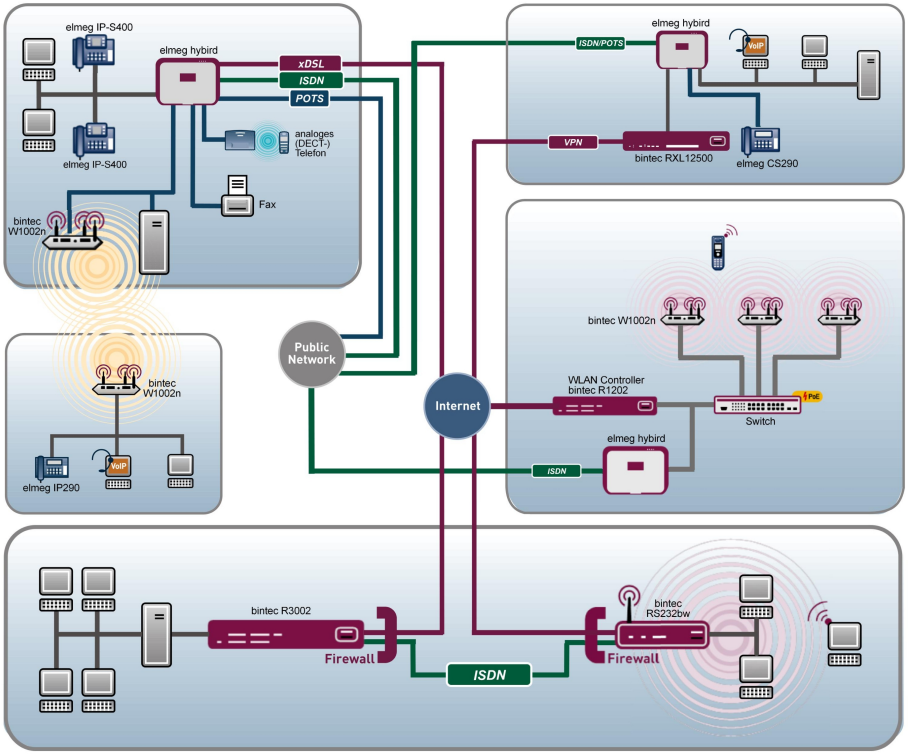


Manual
bintec Next Generation WLAN

Reference

Legal Notice

Aim and purpose
This document is part of the user manual for the installation and configuration of bintec elmeg 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.bintec-elmeg.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. bintec elmeg 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 bintec elmeg devices under *www.bintec-elmeg.com* .

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

Trademarks
bintec elmeg trademarks and the bintec elmeg logo, bintec trademarks and the bintec logo, elmeg trademarks and the elmeg logo are registered trademarks of bintec elmeg 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.bintec-elmeg.com* .

How to reach bintec elmeg GmbH
bintec elmeg GmbH, Südwestpark 94, D-90449 Nuremberg, Germany, Phone: +49 911 9673 0, Fax: +49 911 688 07 25
Teldat 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.teldat.fr*

Table of Contents

Chapter 1 Introduction

The new generation access points are manufactured in an environmentally friendly way and meet the RoHS directive. They support the latest WLAN technology and are designed for use particularly in the professional environment.

Safety notices

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

Installation

How to connect your device is shown in chapter *Installation* on page 6.

Configuration

Chapter *Basic configuration* on page 17 also tells you what preliminary tasks are necessary for configuration. You will then be shown how you can access your device from a Windows PC using a current web browser and how to make basic settings.

Password

If you are familiar with the configuration of bintec elmeg devices and you want to get started right away, all you really need to know is the preset user name and password.

User Name: `admin`

Password: `admin`

Note

Remember to change the password immediately when you log in to the device for the first time. All bintec elmeg 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 24.

Workshops

Step-by-step instructions for the most important configuration tasks can be found in the separate **Application Workshop** guide for each application, which can be downloaded from the *www.bintec-elmeg.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.

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

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

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

Chapter 2 About this guide

This document is valid for bintec elmeg devices with system software as of software version 9.1.9.

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

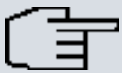
User's Guide - Reference

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** **Wireless LAN Controller** **Networking** **Routing Protocols** **Multicast**	All the configuration options of the **GUI** are described in this chapter. 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
WAN **VPN** **Firewall** **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

Symbol	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, e.g. `ping 192.168.0.252`	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.bintec-elmeg.com*	Indicates hyperlinks.

Chapter 3 Installation

Note

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

3.1 bintec W1003n, W2003n, W2003n-ext and W2004n

3.1.1 Setting up and connecting

Note

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

The devices **bintec W1003n**, **bintec W2003n** and **bintec W2004n** are equipped integrated antennas. Their radiation is optimized for ceiling mounting.

The device **bintec W2003n-ext** uses included external antennas.

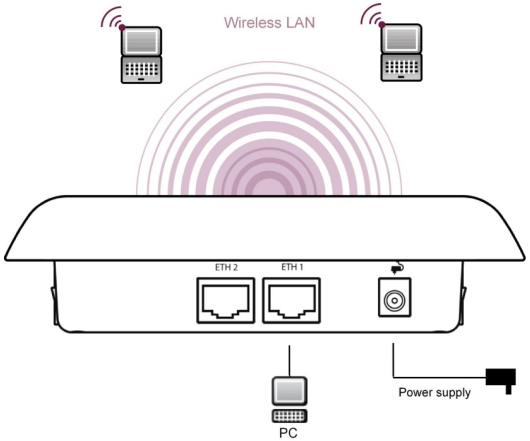


Fig. 2: Connection options **bintec W2003n** *,* **bintec W2003n-ext***,* **bintec W2004n**

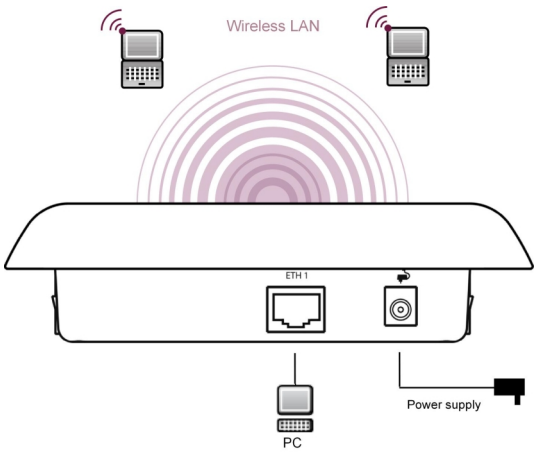


Fig. 3: Connection options **bintec W1003n**

When setting up and connecting, carry out the steps in the following sequence:

(1) Antennas

For **bintec W2003n-ext** screw the standard antennas supplied on to the connectors provided for this purpose. If you are using alternative antennas, please note that you have to connect MIMO antennas to the ports Ant 1 and Ant 2 and a SIMO antenna to port Ant1.

(2) LAN

For the standard configuration of your device via Ethernet, connect port **ETH1** or **ETH2** of your device to your LAN using the Ethernet cable supplied. **bintec W1003n** has a single Gigabit Ethernet port, **ETH1**.

The device automatically detects whether it is connected to a switch or directly to a PC.

Use just one of the ports **ETH1** and **ETH2**, the second port is used to cascade a number of devices. If you use both Ethernet connections on the same switch, loops may be formed.

The standard patch cable (RJ45-RJ45) is symmetrical. It is therefore not possible to mix up the cable ends.

(3) Power connection

Note

The devices **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** and **bintec W2004n** are supplied without a mains unit. The power adapter with EU plug (part number 5500001254) is available as an accessory.

Connect the device to a mains socket. Use the power cord and insert it in the appropriate socket on your device. Now plug the power cord into a power socket

(100–240 V). The status LED signal that your device is correctly connected to the power supply. Optionally, power can be supplied through a standard PoE injector (part number 5530000082).

Installation

The access points are to be mounted either on the wall or on the ceiling, or use as a table-top device.

Use as a table-top device

Attach the four self-adhesive feet on the bottom of the device. Place your device on a solid, level base.

Wall-/ Ceilingmounting

To attach the devices **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** or **bintec W2004n** to the wall or ceiling, use the appropriate support is included (part number 5500001278).

Warning

Before drilling, make sure that there are no building installations where you are drilling. If gas, electricity, water or waste water lines are damaged, you may endanger your life or damage property.

- Screw the mount to the wall or ceiling.
- Hang the device in the mount with the screw nut but do not tighten it. Make sure the device connections are accessible.
- If desired, protect the device against theft with a Kensington lock.

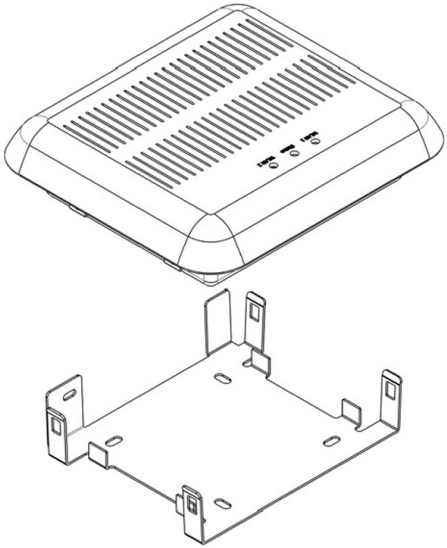


Fig. 4: Ceiling of **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** *and* **bintec W2004n**

3.1.2 Connectors

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

bintec W1003n has an Ethernet port, **bintec W2003n**, **bintec W2003n-ext** and **bintec W2004n** have two Ethernet ports.

The connections are arranged as follows:

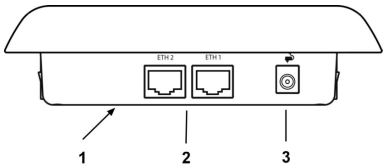


Fig. 5: Underside **bintec W2003n**, **bintec W2003n-ext** *and* **bintec W2004n**

Underside of bintec W2003n, bintec W2003n-ext and bintec W2004n

1	RESET	Reset button performs restart (base plate of the device)
2	ETH1/PoE und ETH2	10/100/1000 Base-T Ethernet interfaces. In **bintec W1003n** only ETH1 is available!

3	POWER	Socket for power supply

3.1.3 LEDs

The LEDs show the radio status and radio activity of your device.

Note

Note that the number of active WLAN LEDs depends on the number of existing wireless modules.

The LEDs on **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** and **bintec W2004n** are arranged as follows:

Fig. 6: LEDs of **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** *and* **bintec W2004n**

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

LED status display

LED	Status	Information
Status (green)	off	The power supply is not connected. If other LEDs are on, also Error.
	on (static)	Error
	on (flashing)	Ready
WLAN 1/2 (grün)	off	Radio or all assigned VSS inactive
	on (slowly flashing)	VSS is active, no client connected
	on (fast flashing)	VSS is active, at least one client connected
	on (flickering)	VSS is active, at least one client connected, active data traffic

You can choose from three different operation modes of the LEDs in the **Global Settings** menu as well as with the **WLAN Controller**.

Note

If you change the LED behavior through the **GUI** or the **WLAN Controller**, this setting is preserved if you reset the device to the ex-works state.

State	Only the status LED flashes once per second.
Flashing	All LEDs show their standard behavior.
Off	All LEDs are deactivated.

3.1.4 Scope of supply

Your device comes with the following accessories:

	Cable sets/mains unit/other	Software	Documentation
bintec W1003n	Ethernet cable (RJ-45, STP) Self-adhesive feet Wall or ceiling mounting	Companion DVD	Quick Install Guide (printed) R&TTE Compliance Information (printed) User's Guide (on DVD) Safety notices
bintec W2003n	Ethernet cable (RJ-45, STP) Self-adhesive feet Wall or ceiling mounting	Companion DVD	Quick Install Guide (printed) R&TTE Compliance Information (printed) User's Guide (on DVD) Safety notices
bintec W2003n-ext	Ethernet cable (RJ-45, STP) 4 external standard RSMA antennas Self-adhesive feet Wall or ceiling mounting	Companion DVD	Quick Install Guide (printed) R&TTE Compliance Information (printed) User's Guide (on DVD) Safety notices
bintec W2004n	Ethernet cable (RJ-45, STP) Self-adhesive feet Wall or ceiling mounting	Companion DVD	Quick Install Guide (printed) R&TTE Compliance Information (printed) User's Guide (on DVD)

	Cable sets/mains unit/other	Software	Documentation
			Safety notices

3.1.5 General Product Features

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

The features are summarised in the following table:

General Product Features

Property	Value
Dimensions and weights:	
Equipment dimensions without cable (W x L x H)	ca. 162 x 145 x 45 mm
Weight	approx. 1,000 g (with WLAN modules)
LEDs	**bintec W1003n**: 3 (1x Power, 1x WLAN, 1x Ethernet) **bintec W2003n**, **bintec W2003n-ext** and **bintec W2004n**: 4 (1x Power, 2x WLAN, 2x Ethernet)
Power consumption of the device	max. 12 W
Voltage supply	9 V, 1.3 A (The power adapter with the part number 5500001254 is available as an accessory.) PoE an Ethernet 1 Class 0, according to 802.3af (max. 12.4 W). The Gigabit PoE Injector with part number 5530000082 is available as an accessory.
Environmental requirements:	
Storage temperature	-40 °C to +85 °C
Operating temperature	0 °C to +40 °C
Relative atmospheric humidity	10 % to 100 %
Available interfaces:	
WLAN	**bintec W1003n**: 1 Radio module 802.11abgn 2,4 oder 5GHz Mimo 2x2 **bintec W2003n**: 1 Radio module 802.11bgn 2,4GHz Mimo 2x2; 1 Radiomodul 802.11an 5GHz Mimo 2x2 **bintec W2003n-ext**: 1 Radio module 802.11abgn 2,4 or 5GHz Mimo 2x2; 1 Radio module 802.11abgn 2,4 or 5GHz Mimo 2x2

Property	Value
	bintec W2004n: 1 Radio module 802.11bgn 2,4GHz Mimo 3x3; 1 Radiomodul 802.11an 5GHz Mimo 3x3
Ethernet IEEE 802.3 LAN	10/100/1000 mbps
Available sockets:	
Ethernet interface	**bintec W1003n**: 1 RJ45 socket **bintec W2003n**, **bintec W2003n-ext** and **bintec W2004n**: 2 RJ45 sockets
Antennas:	
Antenna connection	**bintec W1003n**: 2 internal antennas **bintec W2003n**: 4 internal antennas **bintec W2003n-ext**: 4 externe dualband antennas **bintec W2004n**: 6 internal antennas
Transmit Power (WLAN)	max. 100 mW (20 dBm) EIRP
Standards & Guidelines	R&TTE Directive 1999/5/EC EN 60950-1 (IEC60950); EN 60950-22; EN 301489-1; EN301489-17; EN 55022; EN 300328-1; EN 301893; EN 302502; EN 50371
Buttons	Reset

3.1.6 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 bottom of the device.

All existing configuration data will be deleted.

For **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** and **bintec W2004n** proceed as follows:

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

(2) Keep the **Reset** button on your device pressed.

(3) Look at the LEDs:
The Staus LED is lit. the device runs through the boot sequence.
When the Status LED starts flashing again, release the **Reset** button.

You can now configure your device again as described from *Basic configuration* on page 17

.

Note

If you delete the boot configuration using the **GUI**, all passwords will also be reset and the current boot configuration deleted. The next time, the device will boot with the standard ex works settings.

Note

If you have changed the LED behavior to something other then the default value, this setting is preserved after resetting the device.

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 Pin Assignments

3.3.1 Ethernet interface

The devices **bintec W2003n**, **bintec W2003n-ext** and **bintec W2004n** have two 10/100/1000 Ethernet interfaces, **bintec W1003n** has one 10/100/1000 Ethernet interface.

The connection is made via an RJ45 socket.

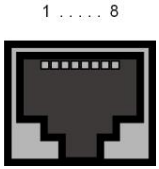


Fig. 7: Ethernet 10/100/1000 BASE-T interface (RJ45 socket)

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

RJ45 socet for LAN connection

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

3.4 Frequencies and channels

Different certification regulations apply around the world. ETSI standards generally apply (predominantly used in Europe). For operation in Europe, please read the notes in the R&TTE Compliance Information.

3.5 Support information

If you have any questions about your new product or are looking for additional information, the bintec elmeg GmbH Support Centre can be reached Monday to Friday between the hours of 9 am and 5 pm. They can be contacted as follows:

International Support Coordination	Telephone: +49 911 9673 0 Fax: +49 911 688 0725

For detailed information about our support and service offers please visit our website at *www.bintec-elmeg.com* .

3.6 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 4 Basic configuration

You can use the **Dime Manager** (IP address assignment) and the **GUI** (other configuration steps) for the basic configuration of your device.

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

This user's guide assumes you have the following basic knowledge:

- Basic knowledge of network structure
- Knowledge of basic network terminology, such as server, client and IP address
- Basic knowledge of using Microsoft Windows operating systems

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

You can find other useful applications on the Internet at *www.bintec-elmeg.com*.

4.1 Presettings

4.1.1 Preconfigured data

You have three ways of accessing your device in your network to perform configuration tasks:

(a) Dynamic IP address

In ex works state, your device is set to DHCP client mode, which means that when it is connected to the network, it is automatically assigned an IP address if a DHCP server is run. You can then access your device for configuration purposes using the IP address assigned by the DHCP server. For information on determining the dynamically assigned IP address, please see your DHCP server documentation.

(b) Fallback IP address

If you do not run a DHCP server, you can connect your device directly to your configuration PC and then reach it using the following, predefined fallback IP configuration:

- **IP Address**: `192.168.0.252`
- **Netmask**: `255.255.255.0`

Make sure that the PC from which the configuration is performed has a suitable IP

configuration (see *Configuring a PC* on page 21).

(c) Assigning a fixed IP address

You can use the **Dime Manager** to assign a new IP address and the required password to your device.

Note

Please note:

If your device has obtained an IP address dynamically from a DHCP server operated in your network for the basic configuration, the fallback IP address 192.168.0.252 is deleted automatically and your device will no longer function over this address.

However, if you have set up a connection to the device over the fallback IP address 192.168.0.252 or have assigned an IP address with the **Dime Manager** in the basic configuration, you will only be able to access your device over this IP address. The device will no longer obtain an IP configuration dynamically over DHCP.

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

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

Note

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

How to change the passwords is described in *Modify system password* on page 24.

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 **GUI** using the **Maintenance**->**Software &Configuration** menu.

For a description of the update procedure, see *Software Update* on page 26.

4.2 System requirements

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

- Internet Explorer oder Mozilla Firefox
- Installed network card (Ethernet)
- DVD drive
- TCP/IP protocol installed (see *Configuring a PC* on page 21)

4.3 Preparation

To prepare for configuration, you need to...

- Obtain the data required for the basic configuration.
- Check whether the PC from which you want to perform the configuration meets the necessary requirements.
- install the **Dime Manager** software, which provides more tools for working with your device.

4.3.1 Gathering data

The main data for the basic configuration can be gathered quickly, as no information is required that needs in-depth network knowledge. If applicable, you can use the example values.

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

- IP configuration (obligatory if your device is in the ex works state)

Note

bintec W1003n, **bintec W2003n**, **bintec W2003n-ext** and **bintec W2004n** do not support WDS or Bridge Links.

- Optional: Configuration of a wireless network connection in Access Point mode
- Optional: Configuration of client links in Client Links mode
- Optional: Configuration of bridge links in Bridge mode.

The following table shows 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:

IP configuration of the access point

Access data	Example value	Your values
IP address of your access point	*192.168.0.252*	
Netmask of your access point	*255.255.255.0*	

Access Point mode

If you run your device in Access Point mode, you can set up the required wireless networks. To do this, you need the following data:

Configuration of a wireless network

Access data	Example value	Your values
Network Name (SSID)	*default*	
Security mode	*WPA-PSK*	
Preshared key	*supersecret*	

Access Client mode

If you run your device in Access Client mode, you can set up the required client links. To do this, you need the following data:

IP configuration of the access client

Access data	Example value	Your values
Network Name (SSID)	*default*	
Security mode	*WPA-PSK*	
Preshared key	*supersecret*	

4.3.2 Configuring a PC

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

- Make sure that the TCP/IP protocol is installed on the PC.
- Select the suitable IP configuration for your configuration PC.

  The PC via which you want to configure the IP address for your device must be in the same network as your device.

Checking the Windows TCP/IP protocol

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

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

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

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

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

Installing the Windows TCP/IP protocol

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

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

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

(3) Click **Add**.

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

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

Allocating PC IP address

Allocate an IP address to your PC as follows:

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

(2) Choose **Use following IP address** and enter a suitable IP address, the matching netmask, your default gateway and your preferred DNS server.

If you run a DHCP server in your network, you can apply the default Windows setting **Obtain IP address automatically** and **Obtain DNS server address automatically**.

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

4.4 IP configuration

In the ex works state, your device is configured in DHCP Client mode and therefore dynamically receives an IP address if you run a DHCP server in your network. If this is not the case, connect your device directly to the configuration PC and use the fallback IP address `192.168.0.252`.

Alternatively, you can assign your device the required fixed IP address by using the **Dime Manager**.

To do this, install the program from the DVD provided to your configuration PC.

Proceed as follows:

(a) Place the DVD provided in the DVD drive of your configuration PC. The installation wizard should start automatically. If it does not, open the following file on the DVD using your file browser: `starter.exe`.

(b) Follow the instructions in the installation wizard.

Then carry out the following steps to configure an IP address for your device:

(1) Start the **Dime Manager** from the Windows Start menu: **Start** -> **Programs** ->-> **Dime Manager**.
The following dialog box appears:

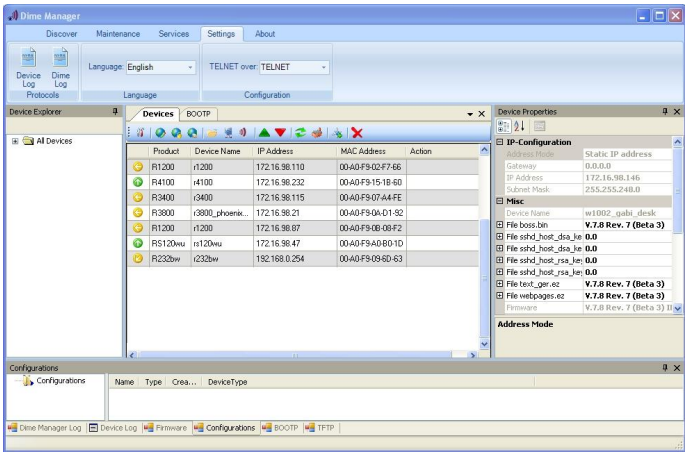


Fig. 9: **Dime Manager** *initial screen*
The **Dime Manager** detects the devices installed in the network.

(2) In the list, double click the device you want to configure.
The following dialog box appears:

Fig. 10: IP address assignment with the **Dime Manager**

(3) Enter the network parameters (**Device name**, **IP address**, **Netmask** and **Gateway**) and click on **OK**.

Note

The maximum length of the **Device name** parameter is 32 characters.

The **Device name** parameter may contain only the letters "a"-"z", "A"-"Z", the digitss "0"-"9", dash "-" and dot "." to avoid errors by other systems during interpretation of the **Device name**. The first character must be a letter, and the last character cannot be a dot "." or dash "-". A single character is not permitted as a name.

Your device can now be reached over the Ethernet with its IP address using a Web browser and can now be configured.

GUI Call up

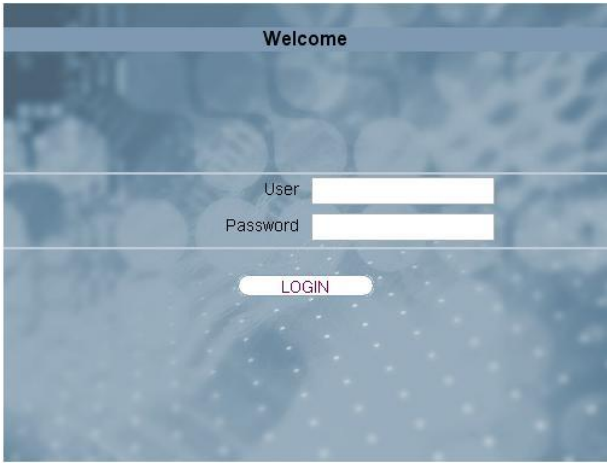


Fig. 11: **GUI** *Login*

Start the configuration interface as follows:

(a) Enter the IP address of your device in the address line of your Web browser.

With DHCP server:

- the IP address that the DHCP server assigned to your device

Without DHCP server:

- With direct connection to the configuration PC: the fallback IP address `192.168.0.252`
- The fixed IP address assigned via the **Dime Manager**

Press the **Enter (Return) key**.

(b) Enter `admin` in the **User** field and `admin` in the **Password** field.

4.5 Modify system password

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

Proceed as follows:

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

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

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

(d) Click **OK**.

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

Note the following rules on password use:

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

4.6 Setting up a wireless network

Proceed as follows to use your device as an access point:

(1) In **GUI** 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.

Configuring the WLAN Adapter under Windows 7

A popup window informs you about all wireless networks within reach. All you have to do is to configure your connection.

(1) First, click the WLAN icon in the system tray of the task bar. Now Windows 7 displays you all wireless networkswithin your reach.

(2) Select the VSS of your device and click **Connect**.

(3) In the opening window, enter the preshared key you have configured for your VSS and click OK.

4.7 Software Update

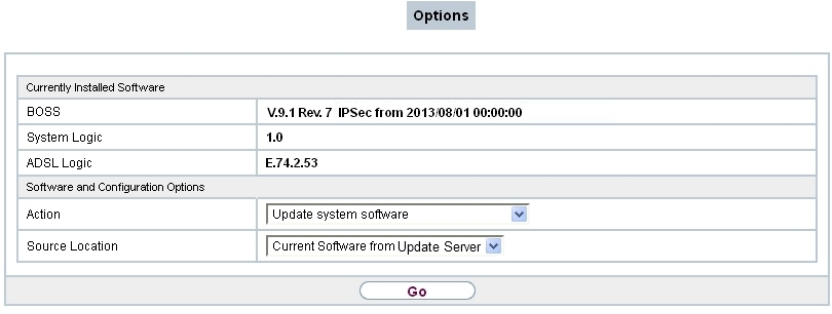
The range of functions of bintec elmeg devices is continuously being extended. These extensions are made available to you by bintec elmeg GmbH free of charge. Checking for new software versions and the installation of updates can be carried out easily with the **GUI**. An existing internet connection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

Proceed as follows:

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

(2) Under **Action** select *Update System Software* and, under **Source Location** *Latest Software from Update Server.*

(3) Confirm with **Go**.



The device will now connect to the bintec elmeg GmbH download server and check wheth-

er an updated version of the system software is available. If so, your device will be updated automatically. When installation of the new software is complete, you will be invited to re-start the device.

Caution

After confirming with **Go**, the update cannot be aborted. If an error occurs during the update, do not re-start the device and contact support.

Chapter 5 Access and configuration

This chapter describes all the access and configuration options.

5.1 Access Options

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

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

- Via your LAN
- Via the serial interface

5.1.1 Access via LAN

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

Caution

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

5.1.1.1 HTTP/HTTPS

With a current web browser, you can use the HTML interfaces to configure your device.

The configuration can be set up using the **GUI**. To do this, enter the IP address of your device in the address field of your Web browser.

With DHCP server:

- the IP address that your DHCP server assigned to your device

Without DHCP server:

- With direct connection to the configuration PC: the fallback IP address `192.168.0.252`
- The fixed IP address assigned via the **Dime Manager**

Press the **Enter (Return) key**.

5.1.1.2 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 34.

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 34.

5.1.1.3 SSH

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

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

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

Encryption keys

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

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

see *Login* on page 33).

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

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

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

```
Flash-Sh > ls -al

Flags Version Length Date Name ...

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

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

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

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

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

Flash-Sh >
```

Note

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

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

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

(2) Launch the **GUI** and log on to your device (see *Calling up GUI* on page 36).

(3) Make sure that *English* 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 key and stores it in the FlashROM. *Generated* indicates that generation was successful.

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

Login via SSH

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

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

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

UNIX

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

(2) Continue with *Login* on page 33.

Windows

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

(2) Continue with *Login* on page 33.

Note

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

5.1.2 Access via the Serial Interface

Your device 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 (192.168.0.252/255.255.255.0).

Windows

To connect your device to your PC via the serial interface, proceed as described in *Installation* **on page 6**.

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) Click on **Programs** -> **Accessories** -> **HyperTerminal** in the Windows Start menu.

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

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

Check

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

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

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

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

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

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

(5) Click **OK**.

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

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

Unix

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

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

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

5.2 Login

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

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

5.2.1 User names and passwords in ex works state

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

User names and passwords in ex works state

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

It is only possible to change and save configurations if you log in with the user name `admin`. Access information (user names and passwords) can also only be changed if you log in with the user name `admin`. For security reasons, passwords are normally shown 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 elmeg devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. How to change the passwords is described in 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.

5.2.2 Logging in for Configuration

Set up a connection to the device. The access options are described in *Access Options* on page 28.

GUI (Graphical User Interface)

Log in via the HTML surface as follows:

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

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

The status page of the **GUI** opens in the browser.

SNMP shell

Log into the SNMP shell as follows:

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

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

Your device logs in with the input prompt, e.g. `w1002:>`. 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**.

5.3 Configuration options

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

You can configure your device in the following ways:

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

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

Types of connections and configurations

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

Therefore, several types of configuration are available for each type of connection.

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.

5.3.1 GUI for advanced users

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

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

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

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

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

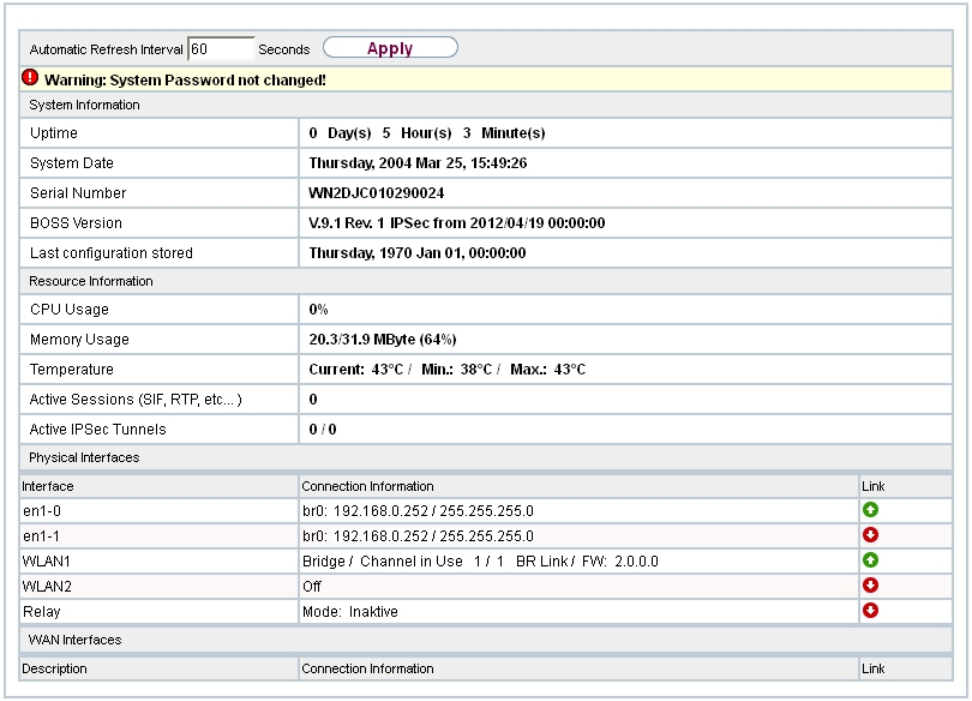


Fig. 12: **GUI** *home page*

5.3.1.1 Calling up GUI

(1) Check whether the device is connected and switched on and that all the necessary cables are correctly connected.

(2) Check the settings of the PC from which you want to configure your device (see *Configuring a PC* on page 21).

(3) Open a Web browser.

(4) Enter `http://192.168.0.252` (or the IP address dynamically assigned by your DHCP server or the address statically assigned by you with the **Dime Manager**) in the web browser's address field.

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

You are not in the status menu of your device's **GUI** (see *Status* on page 48).

5.3.1.2 Operating elements

GUI window

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

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

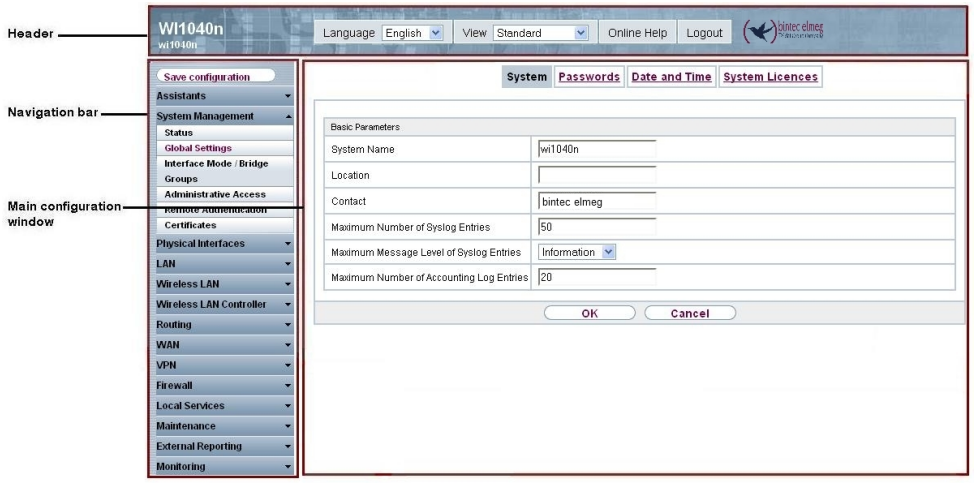


Fig. 13: Areas of the **GUI**

Header

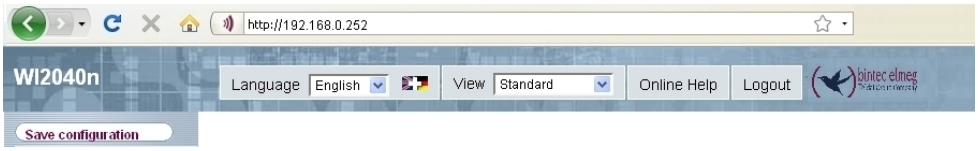


Fig. 14: **GUI** *header*

GUI header

Menu	Position
Language English	**Language**: In the dropdown menu, choose the language in which you want to display the**GUI**. 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	Position
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. 15: Save Configuration button

Fig. 16: 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 **GUI**, 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 and backup previous boot configuration*, i.e. save the current configuration as the boot configuration and also archive the previous boot configuration as a backup.

If you want to load the archived boot configuration into your device, go to the

->**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 **GUI**, the status page of your device is displayed after you log in. The most important data of your device can be seen on this at a glance.

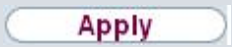
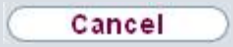
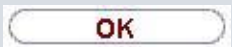
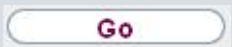
Main configuration window

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

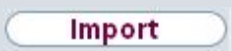
Configuration elements

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

GUI buttons

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

GUI buttons for special functions

Button	Position
	In the **System Management**->**Certificates**->**Certificate List**

Button	Position
	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.

Various icons indicate the following possible actions or statuses:

GUI symbols

Symbol	Position
	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.
	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:

GUI list options

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

Fig. 17: Configuration of the update interval

Fig. 18: Filter list

Structure of the GUI configuration menu

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

GUI Menu architecture

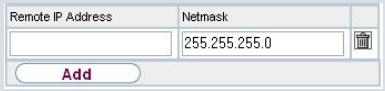
Menu	Position
Basic configuration menu/list	When you select a menu from the navigation bar, the menu of basic parameters is displayed first. In a sub-menu containing several pages, the menu containing the basic parameters is dis-

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

The following options are available for the configuration:

GUI configuration elements

Menu	Position
Input fields	e.g. empty text field  Text field with hidden input  Enter the data.
Radio buttons	e.g.  Select the corresponding option.
Checkboxes	e.g. activation by selecting checkbox  Selection of several possible options 
Dropdown menus	e.g.  Click the arrow to open the list. Select the required option using

Menu	Position
	the mouse.
Internal lists	e.g.  Click Add. A new list entry is created. Enter the corresponding data. If list input fields remain empty, these are not saved when you confirm with **OK**. Delete the entries by clicking the icon.

Display of options that are not available

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

Important

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

Warning symbols

Symbol	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 **GUI**, this can cause inconsistencies or malfunctions. Therefore, it is recommended that the configuration is continued with the Setup Tool.

5.3.1.3 GUI Menus

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

Note

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

5.3.2 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.

5.4 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.
, MAC address and software versions.

