. Emergency calls are not subject to configuration restrictions. If "Calling with prefix plus code number" is set for a a connection, the internal connection is busy. To make an external call, first dial 0 and then the required emergency number.

Encapsulation Encapsulation of data packets in a certain protocol for transmitting the packets over a network that the original protocol does not directly support (e.g. NetBIOS over TCP/IP).

Encryption Refers to the encryption of data, e.g. MPPE.

Entry of external connection data In the ex works setting, all external connections made and received via your PBX are recorded and stored in the form of connection data records.

ESP Encapsulating Security Payload

ESS The Extended Service Set describes several BSS (several access points) that form a single, logical wireless network.

Ethernet A local network that connects all devices in the network (PC, printers, etc.) via a twisted pair or coaxial cable.

Ethernet connections The 4 connections are led equally through an internal switch. Network clients can be directly connected to the connection sockets. The ports are designed as 100/BaseT full-duplex, autosensing, auto MDIX upwardly compatible to 10/Base T. Up to 4 SIP telephones or IP softclients with SIP standard can be directly connected to PCs with a network card.

Eumex Recovery If the power supply to the PBX cuts out while new firmware is being loaded, the PBX functions are deleted.

Euro ISDN Harmonised ISDN standardised within Europe, based on signalling protocol DSS1, the introduction of which network operators in over 20 European countries have committed to. Euro-ISDN has been introduced in Germany, replacing the previous national system 1 TR6.

Eurofile transfer Communication protocol for the exchange of files between two PCs over ISDN using an ISDN card (file transfer) or telephones or PBXs configured for this.

Exchange Node in the public telecommunication network. We differentiate between local exchanges and remote exchanges.

Exchange access right PBXs differentiate between the following "exchange access rights". These can be set up differently for each subscriber in the configuration.

Extended redialling A selected telephone number is "parked" in the telephone's memory. It can be redialled later, even if you have called other numbers in the meantime.

Extension For PBXs, describes the terminal (e.g. telephone) connected to the exchange. Each extension can access PBX services and communicate with other extensions.

Extension number

An extension is an internal number for a terminal or subsystem. In point-to-point ISDN accesses, the extension is usually a number from the extension numbers range assigned by the telephone provider. In point-to-multipoint connections, it can be the MSN or a part of the MSN.

Extension numbers range

(direct dialling range)

Fall Back: Priority of the Internet provider entries

The priority of the Internet provider entries is defined by the sequence in which they are entered in the list. The first entry of a DSL connection is the standard access. If a connection cannot be set up via the standard access after a predefined number of attempts, setup is attempted using the second entry then subsequent entries. If the final entry in the list does not enable a connection to be set up successfully, the operation is terminated until a new request is made. When fall back occurs and all other ISPs can only be reached by dialup connections, both B channels may be occupied. If channel bundling is used, you cannot be reached for the duration of this connection.

Fax

Abbreviation of telefax.

FHSS, Frequency Hopping Spread Spectrum

In a FHSS system, the frequency spread is achieved through constantly changing frequencies based on certain hopping patterns. In contrast to DSSS systems, hopping patterns are configured, not the frequency. The frequency changes very frequently in one second.

File transfer

Data transmission from one computer to another, e.g. based on the Eurofile transfer standard.

Filter

A filter comprises a number of criteria (e.g. protocol, port number, source and destination address). These criteria can be used to select a packet from the traffic flow. Such a packet can then be handled in a specific way. For this purpose, a certain action is associated with the filter, which creates a filter rule.

Firewall

Describes the whole range of mechanisms to protect the local network against external access. Your gateway provides protection mechanisms such as NAT, CLID, PAP/CHAP, access lists, etc.

Firmware

Software code containing all a device's functions. This code is written to a PROM (programmable read only memory) and is retained there, even after the device is switched off. Firmware can be updated by the user when a new software version is available (firmware upgrade).

First-level domain Describes the last part of a name on the Internet. For www.t-com.de, the first-level domain is de and in this case stands for Germany.

Flash key The flash key on a telephone is the R button. R stands for Rückfrage (inquiry). The key interrupts the line briefly to start certain functions such as inquiries via the PBX.

Follow-me Performance feature of a PBX for diverting calls on the destination telephone.

Fragmentation Process by which an IP datagram is divided into small parts in order to meet the requirements of a physical network. The reverse process is known as reassembly.

Frame Unit of information sent via a data connection.

Frame relay A packet switching method that contains smaller packets and fewer error checks than traditional packet switching methods such as X.25. Because of its properties, frame relay is used for fast WAN connections with a high density of traffic.

Freecall Telephone number. Previous service 0130. These telephone numbers have been switched to freecall 0800 since January 1, 1998.

FTP File Transfer Protocol

Full duplex Operating mode in which both communication partners can communicate bidirectionally at the same time.

Function keys Keys on the telephone that can be assigned telephone numbers or network functions.

G.991.1 Data transmission recommendation for HDSL

G.991.2 Data transmission recommendation for SHDSL

G.992.1 Data transmission recommendation for ADSL. See also G.992.1 Annex A and G.992.1 Annex B.