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


W1002 Bootmonitor V.7.9.1 Rev. 1 from 2009/10/19 00:00:00
Copyright (c) 1996-2005 by bintec elmeg 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> _
```

Fig. 19: BOOTmonitor

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

Chapter 6 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 7 System Management

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

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

7.1 Status

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

You see an overview of the following data:

- System status
- Your device's activities: Resource utilisation, active sessions and tunnels
- Status and basic configuration of LAN, WAN and WLAN interfaces

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

Caution

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

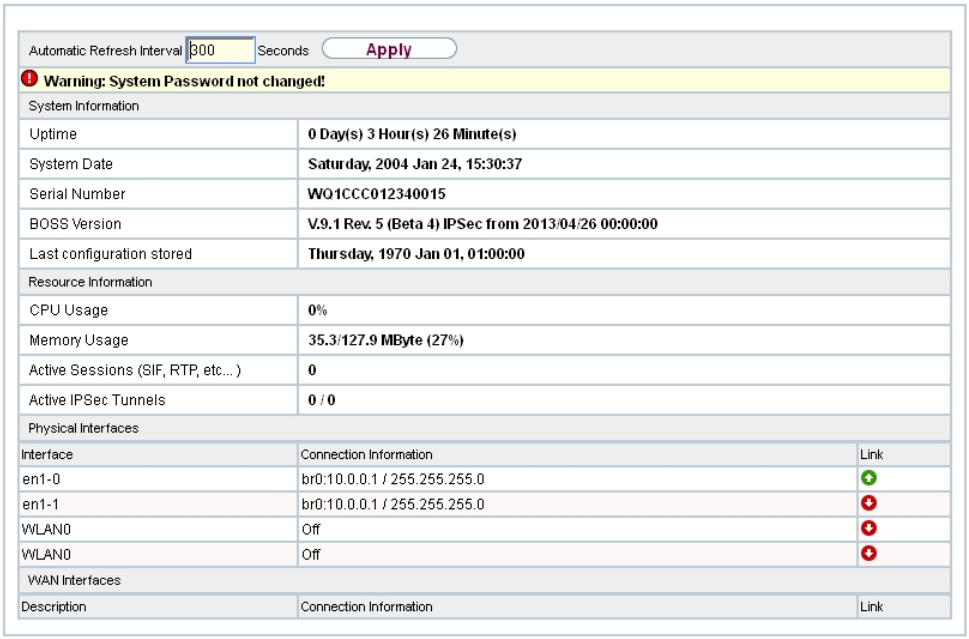


Fig. 20: **System Management->Status**

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 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.
Active Sessions (SIF, RTP, etc...)	Displays the total of all SIF, TDRC, and IP load balancing sessions.

Field	Value
Active IPSec Tunnels	Displays the number of currently active IPSec tunnels in relation to the number of configured IPSec tunnels.

Fields in the Physical Interfaces menu.

Field	Value
Interface - **Connection Information** - **Link**	The physical interfaces are listed here and their most important settings are shown. The system also displays whether the interface is connected or active. Interface specifics for Ethernet interfaces: • IP address • Netmask Interface specifics for serial/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 • Number of connected clients • Software version of the wireless card

Fields in the WAN Interfaces menu.

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

7.2 Global Settings

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

7.2.1 System

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

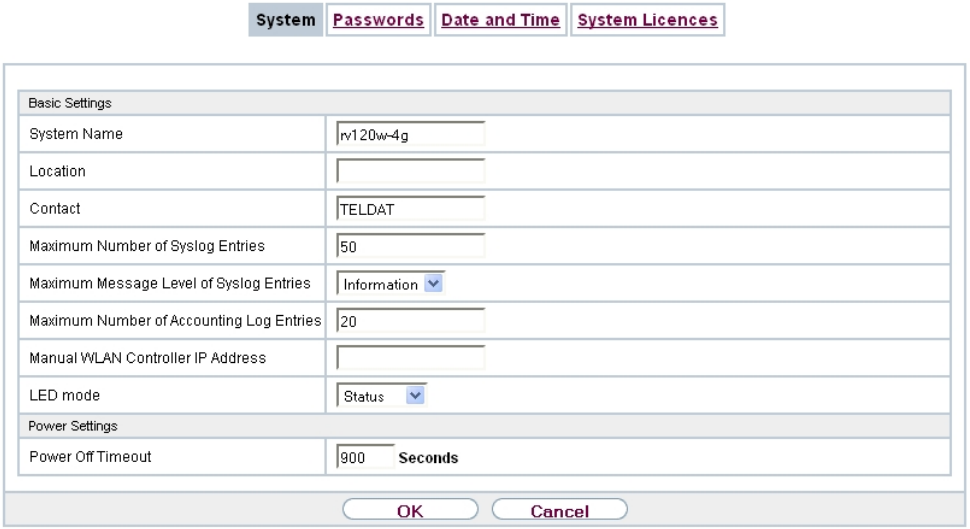


Fig. 21: **System Management**->**Global Settings**->**System**

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

Fields in the menu Basic Settings

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

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

Field	Value
Maximum Number of Accounting Log Entries	Enter the maximum number of login process entries that are stored internally in the device. Possible values are *0* to *1000*. The default value is *20*.
Manual WLAN Controller IP Address	This function is only available on devices with a wireless LAN controller. Enter the IP address of the WLAN controller. The value can only be modified it the WLAN controller function is enabled.
LED mode	This function is only available for **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** and **bintec W2004n**. Select the LEDs' lighting behaviour. Possible values: • *Status* (default value): The LEDS display their default behaviour. • *Flashing*: Only the status LED flashes once per second. • *Off*: All LEDs are disabled.

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

Field	Value
Power Off Timeout	Enter the time, in seconds, for how long the device is to remain switched on after switching the motor off. The default value is *900* seconds.

7.2.2 Passwords

Setting the passwords is another basic system setting.

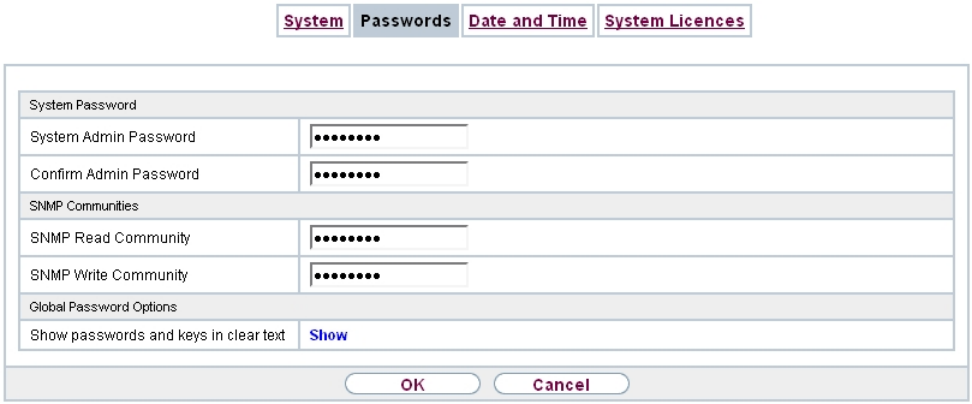


Fig. 22: **System Management->Global Settings->Passwords**

Note

All bintec elmeg devices are delivered with the same username and password. As long as the password remains unchanged, they are not protected against 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 System Password menu.

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

Fields in the SNMP Communities menu.

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

Field	Value
munity	

Fields in the Global Password Options menu

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

7.2.3 Date and Time

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

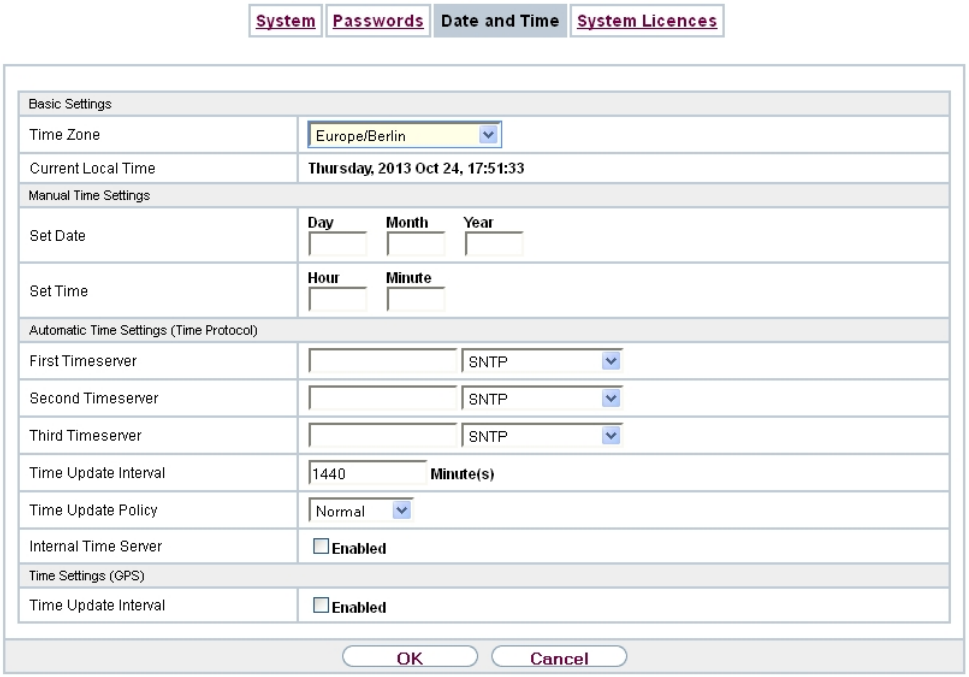


Fig. 23: **System Management->Global Settings->Date and Time**

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

ISDN/Manual

In devices with an ISDN interface, the system time can be updated via ISDN, i. e. the date and time are taken from the ISDN when the first outgoing call is made. The time can also be set manually on the device.

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

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

Time server

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

Note

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

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

Fields in the menu Basic Settings

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

Fields in the menu Manual Time Settings

Field	Description
Set Date	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 menu Automatic Time Settings (Time Protocol)

Field	Description
ISDN Timeserver	Only for devices with an ISDN interface. Determine whether the system time is to be updated via ISDN. If a time server is configured, the time is only determined over ISDN until a successful update is received from this time server. Updating over ISDN is deactivated for the period in which the time is determined by means of a time server. The function is activated by selecting *Enabled*. The function is disabled by default.
First Timeserver	Enter the primary time server, by using either a domain name or an IP address. In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol via UDP port 123. • *Time Service / UDP*: This server uses the Time service with UDP port 37. • *Time Service / TCP*: This server uses the Time service with TCP port 37. • *None*: This time server is not currently used for the time request.
Second Timeserver	Enter the secondary time server, by using either a domain name or an IP address. In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol via UDP port 123. • *Time Service / UDP* : This server uses the Time service with UDP port 37. • *Time Service / TCP* : This server uses the Time service with TCP port 37.

Field	Description
	• *None*: This time server is not currently used for the time request.
Third Timeserver	Enter the third time server, by using either a domain name or an IP address. In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol via UDP port 123. • *Time Service / UDP*: This server uses the Time service with UDP port 37. • *Time Service / TCP*: This server uses the Time service with TCP port 37. • *None*: This time server is not currently used for the time request.
Time Update Interval	Enter the time interval in minutes at which the time is automatically updated. The default value is *1440*.
Time Update Policy	Enter the time period after which the system attempts to contact the time server again following a failed time update. Possible values: • *Normal* (default value): The system attempts to contact the time server after 1, 2, 4, 8, and 16 minutes. • *Aggressive*: For ten minutes, the system attempts to contact the time server after 1, 2, 4, 8 seconds and then every 10 seconds. • *Endless*: For an unlimited period, the system attempts to contact the time server after 1, 2, 4, 8 seconds and then every 10 seconds. If certificates are used to encrypt data traffic in a VPN, it is extremely important that the correct time is set on the device. To ensure this is the case, for **Time Update Policy**, select the value *Endless*.

Field	Description
Internal Time Server	Select whether the internal timeserver is to be used. The function is activated by selecting *Enabled*. Time requests from a client will be answered with the current system time. This is given as GMT, without offset. The function is disabled by default. Time requests from a client are not answered.

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

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

7.2.4 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.bintec-elmeg.com* .

Entering licence data

You can obtain the licence data for extra licences via the online licensing pages in the sup-

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

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

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

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

Possible values for Status

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

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

Note

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

7.2.4.1 Edit or New

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

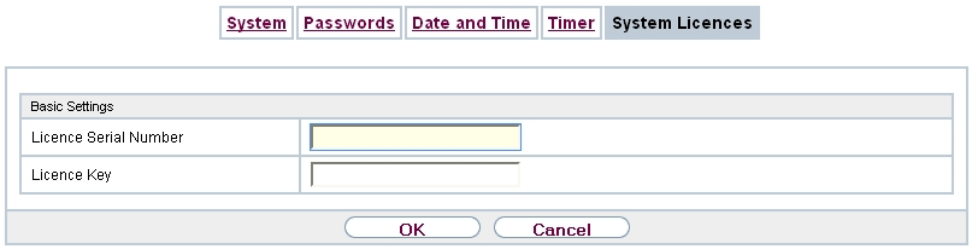


Fig. 24: **System Management**->**Global Settings**->**System Licences**->**New**

Activating extra licences

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

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

Fields in the Basic Settings menu.

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

Note

If *Not OK* is displayed as the status:

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

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

Deactivating a licence

Proceed as follows to deactivate a licence:

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

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

(3) Confirm with **OK**.

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

7.3 Interface Mode / Bridge Groups

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

Routing versus bridging

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

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

Conventions for port/interface names

If your device has a radio port, it receives the interface name WLAN. If there are several radio modules, the names of wireless ports in the user interface of your device are made up of the following parts:

(a) WLAN

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

Example: *WLAN1* The name of the Ethernet port is made up of the following parts:

(a) ETH

(b) Number of the port

Example: *ETH1*

The name of the interface connected to an Ethernet port is made up of the following parts:

(a) Abbreviation for interface type, whereby *en* stands for internet.

(b) Number of the Ethernet port

(c) Number of the interface

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

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

(a) Abbreviation for interface type, whereby *br* stands for bridge group.

(b) Number of the bridge group

Example: *br0* (first bridge group)

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

Abbreviation for interface type, whereby *vss* stands for wireless network.

(a) Number of the wireless module

(b) Number of the interface

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

The name of the WDS link or bridge link is made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the wireless module on which the WDS link or bridge link is configured

(c) Number of the WDS link or bridge link

Example: *wds1-0* (first WDS link or bridge link on the first wireless module)

The name of the client link is made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the wireless module on which the client link is configured

(c) Number of the client link

Example: *sta1-0* (first client link on the first wireless module)

The name of the virtual interface connected to an Ethernet port is made up of the following parts:

(a) Abbreviation for interface type

(b) Number of the Ethernet port

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

(d) Number of the virtual interface

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

7.3.1 Interfaces

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

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

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

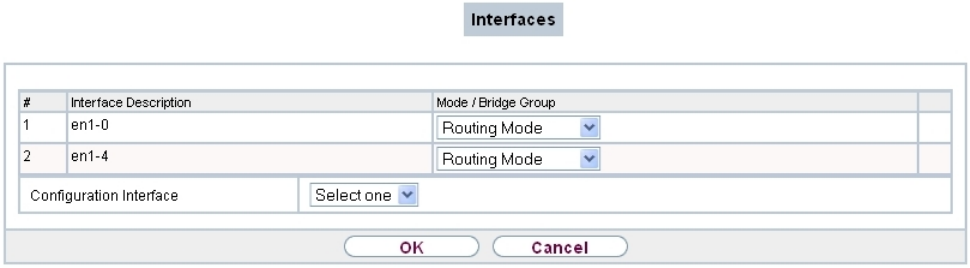


Fig. 25: **System Management->Interface Mode / Bridge Groups->Interfaces**

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

Fields in the Interfaces menu.

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

7.3.1.1 Add or Edit

Add

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

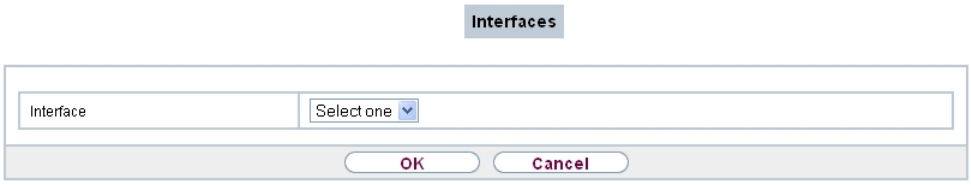


Fig. 26: **System Management->Interface Mode / Bridge Groups->Interfaces->Add**

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

Fields in the Interfaces menu.

Field	Description
Interface	Select the interface whose status should be changed.

Edit for devices the WIxxxxn and RS series

For WLAN clients in bridge mode (so-called MAC Bridge) you can also edit additional settings via the icon.

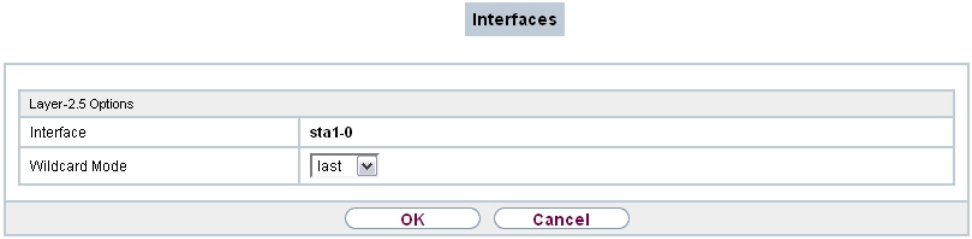


Fig. 27: **System Management->Interface Mode / Bridge Groups->Interfaces->Add**

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

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

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

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

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

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

use the MAC Bridge.

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

Fields in the Layer-2.5 Options menu.

Field	Value
Interface	Shows the interface that is being edited.
Wildcard Mode	Select the Wildcard mode you want to use on the interface. Possible values: • *none* (default value): Wildcard mode is not used. • *static*: With this setting, you must enter the MAC address of a device that is connected over IP under **Wildcard MAC Address**. Each packet without IP and without ARP is forwarded to this device. This occurs even when the device is no longer connected. • *first*: If you choose this setting, the MAC address of the first non-IP unicast frame or non-ARP unicast frame, which occurs on any of the Ethernet interfaces, is used as the wildcard MAC address. This wildcard MAC address can only be reset by rebooting the device or by selecting another wildcard mode. • *last*: If you choose this setting, the internal WLAN MAC address is used to establish a connection to the access point. As soon as a non-IP unicast frame or non-ARP unicast frame appears, it is forwarded to the MAC address from which the last non-IP unicast frame or non-ARP unicast frame was received on the Ethernet interface of the device. This wildcard MAC address is renewed with each non-IP unicast frame or non-ARP unicast frame.
Wildcard MAC Address	Only for **Wildcard Mode** = *static* Enter the MAC address of a device that is connected over IP.
Transparent MAC Address	Only for **Wildcard Mode** = *static*, *first* Choose whether or not the **Wildcard MAC Address** are used in addition as WLAN MAC address to establish the connection to the access point.

Field	Value
	The function is enabled with *Enabled*. The function is disabled by default.

7.4 Administrative Access

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

7.4.1 Access

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

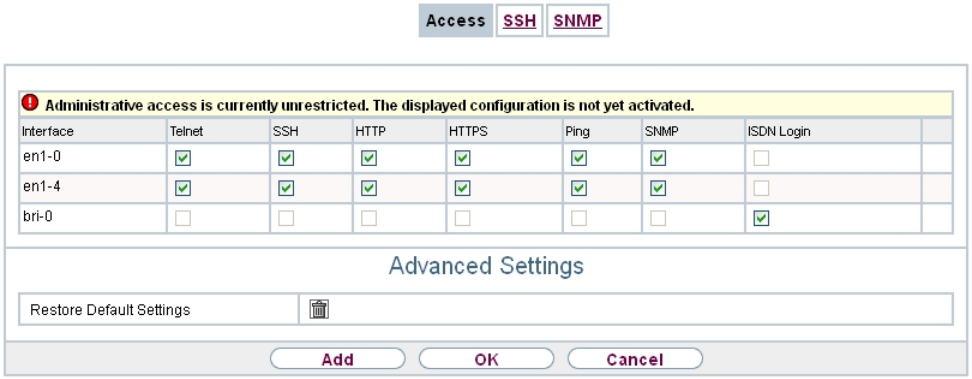


Fig. 28: **System Management**->**Administrative Access**->**Access**

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

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

Service Login (ISDN Web-Access) is disabled by default.

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

Fields in the menu Advanced Settings

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

7.4.1.1 Add

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

Fig. 29: **System Management**->**Administrative Access**->**Access**->**Add**

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

Fields in the menu Access

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

7.4.2 SSH

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

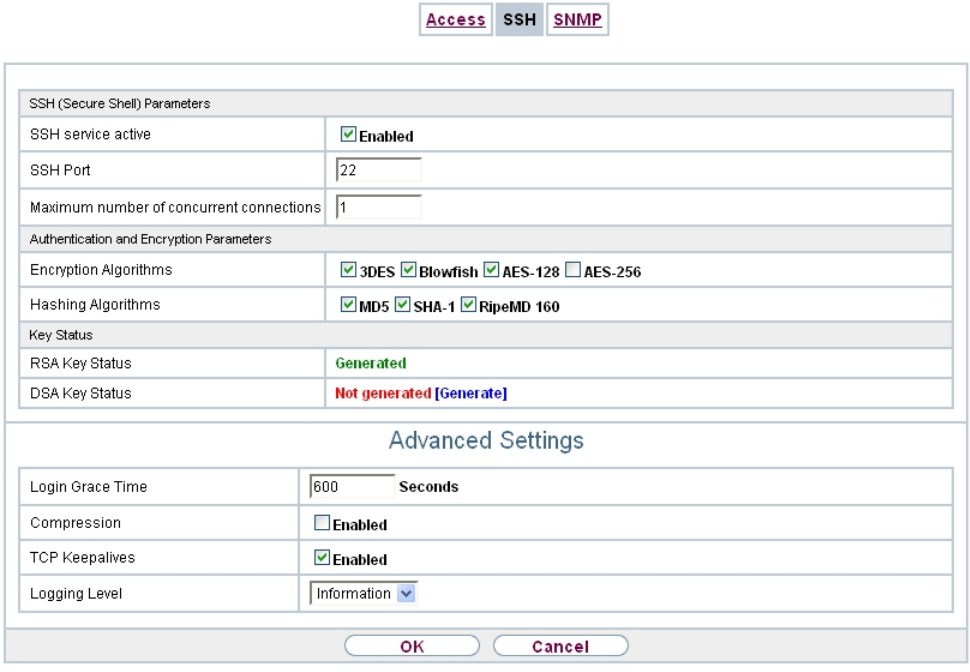


Fig. 30: **System Management->Administrative Access->SSH**

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

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

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

Note

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

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

Fields in the menu SSH (Secure Shell) Parameters

Field	Value
SSH service active	Select whether the SSH Daemon is to be enabled for the inter-

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

Fields in the menu Authentication and Encryption Parameters

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

Fields in the menu Key Status

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

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

Fields in the menu Advanced Settings

Field	Value
Login Grace Time	Enter the time (in seconds) that is available for establishing the connection. If a client cannot be successfully authenticated during this time, the connection is terminated. The default value is *600* seconds.

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

7.4.3 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.

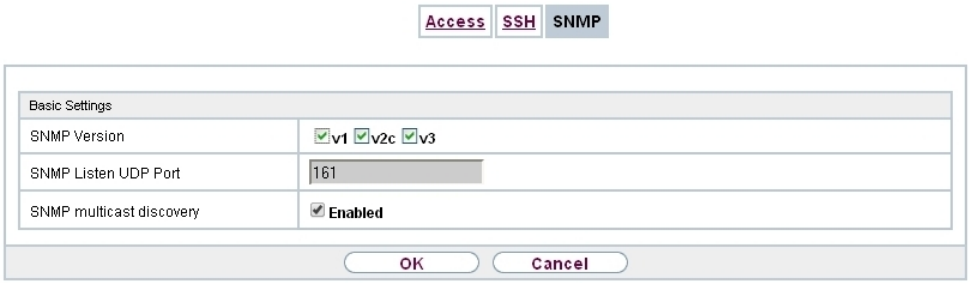


Fig. 31: **System Management->Administrative Access->SNMP**

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

Fields in the Basic Settings menu.

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

Tip

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

7.5 Remote Authentication

This menu contains the settings for user authentication.

7.5.1 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

Field	Value
	If an access request is received by your device, a request is sent to the RADIUS server if no corresponding connection partner has been found on your device.
ACCESS_ACCEPT	Server -> Client If the RADIUS server has authenticated the information contained in the ACCESS_REQUEST, it sends an ACCESS_ACCEPT to your device together with the parameters used for setting up the connection.
ACCESS_REJECT	Server -> Client If the information contained in the ACCESS_REQUEST does not correspond to the information in the user database of the RADIUS server, it sends an ACCESS_REJECT to reject the connection.
ACCOUNTING_START	Client -> Server If a RADIUS server is used for accounting, your device sends an accounting message to the RADIUS server at the start of each connection.
ACCOUNTING_STOP	Client -> Server If a RADIUS server is used for accounting, your device sends an accounting message to the RADIUS server at the end of each connection.

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

7.5.1.1 Edit or New

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

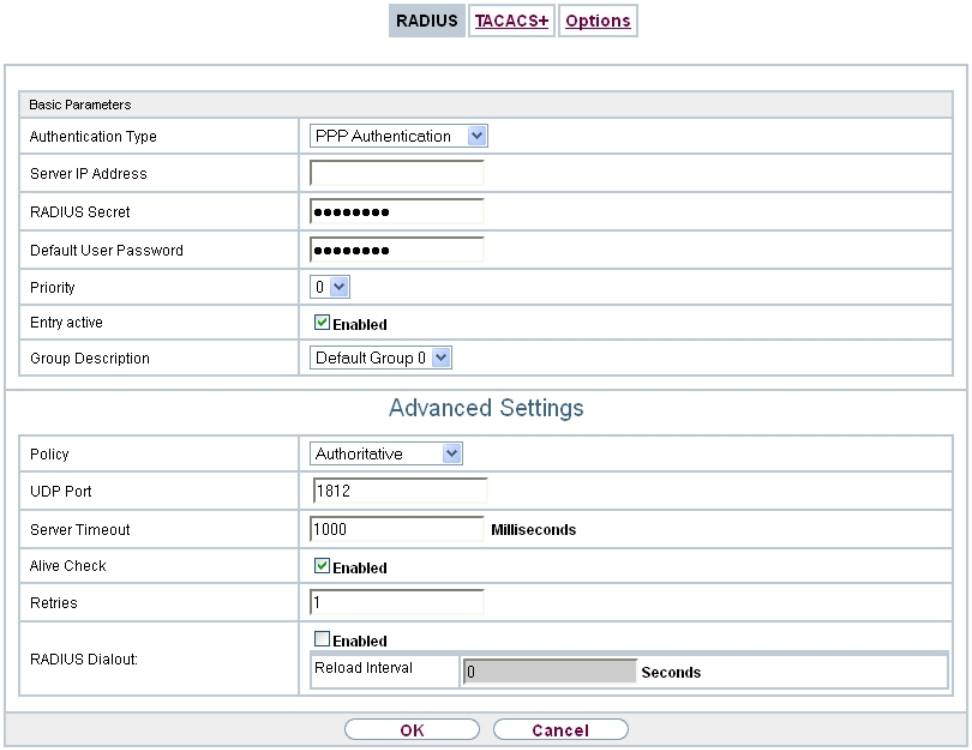


Fig. 32: **System Management->Remote Authentication->RADIUS->New**

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

Fields in the Basic Parameters menu.

Field	Value
Authentication Type	Select what the RADIUS server is to be used for. Possible values: • *PPP Authentication* (default value only for PPP connections): The RADIUS server is used for controlling access to a network. • *Accounting* (for PPP connections only): The RADIUS server is used for recording statistical call data. • *Login Authentication*: The RADIUS server is used for controlling access to the SNMP shell of your device. • *IPSec Authentication*: The RADIUS server is used for sending configuration data for IPSec peers to your device.

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

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

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

Fields in the Advanced Settings menu.

Field	Value
Policy	Select how your device is to react if a negative response to a request is received. Possible values: • *Authoritative* (default value): A negative response to a request is accepted. • *Non-authoritative* : A negative response to a request is not accepted. A request is sent to the next RADIUS server until your device receives a response from a server configured as authoritative.
UDP Port	Enter the UDP port to be used for RADIUS data. RFC 2138 defines the default ports 1812 for authentication (1645 in older RFCs) and 1813 for accounting (1646 in older RFCs). You can obtain the port to be used from the documentation for your RADIUS server. The default value is *1812*.
Server Timeout	Enter the maximum wait time between ACCESS_REQUEST and response in milliseconds. After timeout, the request is repeated according to **Retries** or the next configured RADIUS server is requested. Possible values are whole numbers between *50* and *50000*.

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

Field	Value
	ried out.

7.5.2 TACACS+

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

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

The following TACACS+ functions are available on your device:

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

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

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

7.5.2.1 Edit or New

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

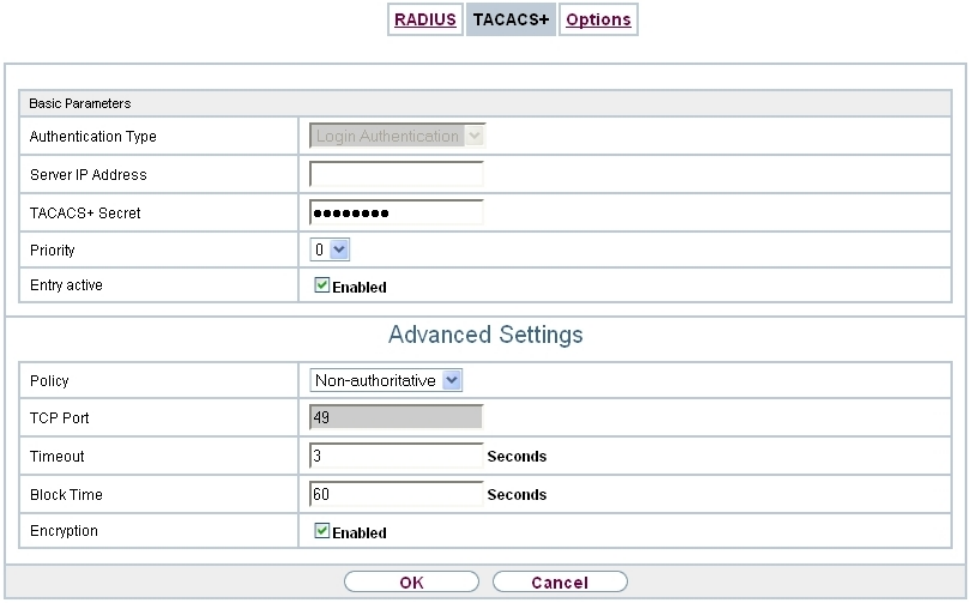


Fig. 33: **System Management->Remote Authentication->TACACS+ ->New**

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

Fields in the Basic Parameters menu.

Field	Description
Authentication Type	Displays which TACACS+ function is to be used. The value cannot be changed. Possible values: • *Login Authentication*: Here, you can define whether the current TACACS+ server is to be used for login authentication to your device.
Server IP Address	Enter the IP address of the TACACS+ server that is to be requested for login authentication.
TACACS+ Secret	Enter the password to be used to authenticate and, if applicable, encrypt data exchange between the TACACS+ server and the network access server (your device). The maximum length of the entry is 32 characters.
Priority	Assign a priority to the current TACACS+ server. The server with the lowest value is the one used first for TACACS+ login

Field	Description
	authentication. If no response is given or access is denied (only if **Policy** = *Non-authoritative*), the entry with the next-highest priority is used. The available values are *0* to *9*, the default value is *0*.
Entry active	Select whether this server is to be used for login authentication. The function is activated by selecting *Enabled*. The function is enabled by default.

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

Fields in the Advanced Settings menu.

Field	Description
Policy	Select the interpretation of the TACACS+ response. Possible values: • *Non-authoritative* (default value): The TACACS+ servers are queried in order of their priority (see **Priority**) until a positive response is received or a negative response has been received from an authoritative server. • *Authoritative*: A negative response to a request is accepted, i.e. a request is not sent to another TACACS+ server. The device's internal user administration is not turned off by TACACS+. It is checked after all TACACS+ servers have been queried.
TCP Port	Shows the default TCP port (*49*) used for the TACACS+ protocol. The value cannot be changed.
Timeout	Enter time in seconds for which the NAS is to wait for a response from TACACS+. If a response is not received during the wait time, the next configured TACACS+ server is queried (only if **Policy** = *Non-authoritative*) and the status of the current server is set to *Blocked*. The possible values are *1* to *60*, the default value is *3*.

Field	Description
Block Time	Enter the time in seconds for which the status of the current server shall remain blocked. When the block has ended, the server is set to the status specified in the **Entry active** field. The possible values are `0` to `3600`, the default value is `60`. The value `0` means that the server is never set to `Blocked` status and thus no other servers are queried.
Encryption	Select whether data exchange between the TACACS+ server and the NAS is to be encrypted with MD5. The function is activated by selecting `Enabled`. The function is enabled by default. If the function is not enabled, the packets and all related information are transferred unencrypted. Unencrypted transfer is not recommended as a default setting and should only be used for debugging.

7.5.3 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.

Fig. 34: **System Management->Remote Authentication->Options**

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

Fields in the Global RADIUS Options menu.

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

7.6 Configuration Access

In the **Configuration Access** menu you can configure user profiles.

To do so, you create access profiles and users and assign each user at least one access profile. An access profile makes available that part of the GUI that a user requires for their tasks. Parts of the GUI that are not required are blocked.

7.6.1 Access Profiles

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

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

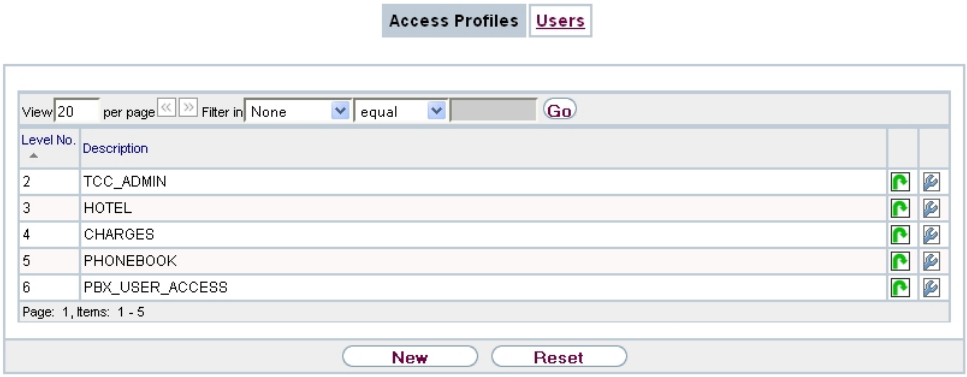


Fig. 35: **System Management->Configuration Access->Access Profiles**

7.6.1.1 Edit or New

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

To create an access profile you can use all the entries in the navigation bar of the GUI plus **Save configuration** and **Switch to SNMP Browser**. You can create a maximum of 29 access profiles.

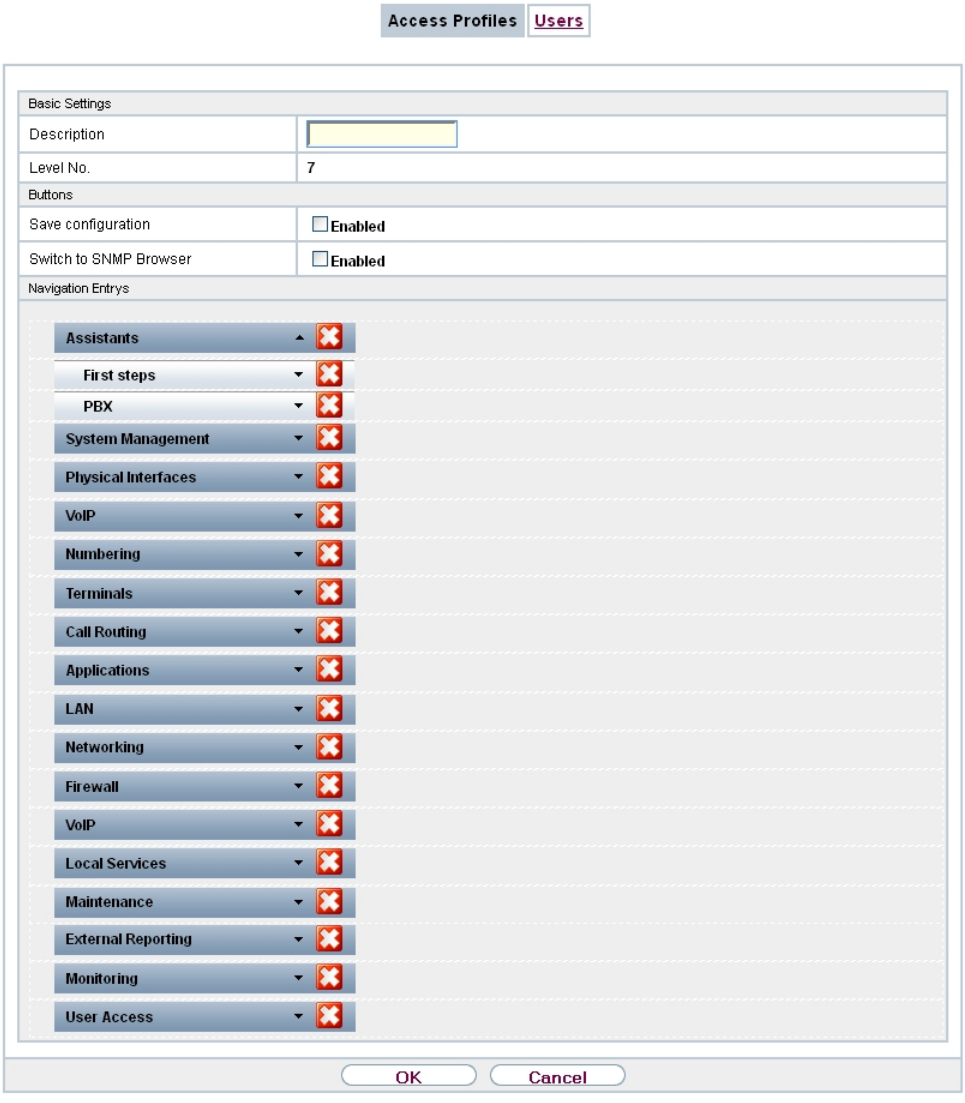


Fig. 36: **System Management->Configuration Access->Access Profiles->New**

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

Fields in the menu Basic Settings

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

Fields in the menu Buttons

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

Fields in the menu Navigation Entrys

Field	Description
Menus	You see all the menus from the GUI's navigation bar. Menus that contain at least one sub-menu are flagged by  and  . The icon  indicates pages. When you create a new access profile, no elements are assigned yet, i.e. all the available menus, sub-menus and pages are flagged with the icon  . Each element in the navigation bar can have three values. Click the icon  in the row you want to display these three values. Possible values: • *Deny*: The menu and all its lower-level menus are blocked. • *Allow*: The menu is released. Lower-level menus may need to be specifically released. • *Allow all*: The menu and all its lower-level menus are released. You can select *Allow* and *Allow all* in the corresponding row to assign elements to the current access profile. Elements that are assigned to the current access profile are flagged with the icon  .  indicates a menu that is blocked, but which has at least one released sub-menu.

7.6.2 Users

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

There are no preconfigured users.

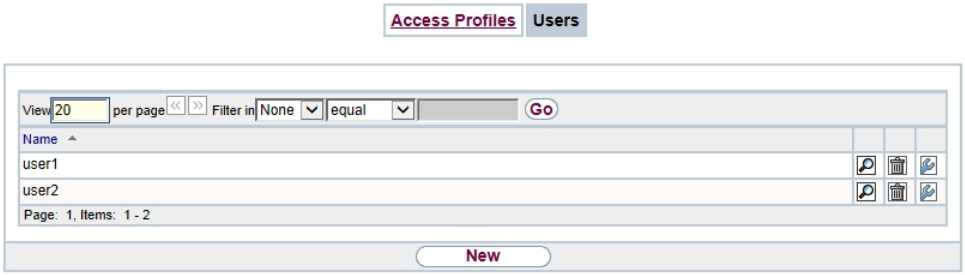


Fig. 37: **System Management->Configuration Access->Users**

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

Fig. 38: **System Management->Configuration Access->Users->**

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

7.6.2.1 Edit or New

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

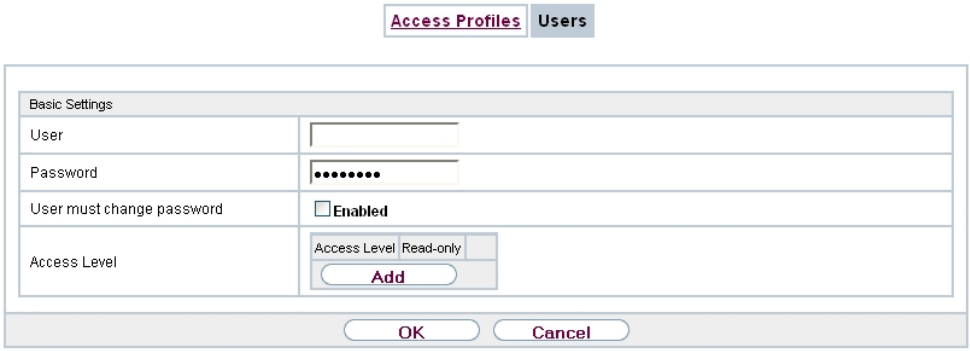


Fig. 39: **System Management->Configuration Access->Users->New**

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

Fields in the menu Basic Settings

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

Field	Description
	If intersecting access profiles are assigned to a user, read and write have a higher priority than **Read-only**. Buttons cannot be set to the setting **Read-only**.

7.7 Certificates

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

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

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

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

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

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

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

7.7.1 Certificate List

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

7.7.1.1 Edit

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

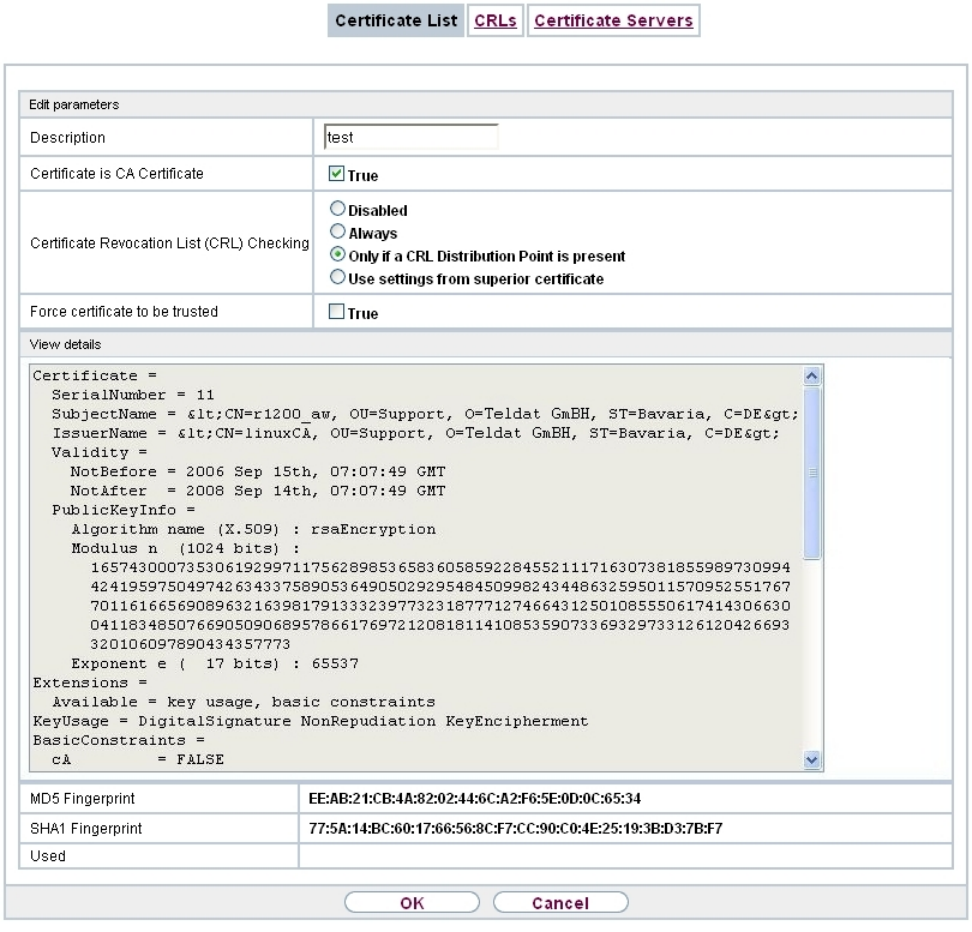


Fig. 40: **System Management->Certificates->Certificate List->**

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

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

Fields in the Edit parameters menu.

Field	Description
Description	Shows the name of the certificate, key, or request.
Certificate is CA Certificate	Mark the certificate as a certificate from a trustworthy certification authority (CA). Certificates issued by this CA are accepted during authentication. The function is enabled with *True*. The function is disabled by default.
Certificate Revocation List (CRL) Checking	Only for **Certificate is CA Certificate** = *True* Define the extent to which certificate revocation lists (CRLs) are to be included in the validation of certificates issued by the owner of this certificate. Possible settings: • *Disabled*: No CRLs check. • *Always*: CRLs are always checked. • *Only if a CRL Distribution Point is present* (default value): A check is only carried out if a CRL Distribution Point entry is included in the certificate. This can be determined under "View Details" in the certificate content. • *Use settings from superior certificate*: The settings of the higher level certificate are used, if one exists. It is does not, the same procedure is used as that described under "Only if a CRL Distribution Point is present".
Force certificate to be trusted	Define that this certificate is to be accepted as the user certificate without further checks during authentication. The function is enabled with *True*. The function is disabled by default.

Caution

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

7.7.1.2 Certificate Request

Registration authority certificates in SCEP

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

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

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

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

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

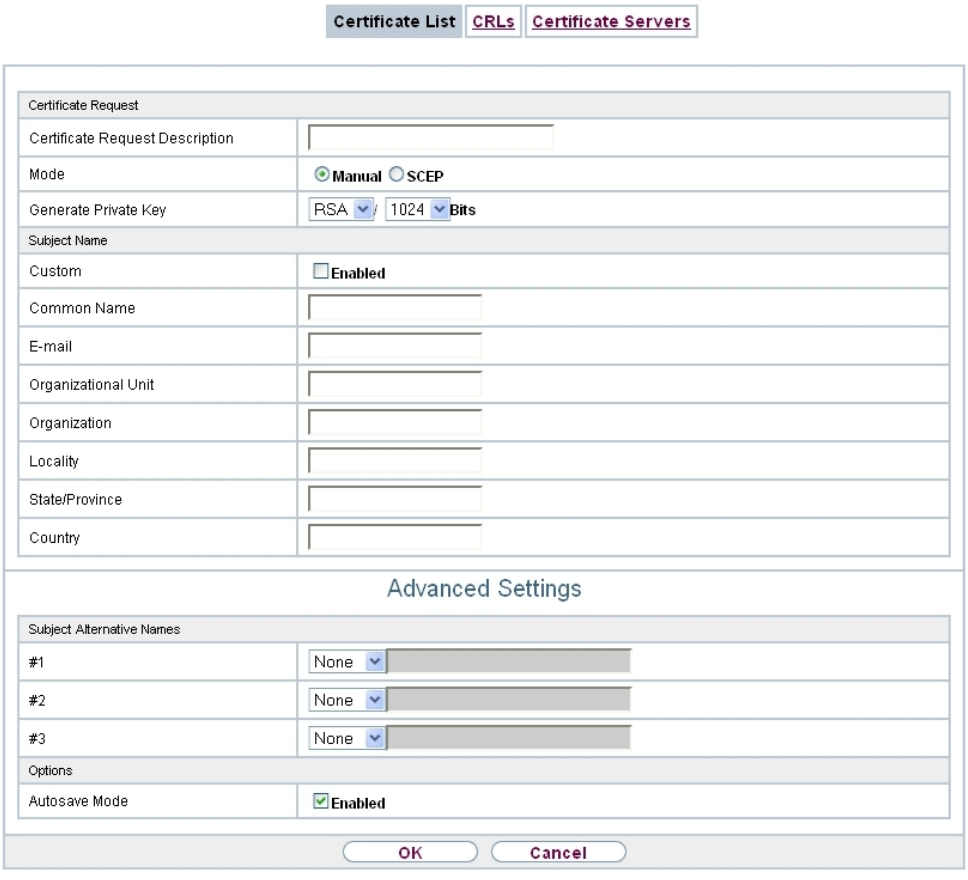


Fig. 41: **System Management->Certificates->Certificate List->Certificate Request**

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

Fields in the Certificate Request menu.

Field	Description
Certificate Request Description	Enter a unique description for the certificate.
Mode	Select the way in which you want to request the certificate. Possible settings: • `Manual` (default value): Your device generates a PKCS#10 for the key. This file can then be uploaded directly in the browser or copied in the menu using the **View details**

Field	Description
	field. This file must be provided to the CA and the received certificate must then be imported manually to your device. • *SCEP*: The key is requested from a CA using the Simple Certificate Enrolment Protocol.
Generate Private Key	Only for **Mode** = *Manual* Select an algorithm for key creation. *RSA* (default value) and *DSA* are available. Also select the length of the key to be created. Possible values: *512*, *768*, *1024*, *1536*, *2048*, *4096*. Please note that a key with a length of 512 bits could be rated as unsecure, whereas a key of 4096 bits not only needs a lot of time to create, but also occupies a major share of the resources during IPSec processing. A value of 768 or more is, however, recommended and the default value is 1024 bits.
SCEP URL	Only for **Mode** = *SCEP* Enter the URL of the SCEP server, e.g. http://scep.bintec-elmeg.com:8080/scep/scep.dll Your CA administrator can provide you with the necessary data.
CA Certificate	Only for **Mode** = *SCEP* Select the CA certificate. • In *-- Download --*: In **CA Name**, enter the name of the CA certificate of the certification authority (CA) from which you wish to request your certificate, e.g. *cawindows*. Your CA administrator can provide you with the necessary data. If no CA certificates are available, the device will first download the CA certificate of the relevant CA. It then continues with the enrolment process, provided no more important parameters are missing. In this case, it returns to the **Generate Certificate Request** menu. If the CA certificate does not contain a CRL distribution point (Certificate Revocation List, CRL), and a certificate server is

Field	Description
	not configured on the device, the validity of certificates from this CA is not checked. • <name of an existing certificate>: If all the necessary certificates are already available in the system, you select these manually.
RA Sign Certificate	Only for **Mode** = *SCEP* Only for **CA Certificate** not = *-- Download --* Select a certificate for signing SCEP communication. The default value is *-- Use CA Certificate --*, i.e. the CA certificate is used.
RA Encrypt Certificate	Only for **Mode** = *SCEP* Only if **RA Sign Certificate** not = *-- Use CA Certificate --* If you use one of your own certificates to sign communication with the RA, you can select another one here to encrypt communication. The default value is *-- Use RA Sign Certificate --*, i.e. the same certificate is used as for signing.
Password	Only for **Mode** = *SCEP* You may need a password from the certification authority to obtain certificates for your keys. Enter the password you received from the certification authority here.

Fields in the Subject Name menu.

Field	Description
Custom	Select whether you want to enter the name components of the subject name individually as specified by the CA or want to enter a special subject name. If *Enabled* is selected, a subject name can be given in **Summary** with attributes not offered in the list. Example: "CN=VPNServer, DC=mydomain, DC=com, c=DE".

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

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

Fields in the Subject Alternative Names menu.

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

Fields in the Options menu

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

7.7.1.3 Import

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

Fig. 42: **System Management->Certificates->Certificate List->Import**

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

Fields in the Import menu.

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

7.7.2 CRLs

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

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

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

7.7.2.1 Import

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

Fig. 43: **System Management->Certificates->CRLs->Import**

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

Fields in the CRL Import menu.

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

Field	Description
	type of encoding. • *Base64* • *Binary*
Password	Enter the password required for the import.

7.7.3 Certificate Servers

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

A certification authority (certification service provider, Certificate Authority, CA) issues your certificates to clients applying for a certificate via a certificate server. The certificate server also issues the private key and provides certificate revocation lists (CRL) that are accessed by the device via LDAP or HTTP in order to verify certificates.

7.7.3.1 New

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

Fig. 44: **System Management**->**Certificates**->**Certificate Servers**->**New**

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

Fields in the Basic Parameters menu.

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

Chapter 8 Physical Interfaces

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.

8.1 Ethernet Ports

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

Note

In the ex works state, the Ethernet ports ETH1 and ETH2 are assigned to the standard bridge group `br0` , which is preconfigured as DHCP client and with the fallback **IP Address** `192.168.0.252` and **Netmask** `255.255.255.0` .

The devices of the **bintec W1003n** series have only the Ethernet port ETH 1.

8.1.1 Port Configuration

Your device allows you to configure the two Ethernet interfaces separately.

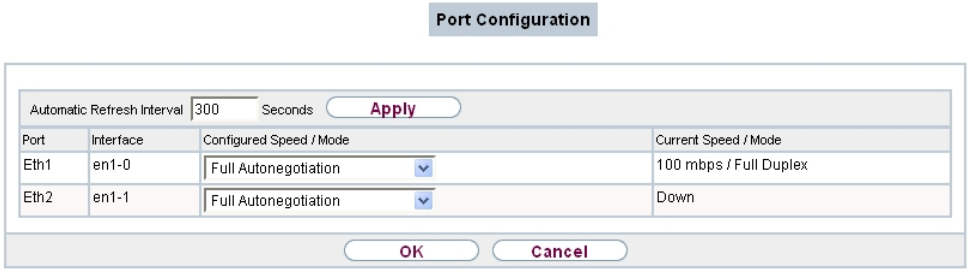


Fig. 45: **Physical Interfaces**->**Ethernet Ports**->**Port Configuration**

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

Fields in the Port Configuration menu.

Field	Description
Port	Shows the respective port. The numbering corresponds to the numbering of the Ethernet ports on the back of the device.
Interface	Displays the interface assigned to the Ethernet port here.
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 / 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: • *100 mbps / Full Duplex* • *100 mbps / Half Duplex* • *10 mbps / Full Duplex* • *10 mbps / Half Duplex* • *Down*

Chapter 9 LAN

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

9.1 IP Configuration

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

9.1.1 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.

Note

Please note:

If your device has obtained an IP address dynamically from a DHCP server operated in your network for the basic configuration, the fallback IP address is deleted automatically and your device will no longer function over this address.

However, if you have set up a connection to the device over the fallback IP address or have assigned an IP address with the **Dime Manager** in the basic configuration, you will only be able to access your device over this IP address. The device will no longer obtain an IP configuration dynamically over DHCP.

Example of subnets

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

The first subnet has two hosts with the IP addresses 192.168.42.1 and 192.168.42.2, for example, and the second subnet has two hosts with the IP addresses 192.168.46.1 and 192.168.46.2. To be able to exchange data packets with the first subnet, your device uses the IP address 192.168.42.3, for example, and 192.168.46.3 for the second subnet. The netmasks for both subnets must also be indicated.

9.1.1.1 Edit or New

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

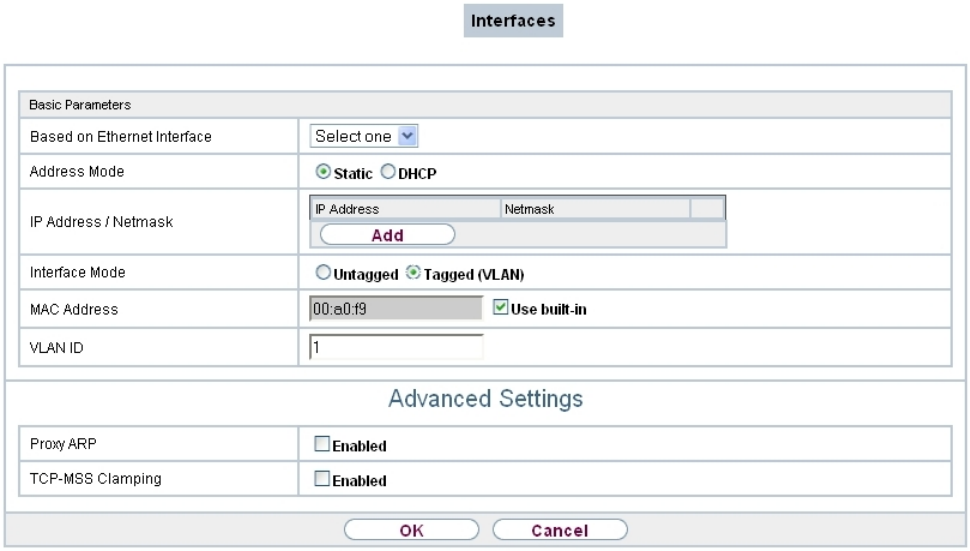


Fig. 46: **LAN->IP Configuration->Interfaces->/New**

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

Fields in the Basic Parameters menu.

Field	Description
Based on Ethernet Interface	This field is only displayed if you are editing a virtual routing interface.

Field	Description
	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 and for virtual interfaces. Select the configuration mode of the interface. Possible values: • *Untagged* (default value): The interface is not assigned for a specific purpose. • *Tagged (VLAN)*: This option only applies for routing interfaces. You use this option to assign the interface to a VLAN. This is done using the VLAN ID, which is displayed in this mode and can be configured. The definition of a MAC address in **MAC Address** is optional in this mode.
MAC Address	Enter the MAC address associated with the interface. For virtual interfaces, you can use the MAC address of the physical interface under which the virtual interface was created by activating **Use built-in**, but VLAN IDs must be different. You can also allocate a virtual MAC address. The first 6 characters of the MAC are preset (but can be changed). If **Use built-in** is active, the predefined MAC address of the allocated physical interface is used.

Field	Description
	Use built-in is activated by default.
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 the set BROADCAST bit. In this case, it is necessary to send DHCP requests in which this bit is not set. In this case, disable this option. The function is activated by selecting *Enabled*. The function is enabled by default.

Field	Description
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.

9.2 VLAN

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

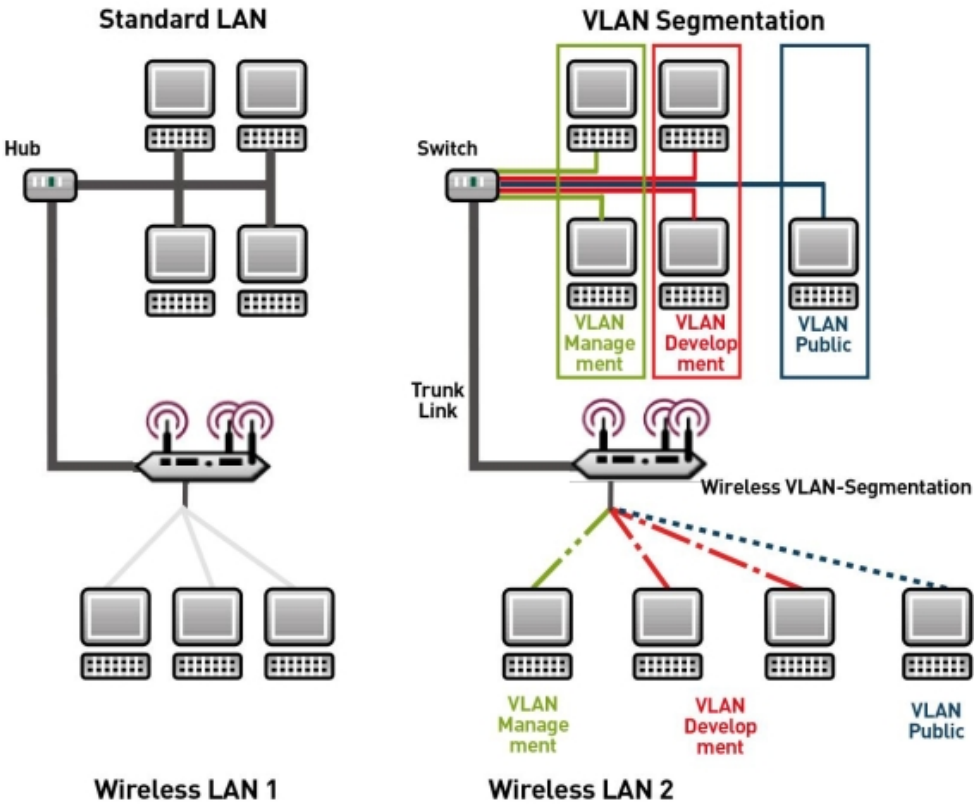


Fig. 47: VLAN segmenting

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**.

9.2.1 VLANs

In this menu, you can display all the VLANs already configured, edit your settings and create new VLANs. By default, the *Management* VLAN with **VLAN Identifier** = *1* is available, to which all interfaces are assigned.

9.2.1.1 Edit or New

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

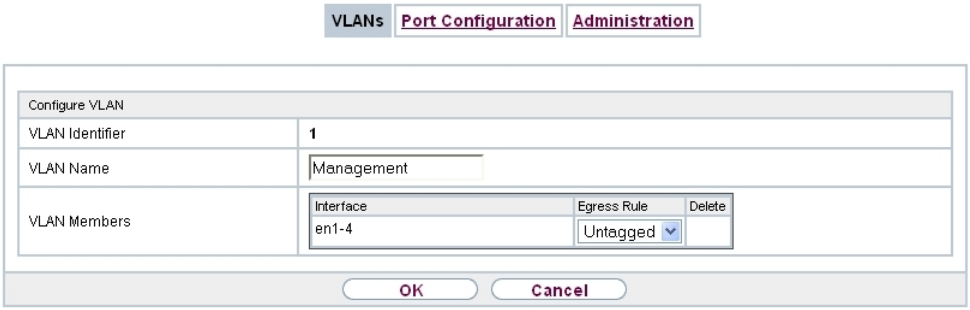


Fig. 48: **LAN->VLAN->VLANs->New**

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

Fields in the Configure VLAN menu.

Field	Description
VLAN Identifier	Enter the number that identifies the VLAN. In the menu, you can no longer change this value. Possible values are *1* (default value) to *4094*.
VLAN Name	Enter a unique name for the VLAN. A character string of up to 32 characters is possible. The predefined VLAN name is *Management*.
VLAN Members	Select the ports that are to belong to this VLAN. You can use the **Add** button to add members. For each entry, also select whether the frames to be transmitted from this port are to be transmitted *Tagged* (i.e. with VLAN in-

Field	Description
	formation) or *Untagged* (i.e. without VLAN information).

9.2.2 Port Configuration

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

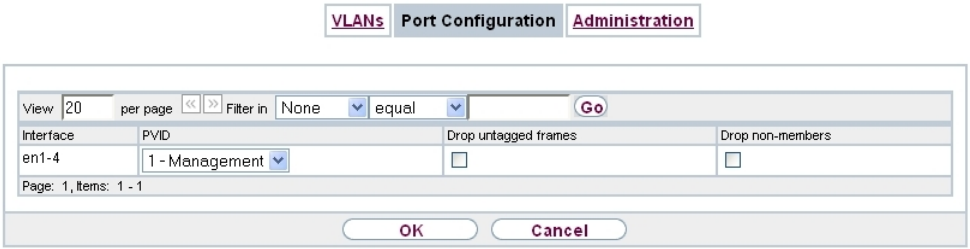


Fig. 49: **LAN->VLANs->Port Configuration**

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.

9.2.3 Administration

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

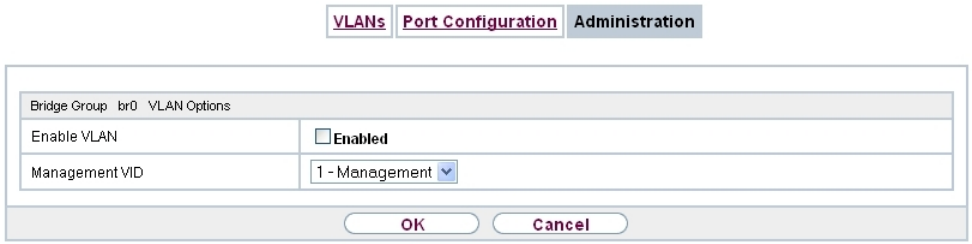


Fig. 50: **LAN->VLANs->Administration**

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

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

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

Chapter 10 Wireless LAN

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

Network functions

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

Currently applicable standard: IEEE 802.11

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.

The standard 802.11n (Draft 2.0) uses MIMO technology (Multiple Input Multiple Output) for data transmission that allows data transfer via WLAN over longer distances or with higher data rates. With a bandwidth of 20 or 40 MHz, a gross data rate of 150 Mbps or 300 Mbps is achieved.

An amendment to the Telecommunications Act (TKG) allowed the 5.8 GHz band (5755 MHz - 5875 MHz) to be used for so-called BFWA applications (Broadband Fixed Wireless Access). This simply requires registration with the Federal Network Agency. However, the use of TPC and DFS is mandatory in this case.

10.1 WLAN

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

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

10.1.1 Radio Settings

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

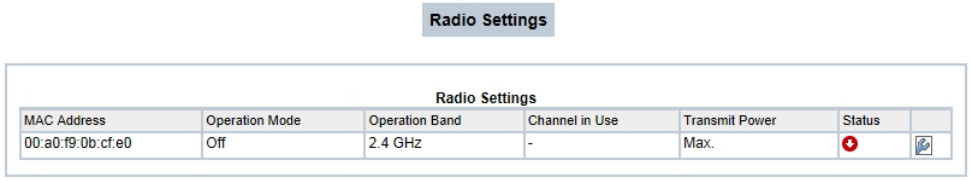


Fig. 51: **Wireless LAN**->**WLAN**->**Radio Settings**

10.1.1.1 Radio Settings->

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

Select the  icon to edit the configuration.

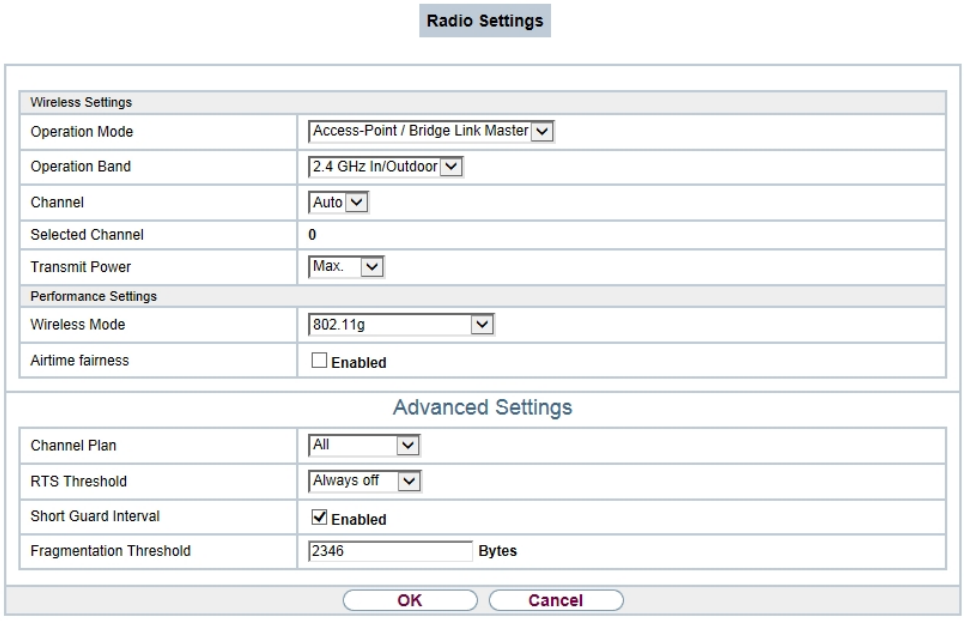


Fig. 52: **Wireless LAN->WLAN->Radio Settings->** *for* **Operation Mode** *Access-Point / Bridge Link Master*

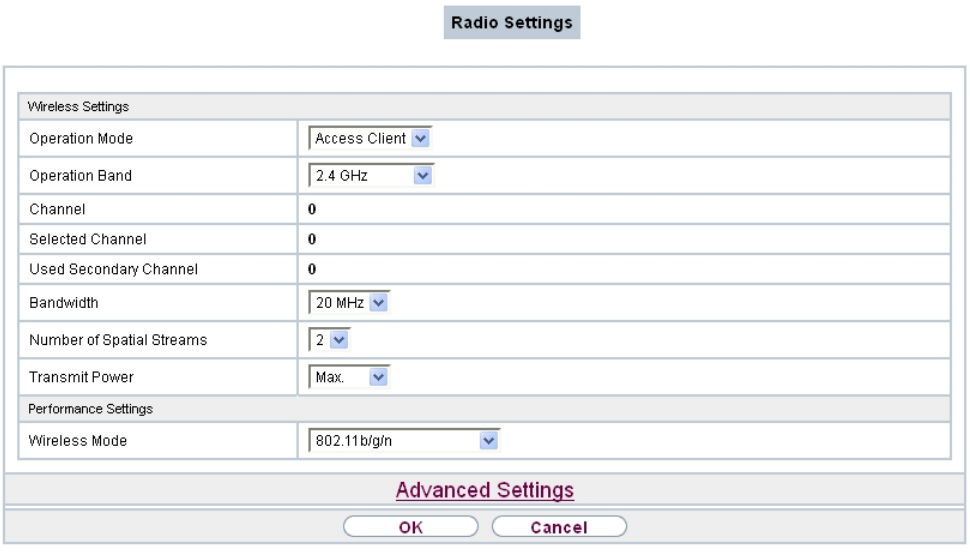


Fig. 53: **Wireless LAN WLAN Radio Settings** *for* **Operation Mode** *Access Client*

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

Fields in the menu Wireless Settings

Field	Description
Operation Mode	Define the mode in which the wireless module of your device is to operate. Possible values: • *Off* (default value): The wireless module is not active. • *Access-Point / Bridge Link Master*: Your device is used as an access point in your network. • *Access Client*: Your device serves as an Access Client in your network. • *Bridge Link Client*: Your device is used as a wireless bridge link in your network (available only for the devices of the **bintec W1003n**, **W2003n**, **W2003n-ext** und **W2004n** series) .
Operation Band	Select the operation band and, where applicable, the usage area of the wireless module. For **Operation Mode** = *Access-Point / Bridge Link Master* or *Bridge Link Client* Possible values: • *2.4 GHz In/Outdoor* (default value): Your device is operated at 2.4 GHz (mode 802.11b and mode 802.11g), inside or outside buildings. • *5 GHz Indoor*: Your device runs in 5 GHz (Mode 802.11a/h) inside buildings. • *5 GHz Outdoor*: Your device runs in 5 GHz (Mode 802.11a/h) outside buildings. • *5 GHz In/Outdoor*: Your device is run with 5 GHz (Mode 802.11a/h) inside or outside buildings.
Usage Area	Only for **Operation Mode** = *Access Client* and **Operation Band** = *2.4 and 5 GHz* or *5 GHz* Possible values: • *Indoor-Outdoor* (default value) • *Indoor*

Field	Description
	• *Outdoor*
Channel	The number of channels you can select depends on the country setting. Please consult the data sheet for your device. **Access Point Mode / Bridge Mode:** Configuring the network name (SSID) in Access Point mode means that wireless networks can be logically separated from each other, but they can still physically interfere with each other if they are operating on the same or closely adjacent wireless channels. So if you are operating two or more radio networks close to each other, it is advisable to allocate the networks to different channels. Each of these should be spaced at least four channels apart, as a network also partially occupies the adjacent channels. In the case of manual channel selection, please make sure first that the clients actually support these channels. Possible values: • For **Operation Band** = *2.4 GHz In/Outdoor* Possible values are *1* to *13* and *Auto* (default value). *Auto* is not possible in bridge mode. • For **Operation Band** = *5 GHz Indoor* Possible values are *36*, *40*, *44*, *48* and *Auto* (standard value) • For **Operation Band** = *5 GHz In/Outdoor* and *5 GHz Outdoor* Only the *Auto* option is possible here. **Access Client Mode:** In the Access Client Mode no channel you can select. The used channel is shown.
Selected Channel	Displays the channel used.
Used Secondary Channel	Not for **Operation Mode** = *Access-Point / Bridge Link Master*

Field	Description
	Displays the second channel used.
Bandwidth	For **Operation Mode** = *Access-Point / Bridge Link Master* or *Bridge Link Client* Not for **Operation Band** = *2.4 GHz In/Outdoor* Select how many channels are to be used. Possible values: • *20 MHz* (default value): One channel with 20 MHz bandwidth is used. • *40 MHz*: Two channels each with 20 MHz bandwidth are used. In the case one channel acts as a control channels and the other as an expansion channel.
Number of Spatial Streams	Not for **Wireless Mode** = *802.11a* Select how many traffic flows are to be used in parallel. Possible values: • *2*: Two traffic flows are used. • *1*: One traffic flow is used.
Transmit Power	Select the maximum value for the radiated antenna power. The actually radiated antenna power may be lower than the maximum value set, depending on the data rate transmitted. The maximum value for Transmit Power is country-dependent. Possible values: • *Max.* (default value): The maximum antenna power is used. • *5 dBm* • *8 dBm* • *11 dBm* • *14 dBm* • *16 dBm* • *17 dBm*

Fields in the menu Performance Settings

Field	Description
Wireless Mode	Select the wireless technology that the access point is to use. Only for **Operation Mode** = *Access Point / Bridge Link Master* and **Operation Band** = *2.4 GHz In/Outdoor* or for **Operation Mode** = *Access Client* and **Operation Band** = *2.4 GHz* Possible values: • *802.11g*: The device operates only in accordance with 802.11g. 802.11b clients have no access. • *802.11b*: Your device operates only in accordance with 802.11b and forces all clients to adapt to it. • *802.11 mixed (b/g)*: Your device adapts to the client technology and operates according to either **802.11b** or **802.11g**. • *802.11 mixed long (b/g)*: Your device adapts to the client technology and operates according to either **802.11b** or **802.11g**. Only a data rate of 1 and 2 mbps needs to be supported by all clients (basic rates). This mode is also needed for Centrino clients if connection problems occur. • *802.11 mixed short (b/g)*: Your device adapts to the client technology and operates according to either **802.11b** or **802.11g**. The following applies for mixed-short: The data rates 5.5 and 11 mbps must be supported by all clients (basic rates). • *802.11b/g/n*: Your device operates according to either 802.11b, 802.11g or 802.11n. • *802.11g/n*: Your device operates according to either 802.11g or 802.11n. • *802.11n*: Your device operates only according to 802.11n. For **Operation Band** = *5 GHz Indoor*, *5 GHz Outdoor*, *5 GHz In/Outdoor*, *5.8 GHz Outdoor* Possible values: • *802.11a*: The device operates only in accordance with 802.11a. • *802.11n*: Your device operates only according to 802.11n. • *802.11a/n*: Your device operates according to either

Field	Description
	802.11a or 802.11n.
Airtime fairness	This function is not available for all devices. The **Airtime fairness** function ensures that the access point's send resources are distributed intelligently to the connected clients. This means that a powerful client (e. g. a 802.11n client) cannot achieve only a poor flow level, because a less powerful client (e. g. a 802.11a client) is treated in the same way when apportioning. The function is enabled with *Enabled*. The function is disabled by default. This fuction is only applied to unprioritized frames of the WMM Classe "Background".

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

Fields in the Advanced Settings menu for operating mode = Access Point / Bridge Link Master

Field	Description
Channel Plan	Only for **Operation Mode** = *Access-Point / Bridge Link Master* and **Channel** = *Auto* Select the desired channel plan. The channel plan makes a preselection when a channel is selected. This ensures that no channels overlap, i.e. a distance of four channels is maintained between the channels used. This is useful if more access points are used with overlapping radio cells. Possible values: • *All*: All channels can be dialled when a channel is selected. • *Auto*: Depending on the region, operation band, wireless mode and bandwidth, the channels that have a distance of 4 channels are provided. • *User defined*: Select the desired channels.
Selected Channels	Only for **Channel Plan** = *User defined*

Field	Description
	The currently selected channels are displayed here. With **Add** you can add channels. If all available channels are displayed, you cannot add any more entries. You can delete entries with the icon.
RTS Threshold	Here, you select how the RTS/CTS mechanism is to be switched on/off. If you choose *User-defined*, you can specify in the input field the data packet length threshold in bytes (1 - 2346) as of which the RTS/CTS mechanism is to be used. This makes sense if several clients that are not in each other's wireless range are run in one access point. The mechanism can also be switched on/off independently of the data packet length by selecting the value *Always on* or *Always off*(default value).
Short Guard Interval	Enable this function to reduce the guard interval (= time between transmission of two data symbols) from 800 ns to 400 ns.
Fragmentation Threshold	Enter the maximum size as of which the data packets are to be fragmented (i.e. split into smaller units). Low values are recommended for this field in areas with poor reception and in the event of radio interference. Possible values are *256* to *2346*. The default value is *2346* bytes.

If *Access Client* is selected for **Operation Mode**, the following parameters are additionally available under **Advanced Settings**:

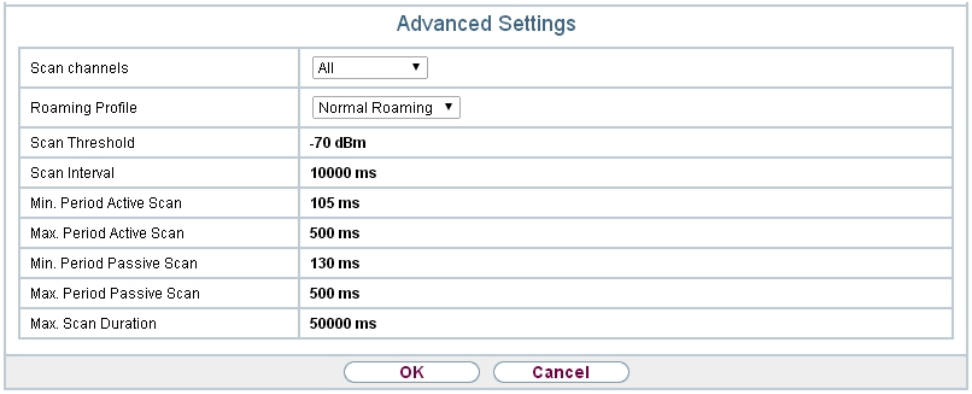


Fig. 54: **Wireless LAN->WLAN->Radio Settings->->Advanced Settings** *for* **Operation Mode** `Access Client`

Fields in the menu Advanced Settings for Access Client Mode.

Field	Description
Scan channels	Choose the channels which the WLAN client automatically scans for available wireless networks. Possible values: • `All` (default value): All channels are scanned. • `Auto`: The channel is automatically selected. • `User defined`: The desired channels can therefore be defined.
User Defined Channel Plan	Only for **Scan channels** = `User defined` Define the channels which the WLAN client automatically scans for available wireless networks.
Roaming Profile	Select the roaming profile. The options available include typical roaming functions. Possible values: • `Fast Roaming`: The WLAN client searches for available wireless networks as soon as the radio signal of the existing radio connection becomes unsuitable for higher data rates. • `Normal Roaming` (default value): Standard roaming. • `Slow Roaming`: The WLAN client searches for available wireless networks as soon as the radio signal of the existing

Field	Description
	radio connection becomes weaker. • *No Roaming*: The WLAN client searches for available wireless networks if it is no longer connected to a wireless network. • *Custom Roaming*: Specify the individual roaming parameters.
Scan Threshold	Indicates the value in dBm above which the system scans for available wireless networks in the background. The value can only be modified for **Roaming Profile** = *Custom Roaming*. The default value is *-70 dBm*.
Scan Interval	Indicates the interval in milliseconds after which the system scans for available wireless networks. The value can only be modified for **Roaming Profile** = *Custom Roaming*. The default value is *5000 ms*.
Min. Period Active Scan	Displays the minimum active scanning time for a frequency in milliseconds. The value can only be modified for **Roaming Profile** = *Custom Roaming*. The default value is *10 ms*.
Max. Period Active Scan	Displays the maximum active scanning time for a frequency in milliseconds. The value can only be modified for **Roaming Profile** = *Custom Roaming*. The default value is *40 ms*.
Min. Period Passive Scan	Displays the minimum passive scanning time for a frequency in milliseconds. The value can only be modified for **Roaming Profile** = *Custom Roaming*. The default value is *20 ms*.
Max. Period Passive Scan	Displays the maximum passive scanning time for a frequency in milliseconds. The value can only be modified for **Roaming Profile** = *Custom Roaming*. The default value is *120 ms*.
Max. Scan Duration	Displays the maximum scanning duration for a frequency in mil-

Field	Description
	liseconds. The value can only be modified for **Roaming Profile** = *Custom Roaming*. The default value is *50000 ms*.

10.1.2 Wireless Networks (VSS)

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

Note

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

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

Setting network names

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

Protection of wireless networks

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

There are three security modes, WEP, WPA-PSK and WPA Enterprise. WPA Enterprise of-

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

WEP

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

IEEE 802.11i

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

WPA

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

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

WPA 2

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

Access control

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

Security measures

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

- Change the access passwords for your device.
- Change the default SSID, **Network Name (SSID)** = *default*, of your access point. Set **Visible** = *Enabled*. This will exclude all WLAN clients that attempt to establish a connection with the general value for **Network Name (SSID)** *Any* and do not know the SSID settings.
- Use the available encryption methods. To do this, select **Security Mode** = *WEP 40*, *WEP 104*, *WPA-PSK* or *WPA Enterprise* and enter the relevant key in the access point under **WEP Key 1 - 4** or **Preshared Key** and in the WLAN clients.
- The WEP key should be changed regularly. To do this, change the **Transmit Key**. Select the longer 104 Bit WEP key.
- For transmission of information with very high security relevance, configure **Security Mode** = *WPA Enterprise*with **WPA Mode** = *WPA 2*. This method contains hardware-based encryption and RADIUS authentication of the client. In special cases, combination with IPSec is possible.
- Restrict WLAN access to permitted clients. Enter the MAC addresses of the wireless network cards for these clients in the **Allowed Addresses** list in the **MAC-Filter** menu (see *Fields in the menu MAC-Filter* on page 134).

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

10.1.2.1 Edit or New

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

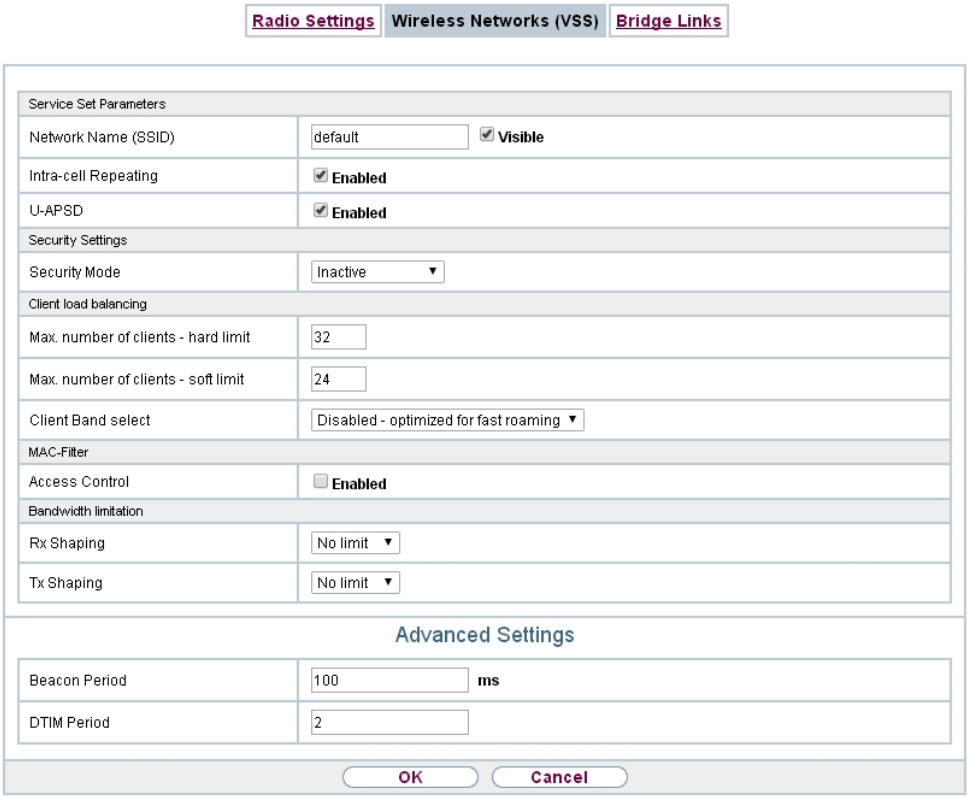


Fig. 55: **Wireless LAN->WLAN->Wireless Networks (VSS)->->New**

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

Fields in the menu Service Set Parameters

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

Field	Description
	be permitted within a radio cell. The function is activated by selecting *Enabled*. The function is enabled by default.
U-APSD	Select whether the Unscheduled Automatic Power Save Delivery (U-APSD) mode is to be enabled. The function is activated by selecting *Enabled*. The function is enabled by default.

Fields in the menu Security Settings

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

Field	Description
WPA Mode	Only for **Security Mode** = *WPA-PSK* and *WPA Enterprise* Select whether you want to use WPA (with TKIP encryption) or WPA 2 (with AES encryption), or both. Possible values: • *WPA and WPA 2* (default value): **WPA and WPA 2** can be applied. • *WPA*: Only **WPA** is applied. • *WPA 2*: Only **WPA 2** is applied.
WPA Cipher	Only for **Security Mode** = *WPA-PSK* and *WPA Enterprise* and for **WPA Mode** = *WPA* and *WPA and WPA 2* Select the type of encryption with which to apply **WPA**. Possible values: • *AES* : AES is used. • *TKIP*: TKIP is used. • *AES and TKIP* (default value): AES or TKIP is used.
WPA2 Cipher	Only for **Security Mode** = *WPA-PSK* and *WPA Enterprise* and for **WPA Mode** = *WPA 2* and *WPA and WPA 2* Select the type of encryption with which to apply **WPA 2**. Possible values: • *AES* : AES is used. • *AES and TKIP* (default value): AES or TKIP is used.
Preshared Key	Only for **Security Mode** = *WPA-PSK* Enter the WPA password. Enter an ASCII string with 8 - 63 characters.

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

Fields in the menu Client load balancing

Field	Description
Max. number of clients - hard limit	Enter the maximum number of clients that can be connected to this wireless network (SSID) The maximum number of clients that can register with a wireless module depends on the specifications of the respective WLAN module. This maximum is distrubuted across all wireless networks configured for this radio module. No more new wireless networks can be created and a warning message will appear if the maximum number of clients is reached. Possible values are whole numbers between *1* and *254*. The default value is *32*.
Max. number of clients - soft limit	Not all devices support this function. To avoid a radio module being fully utilised, you can set a "soft" restriction on the number of connected clients. If this number is reached, new connection queries are initially rejected. If the client cannot find another wireless network and, therefore, repeats its query, the connection is accepted. Queries are only definit-

Field	Description
	ively rejected when the **Max. number of clients - hard limit** is reached. The value of the **Max. number of clients - soft limit** must be the same as or less than that of the **Max. number of clients - hard limit**. The default value is *28*. You can disable this function if you set **Max. number of clients - soft limit** and **Max. number of clients - hard limit** to identical values.
Client Band select	Not all devices support this function. This function requires a dual radio setup where the same wireless networkis configured on both radio modules, but in different frequency bands. The **Client Band select** option enables clients to be moved from the frequency band originally selected to a less busy one, providing the client supports this. To achieve a changeover, the connection attempt of a client is initially refused so that the client repeats the attempt in a different frequency band. Possible values: • *Disabled - optimized for fast roaming*(default value): The function is not used for this VSS. This is useful if clients are to switch between different radio cells with as little delay as possible, e. g. with Voice over WLAN. • *2,4 GHz band preferred*: Preference is given to accepting clients in the 2.4 GHz band. • *5 GHz band preferred*: Preference is given to accepting clients in the 5 GHz band.

Fields in the menu MAC-Filter

Field	Description
Access Control	Select whether only certain clients are to be permitted for this wireless network. The function is activated by selecting *Enabled*.

Field	Description
	The function is disabled by default.
Allowed Addresses	Use **Add** to make entries and enter the MAC addresses (**MAC Address**) of the clients to be permitted.

Fields in the menu Bandwidth limitation for each WLAN client

Field	Description
Rx Shaping	Select a bandwidth limitation in the receive direction. Possible values are • *No limit* (default value) • *1 Mbit/s* up to *10 Mbit/s* in single Mbit/s steps, *15 Mbit/s*, *20 Mbit/s*, *30 Mbit/s*, *40 Mbit/s* and *50 Mbit/s*.
Tx Shaping	Select a bandwidth limitation in the transmit direction. Possible values are • *No limit* (default value) • *1 Mbit/s* up to *10 Mbit/s* in single Mbit/s steps, *15 Mbit/s*, *20 Mbit/s*, *30 Mbit/s*, *40 Mbit/s* and *50 Mbit/s*.

Fields in the menu Advanced Settings

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* ms.
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

Field	Description
	come alive at the right time and receive the data. Possible values are *1* to *255*. The default value is *2*.

10.1.3 Client Link

If you're operating your device in Access Point mode, (**Wireless LAN**->**WLAN**->**Radio Settings**->->**Operation Mode** = *Access Client*), you can edit the existing client links in the **Wireless LAN**->**WLAN**->**Client Link**-> menu.

The **Client Mode** can be operated in infrastructure mode or in ad-hoc mode.

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.

In ad-hoc mode, an access client can be used as central interface between a number of terminals. In this way, devices such as computers and printers can be wirelessly interconnected.

10.1.3.1 Edit

Choose the icon to edit existing entries.

Fig. 56: **Wireless LAN**->**WLAN**->**Client Link**->

The **Wireless LAN**->**WLAN**->**Client Link**-> menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Network Name (SSID)	Enter the name of the wireless network (SSID).

Field	Description
	Enter an ASCII string with a maximum of 32 characters.

Fields in the Security Settings menu.

Field	Description
Security Mode	Select the security mode (encryption and authentication) for the wireless network. Possible values: • *Inactive* (default value): Neither encryption nor authentication • *WEP 40*: WEP 40 bits • *WEP 104*: WEP 104 bits • *WPA-PSK*: WPA Preshared Key
Transmit Key	Only for **Security Mode** = *WEP 104* Select one of the keys configured in **WEP Key** <1 - 4> as a default key. The default value is *Key 1*.
WEP Key 1 - 4	Only for **Security Mode** = *WEP 40*, *WEP 104* Enter the WEP key. Enter a character string with the right number of characters for the selected WEP mode. For *WEP 40* you need a character string with 5 characters, for *WEP 104* with 13 characters, e.g. *hello* for *WEP 40*, *wep1* for *WEP 104*.
WPA Mode	Only for **Security Mode** = *WPA-PSK* Select whether you want to use WPA or WPA 2. Possible values: • *WPA* (default value): Only WPA is used. • *WPA 2*: Only WPA2 is used.
Preshared Key	Only for **Security Mode** = *WPA-PSK* Enter the WPA password.

Field	Description
	Enter an ASCII string with 8 - 63 characters.
WPA Cipher	Only for **Security Mode** = *WPA-PSK* and **WPA Mode** = *WPA* Select which encryption method should be used. Possible values: • *TKIP* (default value): Temporal Key Integrity Protocol • *AES*: Advanced Encryption Standard. Both encryption methods are rated as secure, with AES offering better performance.
WPA2 Cipher	Only for **Security Mode** = *WPA-PSK* and **WPA Mode** = *WPA 2* Select which encryption method is to be used. Possible values: • *AES* (default value): Advanced Encryption Standard. • *TKIP* : Temporal Key Integrity Protocol Both encryption methods are rated as secure, with AES offering better performance.

10.1.3.2 Client Link Scan

After the desired Client Links have been configured, the  icon is shown in the list.

You use this icon to open the **Scan** menu.

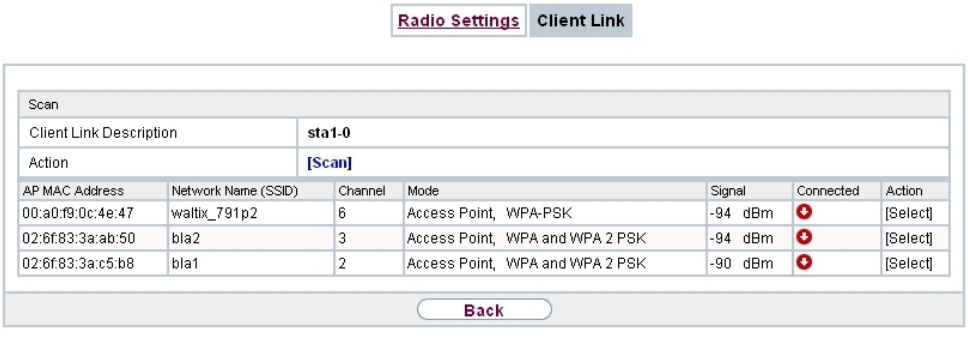


Fig. 57: **Wireless LAN->WLAN->Client Link->Scan**

After successful scanning, a selection of potential scan partners is displayed in the scan list. In the **Action** column, click **Select** to connect the local clients with this client. If the partners are connected with one another, the icon appears in the **Connected** column. The icon appears in the **Connected** column if the connection is active.