G.992.1 Annex A Data transmission recommendation for ADSL: ITU-T G.992.1 Annex A

G.992.1 Annex B Data transmission recommendation for ADSL: ITU-T G.992.1 Annex B

G.SHDSL See G.991.2.

Gateway Entrance and exit, transition point

Half duplex Bidirectional communication method in which it is only possible to either send or receive at a particular point in time. Also known as Simplex.

Handheld unit Mobile component of wireless telephone units. In the event of digital transmission, it is also possible to make telephone calls between the handheld units (DECT).

Hands free If the telephone has a microphone and speaker installed, you can conduct a call without using your hands. As a result, other people in the room can also participate in the call.

Hashing The process of deriving a number (hash) from a character string. A hash is generally far shorter than the text flow it was derived from. The hashing algorithm is designed so that there is a relatively low probability of generating a hash that is the same as another hash generated from a text sequence with a different meaning. Encryption methods use hashing to make sure that intruders cannot change transmitted messages.

HDLC High Level Data Link Control

HDSL High Bit Rate DSL

HDSL2 High Bit Rate DSL, version 2

Headset Combination of headphones and microphone as a useful aid for anyone who makes a lot of telephone calls and wants to keep hands free for making notes.

HMAC Hashed Message Authentication Code

HMAC-MD5 Hashed Message Authentication Code - uses Message Digest Algorithm Version 5.

HMAC-SHA1 Hashed Message Authentication Code - uses Secure Hash Algorithm Version 1.

Holding a call A telephone call is put on hold without breaking the connection (inquiry/brokering).

Holding in the PBX Both B channels of the ISDN connection are needed for the performance features "Call another person during a call" and "Speak alternately with two people" (brokering). As a result, you cannot be reached from outside or make external calls via your PBX's second

B channel. With this setting, an external caller put on hold hears the PBX's on-hold music.

Hook flash
The use of the inquiry, brokerage and three-party conference special features in T-Net and certain performance features of some PBXs is only possible with the hook flash function (long flash) of the signal key on the telephone. On modern telephones, this key is indicated with an "R".

Host name
A name used in IP networks instead of the corresponding address. A host name consists of an ASCII string that uniquely identifies the host computer.

HTTP
HyperText Transfer Protocol

Hub
Network component used to connect several network components together to form a local network (star-shaped).

IAE
ISDN connection unit, ISDN connection socket.

ICMP
Internet Control Message Protocol

ICV
Integrity Check Value

Identify malicious callers (intercept)
You have to request this performance feature from T-Com. The company will provide you with further information on the procedure. If you enter code 77 during a call or after the caller has ended a call (you hear the engaged tone from the exchange), the caller's telephone number is stored in the exchange. ISDN telephones can also use separate functions for this performance feature. For more information on this function, please see your user's guide.

IEEE
The Institute of Electrical and Electronics Engineers (IEEE). A large, global association of engineers, which continuously works on standards in order to ensure different devices can work together.

IETF
Internet Engineering Task Force

Index
The index from 0...9 is fixed. Every external multiple subscriber number entered is assigned to an index. You need this index when configuring performance features using the telephone's codes, e.g. configuring "Call forwarding in the exchange" or "Define telephone number for the next external call".

Infrastructure mode
A network in infrastructure mode is a network that contains at least one access point as the central point of communication and control. In a network in infrastructure mode, all clients communicate with

each other via access points only. There is no direct communication between the individual clients. A network of this kind is also known as a BSS (basic service set), and a network that consists of several BSS is known as an ESS (extended service set). Most wireless networks operate in infrastructure mode to establish a connection with the wired network.

Inquiry Makes it possible to put the first call on hold in the event of a call waiting and take a new call.

Internal call tone Special signal on a PBX to differentiate between internal and external calls.

Internal calls Free-of-charge connection between terminals in a PBX.

Internal telephone numbers Your PBX has a fixed internal telephone number plan.

Internet The Internet consists of a number of regional, local and university networks. The IP protocol is used for data transmission on the Internet.

Internet time sharing Allows several users to surf the Internet simultaneously over an ISDN connection. The information is requested by the individual computers with a time delay.

Intranet Local computer network within a company based on Internet technology providing the same Internet services, e.g. homepages and sending email.

IP Internet Protocol

IP Address The first part of the address by which a device is identified in an IP network, e.g. 192.168.1.254. See also netmask.

IPComP IP payload compression

IPCONFIG A tool used on Windows computers to check or change its own IP settings.

IPoA IP over ATM

ISDN Integrated Services Digital Network

ISDN address The address of an ISDN device that consists of an ISDN number followed by further numbers that relate to a specific terminal, e.g. 47117.

ISDN Basic Rate Interface ISDN subscriber connection. The Basic Rate Interface consists of two B channels and one D channel. In addition to the Basic Rate Interface, there is the Primary Rate Interface. The interface to the subscriber is provided by an So bus.