The **Wireless LAN**->**WLAN**->**Client Link**->**Scan** menu consists of the following fields:

Fields in the Scan menu.

Field	Description
Client Link Description	Displays the name of the client link you configured.
Action	Start the scan by clicking on **Scan**. If the antennas are installed correctly on both sides and LOS is free, the client finds available clients and displays them in the following list. If the partner client cannot be found, check the line of sight and the antenna installation. Then carry out the **Scan**. The partner should then be found.
AP MAC Address	Shows the MAC address of the remote client.
Network Name (SSID)	Displays the name of the remote client.
Channel	Shows the **Channel** used.
Mode	Shows the security mode (encryption and authentication) for the wireless network.
Signal	Displays the signal strength of the detected client link in dBm.
Connected	Displays the status of the link on your client.
Action	You can change the status of the client link. The available actions are displayed in this field.

10.1.4 Bridge Links

Available only for the devices of the **bintec W1003n**, **W2003n**, **W2003n-ext** und **W2004n** series.

Bridge Links allow you to create a dedicated connection between WLAN devices. A radio module operating as a slave exclusively connects to the bridge link master and does not establish or accept any other WLAN connections. A bridge link usually serves to reliably connect two networks via a WLAN connection.

10.1.4.1 Edit oder New

Select the symbol in order to edit an existing entry. Select the **New** button in order to create a new bridge link.

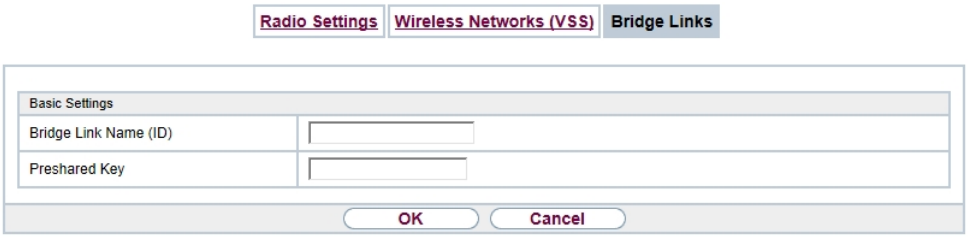


Fig. 58: **Wireless LAN->WLAN->Bridge Links->->New**

The menu **Wireless LAN->WLAN->Bridge Links->->New** contains the follwoing fields:

Fields in the Basic Parameters menu

Field	Description
Bridge Link Name (ID)	Depending on whether you operate the radio module as access point or as wireless bridge link, you create a bridge link in master or in slave mode. If the radio module operates in **Access Point** mode, the bridge link is in master mode. Enter a name for the bridge link. This name also serves as the ID other devices use to connect to this bridge link. If the radio module is in **Bridge Link Client** mode, the bridge link is in slave mode. Enter the ID of the bridge link the device is supposed to connect to.
Preshared Key	Enter a password for this bridge link. In master mode, this is the password other devices use to connect to this bridge link. In slave mode, it is the password of that bridge link the device is to connect to.

10.2 Administration

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

10.2.1 Basic Settings

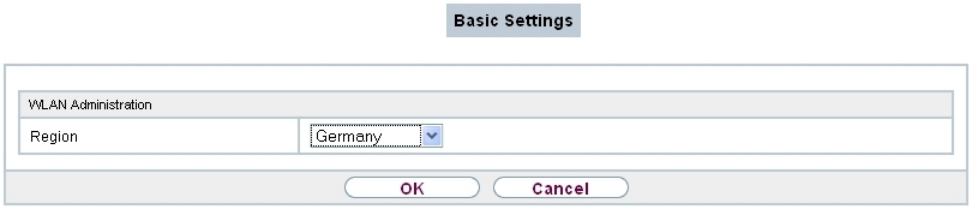


Fig. 59: **Wireless LAN->Administration->Basic Settings**

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

Fields in the WLAN Administration menu.

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

Chapter 11 Wireless LAN Controller

By using the wireless LAN controller, you can set up and manage a WLAN infrastructure with multiple access points (APs). The WLAN controller has a Wizard which assists you in the configuration of your access points. The system uses the CAPWAP protocol (Control and Provisioning of Wireless Access Points Protocol) for any communication between masters and slaves.

In smaller WLAN infrastructures with up to six APs, one of the AP's assumes the master function and manages the other AP's as well as itself. In larger WLAN networks a gateway, e.g. such as a **bintec R1202**, assumes the master function and manages the AP's.

Provided the controller has "located" all of the APs in its system, each of these shall receive a new passport and configuration in succession, i.e. they are managed via the WLAN controller and can no longer be amended "externally".

With the **WLAN controller** you can

- automatically detect individual access points (APs) and connect to a WLAN network
- Load the system software into the APs
- Load the configuration into the APs
- Monitor and manage APs

Please refer to your gateway's data sheet to find out the number of APs that you can manage with your gateway's wireless LAN controller and details of the licenses required.

11.1 Wizard

The **Wizard** menu offers step-by-step instructions for the set up of a WLAN infrastructure. The Wizard guides you through the configuration.

When you select the Wizard you will receive instructions and explanations on the separate pages of the Wizard.

Note

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

11.1.1 Basic Settings

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

The wireless LAN controller uses the following settings:

Region

Select the country in which the wireless controller is to be operated.

Please note: The range of channels that can be used varies depending on the country setting.

Interface

Select the interface to be used for the wireless controller.

DHCP Server

Select whether an external DHCP server shall assign IP addresses to the APs or if you wish to assign fixed IP addresses yourself. Alternatively, you can use your device as a DHCP server. For this internal DHCP server, CAPWAP option 138 is active in order to allow communication between the master and slaves.

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

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

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

IP Address Range

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

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

11.1.2 Radio Profile

Select which frequency band your WLAN controller shall use.

If the *2.4 GHz Radio Profile* is set then the 2.4 GHz frequency band is used.

If the *5 GHz Radio Profile* is set then the 5 GHz frequency band is used.

If the corresponding device contains two wireless modules, you can **Use two independent radio profiles**. This assigns *2.4 GHz Radio Profile* to module 1 and *5 GHz Radio Profile* to module 2.

The function is activated by selecting *Enabled*.

The function is disabled by default.

11.1.3 Wireless Network

All of the configured wireless networks (VSS) are displayed in the list. At least one wireless network (VSS) is set up. This entry cannot be deleted.

Click on to edit an existing entry.

You can also delete entries using the icon.

With **Add**, you can create new entries. You can create up to eight wireless networks (VSS) for a wireless module.

Note

If you wish to use the default wireless network that is set up, you must at least change the **Preshared Key** parameters. Otherwise you will be prompted.

11.1.3.1 Change or add wireless networks

Click on to edit an existing entry.

With **Add**, you can create new entries.

The following parameters are available

Network Name (SSID)

Enter the name of the wireless network (SSID).

Enter an ASCII string with a maximum of 32 characters.

Also select whether the **Network Name (SSID)** *Visible* is to be transmitted.

Security Mode

Select the security mode (encryption and authentication) for the wireless network.

Please note: *WPA Enterprise* means 802.11x.

WPA Mode

Select for **Security Mode** = *WPA-PSK* or *WPA Enterprise*, whether you wish to use WPA oder WPA 2 or both.

Preshared Key

Enter the WPA password for **Security Mode** = *WPA-PSK*.

Enter an ASCII string with 8 - 63 characters.

Important

Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!

Radius Server

You can control access to a wireless network via a RADIUS server.

With **Add**, you can create new entries.

Enter the IP address and the password of the desired RADIUS server.

EAP Preauthentification

For **Security Mode** = *WPA Enterprise*, select whether the EAP preauthentification function is to be *Enabled*. This function tells your device that WLAN clients, which are already connected to another access point, can first carry out 802.1x authentication as soon as they are within range. Such WLAN clients can then simply connect over the existing network connection with your device.

VLAN

Select whether the VLAN segmentation is to be used for this wireless network.

If you wish to use VLAN segmentation, enter a value between *2* and *4094* in the input field in order to identify the VLAN. (VLAN ID *1* is not possible!).

Note

Before you continue, please ensure that all access points that the WLAN controller shall manage are correctly wired and switched on.

11.1.4 Start automatic installation

You will see a list of all detected access points.

If you wish to change the settings of a detected AP, click on in the corresponding entry.

You will see the settings for all selected access points. You can change these settings.

The following parameters are available in the **Access Point Settings** menu:

Location

Displays the stated locality of the AP. You can enter another locality.

Assigned Wireless Network (VSS)

Displays the wireless networks that are currently assigned.

The following parameters are available in the wireless module 1 menu:

(The parts wireless module 1 and wireless module 2 are displayed if the AP has two wireless modules.)

Operation Mode

Select the mode in which the wireless module is to be operated.

Possible values:

- *On* (default value): The wireless module is used as an access point in your network.
- *Off*: The wireless module is not active.

Active Radio Profile

Displays the wireless module profile that is currently selected. You can select another wireless module profile from the list if more than one wireless module profile are being set up.

Channel

Displays the channel that is assigned. You can select an alternative channel.

The number of channels you can select depends on the country setting. Please consult the data sheet for your device.

Note

Configuring the network name (SSID) in Access Point mode means that wireless networks can be logically separated from each other, but they can still physically interfere with each other if they are operating on the same or closely adjacent wireless channels. So if you are operating two or more radio networks close to each other, it is advisable to allocate the networks to different channels. Each of these should be spaced at least four channels apart, as a network also partially occupies the adjacent channels.

In the case of manual channel selection, please make sure first that the APs actually support these channels.

Transmit Power

Displays the transmission power in dBm. You can select another transmission power.

With **OK** you apply the settings.

Select the access points that your WLAN controller shall manage. In the **Manage** column, click on the desired entries or click on **Select all** in order to select all entries. Click the **Deselect all** button to disable all entries and to then select individual entries if required (e.g. for large lists).

Click on **Start** in order to install the WLAN and automatically assign the frequencies.

Note

If there are not enough licences available, the message "The maximum number of slave access points that can be supported has been exceeded". Please check your licences. If this message is displayed then you should obtain additional licences if appropriate.

During the installation of the WLAN and the allocation of frequencies, on the messages displayed you will see how far the installation has progressed. The display is continuously updated.

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

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

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

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

11.2 Controller Configuration

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

11.2.1 General

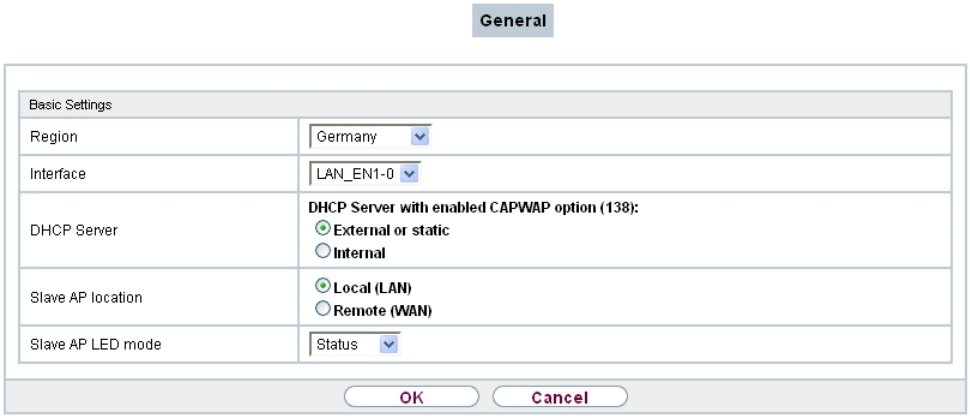


Fig. 60: **Wireless LAN Controller**->**Controller Configuration**->**General**

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

Fields in the Basic Settings menu.

Field	Description
Region	Select the country in which the wireless LAN controller is to be operated. Possible values are all the countries configured on the device's wireless module.

Field	Description
	The range of channels that can be used varies depending on the country setting. The default value is *Germany*.
Interface	Select the interface to be used for the wireless controller.
DHCP Server	Select whether an external DHCP server shall assign IP addresses to the APs or if you wish to assign fixed IP addresses yourself. Alternatively, you can use your device as a DHCP server. For this internal DHCP server, CAPWAP option 138 is active in order to allow communication between the master and slaves. Please note: Make sure that option 138 is active when using an external DHCP server. If you wish to use a bintec elmeg Gateway for example as a DHCP server, click on the **GUI** menu for this device under **Local Services**->**DHCP Server**->**DHCP Pool**->**New**->**Advanced Settings** in the **DHCP Options** field on the **Add** button. Select as **Option** *CAPWAP Controller* and in the **Value** field enter the IP address of the WLAN controller. If you use static IP addresses in your network, you must enter these to all APs manually. The IP addresses of the wireless LAN controller must be entered for each AP in the **System Management**->**Global Settings**->**System** menu in the **Manual WLAN Controller IP Address** field. Possible values: • *External or static* (default value): An external DHCP server with an CAPWAP option 138 enabled assigns the IP addresses to the APs or you can give static IP addresses to the APs. • *Internal*: Your device, on which the CAPWAP option 138 is active, assigns the IP addresses to the APs.
IP Address Range	Only for **DHCP Server** = *Internal* Enter the start and end IP address of the range. These IP addresses and your device must originate from the same network.

Field	Description
Slave AP location	Select whether the APs that the wireless LAN controller is to manage are located in the LAN or the WAN. Possible values: • *Local (LAN)* (default value) • *Remote (WAN)* The *Remote (WAN)* setting is useful if, for example, there is a wireless LAN controller installed at head office and its APs are distributed to different branches. If the APs are linked via VPN, it may be that a connection is terminated. If this happens, the relevant AP with the setting *Remote (WAN)* maintains its configuration until the connection is reestablished. It then boots up and the controller and the AP then resynchronize.
Slave AP LED mode	Select the lighting scheme of the slave AP LEDs. Possible values: • *State* (default value): Only the status LED flashes once per second. • *Flashing*: All LEDs show their standard behavior. • *Off*: All LEDs are deactivated.

11.3 Slave AP configuration

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

11.3.1 Slave Access Points

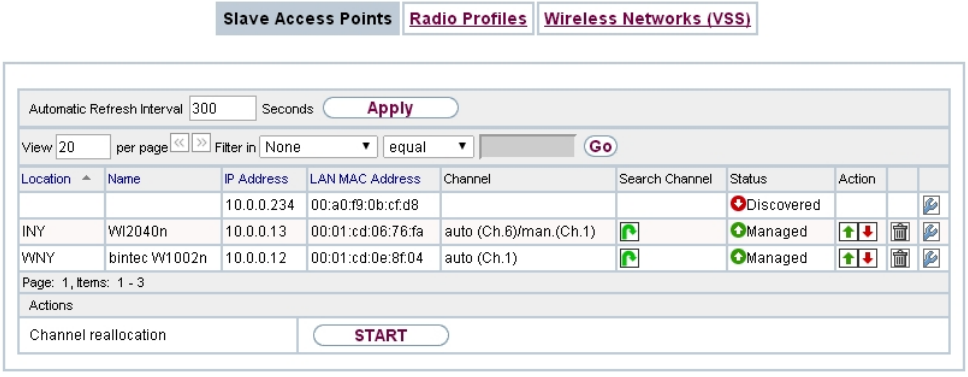


Fig. 61: **Wireless LAN Controller->Slave AP configuration->Slave Access Points**

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

You will see an entry with a parameter set for each access point (**Location**, **Name**, **IP Address**, **LAN MAC Address**, **Channel**, **Search Channel**, **Status**, **Action**). Choose whether the selected Access Pont is to be managed by the WLAN Controller by clicking the button or the button in the **Action** column.

You can disconnect the Access Point from the WLAN Controller and therefore remove it from your WLAN infrastructure by click on the button. The Access Point then receives the *Discovered* status, but is no longer *Managed*.

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

Possible values for Status

Status	Meaning
Discovered	The AP has registered at the wireless LAN controller. The controller has prompted the required parameters from the AP.
Initialising	The WLAN controller and the APs "communicate" via CAPWAP. The configuration is transferred and enabled to the APs.
Managed	The AP is set to "Managed" status. The controller has sent a configuration to the AP and has enabled this. The AP is managed centrally from the controller and cannot be configured via the **GUI**.
No License Available	The AP does not have an unassigned licence for this AP.

Status	Meaning
Offline	The AP is either administratively disabled or switched off or has its power supply cut off etc.

11.3.1.1 Edit

Choose the icon to edit existing entries.

You can also delete entries using the icon. If you have deleted APs, these will be located again but shall not be configured.

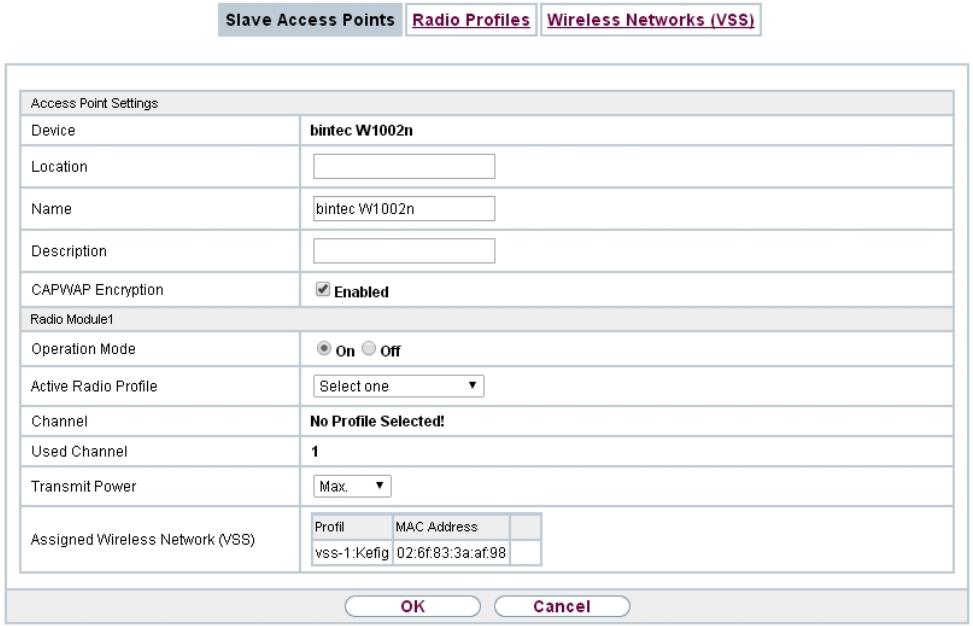


Fig. 62: **Wireless LAN Controller->Slave AP configuration->Slave Access Points->**

The data for wireless module 1 and wireless module 2 are displayed in the **Wireless LAN Controller->Slave AP configuration->Slave Access Points->** menu if the corresponding device has two wireless modules. With devices featuring a single wireless module, the data for wireless module 1 are displayed.

The menu consists of the following fields:

Fields in the Access Point Settings menu.

Field	Description
Device	Displays the type of device for the AP.

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

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

Field	Description
Operation Mode	Displays the mode in which the wireless module is to be operated. You can change the mode. Possible values: • *On* (default value): The wireless module is used as an access point in your network. • *Off*: The wireless module is not active.
Active Radio Profile	Displays the wireless module profile that is currently selected. You can select another wireless module profile from the list if more than one wireless module profile are being set up.
Channel	Displays the channel that is assigned. You can select another channel. The number of channels you can select depends on the country setting. Please consult the data sheet for your device. Access Point mode Configuring the network name (SSID) in Access Point mode means that wireless networks can be logically separated from each other, but they can still physically interfere with each other

Field	Description
	if they are operating on the same or closely adjacent wireless channels. So if you are operating two or more radio networks close to each other, it is advisable to allocate the networks to different channels. Each of these should be spaced at least four channels apart, as a network also partially occupies the adjacent channels. In the case of manual channel selection, please make sure first that the APs actually support these channels. Possible values (according to the selected wireless module profile): • For **Active Radio Profile** = *2.4 GHz Radio Profile* Possible values are *1* to *13* and *Auto* (default value). • For **Active Radio Profile** = *5 GHz Radio Profile* Possible values are *36*, *40*, *44*, *48* and *Auto* (default value)
Used Channel	Only for managed APs. Displays the channel that is currently in use.
Transmit Power	Displays the transmission power. You can select another transmission power. Possible values: • *Max.* (default value): The maximum antenna power is used. • *5 dBm* • *8 dBm* • *11 dBm* • *14 dBm* • *16 dBm* • *17 dBm*
Assigned Wireless Network (VSS)	Displays the wireless networks that are currently assigned.

11.3.2 Radio Profiles

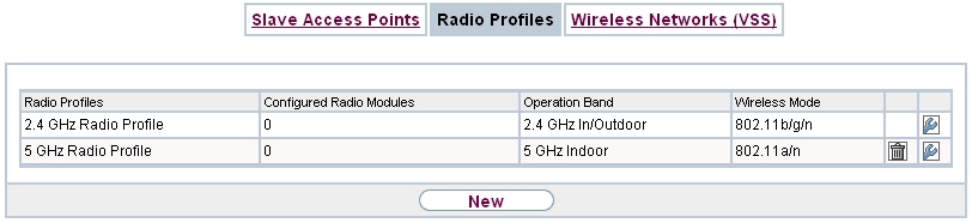


Fig. 63: **Wireless LAN Controller->Slave AP configuration->Radio Profiles**

An overview of all created wireless module profiles is displayed in the **Wireless LAN Controller->Slave AP configuration->Radio Profiles** menu. A profile with 2.4 GHz and a profile with 5 GHz are created by default; the 2.4 GHz profile cannot be deleted.

For each wireless module profile you will see an entry with a parameter set (**Radio Profiles**, **Configured Radio Modules**, **Operation Band**, **Wireless Mode**).

11.3.2.1 Edit or New

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

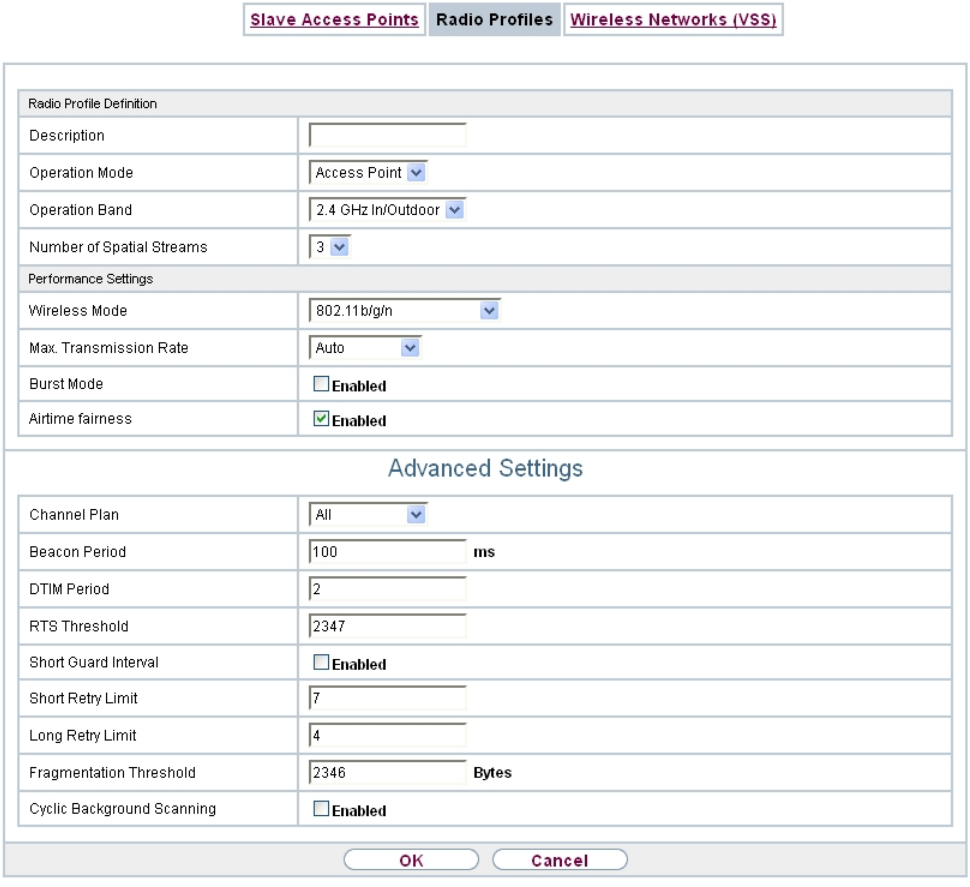


Fig. 64: **Wireless LAN Controller->Slave AP configuration->Radio Profiles->** **/ New**

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

Fields in the menu Radio Profile Definition

Field	Description
Description	Enter the desired description of the wireless module profile.
Operation Mode	Define the mode in which the wireless module profile is to be operated. Possible values: • *Off* (default value): The wireless module profile is not active. • *Access Point*: Your device is used as an access point in

Field	Description
	your network.
Operation Band	Select the frequency band of the wireless module profile. Possible values: • *2.4 GHz In/Outdoor* (default value): Your device is operated at 2.4 GHz (mode 802.11b, mode 802.11g and mode 802.11n), inside or outside buildings. • *5 GHz Indoor*: Your device is operated at 5 GHz (mode 802.11a/h and mode 802.11n) inside buildings. • *5 GHz Outdoor*: Your device is operated at 5 GHz (mode 802.11a/h and mode 802.11n) outside buildings. • *5 GHz In/Outdoor*: Your device is operated at 5 GHz (mode 802.11a/h and mode 802.11n) inside or outside buildings. • *5.8 GHz Outdoor*: Only for so-called Broadband Fixed Wireless Access (BFWA) applications. The frequencies in the frequency range from 5755 MHz to 5875 MHz may only be used in conjunction with commercial offers for public network accesses and requires registration with the Federal Network Agency.
Bandwidth	Not for **Operation Band** = *2.4 GHz In/Outdoor* Select how many channels are to be used. Possible values: • *20 MHz* (default value): One channel with 20 MHz bandwidth is used. • *40 MHz*: Two channels each with 20 MHz bandwidth are used. In the case one channel acts as a control channel and the other as an expansion channel.
Number of Spatial Streams	Select how many traffic flows are to be used in parallel. Possible values: • *3*: Three traffic flows are used. • *2*: Two traffic flows are used. • *1*: One traffic flow is used.

Fields in the menu Performance Settings

Field	Description
Wireless Mode	Select the wireless technology that the access point is to use. For **Operation Band** = *2.4 GHz In/Outdoor* Possible values: • *802.11g*: The device operates only in accordance with 802.11g. 802.11b clients have no access. • *802.11b*: Your device operates only in accordance with 802.11b and forces all clients to adapt to it. • *802.11 mixed (b/g)*: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. • *802.11 mixed long (b/g)*: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. Only a data rate of 1 and 2 mbps needs to be supported by all clients (basic rates). This mode is also needed for Centrino clients if connection problems occur. • *802.11 mixed short (b/g)*: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. The following applies for mixed-short: The data rates 5.5 and 11 mbps must be supported by all clients (basic rates). • *802.11b/g/n*: Your device operates according to either 802.11b, 802.11g or 802.11n. • *802.11g/n*: Your device operates according to either 802.11g or 802.11n. • *802.11n*: Your device operates only according to 802.11n. For **Operation Band** = *5 GHz Indoor*, *5 GHz Outdoor*, *5 GHz In/Outdoor* or *5.8 GHz Outdoor* Possible values: • *802.11a*: The device operates only in accordance with 802.11a. • *802.11n*: Your device operates only according to 802.11n. • *802.11a/n*: Your device operates according to either 802.11a or 802.11n.

Field	Description
Max. Transmission Rate	Select the transmission speed. Possible values: • *Auto* (default value): The transmission speed is determined automatically. • *<Value>*: According to setting for **Operation Band**, **Bandwidth**, **Number of Spatial Streams** and **Wireless Mode** various fixed values in mbps are available.
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 disabled by default. If problems occur with older WLAN hardware, this function should not be active.
Airtime fairness	This function is not available for all devices. The **Airtime fairness** function ensures that the access point's send resources are distributed intelligently to the connected clients. This means that a powerful client (e. g. a 802.11n client) cannot achieve only a poor flow level, because a less powerful client (e. g. a 802.11a client) is treated in the same way when apportioning. The function is enabled with *Enabled*. The function is disabled by default. This fuction is only applied to unprioritized frames of the WMM Classe "Background".

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

Fields in the menu Advanced Settings

Field	Description
Channel Plan	Select the desired channel plan. The channel plan makes a preselection when a channel is se-

Field	Description
	lected. This ensures that no channels overlap, i.e. a distance of four channels is maintained between the channels used. This is useful if more access points are used with overlapping radio cells. Possible values: • *All*: All channels can be dialled when a channel is selected. • *Auto*: Depending on the region, operation band, wireless mode and bandwidth, the channels that have a distance of 4 channels are provided. • *User defined*: You can select the desired channels yourself.
User Defined Channel Plan	Only for **Channel Plan** = *User defined* The currently selected channels are displayed here. With **Add** you can add channels. If all available channels are displayed, you cannot add any more entries. You can also delete entries using the  icon.
Beacon Period	Enter the time in milliseconds between the sending of two beacons. This value is transmitted in Beacon and Probe Response Frames. Possible values are *1* to *65535*. The default value is *100*.
DTIM Period	Enter the interval for the Delivery Traffic Indication Message (DTIM). The DTIM field is a data field in transmitted beacons that informs clients about the window to the next broadcast or multicast transmission. If clients operate in power save mode, they come alive at the right time and receive the data. Possible values are *1* to *255*. The default value is *2*.

Field	Description
RTS Threshold	Here you can specify the data packet length threshold in bytes (1..2346) as of which the RTS/CTS mechanism is to be used. This makes sense if several clients that are not in each other's wireless range are run in one access point.
Short Guard Interval	Enable this function to reduce the guard interval (= time between transmission of two data symbols) from 800 ns to 400 ns.
Short Retry Limit	Enter the maximum number of attempts to send a frame with length less than or equal to the value defined in **RTS Threshold**. After this many failed attempts, the packet is discarded. Possible values are *1* to *255*. The default value is *7*.
Long Retry Limit	Enter the maximum number of attempts to send a data packet of length greater than the value defined in **RTS Threshold**. After this many failed attempts, the packet is discarded. Possible values are *1* to *255*. The default value is *4*.
Fragmentation Threshold	Enter the maximum size as of which the data packets are to be fragmented (i.e. split into smaller units). Low values are recommended for this field in areas with poor reception and in the event of radio interference. Possible values are *256* to *2346*. The default value is *2346*.
Cyclic Background Scanning	Not all devices support this function. You can enable the **Cyclic Background Scanning** function so that a search is run at regular intervals for neighbouring or rogue access points in the network. This search is run without negatively impacting the function as an access point. Enable or disable the function **Cyclic Background Scanning**.

Field	Description
	The function is enabled with *Enabled*. The function is not activated by default.

11.3.3 Wireless Networks (VSS)

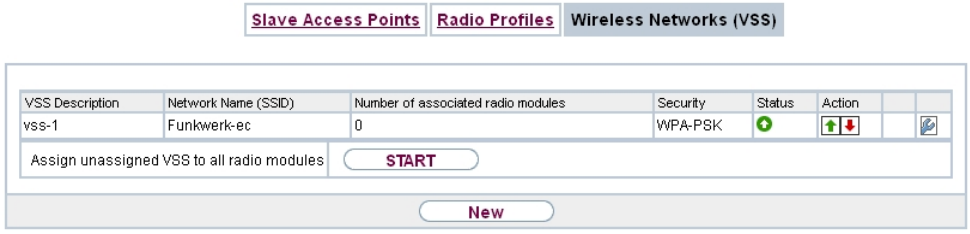


Fig. 65: **Wireless LAN Controller->Slave AP configuration->Wireless Networks (VSS)**

An overview of all created wireless networks is displayed in the **Wireless LAN Controller->Slave AP configuration->Wireless Networks (VSS)** menu. A wireless network is created by default.

For every wireless network (VSS), you see an entry with a parameter set (**VSS Description**, **Network Name (SSID)**, **Number of associated radio modules**, **Security**, **Status**, **Action**).

Under **Assign unassigned VSS to all radio modules** click on the **Start** button to assign a newly-created VSS to all wireless modules.

11.3.3.1 Edit or New

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

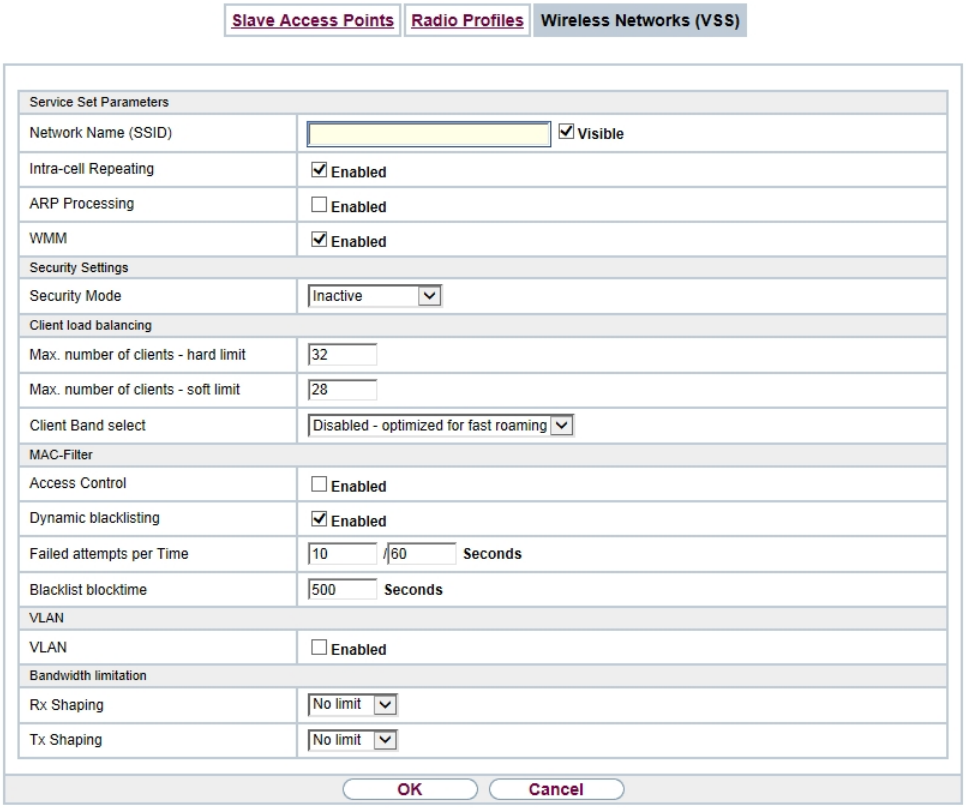


Fig. 66: **Wireless LAN Controller->Slave AP configuration->Wireless Networks (VSS)->New**

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

Fields in the menu Service Set Parameters

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

Field	Description
	be permitted within a radio cell. The function is activated by selecting *Enabled*. The function is enabled by default.
ARP Processing	Select whether the ARP processing function should be enabled. The ARP data traffic is reduced in the network by the fact that ARP broadcasts that have been converted to ARP unicasts are forwarded to IP addresses that are known internally. Unicasts are quicker and clients with an enabled power save function are not addressed. The function is activated by selecting *Enabled*. The function is disabled by default. Make sure that ARP processing cannot be applied together with the MAC bridge function.
WMM	Select whether voice or video prioritisation via WMM (Wireless Multimedia) is to be activated for the wireless network so that optimum transmission quality is always achieved for time-critical applications. Data prioritisation is supported in accordance with DSCP (Differentiated Services Code Point) or IEEE802.1d. The function is activated by selecting *Enabled*. The function is enabled by default.

Fields in the menu Security Settings

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

Field	Description
	• *WPA Enterprise*: 802.11x
Transmit Key	Only for **Security Mode** = *WEP 40* or *WEP 104* Select one of the keys configured in **WEP Key** as a standard key. The default value is *Key 1*.
WEP Key 1-4	Only for **Security Mode** = *WEP 40*, *WEP 104* Enter the WEP key. Enter a character string with the right number of characters for the selected WEP mode. For *WEP 40* you need a character string with 5 characters, for *WEP 104* with 13 characters, e. g. *hello* for *WEP 40*, *wep1* for *WEP 104*.
WPA Mode	Only for **Security Mode** = *WPA-PSK* and *WPA Enterprise* Select whether you want to use WPA (with TKIP encryption) or WPA 2 (with AES encryption), or both. Possible values: • *WPA and WPA 2* (default value): WPA and WPA 2 can be used. • *WPA*: Only WPA is used. • *WPA 2*: Only WPA2 is used.
WPA Cipher	Only for **Security Mode** = *WPA-PSK* and *WPA Enterprise* and for **WPA Mode** = *WPA* and *WPA and WPA 2* Select the type of encryption you want to apply to WPA. Possible values: • *TKIP* (default value): TKIP is used. • *AES*: AES is used. • *AES and TKIP*: AES or TKIP is used.
WPA2 Cipher	Only for **Security Mode** = *WPA-PSK* and *WPA Enterprise* and for **WPA Mode** = *WPA 2* and *WPA and WPA 2*

Field	Description
	Select the type of encryption you want to apply to WPA2. Possible values: • *AES* (default value): AES is used. • *TKIP*: TKIP is used. • *AES and TKIP*: AES or TKIP is used.
Preshared Key	Only for **Security Mode** = *WPA-PSK* Enter the WPA password. Enter an ASCII string with 8 - 63 characters. Note: Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!
Radius Server	You can control access to a wireless network via a RADIUS server. With **Add**, you can create new entries. Enter the IP address and the password of the RADIUS server.
EAP Preauthentification	Only for **Security Mode** = *WPA Enterprise* Select whether the EAP preauthentification function is to be activated. This function tells your device that WLAN clients, which are already connected to another access point, can first carry out 802.1x authentication as soon as they are within range. Such WLAN clients can then simply connect over the existing network connection with your device. The function is activated by selecting *Enabled*. The function is enabled by default.

Fields in the menu Client load balancing

Field	Description
Max. number of clients - hard limit	Enter the maximum number of clients that can be connected to this wireless network (SSID) The maximum number of clients that can register with a wire-

Field	Description
	less module depends on the specifications of the respective WLAN module. This maximum is distrubuted across all wireless networks configured for this radio module. No more new wireless networks can be created and a warning message will appear if the maximum number of clients is reached. Possible values are whole numbers between *1* and *254*. The default value is *32*.