ISDN card Adapter for connecting a PC to the ISDN Basic Rate Interface. From a technical perspective, we differentiate between active and passive cards. Active ISDN cards have their own processor, which handles communication operations independently of the PC processor and therefore does not require any resources. A passive ISDN card, on the other hand, uses the PC's resources.

ISDN Login Function of your gateway. Your gateway can be configured and administrated remotely using ISDN Login. ISDN Login operates on gateways in the ex works state as soon they are connected to an ISDN connection and therefore reachable via an extension number.

ISDN number The network address of the ISDN interface, e.g. 4711.

ISDN router A router that does not have network connections but provides the same functions between PC, ISDN and the Internet.

ISDN-BRI ISDN Basic Rate Interface

ISDN-Dynamic This performance feature requires the installation of the T-ISDN Speedmanager. If you are surfing the Internet and use two B channels for downloading, you cannot be reached by telephone from outside. As a further call is signalled over the D channel, your PBX can, depending on the setting, specifically shut down a B channel so that you can take the call.

ISDN-Internal/External Alternative name for the So bus.

ISDN-PRI ISDN Primary Rate Interface

ISO International Standardization Organization

ISP Internet Service Provider

ITU International Telecommunication Union

Key Escrow Stored keys can be viewed by the government. The US government, in particular, requires key storages to prevent crimes being covered up through data encryption.

LAN Local Area Network

LAPB Link Access Procedure Balanced

Last access The last access by T-Service is stored and displayed in the configuration.

Layer 1 Layer 1 of the ISO OSI Model, the bit transfer layer.

LCD Liquid Crystal Display, a screen in which special liquid crystal is used to display information.

LCP Link Control Protocol

LDAP Lightweight Directory Access Protocol

Lease Time The "Lease Time" is the time a computer keeps the IP address assigned to it without having to "talk" to the DHCP server.

Leased Line Leased line

LLC Link Layer Control

Local exchange Switching node of a public local telephone network that supports the connection of end systems.

Loudspeaker Function on telephones with an integrated loudspeaker: You can press a button so that the people present in the room can also hear the telephone call.

MAC Address Every device in the network is defined by a fixed hardware address (MAC address). The network card of a device defines this internationally unique address.

Man-in-the-Middle Attack Encryption using public keys requires the public keys to be exchanged first. During this exchange, the unprotected keys can be intercepted easily, making a "man-in-the-middle" attack possible. The attacker can set a key at an early stage so that a key known to the "man-in-the-middle" is used instead of the intended key from the real communication partner.

MD5 See HMAC-MD5

MFC Multifrequency code dialling method

MIB Management Information Base

Microphone mute Switch for turning off the microphone. The subscriber on the telephone cannot hear the discussions in the room.

Mixed mode The access point accepts WPA and WPA2.

MLPPP Multilink PPP

Modem Modulator/Demodulator

MPDU MAC Protocol Data Unit - every information packet exchanged on the wireless medium includes management frames and fragmented MSDUs.

MPPC Microsoft Point-to-Point Compression

MPPE Microsoft Point-to-Point Encryption

MSDU MAC Service Data Unit - a data packet that ignores fragmentation in the WLAN.

MSN Multiple subscriber number

MSSID See SSID

MTU Maximum Transmission Unit

Multicast A specific form of broadcast in which a message is simultaneously transmitted to a defined user group.

Multiple subscriber number Multiple subscriber number

Multiprotocol gateway A gateway that can route several protocols, e.g. IP, X.25, etc.

Music on hold (MoH) Your PBX has two internal music-on-hold melodies. On delivery, internal melody 1 is active. You can choose between melody 1 or 2, or deactivate the music on hold.

Music on hold (MoH) Performance feature of a PBX. During an inquiry or call forwarding, a melody is played that the waiting subscriber hears. On your PBX, you can choose between two internal melodies.

MWI Transmission of a voice message from a mailbox e.g. T-NetBox or MailBox to a terminal. The receipt of the message on the terminal is signalled e.g. by a LED.

NAT Network Address Translation

NDIS WAN NDIS WAN is a Microsoft enhancement of this standards in relation to wide area networking (WAN). The NDIS WAN CAPI driver permits the use of the ISDN controller as a WAN card. The NDIS WAN driver enables the use of a DCN network on Windows. NDIS is the abbreviation for Network Device Interface Specification and is a standard for the connection of network cards (hardware) to network protocols (software).

Net surfing A "journey of discovery" for interesting information in wide-ranging data networks such as T-Online. Known mainly from the Internet.

NetBIOS Network Basic Input Output System

Netmask The second part of an address in an IP network, used for identification of a device, e.g. 255.255.255.0. See also IP address.

Network Your PBX has a DSL router so that one or more PCs can surf the Internet and download information.

Network address A network address designates the address of a complete local network.

Network termination (NTBA) In telecommunications, the network termination is the point at which access to a communication network is provided to the terminal.

Netz-Direkt (keypad functions) You can use the "Netz-Direkt" (keypad) function (automatic external line access) to enter a key sequence from your ISDN or analogue telephone to use current T-ISDN functions. For more information on this, consult your T-Com client advisor and request the necessary codes (e.g. call forwarding in the exchange).

NMS Network Management Station

Notebook function During a telephone call, a telephone number can be entered in the telephone's buffer so that it can be dialled at a later point in time.

NT Network Termination

NTBA Network Termination for Basic Access

NTP Network Time Protocol

OAM Operation and Maintenance

Offline Without connection. Connectionless operating state e.g. of the PCs.

Online With connection. For example the state of a connection between a PC and data network or for data exchange between two PCs.

Online banking Term for electronic banking e.g. using T-Online.

Online Pass

Part of the T-Com certification services for the Internet. Digital pass for the Internet. With the Online Pass, an Internet user can be authenticated as a customer in a company.

Online services

Services available around the clock via communication services such as T-Online and the Internet.

OSI model

OSI = Open Systems Interconnection

OSPF

Open Shortest Path First

Outgoing extension number signal

The "outgoing extension number signal" is intended for internal connections on the point-to-point to which an explicit extension number was not assigned. When an external call is made, the extension number entered under Outgoing Extension Number Signal is also transmitted.

Outgoing telephone number

If you have not suppressed transmission of your telephone number, and the telephone of the person you are calling supports the CLIP function, the person you are calling can see the telephone number of the connection you are calling from on their telephone display. This telephone number transmitted during an external call is called the outgoing telephone number.

Packet switching

Packet switching

PAP

Password Authentication Protocol

Parking

The call is held temporarily in the exchange. The main difference to on hold: The call is interrupted, the receiver can be replaced. Can be used for brokering. Possible in T-Net, T-ISDN and PBXs. The terminal must have MFC and the R key.

PBX

Private Branch Exchange

PBX

The features offered by a PBX are manufacturer-specific and enable operation of exchanges, free internal calls, callback on busy, and conference calls, among other things. PBXs are used e.g. for office communication (voice, text and data transfer).

PBX

Private Branch Exchange (PBX)

PBX

Private Automatic Branch Exchange

PBX number

A point-to-point ISDN access includes a PBX number and an extension numbers range. The PBX number is used to reach the PBX. A certain terminal of the PBX is then dialled via one of the extension numbers of the extension numbers range.

PCMCIA The PCMCIA (Personal Computer Memory Card International Association) is an industry association founded in 1989 that represents credit card-sized I/O cards such as WLAN cards.

PDM Abbreviation for pulse dialling method. Conventional dialling procedure in the telephone network. Dialled numbers are represented by a defined number of dc impulses. The pulse dialling method is being replaced by the multifrequency code method (MFC) .

PGP Pretty Good Privacy

PH Packet handler

Phone book The PBX has an internal phone book. You can store up to 300 telephone numbers and the associated names. You can access the PBX's phone book with the funkwerk devices (for example CS 410). You add entries to the phone book using the configuration interface.

PIN Personal identification number

Ping Packet Internet Groper

PKCS Public Key Cryptography Standards

Point-to-multipoint Point-to-multipoint connection

Point-to-multipoint Basic connection in T-ISDN with three telephone numbers and two lines as standard. The ISDN terminals are connected directly on the network termination (NTBA) or ISDN internet connection of a PBX.

Point-to-multipoint Point-to-multipoint

Point-to-multipoint connection for the PBX You enter the multiple subscriber numbers received from T-Com with the order confirmation in the table fields defined for them in the configuration. As a rule, you receive three multiple subscriber numbers, but can apply for up to 10 telephone numbers for each connection. When you enter the telephone numbers, they are assigned to an "index" and also to a team. Note that initially, all telephone numbers are assigned to team 00. The internal telephone numbers 10, 11 and 20 are entered in team 00 ex works. External calls are therefore signalled with the internal telephone numbers 10, 11 and 20 for the connections entered in team 00.

Point-to-point Point-to-point

Point-to-point ISDN access	Point-to-point
Polling	Fax machine function that "fetches" documents provided by other fax machines or fax databases.
Port	Input/output
POTS	Plain Old Telephone System
PPP	Point-to-Point Protocol
PPP authentication	Security mechanism. A method of authentication using passwords in PPP.
PPPoA	Point to Point Protocol over ATM
PPPoE	Point to Point Protocol over Ethernet
PRI	Primary Rate Interface
Primary Rate Interface (PRI)	ISDN subscriber connection. The PRI consists of one D channel and 30 B channels (in Europe). (In America: 23 B channels and one D channel.) There is also the ISDN Basic Rate Interface.
Protocol	Protocols are used to define the manner and means of information exchange between two systems. Protocols control and rule the course of data communication at various levels (decoding, addressing, network routing, control procedures, etc.).
Proxy ARP	ARP = Address Resolution Protocol
PSN	Packet Switched Network
PSTN	Public Switched Telephone Network
PVID	Port VLAN ID
R key	Telephones that have a R key (inquiry key) can also be connected to a PBX. In modern telephones, the R key triggers the hook flash function. This is required for use of performance features in T-Net such as inquiry/brokering and three-party conference.
RADIUS	Remote Authentication Dial In User Service
RADSL	Rate-Adaptive Digital Subscriber Line
RAS	Remote access service

Real Time Clock (RTC) Hardware clock with buffer battery

Receiver volume Function for controlling the volume in the telephone receiver.