Max. number of clients - soft limit	Not all devices support this function. To avoid a radio module being fully utilised, you can set a "soft" restriction on the number of connected clients. If this number is reached, new connection queries are initially rejected. If the client cannot find another wireless network and, therefore, repeats its query, the connection is accepted. Queries are only definitively rejected when the **Max. number of clients - hard limit** is reached. The value of the **Max. number of clients - soft limit** must be the same as or less than that of the **Max. number of clients - hard limit**. The default value is *28*. You can disable this function if you set **Max. number of clients - soft limit** and **Max. number of clients - hard limit** to identical values.
Client Band select	Not all devices support this function. This function requires a dual radio setup where the same wireless networkis configured on both radio modules, but in different frequency bands. The **Client Band select** option enables clients to be moved from the frequency band originally selected to a less busy one, providing the client supports this. To achieve a changeover, the connection attempt of a client is initially refused so that the client repeats the attempt in a different frequency band. Possible values: • *Disabled - optimized for fast roaming* (default

Field	Description
	value): The function is not used for this VSS. This is useful if clients are to switch between different radio cells with as little delay as possible, e. g. with Voice over WLAN. • *2,4 GHz band preferred*: Preference is given to accepting clients in the 2.4 GHz band. • *5 GHz band preferred*: Preference is given to accepting clients in the 5 GHz band.

Fields in the menu MAC-Filter

Field	Description
Access Control	Select whether only certain clients are to be permitted for this wireless network. The function is activated by selecting *Enabled*. The function is disabled by default.
Allowed Addresses	Use **Add** to make entries and enter the MAC addresses (**MAC Address**) of the clients to be permitted.
Dynamic blacklisting	You can use the **Dynamic blacklisting** function to identify clients that want to gain possibly unauthorised access to the network and block them for a certain length of time. A client is blocked if the number of unsuccessful login attempts with a specified time exceeds a certain number. This threshold value and the duration of the block can be configured. A blocked client is blocked at all the APs that are managed by the wireless LAN controller for the VSS concerned, so neither are they able to log into a different radio cell in that VSS. If a client needs to be blocked permanently, this can be done in the **Wireless LAN Controller**->**Monitoring**->**Rogue Clients** menu. The function is activated by selecting *Enabled*. The function is activated by default.
Failed attempts per Time	Enter the number of failed attempts that have to originate from a specific MAC address during a certain time for a blacklist entry to be created. Default values are *10* failed attempts during *60* seconds.

Field	Description
Blacklist blocktime	Enter the time for which an entry in the dynamic blacklist remains valid. Default value is *500* seconds.

Fields in the menu VLAN

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

Fields in the menu Bandwidth limitation for each WLAN client

Field	Description
Rx Shaping	Select a bandwidth limitation in the receive direction. Possible values are • *No limit* (default value) • *1 Mbit/s* up to *10 Mbit/s* in single Mbit/s steps, *15 Mbit/s*, *20 Mbit/s*, *30 Mbit/s*, *40 Mbit/s* and *50 Mbit/s*.
Tx Shaping	Select a bandwidth limitation in the transmit direction. Possible values are • *No limit* (default value) • *1 Mbit/s* up to *10 Mbit/s* in single Mbit/s steps, *15 Mbit/s*, *20 Mbit/s*, *30 Mbit/s*, *40 Mbit/s* and *50 Mbit/s*.

11.4 Monitoring

This menu is used to monitor your WLAN infrastructure.

Note

In order to ensure adequate timing between the WLAN Controller and the connected Slave APs, the internal time server of the WLAN Controller should be enabled.

11.4.1 WLAN Controller

Fig. 67: **Wireless LAN Controller->Monitoring->WLAN Controller**

In the **Wireless LAN Controller->Monitoring->WLAN Controller** menu, an overview of the most relevant Wireless LAN Controller parameters is displayed. The display is refreshed every 30 seconds.

Values in the Overview list

Status	Meaning
AP discovered	Displays the number of discovered access points.
AP offline	Displays the number of access points not connected to the Wireless LAN Controller.

Status	Meaning
AP managed	Displays the number of managed access points.
WLAN Controller: VSS throughput	Displays the data traffic in receive and transmit direction in bytes per second.
CPU usage [%]	Displays the percentaged CPU load over time.
Memory usage [%]	Displays the percentaged memory consumption over time.
Connected clients/VSS	Displays the number of connected clients per wireless network (VSS) over time.

11.4.2 Slave Access Points

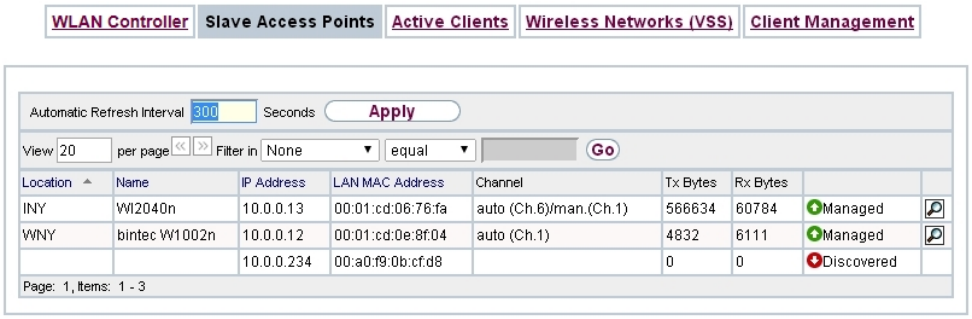


Fig. 68: **Wireless LAN Controller->Monitoring->Slave Access Points**

LAN MAC Address

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

11.4.2.1 Overview

In the **Overview** menu, additional information about the selected access point is displayed. The display is refreshed every 30 seconds.

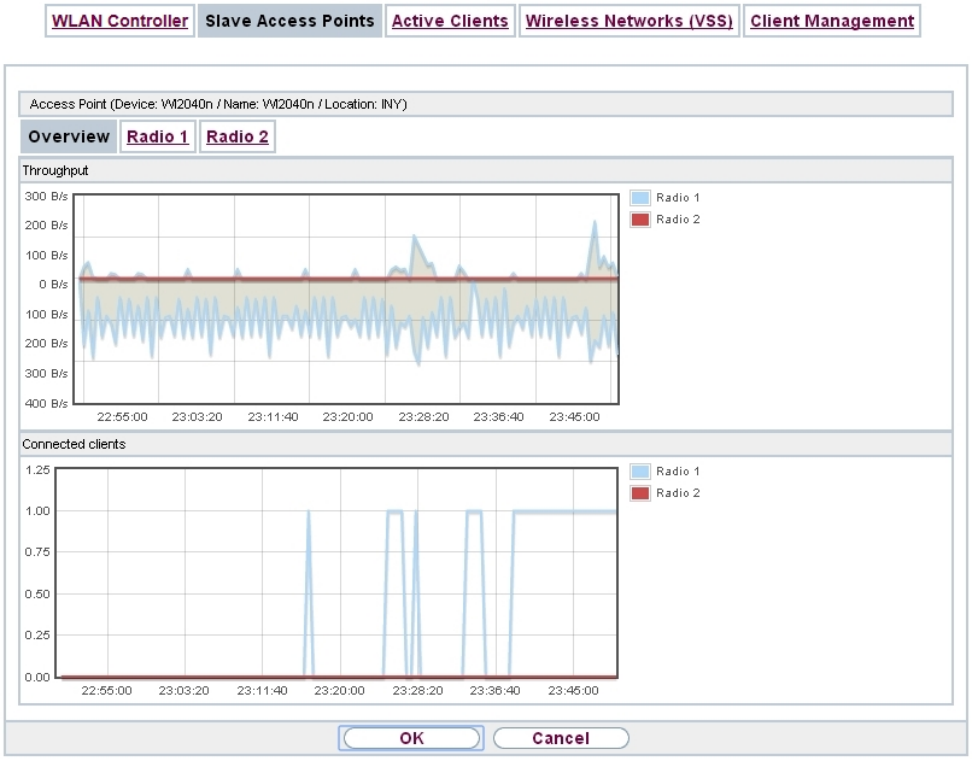


Fig. 69: **Wireless LAN Controller->Monitoring->Slave Access Points->Overview**

Values in the Overview list

Status	Meaning
Throughput	Displays the received and transmitted data traffic per radio module over time.
Connected clients	Displays the number of connected clients per radio module over time.

11.4.2.2 Radio 1

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

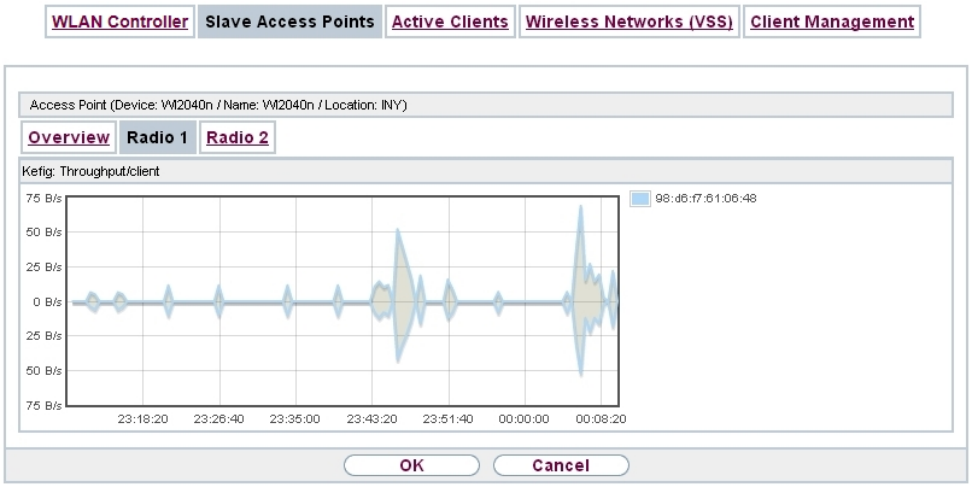


Fig. 70: **Wireless LAN Controller->Monitoring->Slave Access Points->Radio**

Values in the Radio list

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

11.4.3 Active Clients

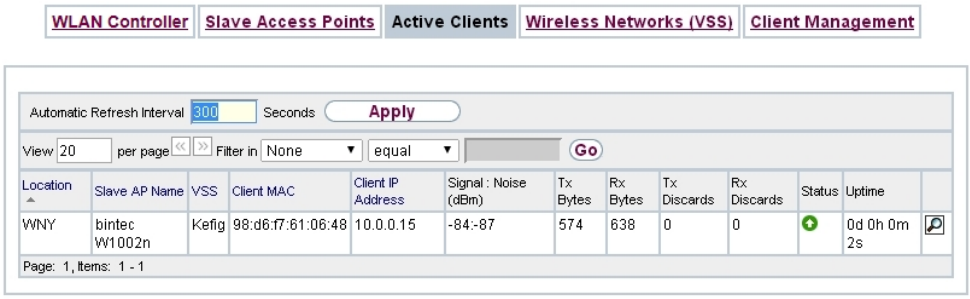


Fig. 71: **Wireless LAN Controller->Monitoring->Active Clients**

In the **Wireless LAN Controller->Monitoring->Active Clients** menu, current values of all active clients are displayed.

For each client you will see an entry with the following parameter set: **Location**, **Slave AP Name**, **VSS**, **Client MAC**, **Client IP Address**, **Signal : Noise (dBm)** , **Tx Bytes**, **Rx Bytes**, **Tx Discards**, **Rx Discards**, **Status**, **Uptime**.

Possible values for Status

Status	Meaning
None	The client is no longer in a valid status.
Logon	The client is currently logging on with the WLAN.
Associated	The client is logged on with the WLAN.
Authenticate	The client is in the process of being authenticated.
Authenticated	The client is authenticated.

Via the icon, you can open a summary with additional details about the **Active Clients**.

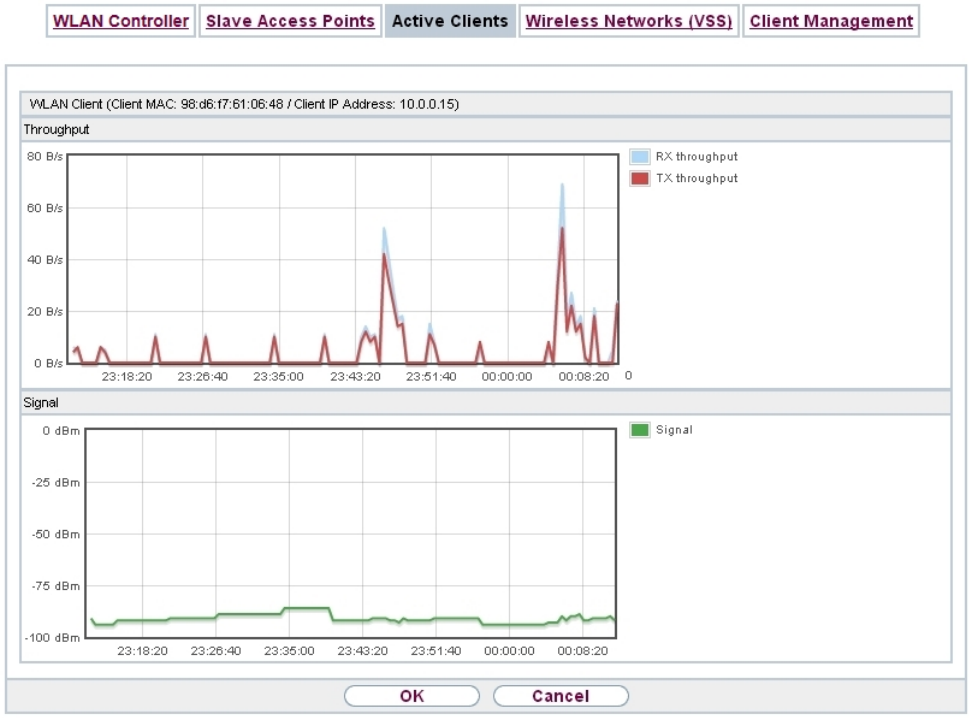


Fig. 72: **Wireless LAN Controller->Monitoring->Active Clients->**

Value in the list WLAN Client list

Status	Meaning
Throughput	Displays the data traffic - separated into received and transmitted traffic - for the selected WLAN client over time.
Signal	Displays the signal strength of the selected WLAN client over time.

11.4.4 Wireless Networks (VSS)

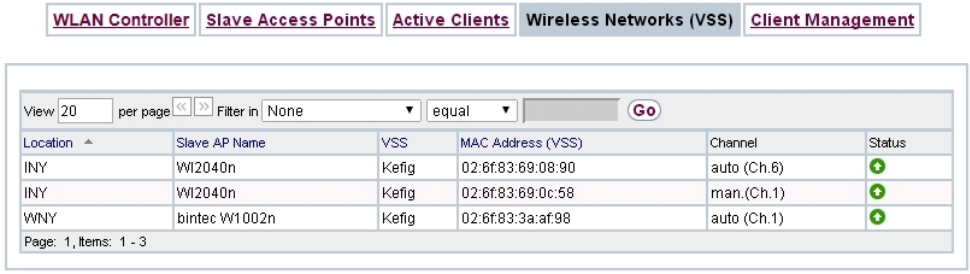


Fig. 73: **Wireless LAN Controller->Monitoring->Wireless Networks (VSS)**

In the **Wireless LAN Controller->Monitoring->Wireless Networks (VSS)** menu, an overview of the currently used AP is displayed. You see which wireless module is assigned to which wireless network. For each wireless a parameter set is displayed (**Location**, **Slave AP Name**, **VSS**, **MAC Address (VSS)**, **Channel**, **Status**).

11.4.5 Client Management

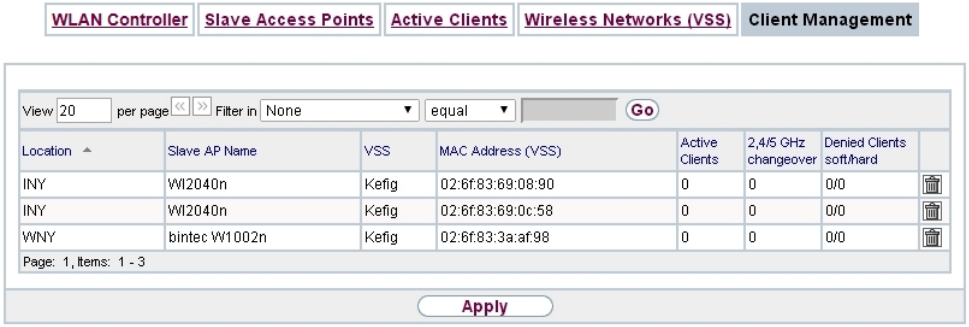


Fig. 74: **Wireless LAN Controller->Monitoring->Client Management**

The **Wireless LAN Controller->Monitoring->Client Management** menu displays information on the client management by the access points. You can, e.g., see the number of connected clients, the number of clients that are affected by the **2,4/5 GHz changeover** and the number of rejected clients.

You can delete the values of an entry using the symbol.

11.5 Neighbor Monitoring

This menu serves the monitoring of remote access points.

11.5.1 Neighbor APs

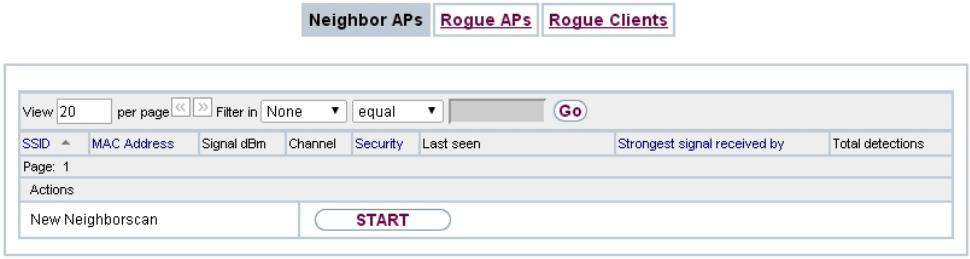


Fig. 75: **Wireless LAN Controller+Neighbor Monitoring->Neighbor APs**

In the **Wireless LAN Controller+Neighbor Monitoring->Neighbor APs** menu, the adjacent AP's found during the scan are displayed. **Rogue APs**, i.e. APs which are not managed by the WLAN controller but are using an SSID managed by the WLAN controller are highlighted in red.

Note

Check the rogue APs shown carefully, as an attacker could attempt to spy on data in your network using a rogue AP.

Although each AP is found more than once, it is only displayed once with the strongest signal. You see the following parameters for each AP: **SSID**, **MAC Address**, **Signal dBm**, **Channel**, **Security**, **Last seen**, **Strongest signal received by** , **Total detections**.

The entries are displayed in alphabetical order by **SSID**. **Security** shows the security settings of the AP. Under **Strongest signal received by**, you will see the parameters **Location** and **Name** of the APs in which the displayed AP was found. **Total detections** shows how often the corresponding AP was found during the scan.

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

11.5.2 Rogue APs

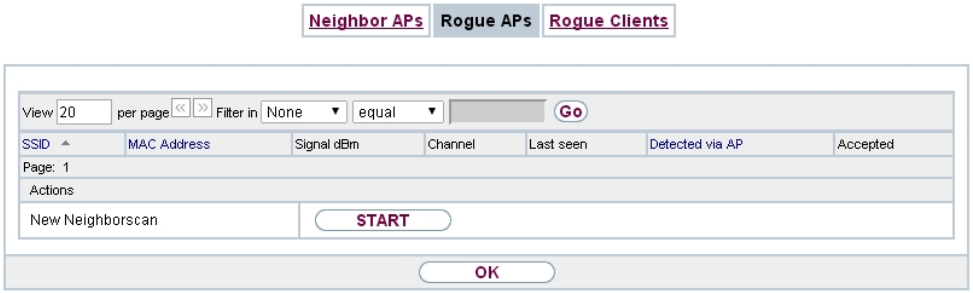


Fig. 76: **Wireless LAN Controller+Neighbor Monitoring->Rogue APs**

APs which are using an SSID from their own network but are not managed by **Wireless LAN Controller** are displayed in the **Wireless LAN Controller+Neighbor Monitoring->Rogue APs** menu. **Rogue APs** which have been found for the first time are displayed with a red background.

For each rogue AP you will see an entry with the following parameter set: **SSID**, **MAC Address**, **Signal dBm**, **Channel**, **Last seen**, **Detected via AP**,**Accepted**.

Note

Check the rogue APs shown carefully, as an attacker could attempt to spy on data in your network using a rogue AP.

You can class a rogue AP as trustworthy by enabling the **Accepted** checkbox. If an alarm has been configured, this is then removed and no longer sent. The red background disappears.

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

11.5.3 Rogue Clients

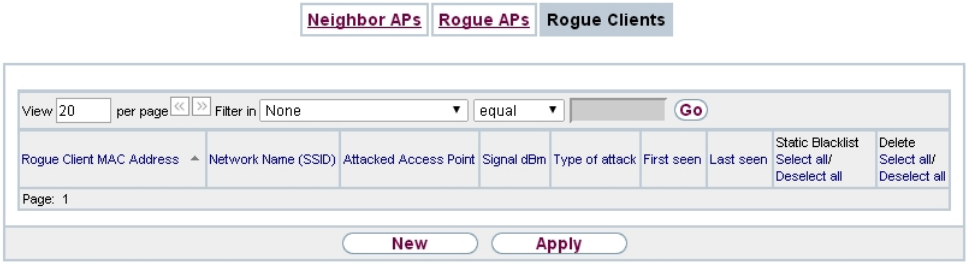


Fig. 77: **Wireless LAN Controller+Neighbor Monitoring->Rogue Clients**

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

Possible values for Rogue Clients

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

11.5.3.1 New

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

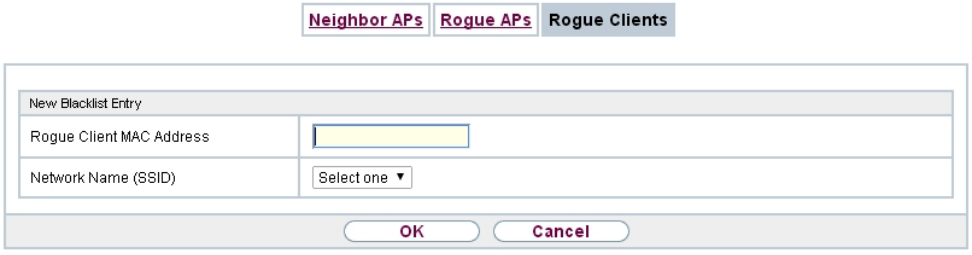


Fig. 78: **Wireless LAN Controller+Neighbor Monitoring->Rogue Clients->New**

The menu consists of the following fields:

Fields in the New Blacklist Entry menu

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

11.6 Maintenance

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

11.6.1 Firmware Maintenance

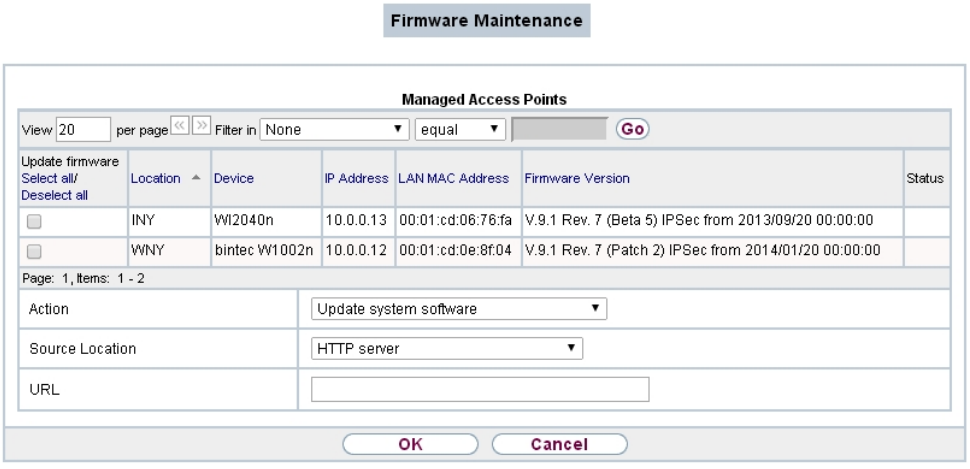


Fig. 79: **Wireless LAN Controller->Maintenance->Firmware Maintenance**

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

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

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

Possible values for Status

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

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

Fields in the Firmware Maintenance menu

Field	Description
Action	Select the action you wish to execute. After each task, a window is displayed showing the other steps that are required. Possible values: • *Update system software*: You can also start an update of the system software. • *Save configuration with state information*: You can save a configuration which contains the AP status information.
Source Location	Select the source for the action. Possible values: • *HTTP server* (default value): The file is stored respectively on a remote server specified in the **URL**. • *Current Software from Update Server*: The file is on the official update server. (Only for **Action**= *Update system software*) • *TFTP server*: The file is stored respectively on a TFTP server specified in the **URL**.
URL	Only for **Source Location** = *HTTP server* or *TFTP server* Enter the URL of the update server from which the system software file is loaded or on which the configuration file is saved.

Chapter 12 Networking

12.1 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**.

12.1.1 IPv4 Route Configuration

A list of all configured routes is displayed in the **Network**->**Routes**->**IPv4 Route Configuration** menu.

In the ex works state, a predefined entry with the parameters **Destination IP Address** = *192.168.0.0*, **Netmask** = *255.255.255.0*,**Gateway** = *192.168.0.250*, **Interface** = *LAN_EN1-0*, **Route Type** = *Network Route via Interface* is displayed.

12.1.1.1 Edit or New

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

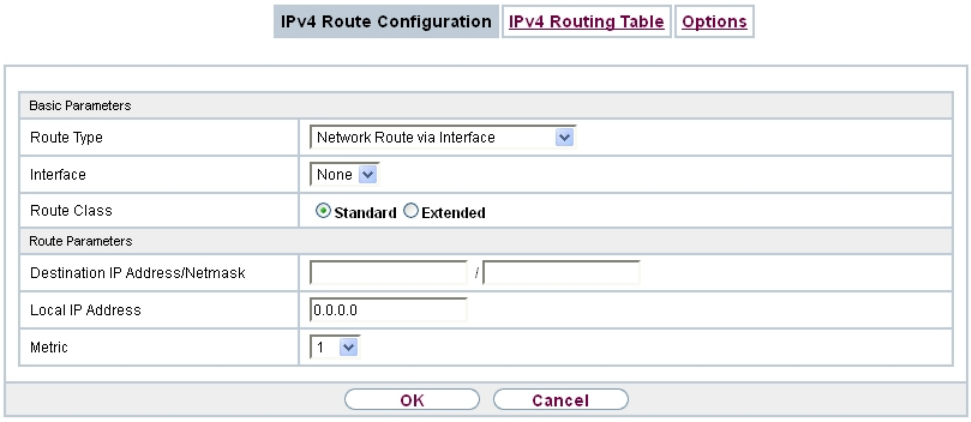


Fig. 80: **Network->Routes->IPv4 Route Configuration->New** *with* **Extended Route** = *Standard.*

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

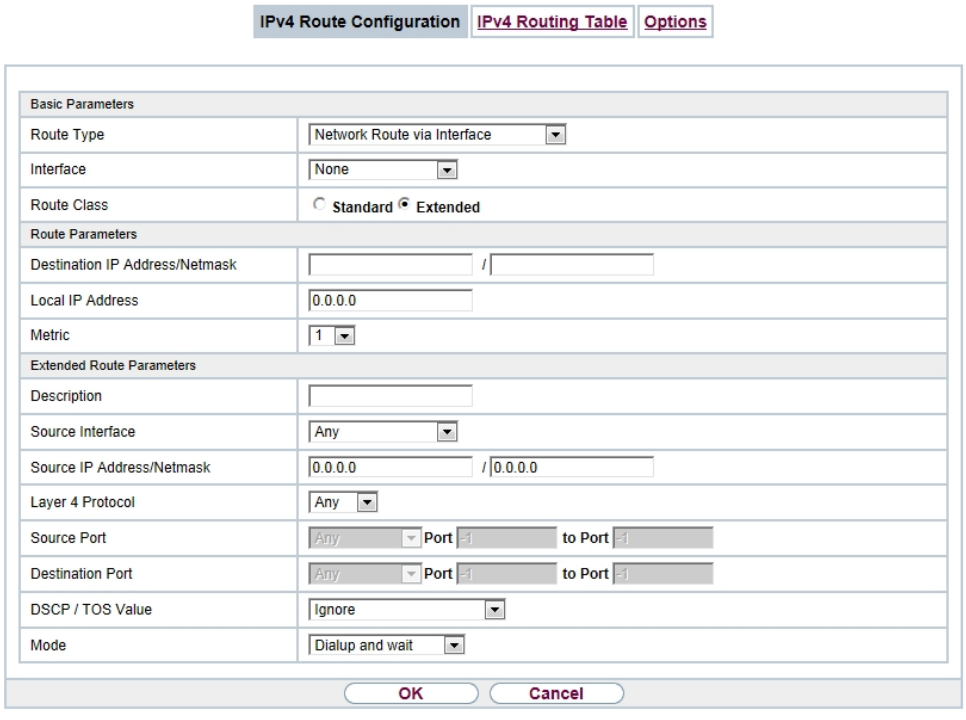


Fig. 81: **Network->Routes->IPv4 Route Configuration->New** *with* **Extended** = `Enabled`

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

fields:

Fields in the menu Basic Parameters

Field	Description
Route Type	Select the type of route. Possible values: • *Default Route via Interface*: Route via a specific interface which is to be used if no other suitable route is available. • *Default Route via Gateway*: Route via a specific gateway which is to be used if no other suitable route is available. • *Host Route via Interface*: Route to an individual host via a specific interface. • *Host Route via Gateway*: Route to an individual host via a specific gateway. • *Network Route via Interface* (default value): Route to a network via a specific interface. • *Network Route via Gateway*: Route to a network via a specific gateway. Only for interfaces that are operated in DHCP client mode: Even if an interface is configured for DHCP client mode, routes can still be configured for data traffic via that interface. The settings received from the DHCP server are then copied, along with those configured here, to the active routing table. This enables, e. g., in the case of dynamically changing gateway addresses, particular routes to be maintained, or routes with different metrics (i. e. of differing priority) to be specified. However, if the DHCP server sends static routes, the settings configured here are not copied to the routing. • *Default Route Template per DHCP*: The routing information is taken entirely from the DHCP server. Only advanced parameters can be additionally configured. This route remains unchanged by other routes created for this interface and is copied to the routing table in parallel with them. • *Host Route Template per DHCP*: The settings received by DHCP are supplemented by routing information about a particular host. • *Network Route Template per DHCP*: The settings re-

Field	Description
	ceived by DHCP are supplemented by routing information about a particular network.  **Note** When the DHCP lease expires or when the device is re-started, the routes that consist from the combination of DHCP settings and those made here are initially deleted once more from the active routing. If the DHCP is reconfigured they are re-generated and re-activated.
Interface	Select the interface to be used for this route.
Route Class	Select the type of **Route Class**. Possible values: • *Standard* (default value): Defines a route with the default parameters. • *Extended*: Select whether the route is to be defined with extended parameters. If the function is active, a route is created with extended routing parameters such as source interface and source IP address, as well as protocol, source and destination port, type of service (TOS) and the status of the device interface.

Fields in the menu Route Parameters

Field	Description
Local IP Address	Only for **Route Type** = *Default Route via Interface*, *Host Route via Interface* or *Network Route via Interface* Enter the IP address of the host to which your device is to forward the IP packets.
Destination IP Address/Netmask	Only for **Route Type** *Host Route via Interface* or *Network Route via Interface* Enter the IP address of the destination host or destination network.

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

Fields in the menu Extended Route Parameters

Field	Description
Description	Enter a description for the IP route.
Source Interface	Select the interface over which the data packets are to reach the device. The default value is *None*.
Source IP Address/ Netmask	Enter the IP address and netmask of the source host or source network.
Layer 4 Protocol	Select a protocol. Possible values: *ICMP*, *IGMP*, *TCP*, *UDP*, *GRE*, *ESP*, *AH*, *OSPF*, *PIM*, *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.

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

Field	Description
	• *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F. Enter the relevant value for *DSCP Binary Value*, *DSCP Decimal Value*, *DSCP Hexadecimal Value*, *TOS Binary Value*, *TOS Decimal Value* and *TOS Hexadecimal Value*.
Mode	Select when the interface defined in **Route Parameters**->**Interface** is to be used. Possible values: • *Dialup and wait* (default value): The route can be used if the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up". • *Authoritative*: The route can always be used. • *Dialup and continue*: The route can be used when the interface is "up". If the interface is "dormant", then select and use the alternative route (rerouting) until the interface is "up". • *Never dialup*: The route can be used when the interface is "up". • *Always dialup*: The route can be used when the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up". In this case, an alternative interface with a poorer metric is used for routing until the interface is "up".

12.1.2 IPv4 Routing Table

A list of all IPv4 routes is displayed in the **Network**->**Routes**->**IPv4 Routing Table** menu. The routes do not all need to be active, but can be activated at any time by relevant data traffic.

In the ex works state, a predefined entry with the parameters **Destination IP Address** = *192.168.0.0*, **Netmask** = *255.255.255.0*,**Gateway** = *192.168.0.250*, **Interface** = *LAN_EN1-0*, **Route Type** = *Network Route via Interface*, **Protocol** = *Local* is displayed.

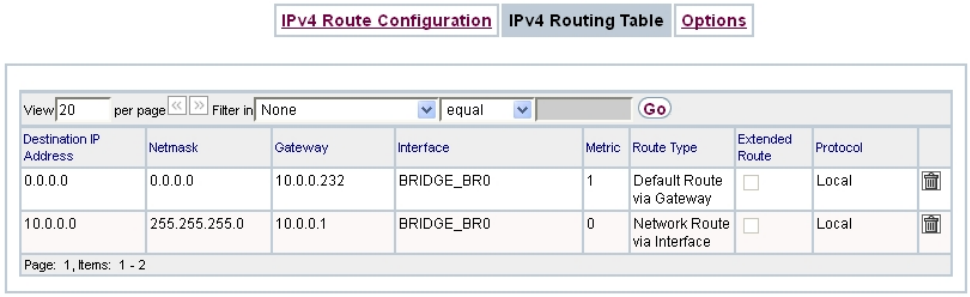


Fig. 82: **Network**->**Routes**->**IPv4 Routing Table**

Fields in the menu IPv4 Routing Table

Field	Description
Destination IP Address	Displays the IP address of the destination host or destination network.
Netmask	Displays the netmask of the destination host or destination network.
Gateway	Displays the gateway IP address. Nothing is displayed here when routes are received by DHCP.
Interface	Displays the interface used for this route.
Metric	Displays the route's priority. The lower the value, the higher the priority of the route
Route Type	Displays the route type.

Field	Description
Extended Route	Displays whether a route has been configured with advanced parameters.
Protocol	Displays how the entry has been created , e.g. manually (*Local*) or via one of the available protocols.
Delete	You can delete entries with the symbol.

12.1.3 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.

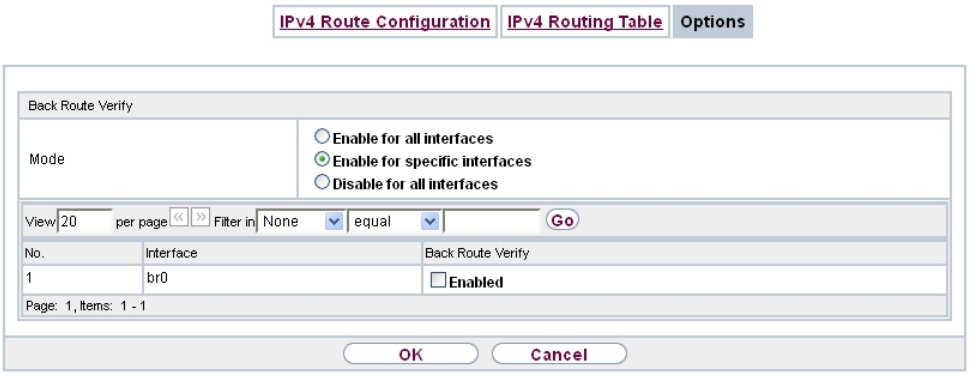


Fig. 83: **Networking->Routes->Options**

In the ex works state, the two entries *en1-0* and *ethoa35-5* are displayed by default setting *Enable for specific interfaces*.

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

Fields in the Back Route Verify menu.

Field	Description
Mode	Select how the interfaces to be activated for Back Route Verify are to be specified.

Field	Description
	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.

12.2 NAT

Network Address Translation (NAT) is a function on your device for defined conversion of source and destination addresses of IP packets. If NAT is activated, IP connections are still only allowed by default in one direction, outgoing (forward) (= protective function). Exceptions to the rule can be configured (in *NAT Configuration* on page 194).

12.2.1 NAT Interfaces

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

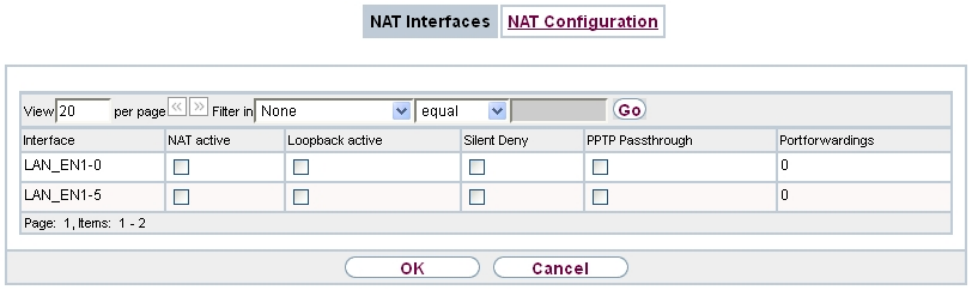


Fig. 84: **Networking->NAT->NAT Interfaces**

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

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

Options in the menu NAT Interfaces

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

Field	Description
	If **PPTP Passthrough** is enabled, the device itself cannot be configured as a tunnel endpoint.
Portforwardings	Shows the number of portforwarding rules configured in **Networking**->**NAT**->**NAT Configuration**.

12.2.2 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.

12.2.2.1 New

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

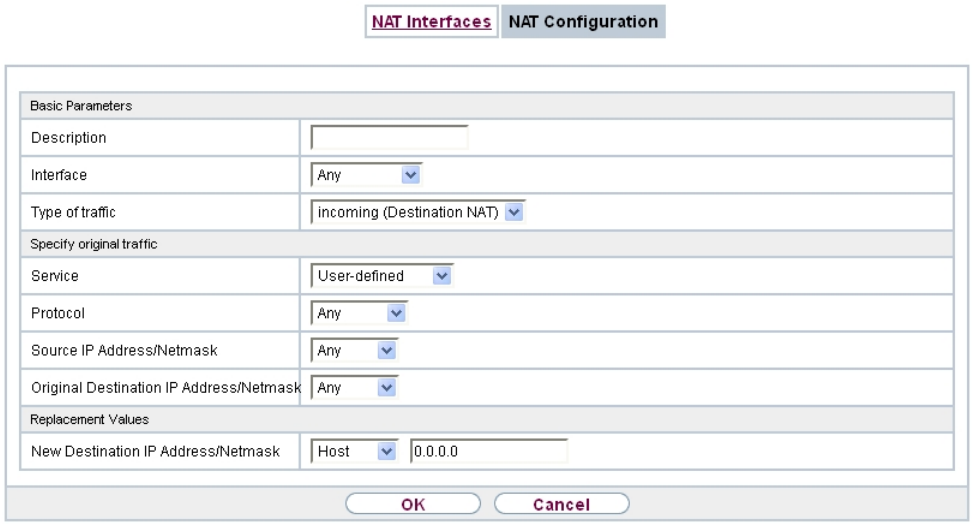


Fig. 85: **Networking**->**NAT**->**NAT Configuration**->**New**

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

Fields in the menu Basic Parameters

Field	Description
Description	Enter a description for the NAT configuration.

Field	Description
Interface	Select the interface for which NAT is to be configured. Possible values: • *Any* (default value): NAT is configured for all interfaces. • *<Interface name>*: Select one of the interfaces from the list.
Type of traffic	Select the type of data traffic for which NAT is to be configured. Possible values: • *incoming (Destination NAT)* (default value): The data traffic that comes from outside. • *outgoing (Source NAT)*: Outgoing data traffic. • *excluding (Without NAT)*: Data traffic excluded from NAT.
NAT method	Only for **Type of traffic** = *outgoing (Source NAT)* Select the NAT method for outgoing data traffic. The starting point for choosing the NAT method is a NAT scenario in which an "internal" source host has initiated an IP connection to an "external" destination host over the NAT interface, and in which an internally valid source address and internally valid source port are translated to an externally valid source address and an externally valid source port. 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

Field	Description
	within the existing connection are allowed.

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

Fields in the menu Specify original traffic

Field	Description
Service	Not for **Type of traffic** = *outgoing (Source NAT)* and **NAT method** = *full-cone*, *restricted-cone* or *port-restricted-cone*. Select one of the preconfigured services. Possible values: • *User-defined* (default value) • *<service name>*
Action	Only for **Type of traffic** = *excluding (Without NAT)* Select which data packets are to be excluded by NAT. Possible values: • *Exclude* (default value): All the data packets that match the following parameters that are to be configured (protocol, source IP address/network mask, destination IP address/netmask, etc.) are excluded by NAT. • *Do not exclude*: All the data packets that do not match the following parameters that are to be configured (protocol, source IP address/network mask, destination IP address/netmask, etc.) are excluded by NAT.
Protocol	Only for certain services. Not for **Type of traffic** = *outgoing (Source NAT)* and **NAT method** = *full-cone*, *restricted-cone* or *port-restricted-cone*. In this case UDP is automatically defined. Select a protocol. According to the selected **Service**, different protocols are available. Possible values:

Field	Description
	• *Any* (default value) • *AH* • *Chaos* • *EGP* • *ESP* • *GGP* • *GRE* • *HMP* • *ICMP* • *IGMP* • *IGP* • *IGRP* • *IP* • *IPinIP* • *IPv6* • *IPX in IP* • *ISO-IP* • *Kryptolan* • *L2TP* • *OSPF* • *PUP* • *RDP* • *RSVP* • *SKIP* • *TCP* • *TLSP* • *UDP* • *VRRP* • *XNS-IDP*
Source IP Address/ Netmask	Only for **Type of traffic** = *incoming (Destination NAT)* or *excluding (Without NAT)* Enter the source IP address and corresponding netmask of the

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

Field	Description
Destination Port/Range	Only for **Type of traffic** = *outgoing (Source NAT)*, **NAT method** = *symmetric*, **Service** = *user-defined* and **Protocol** = *TCP*, *UDP*, *TCP/UDP* or **Type of traffic** = *excluding (Without NAT)*, **Service** = *user-defined* and **Protocol** = *TCP*, *UDP*, *TCP/UDP* Enter the destination port or the destination port range of the original data packets. The default setting *-All-* means that the port remains unspecified.

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

Fields in the menu Replacement Values

Field	Description
New Destination IP Address/Netmask	Only for **Type of traffic** = *incoming (Destination NAT)* Enter the destination IP address and corresponding netmask to which the original destination IP address is to be translated.
New Destination Port	Only for **Type of traffic** = *incoming (Destination NAT)*, **Service** = *user-defined* and **Protocol** = *TCP*, *UDP*, *TCP/UDP* Leave the destination port as it appears or enter the destination port to which the original destination port is to be translated. Select *Original* to leave the original destination port. If you disable *Original*, an input field appears and you can enter a new destination port. *Original*is active by default.
New Source IP Address/Netmask	Only for **Type of traffic** = *outgoing (Source NAT)* and **NAT method** = *symmetric* Enter the source IP address to which the original source IP address is to be translated, with corresponding netmask, as the case arises.
New Source Port	Only for **Type of traffic** = *outgoing (Source NAT)*, **NAT method** = *symmetric*, **Service** = *user-defined* and **Pro-**

Field	Description
	tocol = *TCP*, *UDP*, *TCP/UDP* Leave the source port as it appears or enter a new source port to which the original source port is to be translated. *Original* leaves the original source port. If you disable *Original*, an input field appears in which you can enter a new source port. *Original*is active by default. If you select *Specify port range* for **Original Source Port/Range**, you can choose from the follwing options: • *Use Original Source Port/Range*: The range specified for **Original Source Port/Range** is not changed, all port numbers are retained. • *Use Source Port/Range starting with*: There is an input field for you to specify the port number with which to start the port range that replaces the original port rannge. The count of ports is retained.

12.3 Load Balancing

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

12.3.1 Load Balancing Groups

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

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

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

Note

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

12.3.1.1 New

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

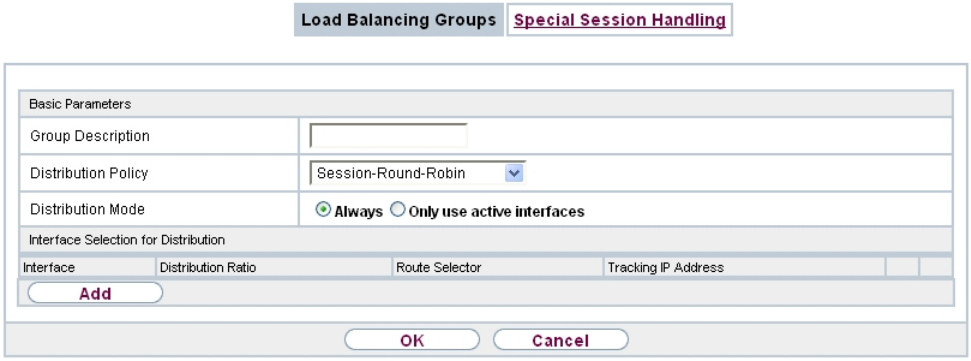


Fig. 86: **Networking**->**Load Balancing**->**Load Balancing Groups**->**New**

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

Fields in the Basic Parameters menu.

Field	Description
Group Description	Enter the desired description of the interface group.
Distribution Policy	Select the way the data traffic is to be distributed to the interfaces configured for the group. Possible values: • *Session-Round-Robin* (default value): A newly added session is assigned to one of the group interfaces according to the percentage assignment of sessions to the interfaces. The number of sessions is decisive. • *Load-dependent Bandwidth*: A newly added session is assigned to one of the group interfaces according to the share

Field	Description
	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.

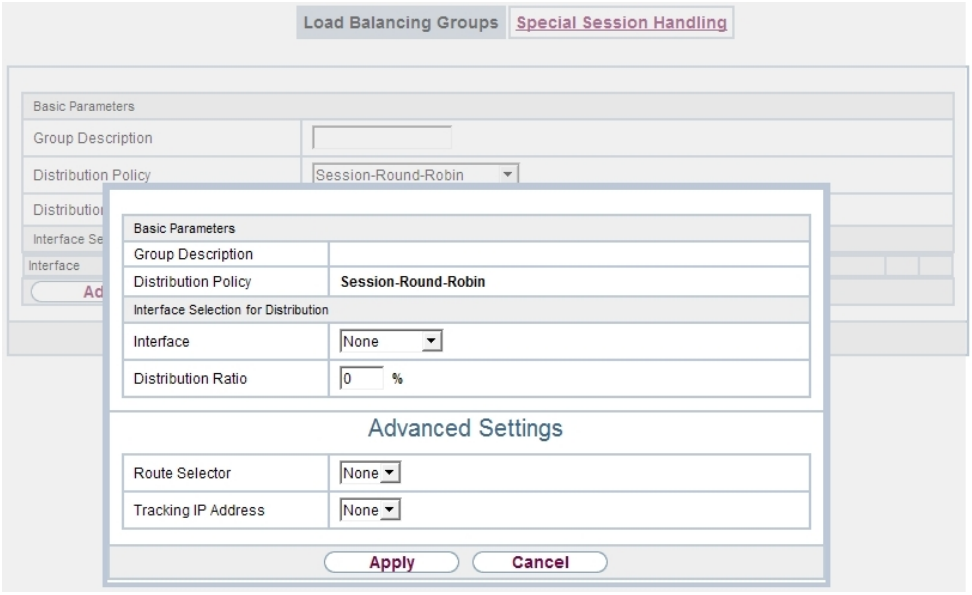


Fig. 87: **Networking->Load Balancing->Load Balancing Groups->Add**

Fields in the Basic Parameters menu.

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

Fields in the Interface Selection for Distribution menu.

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

Field	Description
	cisive factor.

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

Fields in the Advanced Settings menu.

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

Field	Description
	ancing status now varies according to the status of the assigned host surveillance entry. Select the IP address for the route to be monitored. You can choose from the IP addresses you have entered in the **Local Services**->**Surveillance**->**Hosts**->**New** menu under **Monitored IP Address** and which are monitored with the aid of the **Action to be executed** field (**Action** = *Monitor*).

12.3.2 Special Session Handling

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

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

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

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

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

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

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

12.3.2.1 Edit or New

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

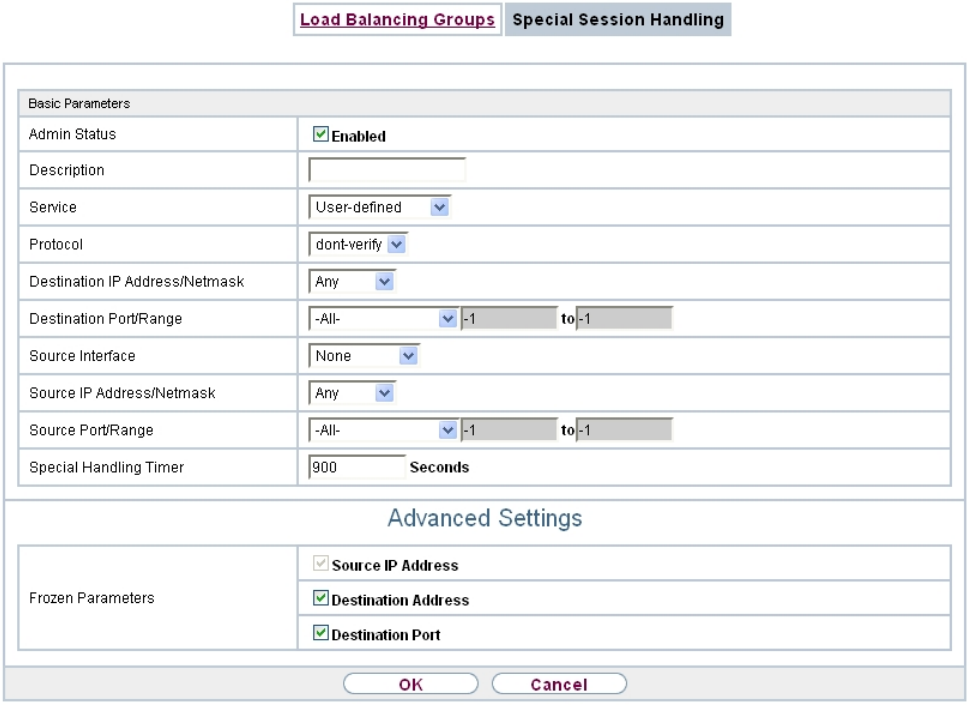


Fig. 88: **Networking->Load Balancing->Special Session Handling->New**

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

Fields in the Basic Parameters menu.

Field	Description
Admin Status	Select whether the Special Session Handling should be activated. The function is activated by selecting *Enabled*. The function is enabled by default.
Description	Enter a name for the entry.
Service	Select one of the preconfigured services, if required. The extensive range of services configured ex works includes the following: • *activity*

Field	Description
	• *apple-qt* • *auth* • *charge* • *clients_1* • *daytime* • *dhcp* • *discard* The default value is *User defined*.
Protocol	Select a protocol, if required. The *Any* option (default value) matches any protocol.
Destination IP Address/Netmask	Enter, if required, the destination IP address and netmask of the data packets. Possible values: • *Any* (default value) • *Host*: Enter the IP address of the host. • *Network*: Enter the network address and the related netmask.
Destination Port/Range	Enter, if required, a destination port number or a range of destination port numbers. Possible values: • *-All-* (default value): The destination port is not specified. • *Specify port*: Enter a destination port. • *Specify port range*: Enter a destination port range.
Source Interface	If required, select your device's source interface.
Source IP Address/ Netmask	Enter, if required, the source IP address and netmask of the data packets. Possible values: • *Any* (default value) • *Host*: Enter the IP address of the host.

Field	Description
	• *Network*: Enter the network address and the related net-mask.
Source Port/Range	Enter, if required, a source port number or a range of source port numbers. Possible values: • *-All-* (default value): The destination port is not specified. • *Specify port*: Enter a destination port. • *Specify port range*: Enter a destination port range.
Special Handling Timer	Enter the time period during which the specified data packets are to be routed via the route that has been defined. The default value is *900* seconds.

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

Fields in the Advanced Settings menu.

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

12.4 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

12.4.1 QoS Filter

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

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

12.4.1.1 New

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

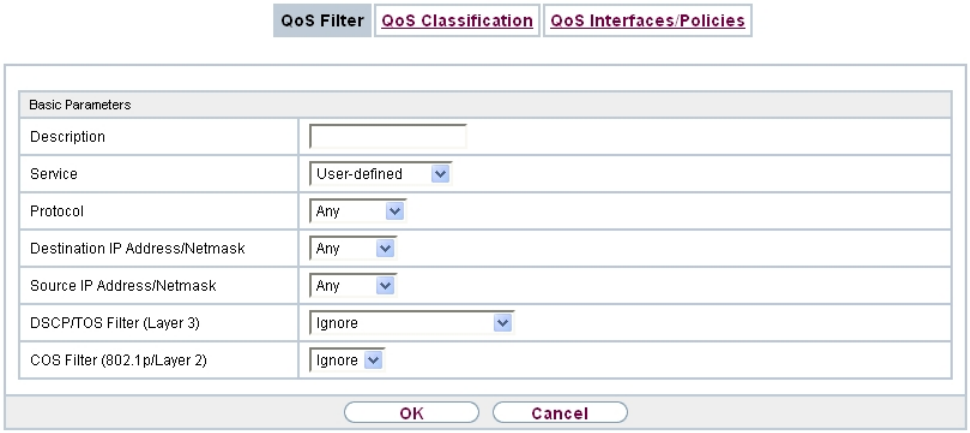


Fig. 89: **Networking**->**QoS**->**QoS Filter**->**New**

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

Fields in the Basic Parameters menu.

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

Field	Description
dress/Netmask	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)	Select the Type of Service (TOS). Possible values: • *Ignore* (default value): The type of service is ignored. • *DSCP Binary Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111.

Field	Description
	• *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F.