Reconnection on the bus (parking) For a point-to-multipoint connection, enables the terminal connection to be reconnected to another ISDN socket during the telephone call.

Recording telephone calls Performance feature of an answering machine. Enables a conversation to be recorded during the telephone call.

Remote Remote, as opposed to local.

Remote access Opposite to local access, see Remote.

Remote CAPI bintec's own interface for CAPI.

Remote diagnosis/remote maintenance Some terminals and PBXs are supported and maintained by T-Service support offices over the telephone line, which often means a service engineer does not have to visit the site.

Remote query Answering machine function. Involves listening to messages remotely, usually in connection with other options such as deleting messages or changing recorded messages.

Repeater A device that transmits electrical signals from one cable connection to another without making routing decisions or carrying out packet filtering. See Bridge and Router.

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

RFC Specifications, proposals, ideas and guidelines relating to the Internet are published in the form of RFCs (request for comments).

Rijndael (AES) Rijndael (AES) was selected as AES due to its fast key generation, low memory requirements and high level of security against attacks. For more information on AES, see http://csrc.nist.gov/encryption/aes.

RIP Routing Information Protocol

RipeMD 160 RipeMD 160 is a cryptographic hash function with 160 bits. It is regarded as a secure replacement for MD5 and RipeMD.

RJ45 Plug or socket for maximum eight wires. Connection for digital terminals.

Roaming In a multicell WLAN, clients can move freely and log off from one access point and log on to another when moving through cells, without the user noticing this. This is known as roaming.

Room monitoring (acoustic) To use the "Room Monitoring" performance feature, the telephone must be activated in the room to be monitored by means of a code, and the receiver must be lifted or "Hands-free" switched on. If you replace the telephone receiver or turn off "Hands-free", room monitored ends and the performance feature is switched off.

Room monitoring from external telephones This function can be used to monitor rooms from an external telephone.

Room monitoring from internal telephones You can acoustically monitor a room from an internal telephone in your PBX. This is set up using the telephone procedures described in the user's guide. Please read the information on the described functions in the user's guide.

Router A device that connects different networks at layer 3 of the OSI model and routes information from one network to the other.

RSA The RSA algorithm (named after its inventors Rivest, Shamir, Adleman) is based on the problem of factoring large integers. It therefore takes a large amount of data processing capacity and time to derive a RSA key.

RTSP Real-Time Streaming Protocol

S2M interface See Primary Rate Interface.

SAD The SAD (=Security Association Database) contains information on security agreements such as AH or ESP algorithms and keys, sequence numbers, protocol modes and SA life. For outgoing IPSec connections, an SPD entry refers to an entry in the SAD i.e. the SPD defines which SA is to be applied. For incoming IPSec connections, the SAD is queried to determine how the packet is to be processed.

SDSL Symmetric Digital Subscriber Line

Server A server offers services used by clients. Often refers to a certain computer in the LAN, e.g. DHCP server.

ServerPass Part of the T-Com certification services for the Internet. Digital pass for a company. With the ServerPass, T-Com confirms that a server on the Internet belongs to a particular company and that this was verified through the presentation of an excerpt from the business register.

Service 0190 Additional voice service from T-Com for the commercial distribution of private information services. The T-Com services are limited to providing the technical infrastructure and collection processing for the information providers. The provided information is accessed using the telephone number 0190 which is uniform across Germany plus a 6-digit telephone number. Information offering: Entertainment, weather, finance, sport, health, support and service hotlines.

Service 0700 Additional voice service from T-Com. Allows calls to be received via a location-independent telephone number uniform across Germany, starting with the numbers 0700. Free-of-charge routing to national fixed network. Enhancement with Vanity possible.

Service 0900 Additional voice service from T-Com. Replaces Service 0190.

Service number 0180 Additional voice service 0180call from T-Com to receive calls from a location-dependent telephone number uniform across Germany, starting with the numbers 0180.

Setup Tool Menu-driven tool for the configuration of your gateway. The Setup Tool can be used as soon as the gateway has been accessed (serial, ISDN Login, LAN).

SHA1 See HMAC-SHA.

SHDSL Single-Pair High-Speed

Short hold Is the defined amount of time after which a connection is cleared if no more data is transmitted. Short hold can be set to static (fixed amount of time) or dynamic (according to charging information).

Signalling Simultaneous signalling: All assigned terminals are called simultaneously. If a telephone is busy, call waiting can be used.

Simplex operation (ISDN subscribers only) This connection can only be used for an ISDN telephone (only T-Concept PX722 system telephones) with a simplex function. If you call an ISDN telephone with a simplex function, this automatically activates the Loudspeaker function so that a conversation can take place immediately. Please see the information on the telephone user's guide on the simplex operation function.

SIP Session Initiation Protocol

SMS Short Message Service

SMS receipt If you have connected an SMS-enabled terminal, you can decide whether SMS receipt is to be permitted for the connection. The ex works setting is no SMS receipt. To receive an SMS with your SMS-enabled terminal, you must register once with the T-Com SMS Service. One-time registration is free. You simply send an SMS containing ANMELD to the destination call number 8888. You then receive a free-of-charge confirmation of registration from the T-Com SMS Service. You can deregister your device or telephone number by sending an SMS containing ABMELD to the destination number 8888. Incoming SMS are then read out. Information on which telephones are SMS-enabled can be obtained from T-Punkt, our customer hotline 0800 330 1000 or on the Internet at http://www.t-com.de.

SMS server telephone numbers You can connect SMS-enabled telephones to your PBX and thus use the SMS performance feature in the T-Com fixed network. SMSs are forwarded to the recipient via the T-Com SMS server. To send an SMS with an SMS-enabled terminal, the telephone number 0193010 of the SMS server must be prefixed to the recipient number. This telephone number is already stored in your PBX, so manual input of the server telephone is not necessary and does not need to be sent from the telephone. To receive an SMS with your SMS-enabled fixed-network telephone, you must register once with the Deutsche Telekom SMS Service. Charges are made for sending SMSs. There are no costs for receiving SMSs.

SNMP Simple Network Management Protocol

SNMP shell Input level for SNMP commands.

So bus All ISDN sockets and the NTBA of an ISDN point-to-multipoint connection. All So buses consist of a four-wire cable. The lines transmit digital ISDN signals. The So bus is terminated with a terminating resistor after the last ISDN socket. The So bus starts at the NTBA and can be up to 150 m long. Any ISDN devices can be operated on this bus. However, only two devices can use the So bus at any one time, as only two B channels are available.

So connection See ISDN Basic Rate Interface

So interface Internationally standardised interface for ISDN systems. This interface is provided on the network side by the NTBA . On the user side, the interface is intended for connecting a PBX (point-to-point connection) and for connecting up to eight ISDN terminals (point-to-multipoint connection).

SOHO
Small Offices and Home Offices

SPD
The SPD (=Security Policy Database) defines the security services available for IP traffic. These security services are dependent on parameters such as the source and destination of the packet etc.

Special features
Performance features of the T-Net and T-ISDN networks such as display of the caller's number, callback on busy, call forwarding, changeable connection lock, changeable telephone number lock, connection without dialling and transmission of charge information. Availability depends on the standard of the connected terminals.

Special-features connection
T-ISDN Basic Rate Interface with an extensive range of services: call waiting, call forwarding, third-party conference, display of call costs at the end of a connection, inquiry/brokering, telephone number transmission. In the special-features connection, three multiple subscriber numbers are included as standard.

Specify own telephone number for next call
If you want to make a business call late in the evening from your private sphere - say the living room - for example, you can define your business telephone number as the outgoing multiple subscriber number (MSN) for this call. The advantages of this are that the costs for the connection are recorded for the selected MSN and the person you are calling can identify you by the transferred MSN. Before you call an external number, you can define which of your telephone numbers is to be sent to the exchange and called party. You make the selection using the telephone number index.

Speeddial number
A speeddial index (000...299) can be assigned to each of the 300 telephone numbers in the telephone book. You then dial this speeddial index instead of the long telephone number. Note that telephone numbers dialled using the speeddial function must also comply with the dialrule.

SPID
Service Profile Identifier

Splitter
The splitter separates data and voice signals on the DSL connection.

Spoofing
Technique for reducing data traffic (and thus saving costs), especially in WANs.

SSID The Service Set Identifier (SSID) or Network Name refers to the wireless network code based on IEEE 802.11.

SSL Secure Sockets Layer A technology, now standard, developed by Netscape, which is generally used to secure HTTP traffic between a web browser and a web server.

STAC Data compression procedure.

Standard connection T-ISDN Basic Rate Interface with the performance features Inquiry/Brokering and Telephone Number Transmission. The standard connection contains three multiple subscriber numbers.

Static IP address A fixed IP address, in contrast to a dynamic IP address.

Station guarding Deactivation of acoustic call signalling: do not disturb.

Subaddressing In addition to the transmission of ISDN telephone numbers, additional information in the form of a subaddress can be transmitted from the caller to the called party over the D channel when the connection is set up. Addressing that goes beyond the pure MSN, which can be used e.g. specifically to locate several ISDN terminals that can be reached on one telephone number for a particular service. In the called terminal - e.g. a PC - various applications can also be addressed and in some cases executed. Costs are charged for the performance feature, and it must be requested separately from the network operator.

Subnet A network scheme that divides individual logical networks into smaller physical units to simplify routing.