COS Filter (802.1p/Layer 2)	Enter the service class of the IP packets (Class of Service, CoS). Value range *0* to *7*. The default value is *0*.

12.4.2 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.

12.4.2.1 New

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

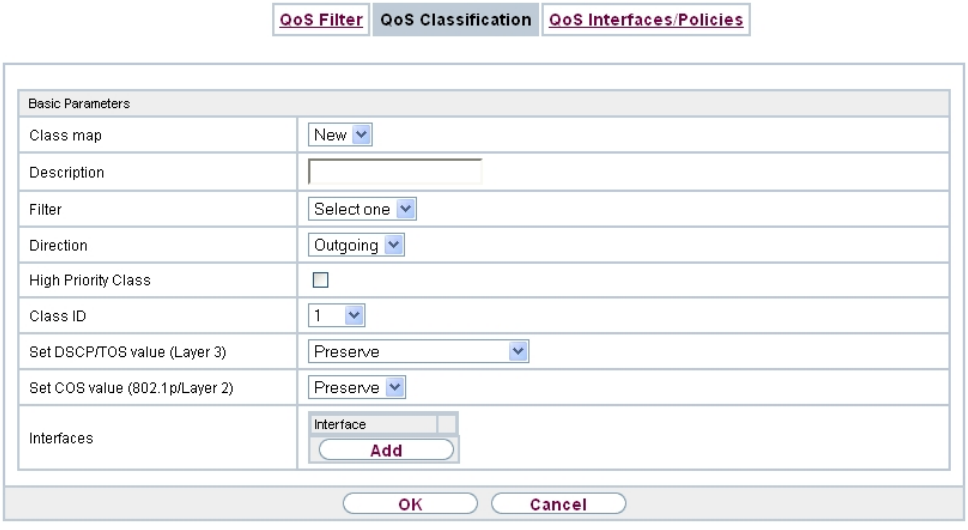


Fig. 90: **Networking**->**QoS**->**QoS Classification**->**New**

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

Fields in the Basic Parameters menu.

Field	Description
Class map	Choose the class plan you want to create or edit. Possible values: • *New* (default value): You can create a new class plan with this setting. • *<Name of class plan>*: Shows a class plan that has already been created, which you can select and edit. You can add new filters.
Description	Only for **Class map** = *New* Enter the name of the class plan.
Filter	Select an IP filter. If the class plan is new, select the filter to be set at the first point of the class plan. If the class plan already exists, select the filter to be attached to the class plan. To select a filter, at least one filter must be configured in the **Networking**->**QoS**->**QoS Filter** menu.
Direction	Select the direction of the data packets to be classified. Possible values: • *Incoming*: Incoming data packets are assigned to the class (**Class ID**) that is then to be defined. • *Outgoing* (default value): Outgoing data packets are assigned to the class (**Class ID**) that is then to be defined. • *Both*: Incoming and outgoing data packets are assigned to the class (**Class ID**) that is then to be defined.
High Priority Class	Enable or disable the high priority class. If the high priority class is active, the data packets are associated with the class with the highest priority and priority 0 is set automatically. The function is enabled with *Enabled*.

Field	Description
	The function is disabled by default.
Class ID	Only for **High Priority Class** not active. Choose a number which assigns the data packets to a class.  **Note** The class ID is a label to assign data packets to specific classes. (The class ID does not define the priority.) Possible values are whole numbers between *1* and *254*.
Set DSCP/TOS value (Layer 3)	Here you can set or change the DSCP/TOS value of the IP data packets, based on the class (**Class ID**) that has been defined. Possible values: • *Preserve* (default value): The DSCP/TOS value of the IP data packets remains unchanged. • *DSCP Binary Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format). • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F.
Set COS value (802.1p/Layer 2)	Here you can set/change the service class (Layer 2 priority) in the VLAN Ethernet header of the IP packets, based on the class (**Class ID**) that has been defined. Possible values are whole numbers between *0* and *7*.

Field	Description
	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.

12.4.3 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.

12.4.3.1 New

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

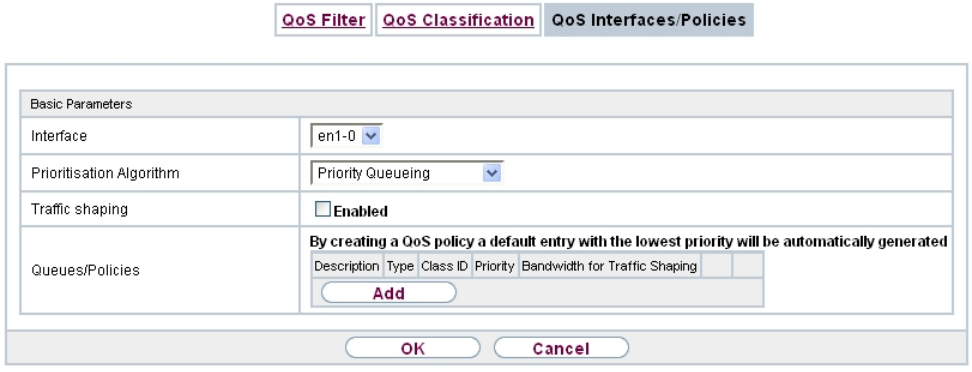


Fig. 91: **Networking->QoS->QoS Interfaces/Policies->New**

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

Fields in the Basic Parameters menu.

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

Field	Description
Traffic shaping	Activate or deactivate data rate limiting in the send direction. The function is enabled with *Enabled*. The function is disabled by default.
Maximum Upload Speed	Only for **Traffic shaping** = enabled. Enter a maximum data rate for the 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	Only for **Traffic shaping** = enabled. Choose the interface type to include the size of the respective overheads of a datagram when calculating the bandwidth. Possible values: • *User defined*: Value in byte. Possible values are *0* to *100*. • *Undefined (Protocol Header Offset=0)* (default value) Can only be selected for Ethernet interfaces • *Ethernet* • *Ethernet and VLAN* • *PPP over Ethernet* • *PPP over Ethernet and VLAN* Can only be selected for IPSec interfaces: • *IPSec over Ethernet* • *IPSec over Ethernet and VLAN* • *IPSec via PPP over Ethernet* • *IPSec via PPPoE and VLAN*
Encryption Method	Only if an IPSec Peers is selected as **Interface**, **Traffic shap-**

Field	Description
	ing is *Active* and **Protocol Header Size below Layer 3** is not *Undefiniert (Protocol Header Offset=0)*. Select the encryption method used for the IPSec connection. The encryption algorithm determines the length of the block cipher which is taken into account during bandwidth calculation. Possible values: • *DES, 3DES, Blowfish, Cast - (cipher block size = 64 Bit)* • AES128, AES192, AES256, Twofish - (cipher block size = 128 Bit)
Real Time Jitter Control	Only for **Traffic shaping** = enabled Real Time Jitter Control optimises latency when forwarding real time datagrams. The function ensures that large data packets are fragmented according to the available upload bandwidth. Real Time Jitter Control is useful for small upload bandwidths (< 800 kbps). Activate or deactivate Real Time Jitter Control. The function is enabled with *Enabled*. The function is disabled by default.
Control Mode	Only for **Real Time Jitter Control** = enabled. Select the mode for optimising voice transmission. Possible values: • *All RTP Streams*: All RTP streams are optimised. The function activates the RTP stream detection mechanism for the automatic detection of RTP streams. In this mode, the Real Time Jitter Control is activated as soon as an RTP 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.

Field	Description
	• *Always*: Real Time Jitter Control is always active, even if no real time data is routed.
Queues/Policies	Configure the desired QoS queues. For each class created from the class plan, which is associated with the selected interface, a queue is generated automatically and displayed here (only for data traffic classified as outgoing and for data traffic classified as moving in both directions). Add new entries with **Add**. The **Edit Queue/Policy** menu opens. By creating a QoS policy a DEFAULT entry with the lowest priority 255 is automatically created.

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

Fields in the Edit Queue/Policy menu.

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

Field	Description
	Choose the priority of the queue. Possible values are *1* (high priority) to *254* (low priority). The default value is *1*.
Weight	Only for **Prioritisation Algorithm** = *Weighted Round Robin* or *Weighted Fair Queueing* Choose the priority of the queue. Possible values are *1* to *254*. The default value is *1*.
RTT Mode (Realtime Traffic Mode)	Active or deactivate the real time transmission of the data. The function is enabled with *Enabled*. The function is disabled by default. RTT mode should be activated for QoS classes in which real time data has priority. This mode improves latency when forwarding real time datagrams. It is possible to configure multiple queues when RTT mode is enabled. Queues with enabled RTT mode must always have a higher priority than queues with disabled RTT mode.
Traffic Shaping	Activate or deactivate data rate (=Traffic Shaping) limiting in the send direction. The data rate limit applies to the selected queue. (This is not the limit that can be defined on the interface.) The function is enabled with *Enabled*. The function is disabled by default.
Maximum Upload 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.

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

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

Fields in the Advanced Settings menu.

Field	Description
Dropping Algorithm	Choose the procedure for rejecting packets in the QoS queue, if the maximum size of the queue is exceeded. Possible values: • *Tail Drop* (default value): The newest packet received is dropped. • *Head Drop*: The oldest packet in the queue is dropped. • *Random Drop*: A randomly selected packet is dropped from the queue.
Congestion Avoidance (RED)	Enable or disable preventative deletion of data packets. Packets which have a data size of between **Min. queue size** and **Max. queue size** are preventively dropped to prevent queue overflow (RED=Random Early Detection). This proced-

Field	Description
	ure ensures a smaller long-term queue size for TCP-based data traffic, so that traffic bursts can also usually be transmitted without large packet losses. The function is activated with *Enabled*. The function is disabled by default.
Min. queue size	Enter the lower threshold value for the process **Congestion Avoidance (RED)** in bytes. Possible values are *0* to *262143*. The default value is *0*.
Max. queue size	Enter the upper threshold value for the process **Congestion Avoidance (RED)** in bytes. Possible values are *0* to *262143*. The default value is *16384*.

12.5 Access Rules

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

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

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

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

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

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

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

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

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

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

or

Allow all packets that are explicitly allowed, i.e.:

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

or

Combination of the two possibilities described above.

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

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

Caution

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

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

12.5.1 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.

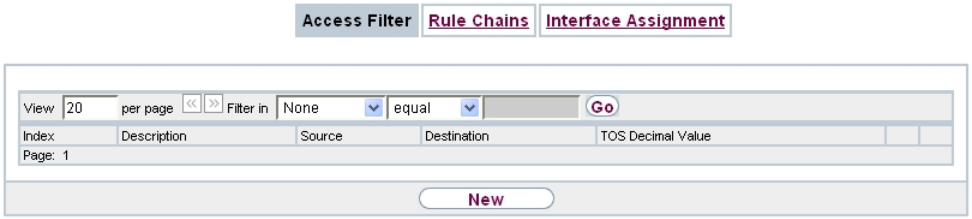


Fig. 92: **Networking**->**Access Rules**->**Access Filter**

12.5.1.1 Edit or New

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

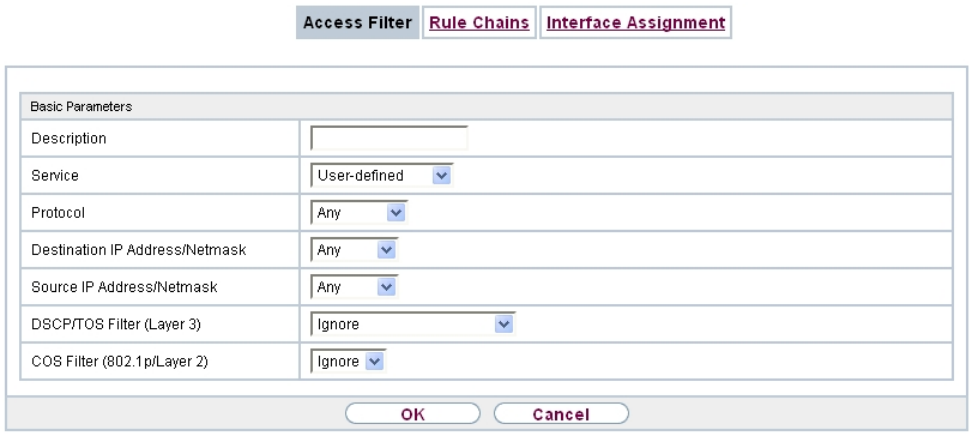


Fig. 93: **Networking**->**Access Rules**->**Access Filter**->**New**

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

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for the filter.
Service	Select one of the preconfigured services. The extensive range of services configured ex works includes the following: • *activity* • *apple-qt* • *auth* • *charge* • *clients_1* • *daytime* • *dhcp* • *discard* The default value is *User defined*.
Protocol	Select a protocol. The *Any* option (default value) matches any protocol.
Type	Only if **Protocol** = *ICMP* Possible values: • *Any* • *Echo reply* • *Destination unreachable* • *Source quench* • *Redirect* • *Echo* • *Time exceeded* • *Timestamp* • *Timestamp reply* The default value is *Any*. See RFC 792.
Connection State	Only if **Protocol** = *TCP*

Field	Description
	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. 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 a destination port number or a range of destination port numbers that matches the filter. Possible values: • *-All-* (default value): The filter is valid for all port numbers • *Specify port*: Enables the entry of a port number. • *Specify port range*: Enables the entry of a range of port numbers.
Source IP Address/ Netmask	Enter the source IP address and netmask of the data packets.
Source Port/Range	Only if **Protocol** = *TCP*, *UDP* Enter a source port number or the range of source port numbers. Possible values: • *-All-* (default value): The filter is valid for all port numbers • *Specify port*: Enables the entry of a port number. • *Specify port range*: Enables the entry of a range of port

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

12.5.2 Rule Chains

Rules for IP filters are configured in the **Rule Chains** menu. These can be created separately or incorporated in rule chains.

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

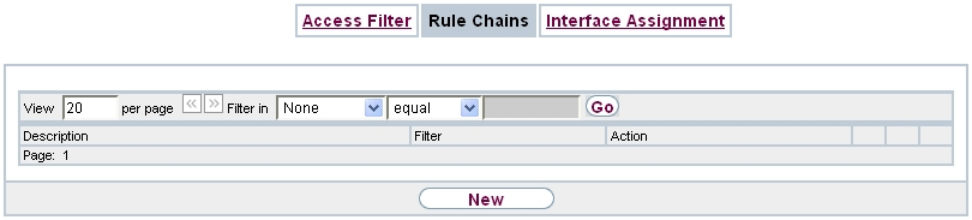


Fig. 94: **Networking->Access Rules->Rule Chains**

12.5.2.1 Edit or New

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

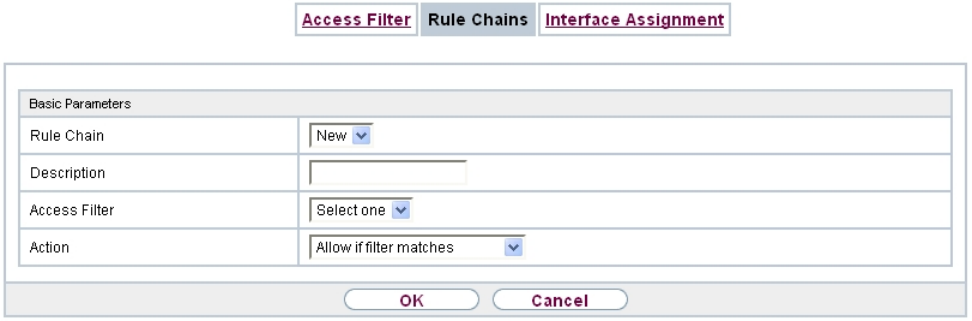


Fig. 95: **Networking->Access Rules->Rule Chains->New**

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

Fields in the Basic Parameters menu.

Field	Description
Rule Chain	Select whether to create a new rule chain or to edit an existing one. Possible values: • *New* (default value): You can create a new rule chain with this setting. • *<Name of the rule chain>*: Select an already existing rule chain, and thus add another rule to it.
Description	Enter the name of the rule chain.

Field	Description
Access Filter	Select an IP filter. If the rule chain is new, select the filter to be set at the first point of the rule chain. If the rule chain already exists, select the filter to be attached to the rule chain.
Action	Define the action to be taken for a filtered data packet. Possible values: • *Allow if filter matches* (default value): Allow packet if it matches the filter. • *Allow if filter does not match*: Allow packet if it does not match the filter. • *Deny if filter matches*: Deny packet if it matches the filter. • *Deny if filter does not match*: Deny packet if it does not match the filter. • *Ignore*: Use next rule.

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

12.5.3 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.

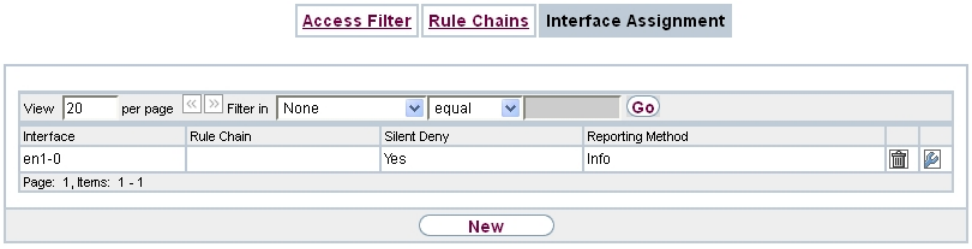


Fig. 96: **Networking->Access Rules->Interface Assignment**

12.5.3.1 Edit or New

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

Fig. 97: **Networking->Access Rules->Interface Assignment->New**

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

Fields in the Basic Parameters menu.

Field	Description
Interface	Select the interface for which a configured rule chain is to be assigned.
Rule Chain	Select a rule chain.
Silent Deny	Define whether the sender is to be informed if an IP packet is denied. • `Enabled` (default value): The sender is not informed. • `Disabled`: The sender receives an ICMP message.
Reporting Method	Define whether a syslog message is to be generated if a packet

Field	Description
	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.

12.6 Drop In

"Drop-in mode" allows you to split a network into smaller segments without having to divide the IP network into subnets. Several interfaces can be combined in a drop-in group and assigned to a network to do this. All of the interfaces are then configured with the same IP address.

Within a segment, network components which are connected to a connection can then be grouped and, for example, be protected by firewall. Data traffic from network components between individual segments which are assigned to different ports are then controlled according to the configured firewall rules.

12.6.1 Drop In Groups

The **Networking**->**Drop In**->**Drop In Groups** menu displays a list of all the configured **Drop In Groups**. Each **Drop In** group represents a network.

12.6.1.1 New

Select the **New** button to set up other **Drop In Groups**.

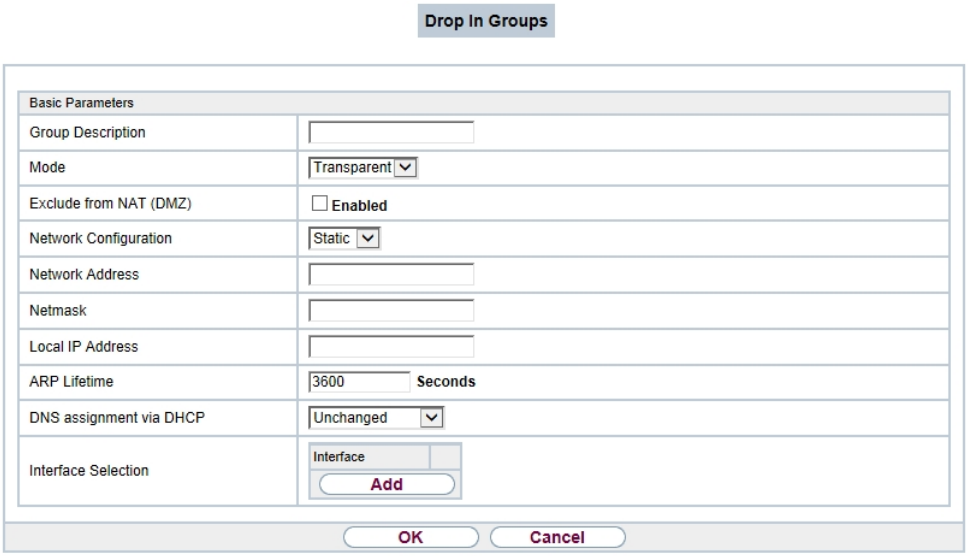


Fig. 98: **Networking->Drop In->Drop In Groups->New**

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

Fields in the Basic Parameters menu.

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

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

Field	Description
	• *Own IP Address*
Interface Selection	Select all the ports which are to be included in the **Drop In** group (in the network). Add new entries with **Add**.

Chapter 13 Routing Protocols

13.1 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.

13.1.1 RIP Interfaces

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

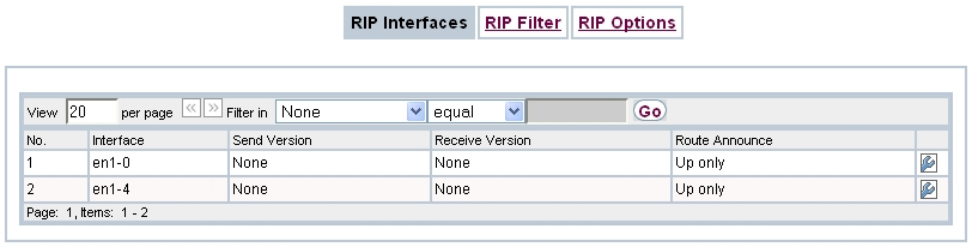


Fig. 99: **Routing Protocols**->**RIP**->**RIP Interfaces**

13.1.1.1 Edit

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

Fig. 100: **Routing Protocols->RIP->RIP Interfaces->**

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

Fields in the RIP Parameters for menu.

Field	Description
Send Version	Decide whether routes are to be propagated via RIP and if so, select the RIP version for sending RIP packets over the interface in send direction. Possible values: • *None* (default value): RIP is not enabled. • *RIP V1*: Enables sending and receiving of version 1 RIP packets. • *RIP V2*: Enables sending and receiving of version 2 RIP packets. • *RIP V1/V2*:Enables sending and receiving RIP packets of both version 1 and 2. • *RIP V2 Multicast*: For sending RIP V2 messages over multicast address 224.0.0.9. • *RIP V1 Triggered*: RIP V1 messages are sent, received and processed as per RFC 2091 (triggered RIP). • *RIP V2 Triggered*: RIP V2 messages are sent, received and processed as per RFC 2091 (triggered RIP).
Receive Version	Decide whether routes are to be imported via RIP and if so, select the RIP version for receiving RIP packets over the interface in receive direction. Possible values:

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

13.1.2 RIP Filter

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

You can use the following strategies for this:

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

tion.

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

- **IP Address / Netmask** = no entry for IP address (this corresponds to IP address 0.0.0.0), for netmask = 255.255.255.255

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

Fig. 101: **Routing Protocols**->**RIP**->**RIP Filter**

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.

13.1.2.1 New

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

Fig. 102: **Routing Protocols**->**RIP**->**RIP Filter**->**New**

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

Fields in the Basic Parameters menu.

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

13.1.3 RIP Options

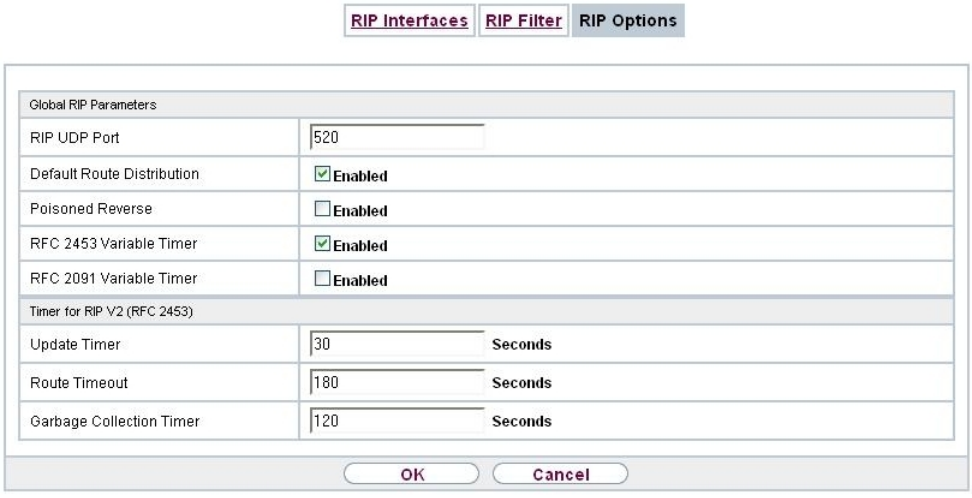


Fig. 103: **Routing Protocols->RIP->RIP Options**

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

Fields in the Global RIP Parameters menu.

Field	Description
RIP UDP Port	The setting option UDP Port, which is used for sending and receiving RIP updates, is only for test purposes. If the setting is changed, this can mean that your device sends and listens at a port that no other devices use. The default value *520* should be retained.
Default Route Distribution	Select whether the default route of your device is to be propagated via RIP updates. The function is enabled with *Enabled*. The function is enabled by default.
Poisoned Reverse	Select the procedure for preventing routing loops. With standard RIP, the routes learnt are propagated over all interfaces with RIP SEND activated. With **Poisoned Reverse**, however, your device propagates over the interface via which it learnt the routes, with the metric (Next Hop Count) 16

Field	Description
	(=“Network is not reachable“). The function is enabled with *Enabled*. The function is disabled by default.
RFC 2453 Variable Timer	For the timers described in RFC 2453, select whether the same values that you can configure in the **Timer for RIP V2 (RFC 2453)** menu should be used. The function is enabled with *Enabled*. The function is enabled by default. If you deactivate the function, the times defined in RFC are retained for the timeouts.
RFC 2091 Variable Timer	For the timers described in RFC 2091, select whether the same values that you can configure in the **Timer for Triggered RIP (RFC 2091)** menu should be used. The function is enabled with *Enabled*. The function is disabled by default. If the function is not activated, the times defined in RFC are retained for the timeouts.

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

Field	Description
Update Timer	Only for **RFC 2453 Variable Timer** = *Enabled* An RIP update is sent on expiry of this period of time. The default value is *30* (seconds).
Route Timeout	Only for **RFC 2453 Variable Timer** = *Enabled* After the last update of a route, the route time is active. After timeout, the route is deactivated and the Garbage Collection Timer is started. The default value is *180* (seconds).

Field	Description
Garbage Collection Timer	Only for **RFC 2453 Variable Timer** = *Enabled* The Garbage Collection Timer is started as soon as the route timeout has expired. After this timeout, the invalid route is deleted from the IPROUTETABLE if no update is carried out for the route. The default value is *120* (seconds).

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

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

Chapter 14 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.

14.1 General

14.1.1 General

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

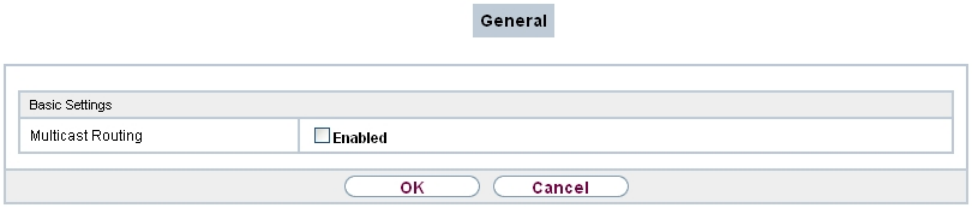


Fig. 104: **Multicast**->**General**->**General**

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

Fields in the Basic Settings menu.

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

14.2 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.

14.2.1 IGMP

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

14.2.1.1 Edit or New

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

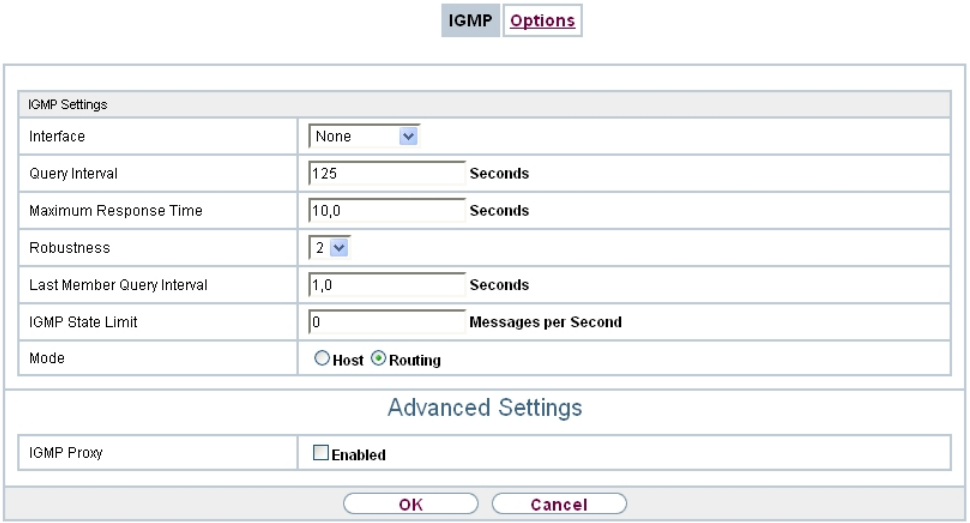


Fig. 105: **Multicast->IGMP->IGMP->New**

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

Fields in the IGMP Settings menu.

Field	Description
Interface	Select the interface on which IGMP is to be enabled, i.e. queries are sent and responses are accepted.
Query Interval	Enter the interval in seconds in which IGMP queries are to be sent. Possible values are *0* to *600*. The default value is *125*.
Maximum Response	For the sending of queries, enter the time interval in seconds

Field	Description
Time	within which hosts must respond. The hosts randomly select a time delay from this interval before sending the response. This spreads the load in networks with several hosts, improving performance. Possible values are *0,0* to *25,0*. The default value is *10,0*.
Robustness	Select the multiplier for controlling the timer values. A higher value can e.g. compensate for packet loss in a network susceptible to loss. If the value is too high, however, the time between logging off and stopping of the data traffic can be increased (leave latency). Possible values are *2* to *8*. The default value is *2*.
Last Member Query Interval	Define the time after a query for which the router waits for an answer. If you shorten the interval, it will be more quickly detected that the last member has left a group so that no more packets for this group should be forwarded to this interface. Possible values are *0,0* to *25,0*. The default value is *1,0*.
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.

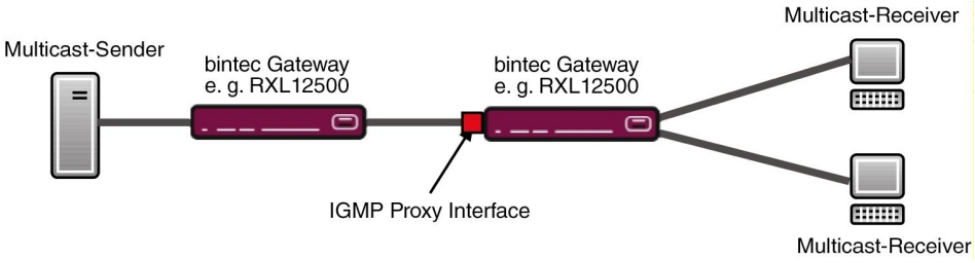


Fig. 106: IGMP Proxy

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

Fields in the Advanced Settings menu.

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

14.2.2 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.

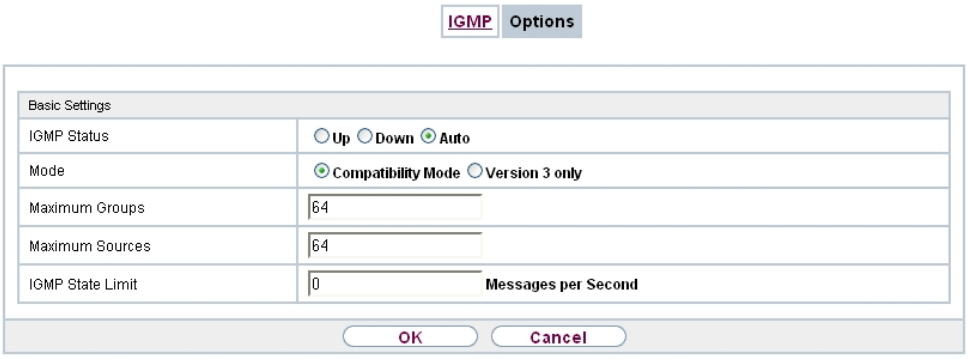


Fig. 107: **Multicast->IGMP->Options**

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

Fields in the Basic Settings menu.

Field	Description
IGMP Status	Select the IGMP status. Possible values: • *Auto* (default value): Multicast is activated automatically for hosts if the hosts open applications that use multicast. • *Up*: Multicast is always on. • *Down*: Multicast is always off.
Mode	Only for **IGMP Status** = *Up* or *Auto* Select Multicast Mode. Possible values: • *Compatibility Mode* (default value): The router uses IGMP version 3. If it notices a lower version in the network, it uses the lowest version it could detect. • *Version 3 only*: Only IGMP version 3 is used.
Maximum Groups	Enter the maximum number of groups to be permitted, both internally and in reports. The default value is *64*.
Maximum Sources	Enter the maximum number of sources that are specified in version 3 reports and the maximum number of internally managed

Field	Description
	sources per group. The default value is `64`.
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.

14.3 Forwarding

14.3.1 Forwarding

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

14.3.1.1 New

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

Fig. 108: **Multicast->Forwarding->Forwarding->New**

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

Fields in the Basic Parameters menu.

Field	Description
All Multicast Groups	Select whether all multicast groups, i.e. the complete multicast address range 224.0.0.0/4, are to be forwarded from the defined **Source Interface** to the defined **Destination Interface**. To do

Field	Description
	this, check *Enabled* Disable the option if you only want to forward one defined multicast group to a particular interface. The option is deactivated by default.
Multicast Group Address	Only for **All Multicast Groups** = not active. Enter here the address of the multicast group you want to forward from a defined **Source Interface** to a defined **Destination Interface**.
Source Interface	Select the interface on your device to which the selected multicast group is sent.
Destination Interface	Select the interface on your device to which the selected multicast group is to be forwarded.

14.4 PIM

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

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

14.4.1 PIM Interfaces

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

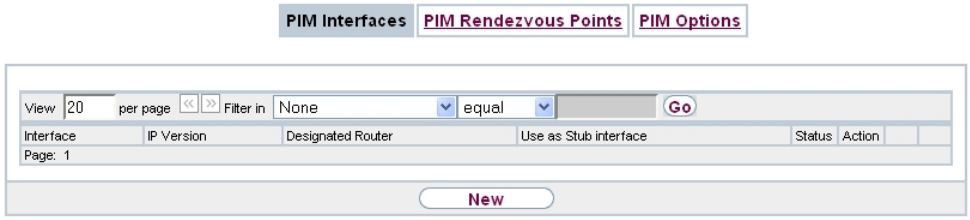


Fig. 109: **Multicast->PIM->PIM Interfaces**

14.4.1.1 Edit or New

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

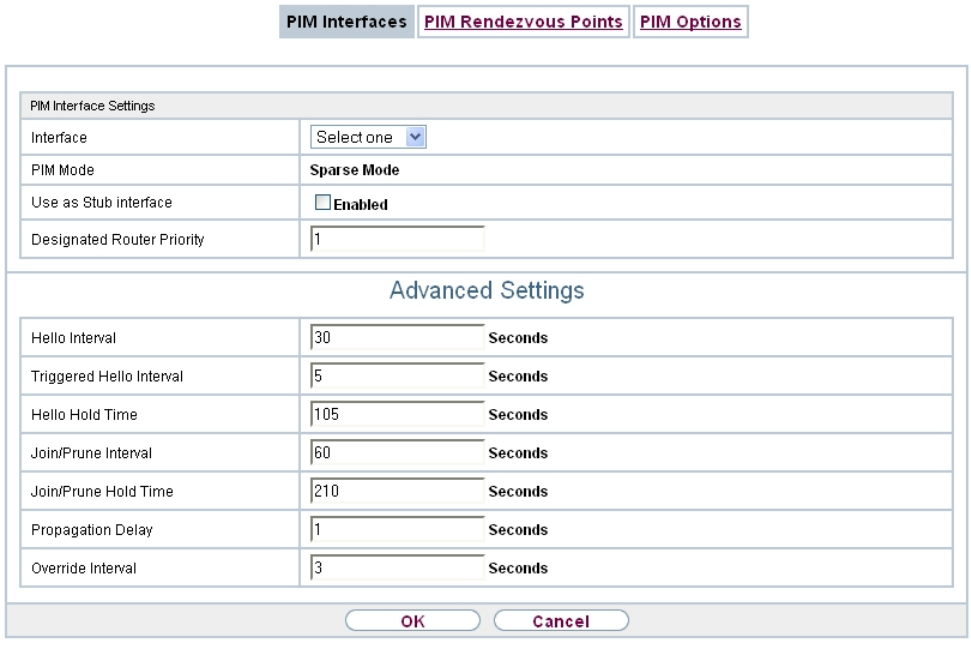


Fig. 110: **Multicast->PIM->PIM Interfaces->New**

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

Fields in the PIM Interface Settings menu.

Field	Description
Interface	Choose the interface used for PIM, i.e. over which multicast routing is operated.
PIM Mode	Indicates the mode to be used for PIM. Your device uses PIM in sparse mode. The entry cannot be changed.

Field	Description
Use as Stub interface	Determine whether or not the interface is used for PIM data packets. This parameter allows you to use an interface for IGMP, for example, whilst preventing (fake) PIM messages. If this function is deactivated (default value), the PIM data packets for this interface are blocked. If the function is active, the interface for the PIM data packets are released.
Designated Router Priority	Define the value of the designated router priority entered in the **Designated Router Priority** option. The higher the value, the greater the probability that the corresponding router will be used as the designated router. The default value is *1*.

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

Fields in the Advanced Settings menu.

Field	Description
Hello Interval	Define the interval (in seconds) at which PIM Hello messages are sent over this interface. The value *0* means that no PIM Hello messages are sent on this interface. Possible values: *0* to *18000* seconds. The default value is *30*.
Triggered Hello Interval	Define the maximum waiting time until a PIM Hello message is sent after a system boot or after a reboot of a neighbour. The value *0* means that PIM Hello messages are always sent straight away. Possible values: *0* to *60* seconds. The default value is *5*.
Hello Hold Time	Define the value of the holdtime field in a PIM Hello message.

Field	Description
	This indicates how long a PIM route is available. As soon as the **Hello Hold Time** has expired and no other Hello messages have been received, the PIM router will be classed as unavailable. Possible values: *0* to *65535* seconds. The default value is *105*.
Join/Prune Interval	Define the frequency at which the PIM Join/Prune messages are sent on the interface. The value *0* means that no periodic PIM Join/Prune messages are sent on this interface. Possible values: *0* to *18000* seconds. The default value is *60*.
Join/Prune Hold Time	Define the value entered in the holdtime field of a PIM Join/Prune message. This is the time for which a recipient must maintain the Join/Prune state. Possible values: *0* to *65535* seconds. The default value is *210*.
Propagation Delay	Define the value entered in the Propagation Delay field. This field is part of the LAN Prune Delay option in the PIM Hello messages, which are sent on this interface. Propagation Delay and Override Interval represent the so-called LAN-Prune-Delay settings. These result in a delay in processing prune messages for upstream routers. If the **Propagation Delay** is too short, the transfer of multicast packets may be cancelled before a downstream router has sent a prune override message. Possible values: *0* to *32* seconds. The default value is *1*.

Field	Description
Override Interval	Define the value that the gateway enters in the Override_Interval field for the LAN Prune Delay option. **Override Interval** defines the maximum time a downstream router can wait until sending a prune override message. Possible values: *0* to *65* seconds. The default value is *3*.

14.4.2 PIM Rendezvous Points

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

A list of all PIM Rendezvous Points is displayed.

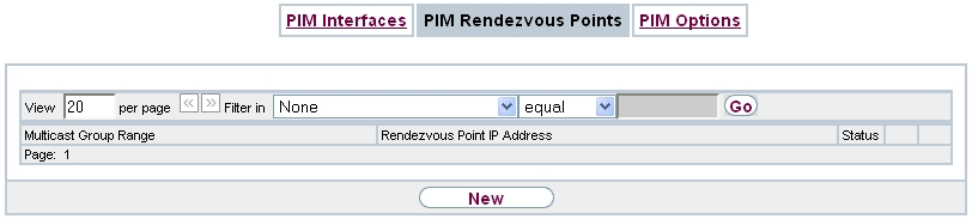


Fig. 111: **Multicast->PIM->PIM Rendezvous Points**

14.4.2.1 Edit or New

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

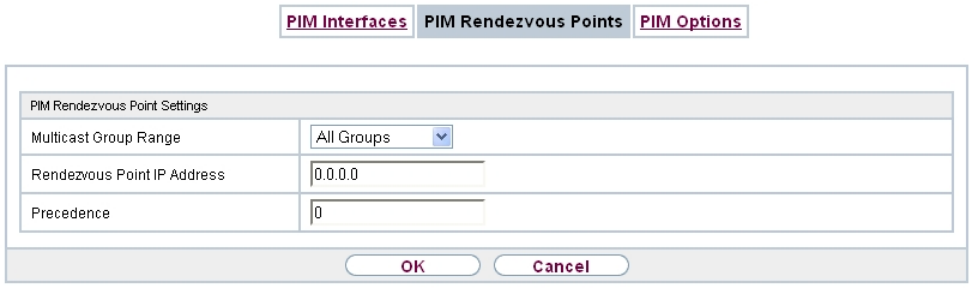


Fig. 112: **Multicast->PIM->PIM Rendezvous Points->New**

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

Fields in the PIM Rendezvous Point Settings menu.

Field	Description
Multicast Group Range	Select the Multicast group for the PIM Rendezvouz point. You can enter *All Groups* (default value), or specify a multicast network segment by selecting *Specific Range*.
Multicast Group Address	Only if **Multicast Group Range** = *Specific Range* Here you enter the IP address of the multicast network segment.
Multicast Group Prefix Length	Only if **Multicast Group Range** = *Specific Range* Here you enter the network mask length of the multicast network segment. 224.0.0.0/4 indicates the entire multicast class D segment. Possible values: *4* (default value) to *32*.
Rendezvous Point IP Address	Enter the IP address or the hostname of the rendezvous points.
Precedence	Enter the value for pimGroupMappingPrecedence to be used for static RP configurations. This allows precise control over which configuration is to be replaced by this static configuration. When the function is activated pimStaticRPOverrideDynamic is ignored. The absolute values of this object are only significant on the local router and need not be synchronised with other routers. The function is deactivated with the default value *0*. If the function is not activated by setting a value not 0, this can different consequences for other routers. Hence, avoid using this function if exact control of the behaviour of the static RP is not required.

14.4.3 PIM Options

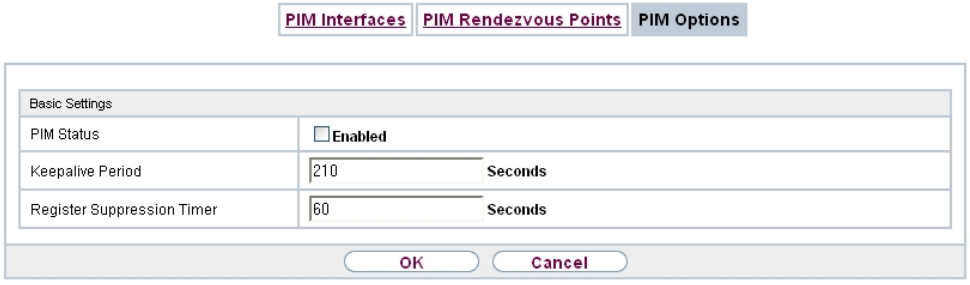


Fig. 113: **Multicast->PIM->PIM Options**

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

Fields in the Basic Settings menu.

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

Chapter 15 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.

15.1 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) and PPP-over-PPTP protocols.

Note

Note your provider's instructions.

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

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

Possible values for Status

Field	Description
	connected
	not connected (dialup connection); connection setup possible
	not connected (e.g. because of an error during setup of an outgoing connection, a renewed attempt is only possible after a specified number of seconds)
	administratively set to down (deactivated); connection setup not possible for leased lines:

Authentication

If a call is received, PPP authentication is carried out with the connection partner depending on the configuration, before the call is accepted. Your device needs the necessary data for this, which you should enter here. First 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.

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, be aware of differing values for **Metric**.

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 where necessary.

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.

15.1.1 PPPoE

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

PPP over Ethernet (PPPoE) is the use of the Point-to-Point Protocol (PPP) network protocol over an Ethernet connection. Today, PPPoE is used for ADSL connections in Germany. In Austria, the Point To Point Tunnelling Protocol (PPTP) was originally used for ADSL access. However, PPPoE is now offered here too by some providers.