Subnet mask A method of splitting several IP networks into a series of subgroups or subnetworks. The mask is a binary pattern that must match the IP addresses in the network. 255.255.255.0 is the default subnet mask. In this case, 254 different IP addresses can occur in a subnet, from x.x.x.1 to x.x.x.254.

Subscriber Name To distinguish between connections more easily, you can assign a subscriber name for each internal subscriber.

Suppress A-telephone number (CLIR) CLIP/CLIR: Calling line identification presentation/calling line identification restriction

Suppress B telephone number (COLR) COLP/COLR: Connected line identification presentation/connected line identification restriction = Activate/suppress transmission of called party's telephone number to caller. This performance feature suppresses the display of the called subscriber's telephone number. If display of the B telephone number is suppressed, your telephone number is not transmitted to the caller when you take a call.

Suppress own telephone number
Temporary deactivation of the transmission of your own telephone number.

Suppression of the telephone number
Performance feature of a PBX. The display of the telephone number can be deactivated on an individual basis.

Switch
LAN switches are network components with a similar function to bridges or even gateways. They switch data packets between the input and output port. In contrast to bridges, switches have several input and output ports. This increases the bandwidth in the network. Switches can also be used for conversion between networks with different speeds (e.g. 100-mbps and 10-mbps networks).

Switchable dialling method
Option of switching between the pulse dialling method and MFC method by means of a switch or key input on the terminal, such as the telephone or fax machine.

Synchronous
Transmission process in which the sender and receiver operate with exactly the same clock signals – in contrast to asynchronous transmission. Spaces are bridged by a stop code.

Syslog
Syslog is used as the de facto standard for transmitting log messages in an IP network. Syslog messages are sent as unencrypted text messages over the UDP port 514 and collected centrally. They are usually used to monitor computer systems.

System telephones
Telephone that belongs to a modern PBX, which - depending on the PBX - has a number of special features and keys, e.g. the T-Concept PX722.

T-DSL
Product name used by Deutsche Telekom AG for its DSL services and products.

T-Fax
Product name for T-Com fax machines.

T-ISDN
Telephony, faxing, data transfer and online services from one network and a single connection: T-ISDN offers exciting services with numerous benefits, for example a point-to-multipoint connection - the ideal solution for families or small businesses. This connection option, which can be used with the existing telephone cable, costs less than two telephone connections but offers far greater quality and ease of use: Two independent lines, so that you can still make a

phone call, receive a fax, or surf the Internet when another family member is making a long call on the other line. Three or more telephone numbers, which you can assign individually to your devices and distribute differently if needed through simple programming steps. Most ISDN telephones can "manage" several telephone numbers, so you can set up a "central" telephone in your household, for example, to allow you to react to calls to all ISDN telephone numbers with this telephone. The fax and telephone in your home office can also each be assigned a number, as can your son or daughter's phone. As a result, each family member can be contacted with a separate number, helping to eliminate "day-to-day friction"! And as far as the costs are concerned, on request you can have your bill broken down to show which units have been charged for the individual ISDN telephone numbers.

T-Net The digital telephone network of T-Com for connecting analogue terminals.

T-NetBox The answering machine in T-Net and T-ISDN. The T-NetBox can store up to 30 messages.

T-NetBox telephone number Enter the current T-NetBox telephone number here if it differs from the 08003302424 entered ex works. As soon as your T-NetBox receives a voice or fax message, notification is sent to your PBX.

T-Online Umbrella term the T-Com online platform. Offers services such as e-mail and Internet access.

T-Online software T-Com software decoder for all conventional computer systems that enables access to T-Online. Supports all functions such as KIT, e-mail and the Internet with a browser. T-Online users receive this software free of charge.

T-Service T-Service carries out all installation work and configurations for the PBX at the customer's request. The service ensures optimum voice and data transmission at all times thanks to maintenance work.

T-Service access T-Service access enables you to have your PBX configured by T-Service. Give T-Service a call! Get advice and provide information on your configuration requirements. T-Service will then configure your PBX remotely without you having to do anything.

TA Terminal Adapter

TAPI Telephony Application Program Interface

TAPI configuration You can use the TAPI configuration to modify the TAPI driver in line with the program that uses this driver. You can check which MSN is to be assigned to a terminal, define a line name, and configure the dialling parameters. First configure your PBX. You must then configure the TAPI interface. Use the "TAPI Configuration" program.

TCP Transmission Control Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

TCU Telecommunication connection unit

TE Terminal equipment

TEI Terminal Endpoint Identifier

Telefax Term that describes the remote copying for transmitting texts, graphics and documents true to the original over the telephone network.

Telematics Telematics is a combination of telecommunication and computer technology and describes data communication between systems and devices.

Telnet Protocol from the TCP/IP protocol family. Telnet enables communication with a remote device in the network.

Terminal adapter Device for interface adaptation. It enables different equipment to be connected to T-ISDN. The terminal adapter a/b is used to connect analogue terminals to the So interface of the ISDN Basic Rate Interface. Existing analogue terminals can still be operated with tone dialling.

TFTP Trivial File Transfer Protocol

Tiger 192 Tiger 192 is a relatively new and very fast hash algorithm.

TLS Transport Layer Security

Tone dialling Multifrequency code method (MFC)

Transfer internal code If you receive an internal call, e.g. from the subscriber with internal telephone number 22, while you are away, this subscriber's internal telephone number is stored in your telephone's caller list. However, because your connection is automatically set to Automatic Outside Line as a result of the ex works settings, you would first have to dial ** for a callback in order to obtain the internal dialling tone, and then

22. If "Transfer Internal Code" is active, ** is placed before the 22 and the callback can be made directly from the caller list.

Transmission speed The number of bits per second transmitted in T-Net or T-ISDN from the PC or fax machine. Fax machines achieve up to 14.4 kbps, modems 56 kbps. In the ISDN, data and fax exchange with 64 kbps is possible. With T-DSL, up to 8 mbps can be received and up to 768 kbps sent.

TSD Terminal Selection Digit

TTL TTL stands for Time to Live and describes the time during which a data packet is sent between the individual servers before it is discarded.

Twofish Twofish was a possible candidate for the AES (Advanced Encryption Standard). It is regarded as just as secure as Rijndael (AES), but is slower.

U-ADSL Universal Asymmetric Digital Subscriber Line

UDP User Datagram Protocol

Update Update to a software program (PBX firmware). An update is the updated version of an existing software product, and is indicated by a new version number.

Upload Data transfer during online connections, where files are transferred from the user's PC to another PC or to a data network server.

UPnP Universal Plug and Play

Upstream Data transmission rate from the client to the ISP.

URL Universal/Uniform Resource Locator

USB Universal Serial Bus

User guidance Electronic user guidance that takes the user through the required functions of a terminal such as a telephone, answering machine or fax machine step by step (menu-guided operation).

UUS1 (User to User Signalling 1) This function is only possible for system telephones and ISDN telephones.

V.11 ITU-T recommendation for balanced dual-current interface lines (up to 10 mbps).

V.24	CCITT and ITU-T recommendation that defines the interface between a PC or terminal as Data Terminal Equipment (DTE) and a modem as Data Circuit-terminating Equipment (DCE).
V.28	ITU-T recommendation for unbalanced dual-current interface line.
V.35	ITU-T recommendation for data transmission at 48kbps in the range from 60 to 108kHz.
V.36	Modem for V.35.
V.42bis	Data compression procedure.
V.90	ITU standard for 56 kbps analogue modems. In contrast to older V.34 modems, data is sent in digital form to the client when the V.90 standard is used and does not need to be first converted from digital to analogue on one side of the modem (provider), as was the case with V.34 and earlier modems. This makes higher transmission rates possible. A maximum speed of 56 kbps can be achieved only under optimum conditions.
Vanity	Letter dialling
VDSL	Very high bit rate digital subscriber line (also called VADSL or BD-SL).
VID	VLAN ID
VJHC	Van Jacobson Header Compression
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
VSS	Virtual Service Set
WAN	Wide Area Network
WAN interface	WAN interface
WAN partner	Remote station that is reached over a WAN, e.g. ISDN.
Web server	Server that provides documents in HTML format for access over the Internet (WWW).
Webmail	T-Online service with which e-mails can be sent and received world-

wide on the Internet by means of a browser.

WEP Wired Equivalent Privacy

Western plug (also known as RJ-45 plug) Plug used for ISDN terminals with eight contacts. Developed by the US telephone company Western Bell. Western plugs for analogue telephones have four or six contacts.

WINIPCFG A graphical tool on Windows 95, 98 and Millennium that uses Win32 API to view and configure the IP address configuration of computers.

WLAN A group of computers wirelessly connected to each other (wireless LAN).

WMM Wireless multimedia

WPA Wi-Fi-protected access

WPA Enterprise Concentrates primarily on the needs of companies and offers secure encryption and authentication. Uses 802.1x and the Extensible Authentication Protocol (EAP) and thus offers an effective means of user authentication.

WPA-PSK Intended for private users or small businesses that do not run a central authentication server. PSK stands for Pre-Shared Key and means that AP and client use a fixed character string (8 to 63 characters) known to all subscribers as the basis for key calculation for wireless traffic.

WWW World Wide Web

X.21 The X.21 recommendation defines the physical interface between two network components in packet-switched data networks (e.g. Datex-P).

X.21bis The X.21bis recommendation defines the DTE/DCE interface to V-series synchronous modems.

X.25 An internationally agreed standard protocol that defines the interface between network components and a packet-switched data network.

X.31 ITU-T recommendation on the integration of X.25-compatible DTEs in ISDN (D channel).

X.500 ITU-T standards that cover user directory services, see LDAP. Example: The phone book is the directory in which you find people on the basis of their name (agreement with the telephone directory). The Internet supports several databases with information on users, such as e-mail addresses, telephone numbers and postal addresses. You can search these databases to obtain information about individuals.

X.509 ITU-T standards that define the format of the certificates and certificate queries and their use.

Index