15.1.1.1 New

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

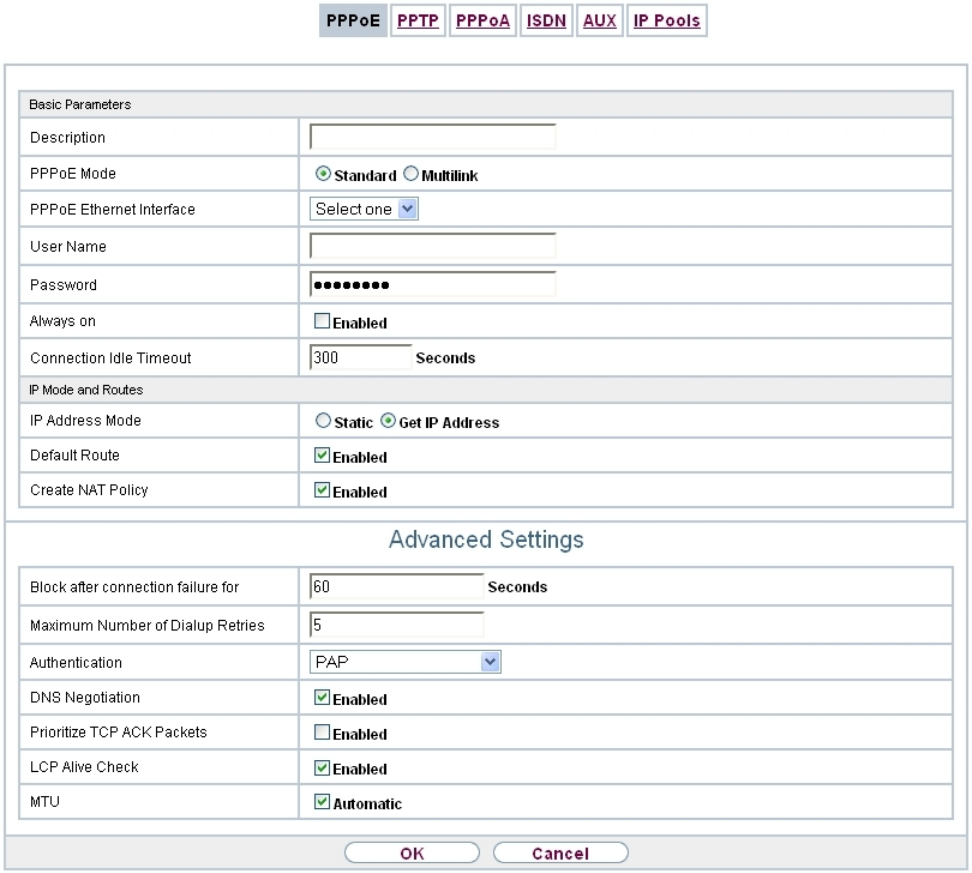


Fig. 114: **WAN**->**Internet + Dialup**->**PPPoE**->**New**

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

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a name to uniquely identify the PPPoE partner. The first character in this field must not be a number No special characters or umlauts must be used.
PPPoE Mode	Select whether you want to use a standard Internet connection over PPPoE (*Standard*) or your Internet access is to be set up over several interfaces (*Multilink*). If you choose *Multilink*, you can connect several DSL connections from a provider over PPP as a static bundle in order to obtain more bandwidth. Each of these DSL connections should use a separate Ethernet connection for this. At the moment, many providers are still in the process of preparing the PPPoE Multilink function. For PPPoE Multilink, we recommend using your device's Ethernet switch in Split-Port mode and to use a separate Ethernet interface e.g. *en1-1*, *en1-2* for each PPPoE connection. If you also want to use an external modem for PPPoE Multilink, you must run your device's Ethernet switch in Split-Port mode.
PPPoE Ethernet Interface	Only for **PPPoE Mode** = *Standard* Select the Ethernet interface specified for a standard PPPoE connection. If you want to use an external DSL modem, select the Ethernet port to which the modem is connected. When using the internal DSL modem, select here the EthoA interface configured in **WAN**->**ATM**->**Profiles**->**New**.
PPPoE Interfaces for Multilink	Only for **PPPoE Mode** = *Multilink* Select the interfaces you want to use for your Internet connection. Click the **Add** button to create new entries.
User Name	Enter the user name.
Password	Enter the password.
VLAN	Certain Internet service providers require a VLAN-ID. Activate this function to be able to enter a value under **VLAN ID**.

Field	Description
VLAN ID	Only if **VLAN** is enabled. Enter the VLAN-ID that you received from your provider.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the short hold. The default value is *300*. Example: *10* for FTP transmission, *20* for LAN-to-LAN transmission, *90* for Internet connections.

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Get IP Address* (default value): Your device is dynamically assigned an IP address. • *Static*: You enter a static IP address.
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*.

Field	Description
	The function is enabled by default.
Create NAT Policy	Specify whether Network Address Translation (NAT) is to be activated. The function is enabled with *Enabled*. The function is enabled by default.
Local IP Address	Only if **IP Address Mode** = *Static* Enter the static IP address of the connection partner.
Route Entries	Only if **IP Address Mode** = *Static* Define other routing entries for this connection partner. Add new entries with **Add**. • *Remote IP Address*: IP address of the destination host or network. • *Netmask*: Netmask for **Remote IP Address** If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (range of values *0*... *15*). The default value is *1*.

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.

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

Field	Description
MTU	Enter the maximum packet size (Maximum Transfer Unit, MTU) in bytes that is allowed for the connection. With default value *Automatic*, the value is specified by link control at connection setup. If you disable *Automatic*, you can enter a value. Possible values are *1* to *8192*. The default value is *0*.

15.1.2 PPTP

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

In this menu, you configure an Internet connection that uses the Point Tunnelling Protocol (PPTP) to set up a connection. This is required in Austria, for example.

15.1.2.1 New

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

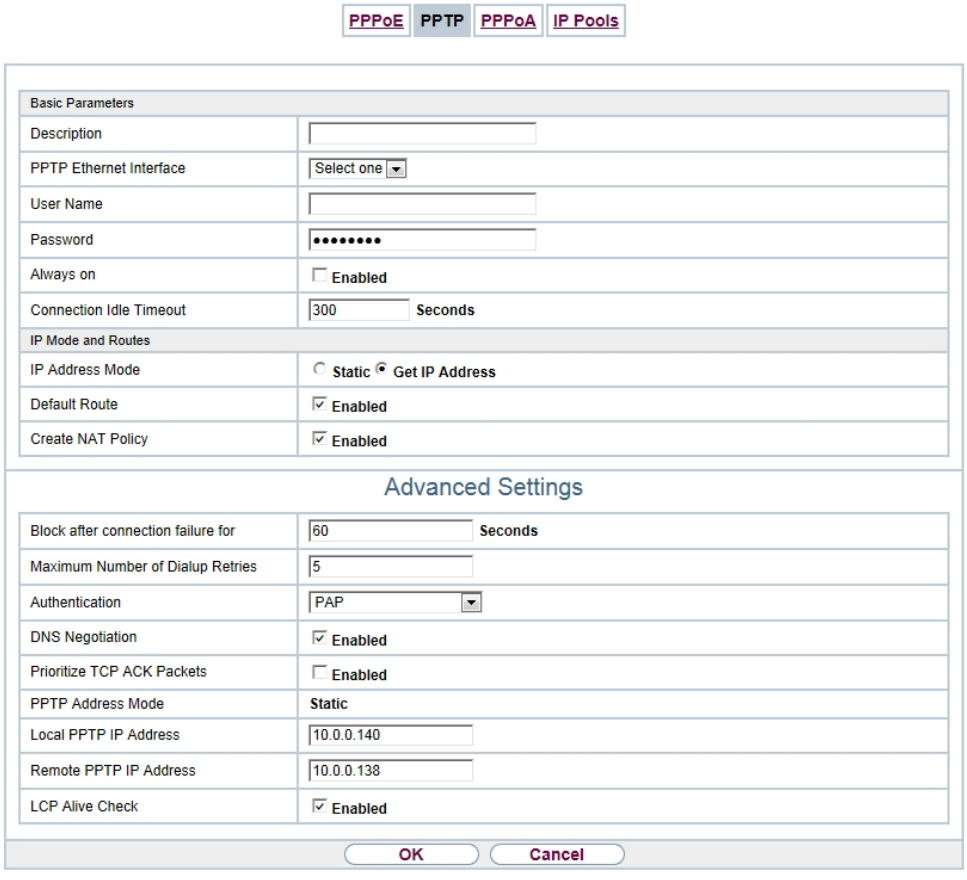


Fig. 115: **WAN->Internet + Dialup->PPTP->New**

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

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a name for uniquely identifying the internet connection. The first character in this field must not be a number No special characters or umlauts must be used.
PPTP Ethernet Interface	Select the IP interface over which packets are to be transported to the remote PPTP terminal. If you want to use an external DSL modem, select the Ethernet port to which the modem is connected.

Field	Description
	When using the internal DSL modem, select here the EthoA interface configured in **Physical Interfaces**->**ATM**->**Profiles**->**New**, e.g. *ethoa50-0*.
User Name	Enter the user name.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle interval in seconds. This determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the timeout. The default value is *300*. Example: *10* for FTP transmission, *20* for LAN-to-LAN transmission, *90* for Internet connections.

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *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

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

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

Fields in the Advanced Settings menu.

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

Field	Description
	The default value is *5*.
Authentication	Select the authentication protocol for this Internet connection. Select the authentication specified by your provider. Possible values: • *PAP* (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP*: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server** and **Secondary DNS Server** from the connection partner or sends these to the connection partner. The function is enabled with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is enabled with *Enabled*. The function is disabled by default.
PPTP Address Mode	Displays the address mode. The value cannot be changed. Possible values: • *Static*: The **Local PPTP IP Address** will be assigned to the

Field	Description
	selected Ethernet port.
Local PPTP IP Address	Assign the PPTP interface an IP address that is used as the source address. The default value is *10.0.0.140*.
Remote PPTP IP Address	Enter the IP address of the PPTP partner. The default value is *10.0.0.138*.
LCP Alive Check	Select whether the availability of the remote terminal is to be checked by sending LCP echo requests or replies. This makes it possible to switch to a backup connection more quickly in the event of line faults. The function is enabled with *Enabled*. The function is enabled by default.

15.1.3 IP Pools

The **IP Pools** menu displays a list of all IP pools.

Your device can operate as a dynamic IP address server for PPP connections. You can use this function by providing one or more pools of IP addresses. These IP addresses can be assigned to dialling-in connection partners for the duration of the connection.

Any host routes entered always have priority over IP addresses from the address pools. This means that, if an incoming call has been authenticated, your device first checks whether a host route is entered in the routing table for this caller. If not, your device can allocate an IP address from an address pool (if available). If address pools have more than one IP address, you cannot specify which connection partner receives which address. The addresses are initially assigned in order. If a new dial-in takes place within an interval of one hour, an attempt is made to allocate the same IP address that was assigned to this partner the previous time.

15.1.3.1 Edit or New

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

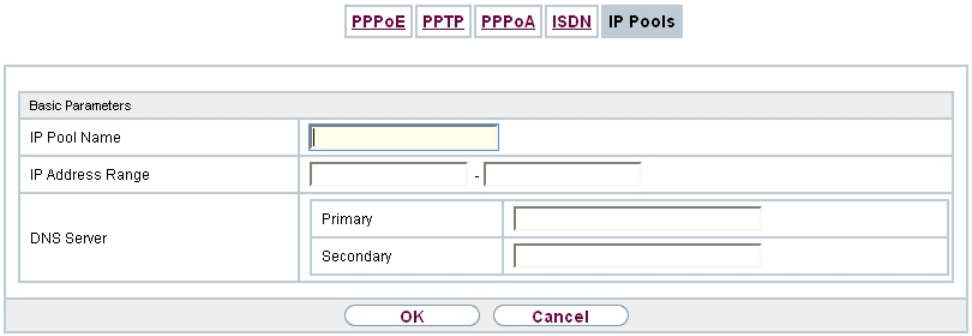


Fig. 116: **WAN->Internet + Dialup->IP Pools->New**

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	**Primary**: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. **Secondary**: Optionally, enter the IP address of an alternative DNS server.

15.2 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.

15.2.1 Controlled Interfaces

In the **WAN->Real Time Jitter Control->Controlled Interfaces** a list of functions is displayed for which the Real Time Jitter Control function is configured.

15.2.1.1 New

Click the **New** button to optimise voice transmission for other interfaces.

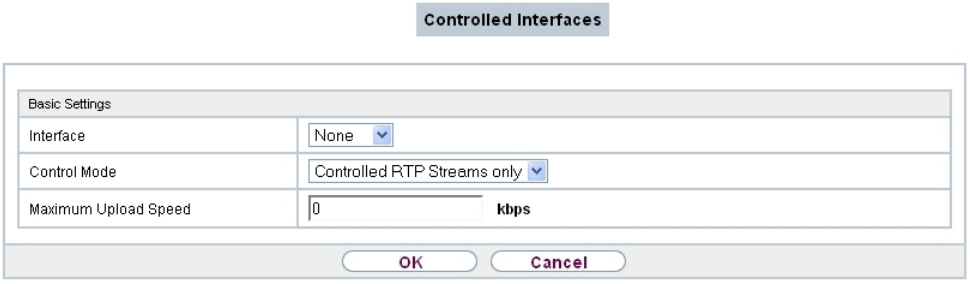


Fig. 117: **WAN->Real Time Jitter Control->Controlled Interfaces->New**

The menu **WAN->Real Time Jitter Control->Controlled Interfaces->New** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Interface	Define for which interfaces voice transmission is to be optimised.
Control Mode	Select the mode for the optimisation. Possible values: • *Controlled RTP Streams only* (default value): By means of the data routed via the media gateway, the system detects voice data traffic and optimises the voice transmission. • *All RTP Streams*: All RTP streams are optimised. • *Inactive*: Voice data transmission is not optimised. • *Always*: Voice data transmission is always optimised.
Maximum Upload Speed	Enter the maximum available upstream bandwidth in kbp/s for the selected interface.

Chapter 16 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.

16.1 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 93). IPSec implementation achieves this firstly by using the Authentication Header (AH) protocol and Encapsulated Security Payload (ESP) protocol and secondly through the use of cryptographic key administration mechanisms like the Internet Key Exchange (IKE) protocol.

Additional Traffic Filter

bintec elmeg gateways support two different methods of setting up IPSec connections:

- a method based on policies and
- a method based on routing.

The policy-based method uses data traffic filters to negotiate the IPSec phase 2 SAs. This allows for a very "fine-grained" filter to be applied to the IP packet, even at the level of the protocol and the port.

The routing-based method offers various advantages over the policy-based method, e.g., NAT/PAT within a tunnel, IPSec in combination with routing protocols and the creation of VPN backup scenarios. With the routing-based method, the configured or dynamically learned routes are used to negotiate the IPSec phase 2 SAs. Although this method does simplify many configurations, problems may also be caused by competing routes or the "coarser" filtering of data traffic.

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

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

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

Note

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

Note

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

16.1.1 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.

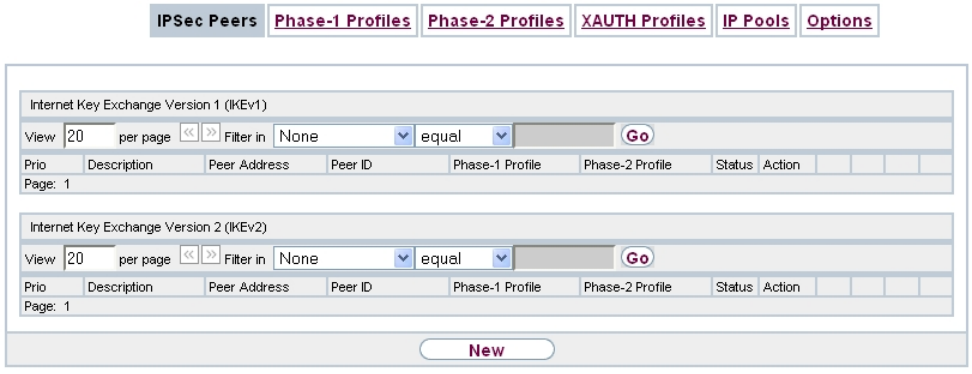


Fig. 118: **VPN->IPSec->IPSec Peers**

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 434.

16.1.1.1 New

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

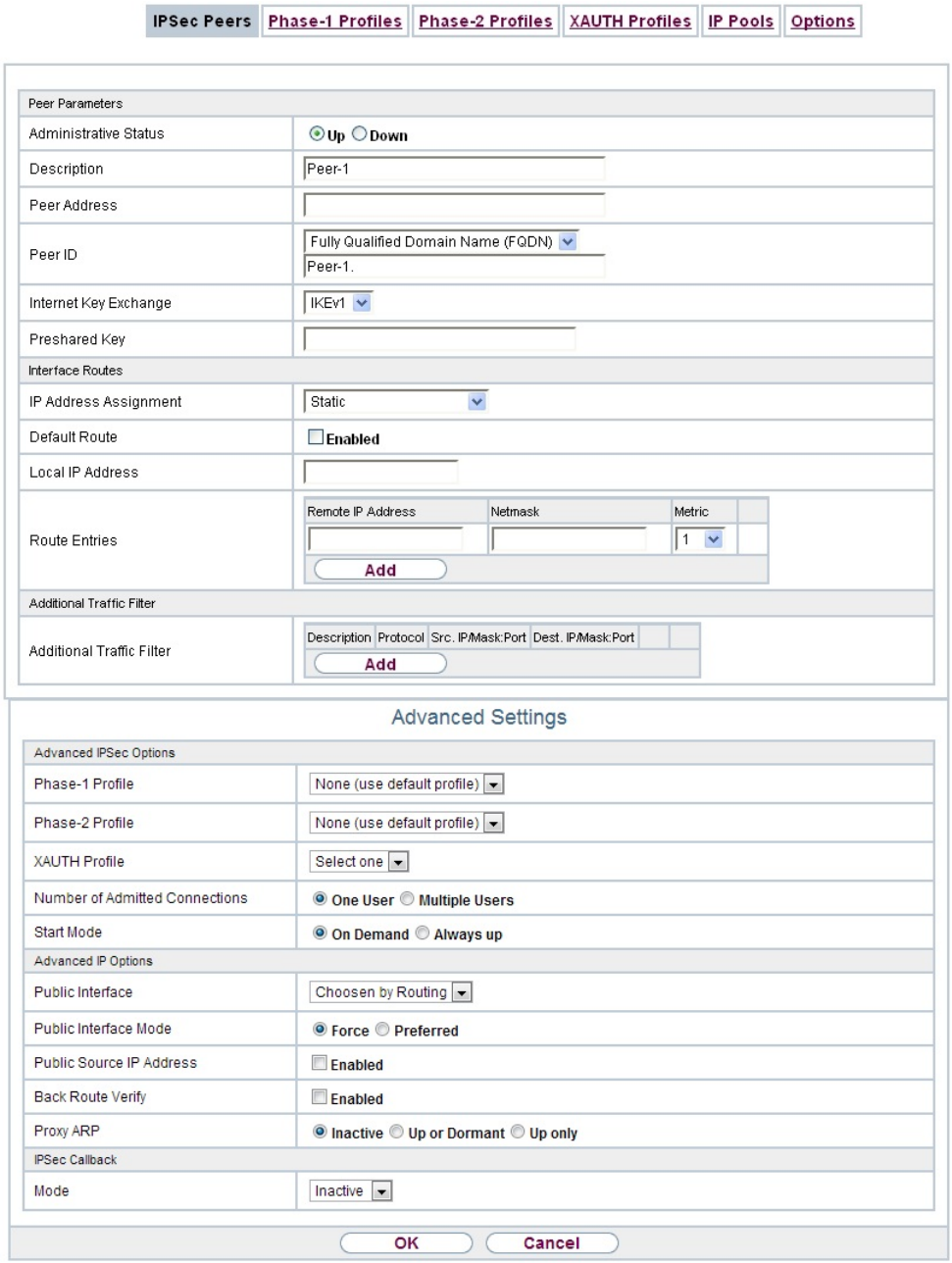


Fig. 119: **VPN->IPSec->IPSec Peers->New**

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

Fields in the menu Peer Parameters

Field	Description
Administrative Status	Select the status to which you wish to set the peer after saving the peer configuration. Possible values: • *Up* (default value): The peer is available for setting up a tunnel immediately after saving the configuration. • *Down*: The peer is initially not available after the configuration has been saved.
Description	Enter a description of the peer that identifies it. The maximum length of the entry is 255 characters.
Peer Address	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)*: Any string • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)* • *Key ID*: Any string On the peer device, this ID corresponds to the **Local ID Value**.
Internet Key Exchange	Not available for devices in the **WIxxxxn** series. Those devices only support IKEv1. Select the version of the Internet Exchange Protocol to be used. Possible values: • *IKEv1* (default value): Internet Key Exchange Protocol Ver-

Field	Description
	sion 1 • *IKEv2*: Internet Kex Exchange Protocol Version 2
Authentication Method	Only for **Internet Key Exchange** = *IKEv2* Select the authentication method. Possible values: • *Preshared Keys* (default value): If you do not use certificates for the authentication, you can select Preshared Keys. These are configured during peer configuration in the **IPSec Peers**. The preshared key is the shared password. • *RSA Signature*: Phase 1 key calculations are authenticated using the RSA algorithm.
Local ID Type	Only for **Internet Key Exchange** = *IKEv2* Select the local ID type. Possible ID types: • *Fully Qualified Domain Name (FQDN)* • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)* • *Key ID*: Any string
Local ID	Only for **Internet Key Exchange** = *IKEv2* Enter the ID of your device. For **Authentication Method** = *DSA Signature* or *RSA Signature* the option **Use Subject Name from certificate** is displayed. When you enable the option **Use Subject Name from certificate**, the first alternative subject name indicated in the certificate is used, or, if none is specified, the subject name of the certificate is used. Note: If you use certificates for authentication and your certificate contains alternative subject names (see *Certificates* on page 93), you must make sure your device selects the first al-

Field	Description
	ternative subject name by default. Make sure you and your peer both use the same name, i.e. that your local ID and the peer ID your partner configures for you are identical.
Preshared Key	Enter the password agreed with the peer. The maximum length of the entry is 50 characters. All characters are possible except for *0x* at the start of the entry.

Fields in the menu Interface Routes

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*: Can only be selected for IKEv1. Select this option if your gateway receives an IP address from the server as IPSec client. • *IKE Config Mode Server*: Select this option if your gateway assigns an IP address as server for connecting clients. This is taken from the selected **IP Assignment Pool**.
Config Mode	Only where **IP Address Assignment** = *IKE Config Mode Server* or *IKE Config Mode Client* Possible values: • *Pull* (default value): The client requests the IP address and the gateway answers the request. • *Push*: The gateway suggests an IP address to the client and the client must either accept or reject this. This value must be identical for both sides of the tunnel.
IP Assignment Pool	Only if **IP Address Assignment** = *IKE Config Mode Server* Select an IP pool configured in the **VPN**->**IPSec**->**IP Pools**menu. If an IP pool has not been configured here yet, the message *Not yet defined* appears in this field.
Default Route	Only for **IP Address Assignment** = *Static* or *IKE Config*

Field	Description
	Mode Client Select whether the route to this IPSec peer is to be defined as the default route. The function is enabled with *Enabled*. The function is disabled by default.
Local IP Address	Only for **IP Address Assignment** = *Static* or *IKE Config Mode Server* Enter the WAN IP address of your IPSec tunnel. This can be the same IP address as the address configured on your router as the LAN IP address.
Metric	Only for **IP Address Assignment** = *Static* or *IKE Config Mode Client* and **Default Route** = *Enabled* Select the priority of the route. The lower the value, the higher the priority of the route. Value range from *0* to *15*. The default value is *1*.
Route Entries	Only for **IP Address Assignment** = *Static* or *IKE Config Mode Client* Define routing entries for this connection partner. • *Remote IP Address*: IP address of the destination host or LAN. • *Netmask*: Netmask for *Remote IP Address*. • *Metric*: The lower the value, the higher the priority of the route (possible values *0..15*). The default value is *1*.

Fields in the menu Additional Traffic Filter

Field	Description
Additional Traffic Filter	Only for **Internet Key Exchange** = *IKEv1* Use **Add** to create a new filter.

Additional data traffic filters

bintec elmeg Gateways support two different methods for establishing IPSec connections:

- a method based on policies and
- a method based on routing.

The policy-based method uses data traffic filters to negotiate the IPSec phase 2 SAs. This enables the filtering of the IP packets to be very "fine grained" down to protocol and port level.

The routing-based method offers various advantages over the policy-based method, e.g., NAT/PAT within a tunnel, IPSec in combination with routing protocols and the creation of VPN backup scenarios. With the routing-based method, the configured or dynamically learned routes are used to negotiate the IPSec phase 2 SAs. While it is true that this method simplifies many configurations, at the same time there can be problems due to competing routes or the "coarser" filtering of the data traffic.

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

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

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

Note

The parameter **Additional Traffic Filter** is only relevant to the initiator of the IPSec connection, it only applies to outgoing data traffic.

Note

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

Add new entries with **Add**.

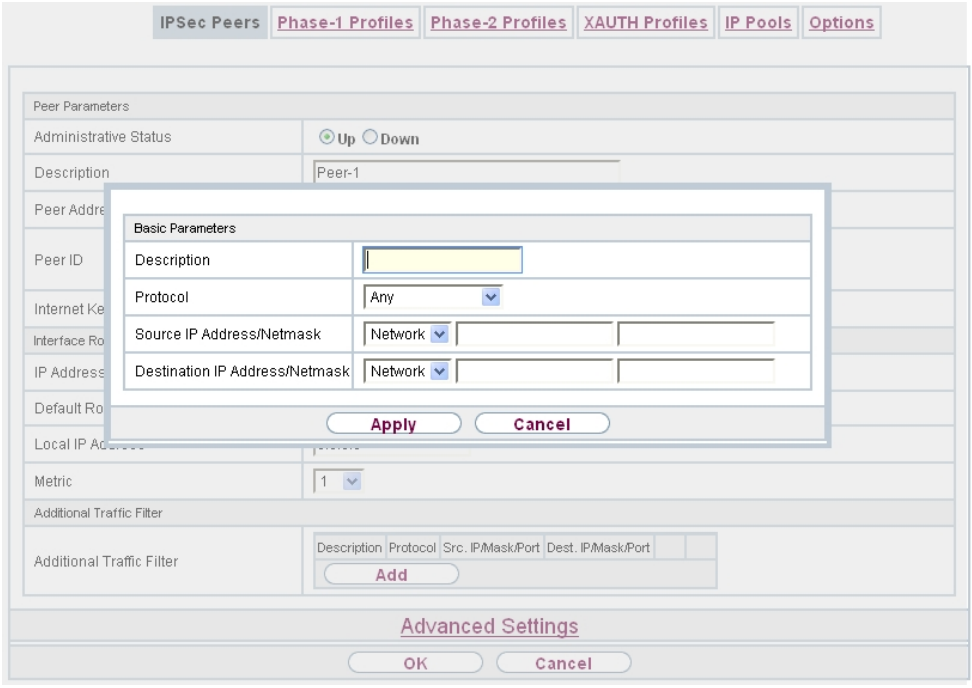


Fig. 120: **VPN->IPSec->IPSec Peers->New->Add**

Fields in the menu Basic Parameters

Field	Description
Description	Enter a description for the filter.
Protocol	Select a protocol. The *Any* option (default value) matches all protocols.
Source IP Address/ Netmask	Enter, if required, the source IP address and netmask of the data packets. Possible values: • *Any* • *Host*: Enter the IP address of the host. • *Network* (default value): Enter the network address and the related netmask.
Source Port	Only for **Protocol** = *TCP* or *UDP* Enter the source port of the data packets. The default setting –

Field	Description
	All- (= -1) means that the port remains unspecified.
Destination IP Address/Netmask	Enter the destination IP address and corresponding netmask of the data packets.
Destination Port	Only for **Protocol** = *TCP* or *UDP* Enter the destination port of the data packets. The default setting *-All-* (= -1) means that the port remains unspecified.

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

Fields in the menu Advanced IPSec Options

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

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. The dynamic peer configuration on the gateway must not specify a peer ID or a peer IP address. Clients connecting to the gateway, however, must have a peer ID specified in the client peer configuration, since the ID is still used to differentiate the tunnels created via the dynamic peer. The resulting gateway peer would match all incoming tunnel requests. It is, therefore, essential to put it at the end of the IPSec peer list on the gateway. Otherwise all peers that follow the dynamic peer in the peer list would be inactive.
Start Mode	Select how the peer is to be switched to the active state. Possible values: • *On Demand* (default value): The peer is switched to the active state by a trigger. • *Always up*: The peer is always active.

Fields in the menu Advanced IP Options

Field	Description
Public Interface	Specify the public (or WAN) interface that this peer is to use to connect to its VPN partner. If you select *Choosen by Routing*, the decision as to via which interface the data traffic is routed is made based on the current routing table. If you select an interface, the interface is used taking into consideration the

Field	Description
	setting under **Public Interface Mode**.
Public Interface Mode	Specify how strictly the setting under **Public Interface** is handled. Possible values: • *Force*: Only the selected interface is used, whatever the priorities in the current routing table. • *Preferred*: Depending on the priorities in the current routing table, the selected interface is used if no more favourable route is available via a different interface.
Public Source IP Address	If you are operating more than one Internet connection in parallel, here you can specify the public IP address that is to be used as the source address for the peer's data traffic. Select whether the **Public Source IP Address** is to be enabled. The function is enabled with *Enabled*. In the input field, enter the public IP address that is to be used as the sender address. The function is disabled by default.
Back Route Verify	Select whether a check on the back route should be activated for the interface to the connection partner. The function is enabled with *Enabled*. The function is disabled by default.
MobIKE	Only for peers with IKEv2. **MobIKE** In cases of changing public IP addresses, enables only these addresses to be updated in the SAs without the SAs themselves having to be renegotiated. The function is enabled by default. Note that MobIKE requires a current IPSec client, e. g. the current Windows 7 or Windows 8 client or the latest version of the bintec elmeg IPSec client.
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:

Field	Description
	• *Inactive* (default value): Deactivates Proxy ARP for this IPSec peer. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the IPSec peer is *Up* (active) or *Dormant* (dormant). In the case of *Dormant*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device responds to an ARP request only if the status of the connection to the IPSec peer is *Up* (active), i.e. a connection already exists to the IPSec peer.

IPSec Callback

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

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

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

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

Note

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

Transfer of IP Address over ISDN

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

Note

To use the IP address transfer over ISDN function, you must obtain a free-of-charge extra licence.

You can obtain the licence data for extra licences via the online licensing pages in the support section at *www.bintec-elmeg.com* . Please follow the online licensing 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 menu IPSec Callback* on page 288. Not all transfer modes are supported by all telephone companies. If you are not sure, automatic selection by the device can be used to ensure that all the available possibilities can be used.

Note

The callback configuration should be the same on the two devices so that your device is able to identify the IP address information from the called peer.

The following roles are possible:

- One side takes on the active role, the other the passive role.
- Both sides can take on both roles (both).

The IP address transfer and the start of IKE phase 1 negotiation take place in the following steps:

(1) Peer A (the callback initiator) sets up a connection to the Internet in order to be assigned a dynamic IP address and be reachable for peer B over the Internet.

(2) Your device creates a token with a limited validity and saves it together with the current IP address in the MIB entry belonging to peer B.

(3) Your device sends the initial ISDN call to peer B, which transfers the IP address of peer A and the token as per the callback configuration.

(4) Peer B extracts the IP address of peer A and the token from the ISDN call and assigns them to peer A based on the calling party number configured (the ISDN number used by peer A to send the initial call to peer B).

(5) The IPSec Daemon at peer B's device can use the transferred IP address to initiate phase 1 negotiation with peer A. Here the token is returned to peer A in part of the payload in IKE negotiation.

(6) Peer A is now able to compare the token returned by peer B with the entries in the MIB and so identify the peer without knowing its IP address.

As peer A and peer B can now mutually identify each other, negotiations can also be conducted in the ID Protect mode using preshared keys.

Note

In some countries (e.g. Switzerland), the call in the D channel can also incur costs. An incorrect configuration at the called side can mean that the called side opens the B channel the calling side incurs costs.

The following options are only available on devices with an ISDN connection:

Fields in the menu IPSec Callback

Field	Description
Mode	Select the Callback Mode. Possible values: • *Inactive* (default value): IPSec callback is deactivated. The local device neither reacts to incoming ISDN calls nor initiates ISDN calls to the remote device. • *Passive*: The local device only reacts to incoming ISDN calls and, if necessary, initiates setting up an IPSec tunnel to the peer. No ISDN calls are sent to the remote device to cause this to set up an IPSec tunnel. • *Active*: The local device sends an ISDN call to the remote device to cause this to set up an IPSec tunnel. The device does not react to incoming ISDN calls. • *Both*: Your device can react to incoming ISDN calls and send ISDN calls to the remote device. The setting up of an IPSec tunnel is executed (after an incoming ISDN call) and initiated (by an outgoing ISDN call).
Incoming Phone Number	Only for **Mode** = *Passive* or *Both* Enter the ISDN number from which the remote device calls the local device (calling party number). Wildcards may also be used.
Outgoing Phone Number	Only for **Mode** = *Active* or *Both* Enter the ISDN number with which the local device calls the remote device calls (called party number). Wildcards may also be used.
Transfer own IP address over ISDN/GSM	Select whether the IP address of your own device is to be transferred over ISDN for IPSec callback. The function is enabled with *Enabled*. The function is disabled by default.
Transfer Mode	Only for **Transfer own IP address over ISDN/GSM** = enabled Select the mode in which your device is to attempt to transfer its IP address to the peer.

Field	Description
	Possible values: • *Autodetect best mode*: Your device automatically determines the most favourable mode. It first tries all D channel modes before switching to the B channel. (Costs are incurred for using the B channel.) • *Autodetect only D Channel Modes*: Your device automatically determines the most favourable D channel mode. The use of the B channel is excluded. • *Use specific D Channel Mode*: Your device tries to transfer the IP address in the mode set in the **Mode** field. • *Try specific D Channel Mode, fall back to B Channel*: Your device tries to transfer the IP address in the mode set in the **Mode** field. If this does not succeed, the IP address is transferred in the B channel. (This incurs costs.) • *Use only B Channel Mode*: Your device transfers the IP address in the B channel. This incurs costs.
D Channel Mode	Only for **Transfer Mode** = *Use specific D Channel Mode* or *Try specific D Channel Mode, fall back to B Channel* Select the D channel mode in which your device tries to transfer the IP address. Possible values: • *LLC* (default value): The IP address is transferred in the "LLC information elements" of the D channel. • *SUBADDR*: The IP address is transferred in the subaddress "information elements" of the D channel. • *LLC and SUBADDR*: The IP address is transferred in both the "LLC" and "subaddress information elements".

16.1.2 Phase-1 Profiles

A list of all configured tunnel profiles is displayed in the **VPN**->**IPSec**->**Phase-1 Profiles** menu.

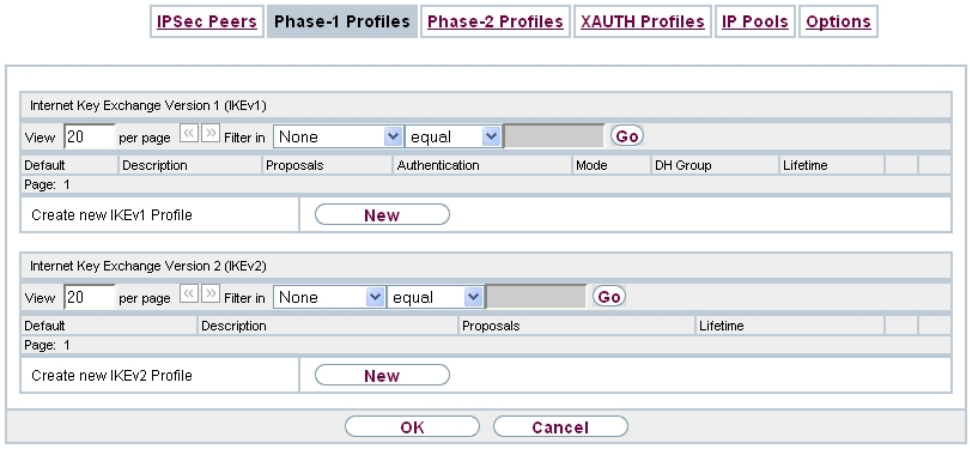


Fig. 121: **VPN->IPSec->Phase-1 Profiles**

In the **Default** column, you can mark the profile to be used as the default profile.

16.1.2.1 New

Choose the **New** (at **Create new IKEv1 Profile** or **Create new IKEv2 Profile**) button to create additional profiles.

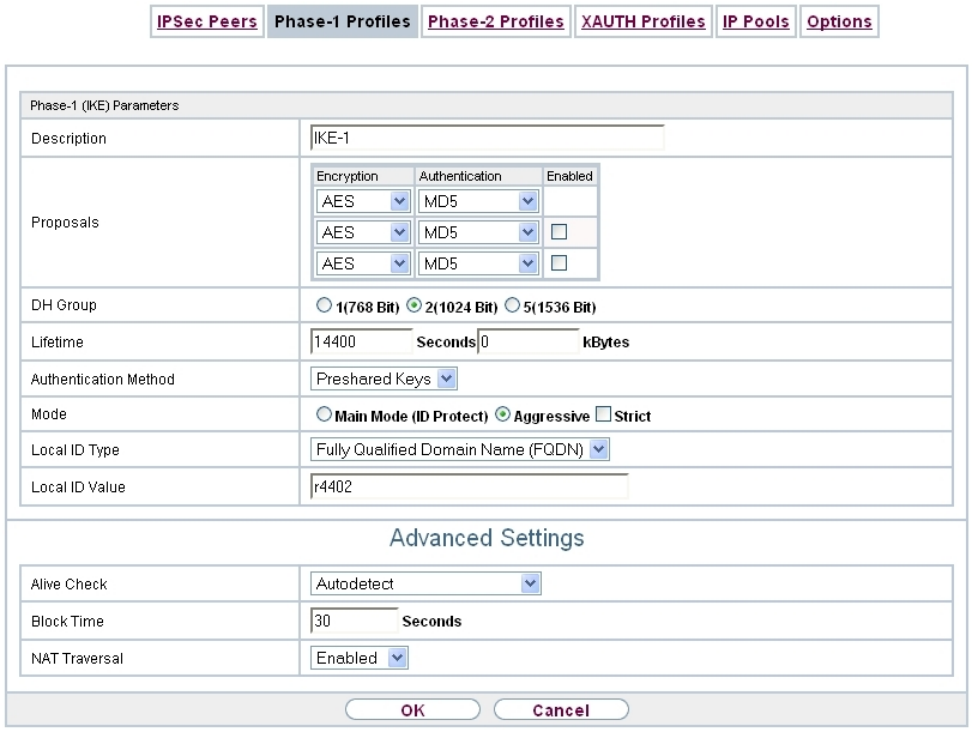


Fig. 122: **VPN->IPSec->Phase-1 Profiles->New**

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

Fields in the Phase-1 (IKE) Parameters menu.

Field	Description
Description	Enter a description that uniquely defines the type of rule.
Proposals	In this field, you can select any combination of encryption and message hash algorithms for IKE phase 1 on your device. The combination of six encryption algorithms and four message hash algorithms gives 24 possible values in this field. At least one proposal must exist. Therefore the first line of the table cannot be deactivated. Encryption algorithms (**Encryption**): • *3DES* (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

Field	Description
	(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. The partner's AES key length is used here. If this has also selected the parameter *AES* , a key length of 128 bits is used. • *AES-128*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 128 bits. • *AES-192*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 192 bits. • *AES-256*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 256 bits. Hash algorithms (**Authentication**): • *MD5* (default value): MD5 (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 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 authentic-

Field	Description
	ation 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	Only for **Phase-1 (IKE) Parameters** The Diffie-Hellman group defines the parameter set used as the basis for the key calculation during phase 1. "MODP" as supported by bintec elmeg 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.
Lifetime	Create a lifetime for phase 1 keys. The following options are available for defining the **Lifetime**: • Input in **Seconds**: Enter the lifetime for phase 1 key in seconds. The value can be a whole number from 0 to 2147483647. The default value is *14400*, which means the key must be renewed once four hours have elapsed. • Input in **kBytes**: Enter the lifetime for phase 1 keys as amount of data processed in kBytes. The value can be a whole number from 0 to 2147483647. The default value is *0*, which means that the number of transmitted kBytes is irrelevant.
Authentication Method	Only for **Phase-1 (IKE) Parameters** Select the authentication method. Possible values:

Field	Description
	• *Preshared Keys* (default value): If you do not use certificates for the authentication, you can select Preshared Keys. These are configured during peer configuration in the **VPN**->**IPSec**->**IPSec Peers**. The preshared key is the shared password. • *DSA Signature*: Phase 1 key calculations are authenticated using the DSA algorithm. • *RSA Signature*: Phase 1 key calculations are authenticated using the RSA algorithm. • *RSA Encryption*: In RSA encryption the ID payload is also encrypted for additional security.
Local Certificate	Only for **Phase-1 (IKE) Parameters** Only for **Authentication Method** = *DSA Signature*, *RSA Signature* or *RSA Encryption* This field enables you to select one of your own certificates for authentication. It shows the index number of this certificate and the name under which it is saved. This field is only shown for authentication settings based on certificates and indicates that a certificate is essential.
Mode	Only for **Phase-1 (IKE) Parameters** Select the phase 1 mode. Possible values: • *Aggressive* (default value): The Aggressive Mode is necessary if one of the peers does not have a static IP address and preshared keys are used for authentication. It requires only three messages to configure a secure channel. • *Main Mode (ID Protect)*: This mode (also designated Main Mode) requires six messages for a Diffie-Hellman key calculation and thus for configuring a secure channel, over which the IPSec SAs can be negotiated. A condition is that both peers have static IP addresses if preshared keys are used for authentication. Also define whether the selected mode is used exclusively (**Strict**), or the peer can also propose another mode.

Field	Description
Local ID Type	Only for **Phase-1 (IKE) Parameters** Select the local ID type. Possible values: • *Fully Qualified Domain Name (FQDN)* • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)*
Local ID Value	Only for **Phase-1 (IKE) Parameters** Enter the ID of your device. For **Authentication Method** = *DSA Signature*, *RSA Signature* or *RSA Encryption* the **Use Subject Name from certificate** option is displayed. When you enable the **Use Subject Name from certificate** option, the first alternative subject name indicated in the certificate is used, or, if none is specified, the subject name of the certificate is used. Note: If you use certificates for authentication and your certificate contains alternative subject names (see *Certificates* on page 93), you must make sure your device selects the first alternative subject name by default. Make sure you and your peer both use the same name, i.e. that your local ID and the peer ID your partner configures for you are identical.

Alive Check

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

Two methods are available: Heartbeats and Dead Peer Detection.

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

Fields in the Advanced Settings menu.

Field	Description
Alive Check	Only for **Phase-1 (IKE) Parameters** Select the method to be used to check the functionality of the IPSec connection. In addition to the default method Dead Peer Detection (DPD), the (proprietary) Heartbeat method is implemented. This sends and receives signals every 5 seconds, depending on the configuration. If these signals are not received after 20 seconds, the SA is discarded as invalid. Possible values: • *Autodetect* (default value): Your device detects and uses the mode supported by the remote terminal. • *Inactive*: Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers. • *Heartbeats (Expect only)*: Your device expects a heartbeat from the peer but does not send one itself. • *Heartbeats (Send only)*: Your device expects no heartbeat from the peer, but sends one itself. • *Heartbeats (Send &Expect)*: Your device expects a heartbeat from the peer and sends one itself. • *Dead Peer Detection*: Use DPD (dead peer detection) in accordance with RFC 3706. DPD uses a request-reply protocol to check the availability of the remote terminal and can be configured independently on both sides. This option only checks the availability of the peer if data is to be sent to it. • *Dead Peer Detection (Idle)*: Use DPD (dead peer detection) in accordance with RFC 3706. DPD uses a request-reply protocol to check the availability of the remote terminal and can be configured independently on both sides. This option is used to carry out a check at certain intervals depending on forthcoming data transfers. Only for **Phase-1 (IKEv2) Parameters** Enable or disable alive check. The function is enabled by default.

Field	Description
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. Only for *IKEv1 profiles* Possible values: • *Enabled* (default value): NAT Traversal is enabled. • *Disabled*: NAT Traversal is disabled. • *Force*: The device always behaves as it would if NAT were in use. Only for *IKEv2 profiles* The function is enabled with *Enabled*. The function is enabled by default.
CA Certificates	Only for **Phase-1 (IKE) Parameters** Only for **Authentication Method** = *DSA Signature*, *RSA Signature* or *RSA Encryption* If you enable the **Trust the following CA certificates** option, you can select up to three CA certificates that are accepted for this profile.

Field	Description
	This option can only be configured if certificates are loaded.

16.1.3 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.

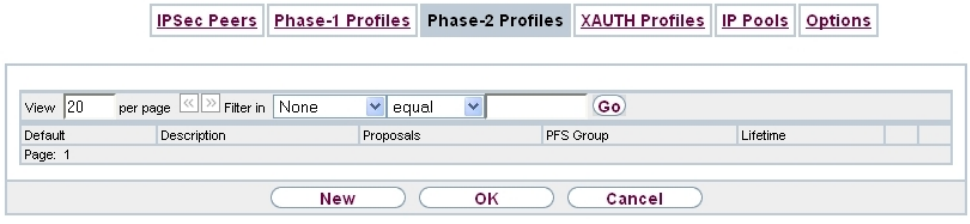


Fig. 123: **VPN**->**IPSec**->**Phase-2 Profiles**

In the **Default** column, you can mark the profile to be used as the default profile.

16.1.3.1 New

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

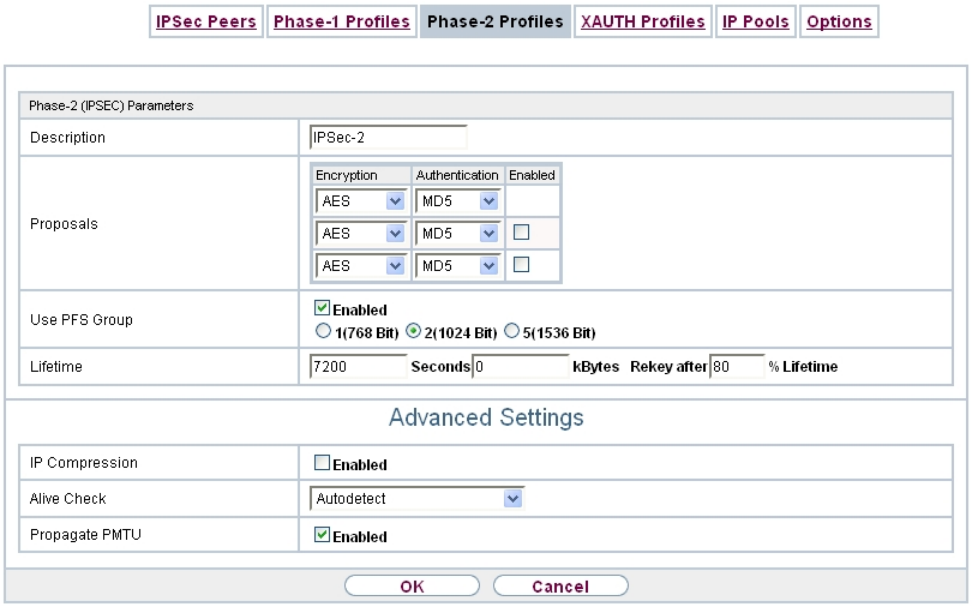


Fig. 124: **VPN->IPSec->Phase-2 Profiles->New**

The menu **VPN->IPSec->Phase-2 Profiles->New** consists of the following fields:

Fields in the Phase-2 (IPSEC) Parameters menu.

Field	Description
Description	Enter a description that uniquely identifies the profile. The maximum length of the entry is 255 characters.
Proposals	In this field, you can select any combination of encryption and message hash algorithms for IKE phase 2 on your default. The combination of six encryption algorithms and two message hash algorithms gives 12 possible values in this field. Encryption algorithms (**Encryption**): • *3DES* (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*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. The partner's AES key length is used here. If this has also selected the parameter

Field	Description
	AES , a key length of 128 bits is used. • *AES-128*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 128 bits. • *AES-192*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 192 bits. • *AES-256*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 256 bits. • *Twofish*: Twofish was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower. • *Blowfish*: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish. • *CAST*: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES. • *DES*: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits. Hash algorithms (**Authentication**): • *MD5* (default value): MD5 (Message Digest #5) is an older hash algorithm. It is used with a 96 bit digest length for IPSec. • *-- ALL --*: All options can be used. • *SHA1*: SHA1 (Secure Hash Algorithm #1) is a hash algorithm developed by NSA (United States National Security Association). It is rated as secure, but is slower than MD5. It is used with a 96 bit digest length for IPSec. 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 enable PFS (*Enabled*), the options are the same as for the configuration of **DH Group** in the **VPN**->**IPSec**->**Phase-1 Profiles** menu. PFS is

Field	Description
	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, 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*. **Rekey after**: Specify the percentage in the course of the lifetime at which the phase 2 keys are to be regenerated. The percentage entered is applied to both the lifetime in seconds and the lifetime in kBytes. The default value is *80* %.

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

Fields in the Advanced Settings menu.

Field	Description
IP Compression	Select whether compression is to be activated before data encryption. If data is compressed effectively, this can result in higher performance and a lower volume of data to be transferred. In the case of fast lines or data that cannot be compressed, you are advised against using this option as the performance can be significantly affected by the increased effort during compression. The function is enabled with *Enabled*. The function is disabled by default.
Alive Check	Select whether and how IPSec heartbeats are used. A bintec elmeg IPSec heartbeat is implemented to determine whether or not a Security Association (SA) is still valid. This function sends and receives signals every 5 seconds, depending on the configuration. If these signals are not received after 20 seconds, the SA is discarded as invalid. Possible values: • *Autodetect* (default value): Automatic detection of whether the remote terminal is a bintec elmeg device. If it is, *Heartbeats (Send &Expect)* (for a remote terminal with bintec elmeg) or *Inactive* (for a remote terminal without bintec elmeg) is set. • *Inactive*: Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers. • *Heartbeats (Expect only)*: Your device expects a heartbeat from the peer but does not send one itself. • *Heartbeats (Send only)*: Your device expects no heartbeat from the peer, but sends one itself. • *Heartbeats (Send &Expect)*: Your device expects a heartbeat from the peer and sends one itself.
Propagate PMTU	Select whether the PMTU (Path Maximum Transfer Unit) is to be propagated during phase 2. The function is enabled with *Enabled*. The function is enabled by default.

16.1.4 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.

16.1.4.1 New

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

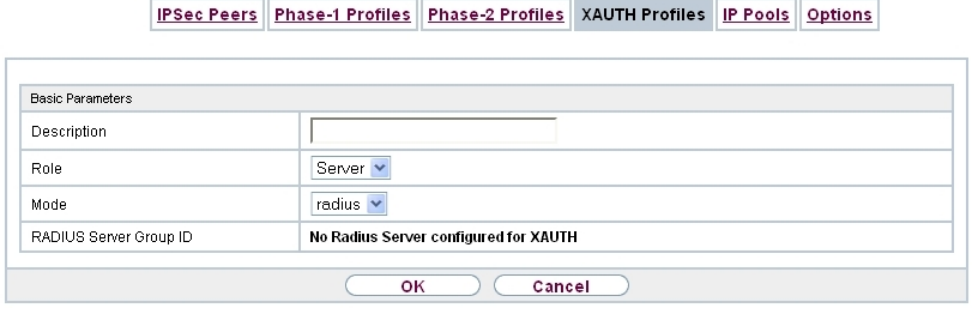


Fig. 125: **VPN->IPSec->XAUTH Profiles->New**

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

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for this XAuth profile.
Role	Select the role of the gateway for XAuth authentication. Possible values: • *Server* (default value): The gateway requires a proof of authorisation. • *Client*: The gateway provides proof of authorisation.
Mode	Only for **Role** = *Server* Select how authentication is carried out. Possible values: • *RADIUS* (default value): Authentication is carried out via a Radius server. It is configured in the **System Management**->**Remote Authentication**->**RADIUS**menu and selected in the **RADIUS Server Group ID** field. • *Local*: Authentication is carried out via a local list.
Name	Only for **Role** = *Client* Enter the authentication name of the client.
Password	Only for **Role** = *Client* Enter the authentication password.
RADIUS Server Group ID	Only for **Role** = *Server* Select the desired list in **System Management**->**Remote Authentication**->**RADIUS** configured RADIUS group.
Users	Only for **Role** = *Server* and **Mode** = *Local* If your gateway is configured as an XAuth server, the clients can be authenticated via a locally configured user list. Define the members of the user group of this XAUTH profile here by

Field	Description
	entering the authentication name of the client (**Name**)) and the authentication password (**Password**). Add new members with **Add**.

16.1.5 IP Pools

In the **IP Pools** menu a list of all IP pools for your configured IPSec connections is displayed.

If for an IPSec peer you have set **IP Address Assignment** *IKE Config Mode Server*, you must define the IP pools here from which the IP addresses are assigned.

16.1.5.1 Edit or New

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

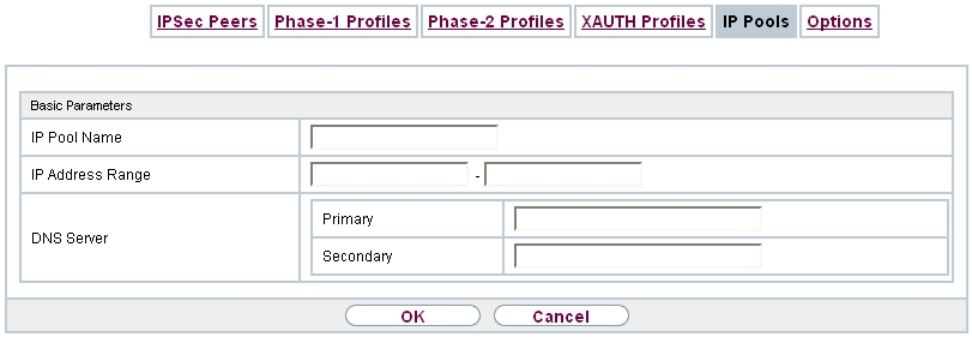


Fig. 126: **VPN->IPSec->IP Pools->New**

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	**Primary**: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. **Secondary**: Optionally, enter the IP address of an alternative

Field	Description
	DNS server.

16.1.6 Options

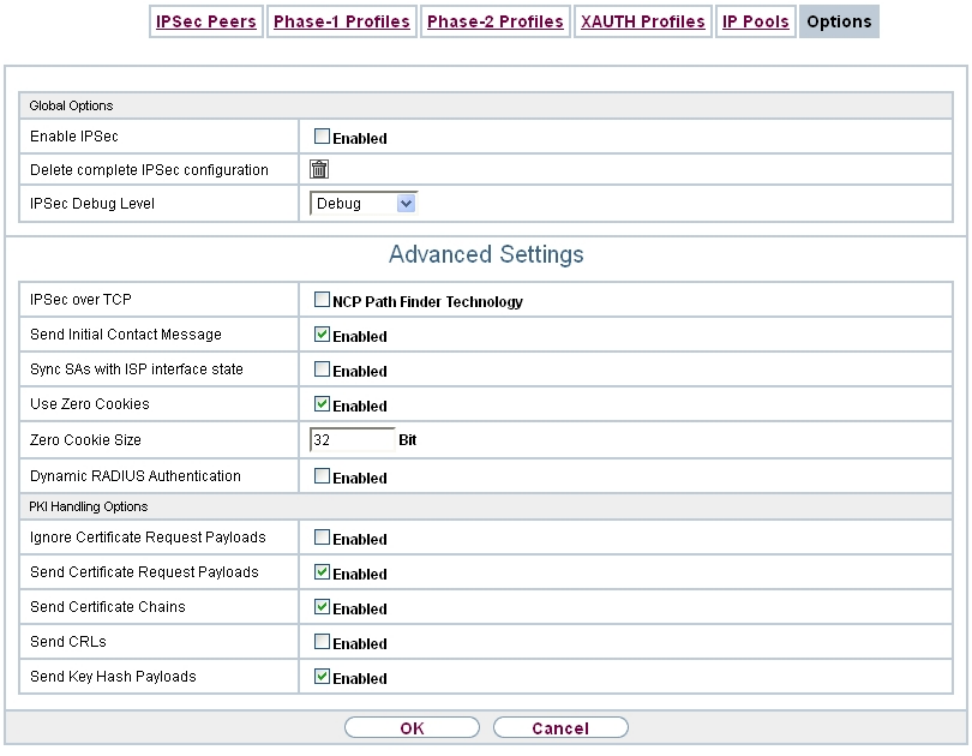


Fig. 127: **VPN->IPSec->Options**

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

Fields in the Global Options menu.

Field	Description
Enable IPSec	Select whether you want to activate IPSec. The function is enabled with *Enabled*. The function is active as soon as an IPSec Peer is configured.
Delete complete IPSec configuration	If you click the icon, delete the complete IPSec configuration of your device.

Field	Description
	This cancels all settings made during the IPSec configuration. Once the configuration is deleted, you can start with a completely new IPSec configuration. You can only delete the configuration if **Enable IPSec** = not activated.
IPSec Debug Level	Select the priority of the syslog messages of the IPSec subsystem to be recorded internally. Possible values: • *Emergency* (highest priority) • *Alert* • *Critical* • *Error* • *Warning* • *Notice* • *Information* • *Debug* (default value, lowest priority) Syslog messages are only recorded internally if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level "debug".

The **Advanced Settings** menu is for adapting certain functions and features to the special requirements of your environment, i.e. mostly interoperability flags are set. The default values are globally valid and enable your system to work correctly to other bintec elmeg devices, so that you only need to change these values if the remote terminal is a third-party product or you know special settings are necessary. These may be needed, for example, if the remote end operates with older IPSec implementations.

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

Fields in the Advanced Settings menu.

Field	Description
IPSec over TCP	Determine whether IPSec over TCP is to be used. IPSec over TCP is based on NCP pathfinder technology. This technology insures that data traffic (IKE, ESP, AH) between peers is integrated into a pseudo HTTPS session.

Field	Description
	The function is enabled with *Enabled*. The function is disabled by default.
Send Initial Contact Message	Select whether IKE Initial Contact messages are to be sent during IKE (phase 1) if no SAs with a peer exist. The function is enabled with *Enabled*. The function is enabled by default.
Sync SAs with ISP interface state	Select whether all SAs are to be deleted whose data traffic was routed via an interface on which the status has changed from *Up* to *Down*, *Dormant* or *Blocked*. The function is enabled with *Enabled*. The function is disabled by default.
Use Zero Cookies	Select whether zeroed ISAKMP Cookies are to be sent. These are equivalent to the SPI (Security Parameter Index) in IKE proposals; as they are redundant, they are normally set to the value of the negotiation currently in progress. Alternatively, your device can use zeroes for all values of the cookie. In this case, select *Enabled*.
Zero Cookie Size	Only for **Use Zero Cookies** = enabled. Enter the length in bytes of the zeroed SPI used in IKE proposals. The default value is *32*.
Dynamic RADIUS Authentication	Select whether RADIUS authentication is to be activated via IPSec. The function is enabled with *Enabled*. The function is disabled by default.

Fields in the PKI Handling Options menu.

Field	Description
Ignore Certificate 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 for RSA encryption. Activate this function with *Enabled* to suppress this behaviour.

16.2 L2TP

The layer 2 tunnel protocol (L2TP) enables PPP connections to be tunnelled via a UDP connection.

Your bintec elmeg device supports the following two modes:

- L2TP LNS Mode (L2TP Network Server): for incoming connections only
- L2TP LAC Mode (L2TP Access Concentrator): for outgoing connections only

Note the following when configuring the server and client: An L2TP tunnel profile must be created on each of the two sides (LAC and LNS). The corresponding L2TP tunnel profile is used on the initiator side (LAC) to set up the connection. The L2TP tunnel profile is needed on the responder side (LNS) to accept the connection.

16.2.1 Tunnel Profiles

A list of all configured tunnel profiles is displayed in the **VPN**->**L2TP**->**Tunnel Profiles** menu.

16.2.1.1 New

Choose the **New** button to create additional tunnel profiles.

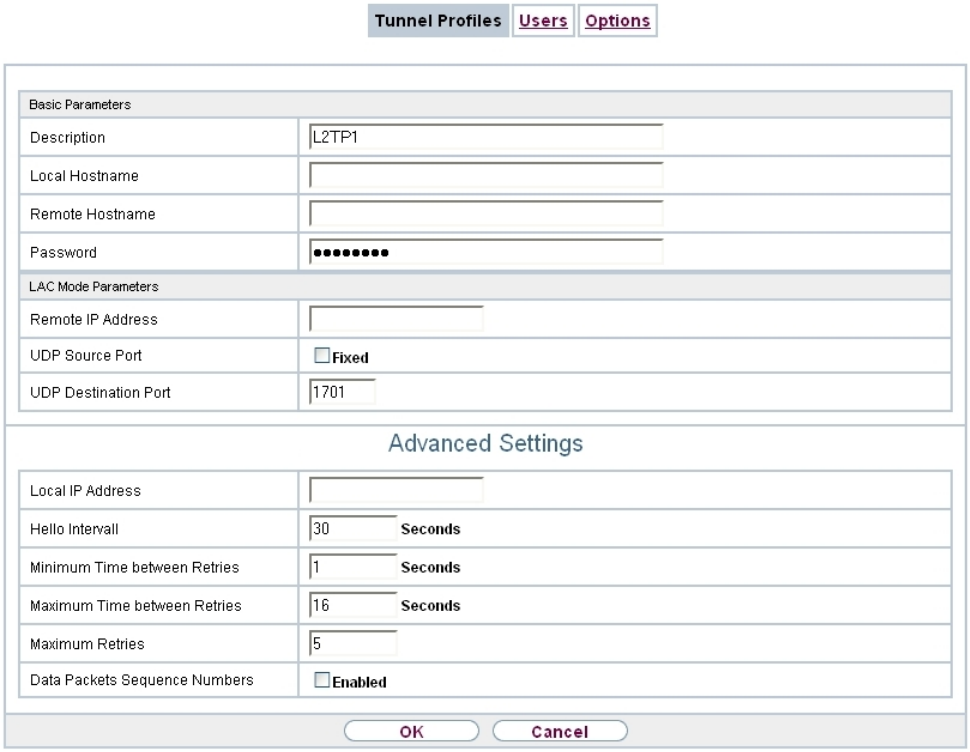


Fig. 128: **VPN**->**L2TP**->**Tunnel Profiles**->**New**

The menu **VPN**->**L2TP**->**Tunnel Profiles**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for the current profile. The device automatically names the profiles *L2TP* and numbers them, but the value can be changed.
Local Hostname	Enter the host name for LNS or LAC. • *LAC*: The local hostname is used in outgoing tunnel setup messages to identify this device and is associated with the remote hostname of a tunnel profile configured on the LNS. These tunnel setup messages are SCCRQs (Start Control Connection Request) sent from the LAC and SCCRPs (Start Control Connection Reply) sent from the LNS. • *LNS*: Is the same as the value for **Remote Hostname** of the incoming tunnel setup message from the LAC.
Remote Hostname	Enter the host name of the LNS or LAC. • *LAC*: Defines the value for **Local Hostname** of the LNS (contained in the SCCRQs received from the LNS and the SCCRPs received from the LAC). A **Local Hostname** configured in the LAC must match **Remote Hostname** configured for the intended profile in the LNS and vice versa. • *LNS*: Defines the **Local Hostname** of the LAC. If the **Remote Hostname** field remains empty on the LNS, the related profile qualifies as the standard entry and is used for all incoming calls for which a profile with a matching remote hostname cannot be found.
Password	Enter the password to be used for tunnel authentication. Authentication between LAC and LNS takes place in both directions, i.e. the LNS checks the **Local Hostname** and the **Password**contained in the SCCRQ of the LAC and compares them with those specified in the relevant profile. The LAC does the same with the fields of the SCCRP of the LNS. If this field remains empty, authentication data in the tunnel setup messages are not sent and are ignored.

Fields in the LAC Mode Parameters menu.

Field	Description
Remote IP Address	Enter the fixed IP address of the LNS used as the destination address for connections based on this profile. The destination must be a device that can behave like an LNS.
UDP Source Port	Enter how the port number to be used as the source port for all outgoing L2TP connections based on this profile is to be determined. By default, the **Fixed** option is disabled, which means that ports are dynamically assigned to the connections that use this profile. If you want to enter a fixed port, enable the *Fixed* option. Select this option if you encounter problems with the firewall or NAT. The available values are *0* to *65535*.
UDP Destination Port	Enter the destination port number to be used for all calls based on this profile. The remote LNS that receives the call must monitor this port on L2TP connections. Possible values are *0* to *65535*. The default value is *1701* (RFC 2661).

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

Fields in the Advanced Settings menu.

Field	Description
Local IP Address	Enter the IP address to be used as the source address for all L2TP connections based on this profile. If this field is left empty, your device uses the IP address of the interface used to reach the remote IP Address by the L2TP tunnel.
Hello Intervall	Enter the interval (in seconds) between the sending of two L2TP HELLO messages. These messages are used to keep the tunnel open. The available values are *0* to *255*, the default value is *30*. The

Field	Description
	value *0* means that no L2TP HELLO messages are sent.
Minimum Time between Retries	Enter the minimum time (in seconds) that your device waits before resending a L2TP control packet for which it received no response. The wait time is dynamically extended until it reaches the **Maximum Time between Retries**. The available values are *1* to *255*, the default value is *1*.
Maximum Time between Retries	Enter the maximum time (in seconds) that your device waits before resending a L2TP control packet for which it received no response. The available values are *8* to *255*, the default value is *16*.
Maximum Retries	Enter the maximum number of times your device is to try to resend the L2TP control packet for which is received no response. The available values are *8* to *255*, the default value is *5*.
Data Packets Sequence Numbers	Select whether your device is to use sequence numbers for data packets sent through a tunnel on the basis of this profile. The function is enabled with *Enabled*. The function is disabled by default.

16.2.2 Users

A list of all configured interface L2TP partners is displayed in the **VPN**->**L2TP**->**Users** menu.

16.2.2.1 New

Choose the **New** button to set up new L2TP partners.

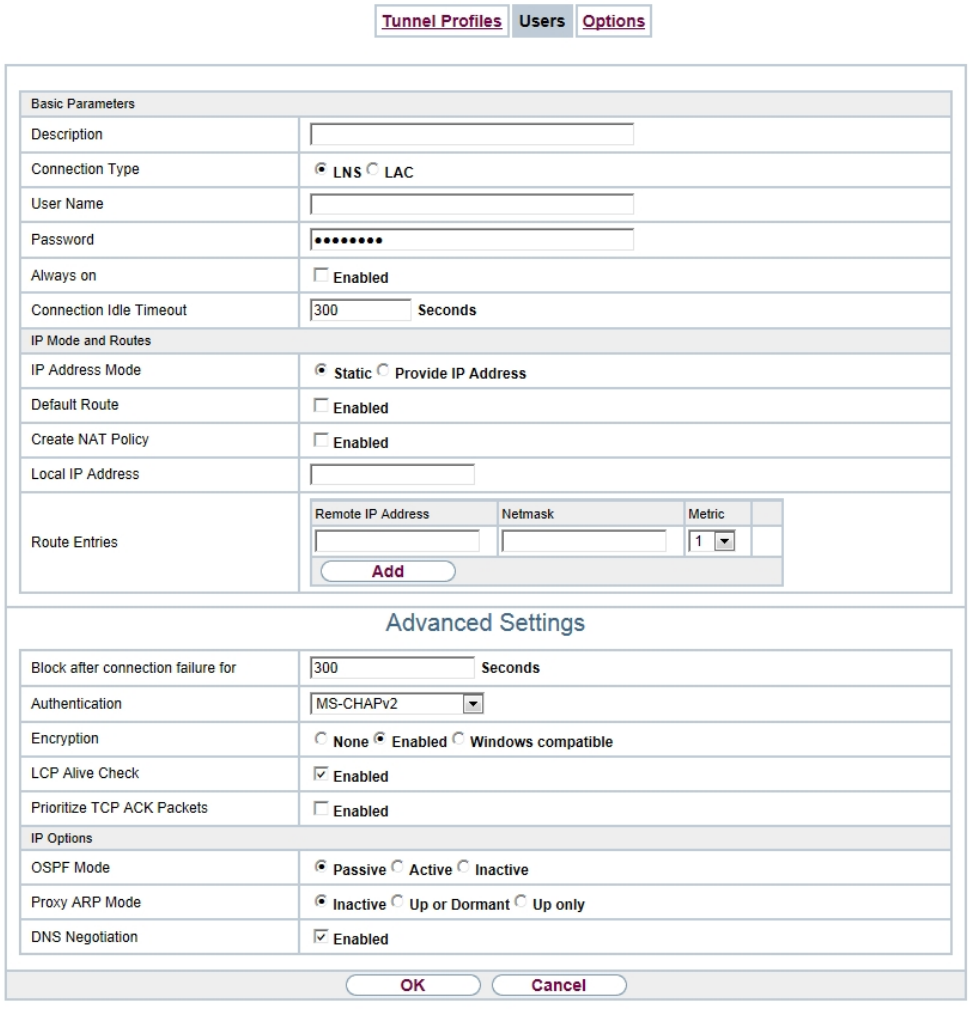


Fig. 129: **VPN->L2TP->Users->New**

The menu **VPN->L2TP->Users->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a name for uniquely identifying the L2TP partner. The first character in this field must not be a number No special characters or umlauts must be used. The maximum length of the entry is 25 characters.
Connection Type	Select whether the L2TP partner is to take on the role of the

Field	Description
	L2TP network server (LNS) or the functions of a L2TP access concentrator client (LAC client). Possible values: • *LNS* (default value): If you select this option, the L2TP partner is configured so that it accepts L2TP tunnels and restores the encapsulated PPP traffic flow. • *LAC*: If you select this option, the L2TP partner is configured so that it encapsulates a PPP traffic flow in L2TP and sets up a L2TP tunnel to a remote LNS.
Tunnel Profile	Only for **Connection Type** = *LAC* Select a profile created in the **Tunnel Profile** menu for the connection to this L2TP partner.
User Name	Enter the code of your device.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default.
Connection Idle Timeout	Only if **Always on** is disabled Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the short hold. The default value is *300*.

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values:

Field	Description
	• *Static* (default value): You enter a static IP address. • *Provide IP Address*: Only for **Connection Type** = *LNS*. Your device dynamically assigns an IP address to the remote terminal. • *Get IP Address*: Only for **Connection Type** = *LAC*. Your device is dynamically assigned an IP address.
Default Route	Only for **IP Address Mode** = *Get IP Address* and *Static* Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is disabled by default.
Create NAT Policy	Only for **IP Address Mode** = *Get IP Address* and *Static* Specify whether Network Address Translation (NAT) is to be activated for this connection. The function is enabled with *Enabled*. The function is disabled by default.
IP Assignment Pool (IPCP)	Only for **IP Address Mode** = *Provide IP Address* Select an IP pool configured in the **WAN**->**Internet + Dialup**->**IP Pools** menu.
Local IP Address	Only for **IP Address Mode** = *Static* Enter the WAN IP address of your device.
Route Entries	Only for **IP Address Mode** = *Static* Enter **Remote IP Address** and **Netmask** of the LANs for L2TP partners and the corresponding **Metric**. Add new entries with **Add**.

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

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *300*.
Authentication	Select the authentication protocol for this L2TP partner. Possible values: • *PAP/CHAP/MS-CHAP* (default value): Primarily run CHAP, on denial, the authentication protocol required by the PPTP partner. (MSCHAP version 1 or 2 possible.) • *PAP*: Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
Encryption	If necessary, select the type of encryption that should be used for data traffic to the L2TP partner. This is only possible if STAC or MS-STAC compression is not activated for the connection. If **Encryption** is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: • *None*: MPP encryption is not used. • *Enabled* (default value): MPP encryption V2 with 128 bit is used to RFC 3078. • *Windows compatible*: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
LCP Alive Check	Select whether the availability of the remote terminal is to be

Field	Description
	checked by sending LCP echo requests or replies. This is recommended for leased lines, PPTP and L2TP connections. The function is enabled with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is enabled with *Enabled*. The function is disabled by default.

Fields in the IP Options menu.

Field	Description
OSPF Mode	Select whether and how routes are propagated via the interface and/or OSPF protocol packets are sent. 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 un-

Field	Description
	til someone actually wants to use the route. • *Up only*: Your device responds to an ARP request only if the status of the connection to the L2TP partner is *Up* (active), i.e. a connection already exists to the L2TP partner.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server** und **Secondary DNS Server** and **WINS Server Primary** and **Secondary** from the L2TP partner or sends these to the L2TP partner. The function is enabled with *Enabled*. The function is enabled by default.

16.2.3 Options

Fig. 130: **VPN->L2TP->Options**

The menu **VPN->L2TP->Options** consists of the following fields:

Fields in the Global Options menu.

Field	Description
UDP Destination Port	Enter the port to be monitored by the LNS on incoming L2TP tunnel connections. Available values are all whole numbers from *1* to *65535*, the default value is *1701*, as specified in RFC 2661.
UDP Source Port Selection	Select whether the LNS should only use the monitored port (**UDP Destination Port**) as the local source port for the L2TP connection. The function is enabled with *Fixed*.

Field	Description
	The function is disabled by default.

16.3 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).

16.3.1 PPTP Tunnels

A list of all PPTP tunnels is displayed in the **PPTP Tunnels** menu.

16.3.1.1 New

Click on **New** to set up further PPTP partners.

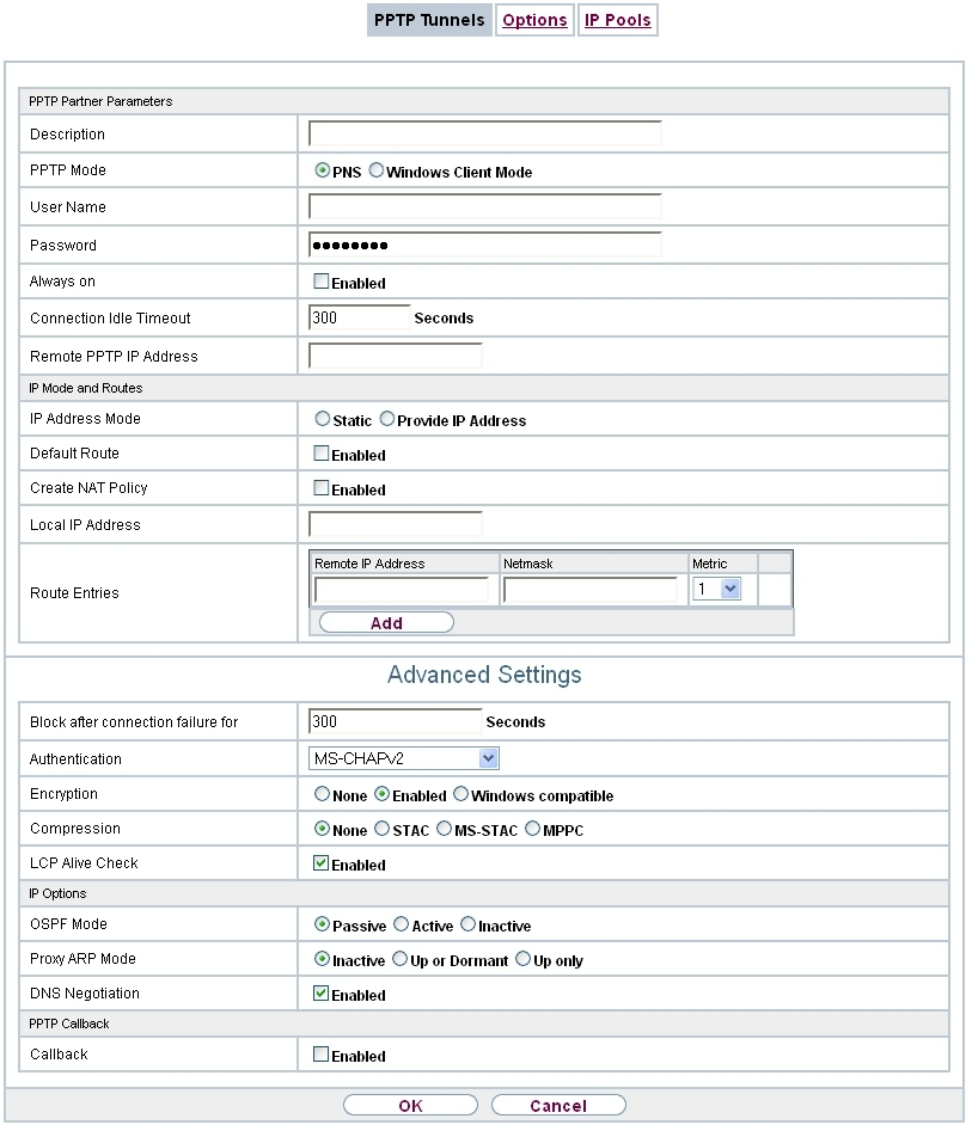


Fig. 131: **VPN->PPTP->PPTP Tunnels->New**

The **VPN->PPTP->PPTP Tunnels->New** menu consists of the following fields:

Fields in the PPTP Partner Parameters menu.

Field	Description
Description	Enter a unique name for the tunnel. The first character in this field must not be a number No special characters or umlauts must be used.
PPTP Mode	Enter the role to be assigned to the PPTP interface. Possible values: • *PNS* (default value): this assigns the PPTP interface the role of PPTP server. • *Windows Client Mode*: This assigns the PPTP interface the role of PPTP client.
User Name	Enter the user name.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle interval in seconds. This determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the timeout. The default value is *300*. Example: *10* for FTP transmission, *20* for LAN-to-LAN transmission, *90* for Internet connections.
Remote PPTP IP Address	Only for **PPTP Mode** = *PNS* Enter the IP address of the PPTP partner.
Remote PPTP IP AddressHost Name	Only for **PPTP Mode** = *Windows Client Mode* Enter the IP address of the PPTP partner.

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Static* (default value): You enter a static IP address. • *Provide IP Address*: Only for **PPTP Mode** = *PNS*: Your device dynamically assigns an IP address to the remote terminal. • *Get IP Address*: Only for **PPTP Mode** = *Windows Client Mode*: Your device is dynamically assigned an IP address.
Default Route	Only if **IP Address Mode** = *Static* Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is disabled by default.
Create NAT Policy	Only if **IP Address Mode** = *Static* When you configure an PPTP connection, specify whether Network Address Translation (NAT) is to be enabled. The function is enabled with *Enabled*. The function is disabled by default.
Local IP Address	Only for **IP Address Mode** = *Static* Assign the IP address from your LAN to the PPTP interface which is to be used as your device's internal source address.
Route Entries	Only if **IP Address Mode** = *Static* Define routing entries for this connection partner. • *Remote IP Address*: IP address of the destination host or LAN. • *Netmask*: Netmask for **Remote IP Address**

Field	Description
	• *Metric*: The lower the value, the higher the priority of the route (possible values *0...15*). The default value is *1*.
IP Assignment Pool (IPCP)	Only if **PPTP Mode** = *PNS*, **IP Address Mode** = *Provide IP Address* Select a IP pool configured in the **VPN**->**PPTP**->**IP Pools** menu.

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

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *300*.
Authentication	Select the authentication protocol for this PPTP partner. Possible values: • *PAP*: Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP*: Give priority to CHAP, if refused use the authentication protocol requested by the PPTP partner. (MSCHAP version 1 or 2 possible.) • *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.

Field	Description
	Possible values: • *None*: MPP encryption is not used. • *Enabled* (default value): MPP encryption V2 with 128 bit is used to RFC 3078. • *Windows compatible*: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
Compression	If necessary, select the type of encryption that should be used for data traffic to the connection partner. If encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: • *None* (default value): Encryption is not used. • *STAC* • *MS-STAC* • *MPPC*: Microsoft Point-to-Point Compression
LCP Alive Check	Select whether the availability of the remote terminal is to be checked by sending LCP echo requests or replies. This is recommended for leased lines, PPTP and L2TP connections. The function is enabled with *Enabled*. The function is enabled by default.

Fields in the IP Options menu.

Field	Description
OSPF Mode	Select whether and how routes are propagated via the interface and/or OSPF protocol packets are to be sent. 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

Field	Description
	propagated or OSPF protocol packets sent over this interface. • *Inactive*: OSPF is disabled for this interface.
Proxy ARP Mode	Select whether your device is to answer APR requests from your LAN on behalf of the specific PPTP partner. Possible values: • *Inactive* (default value): Disables Proxy-ARP (Address Resolution Protocol) for this PPTP partner. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the PPTP partner is *Up* (active) or *Dormant*. In the case of *Idle*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device answers an APR request only if the status of the connection to the PPTP partner is *Active*, i.e. if a connection to the PPTP partner has already been established.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server** and **Secondary DNS Server** from the PPTP partner or sends these to the PPTP partner. The function is enabled with *Enabled*. The function is enabled by default.

Fields in the PPTP Callback menu.

Field	Description
Callback	Enables a PPTP tunnel through the Internet to be set up with a PPTP partner, even if the partner is currently inaccessible. As a rule, the PPTP partner will be requested by means of an ISDN 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 spe-

Field	Description
	cial applications.
Incoming ISDN Number	Only if **Callback** is enabled. Enter the ISDN number from which the remote device calls the local device (calling party number).
Outgoing ISDN Number	Only if **Callback** is enabled. Enter the ISDN number with which the local device calls the remote device calls (called party number).

Fields in the Dial Port Selection (only if callback = activated)

Field	Description
Selected Ports	Enter the ISDN port over which callback is carried out. Possible values: • *All Ports*: The callback is routed over an available ISDN port. • *Specify port*: In **Specific Ports** You can select the required ISDN port.
Specific Ports	Only for **Selected Ports** = *Specify port*, you can select additional ports with **Add**.

16.3.2 Options

In this menu, you can make general settings of the global PPTP profile.

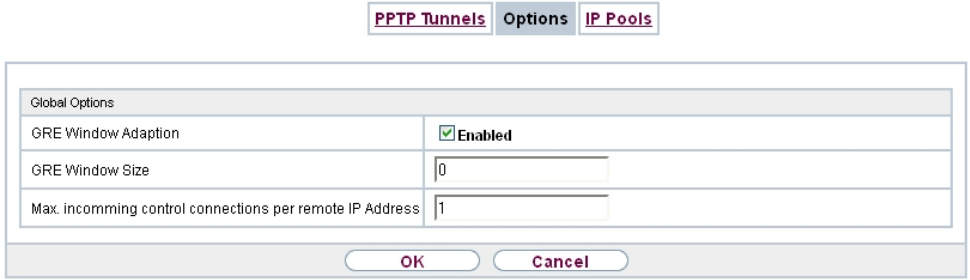


Fig. 132: **VPN->PPTP->Options**

The **VPN->PPTP->Options**menu consists of the following fields:

Fields in the Global Options menu.

Field	Description
GRE Window Adaption	Select whether the GRE Window Adaptation is to be enabled. This adaptation only becomes necessary if you have installed service pack 1 from Microsoft Windows XP. Since, in SP 1, Microsoft has changed the confirmation algorithm in the GRE protocol, the automatic window adaptation for GRE must be turned off for bintec elmeg devices. The function is enabled with *Enabled*. The function is enabled by default.
GRE Window Size	Enter the maximum number of GRE packets that can be sent without confirmation. Windows XP uses a higher initial reception window in the GRE, which is why the maximum send window size must be adjusted here by the **GRE Window Size** value. Possible values are *0* to *256*. The default value is *0*.
Max. incoming control connections per remote IP Address	Enter the maximum number of control connections.

16.3.3 IP Pools

The **IP Pools** menu displays a list of all IP pools for PPTP connections.

Your device can operate as a dynamic IP address server for PPTP connections. You can use this function by providing one or more pools of IP addresses. These IP addresses can be assigned to dialling-in connection partners for the duration of the connection.

Any host routes entered always have priority over IP addresses from the address pools. This means if an incoming call has been authenticated, your device first checks whether a host route is entered in the routing table for this caller. If not, your device can allocate an IP address from an address pool (if available). If address pools have more than one IP address, you cannot specify which connection partner receives which address. The addresses are initially assigned in order. If a new dial-in takes place within an interval of one hour, an attempt is made to allocate the same IP address assigned to this partner the last time.

Choose the**Add** button to set up new IP pools.

16.3.3.1 Edit or New

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

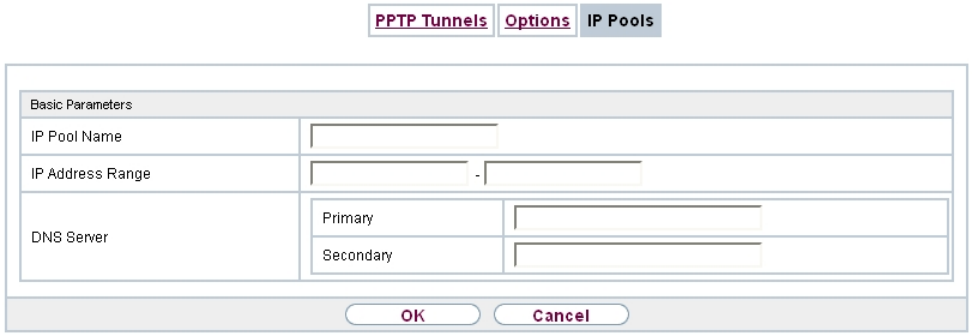


Fig. 133: **VPN->PPTP->IP Pools->New**

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	**Primary**: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. **Secondary**: Optionally, enter the IP address of an alternative DNS server.

16.4 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.

16.4.1 GRE Tunnels

A list of all configured GRE tunnels is displayed in the **VPN**->**GRE**->**GRE Tunnels** menu.

16.4.1.1 New

Choose the **New** button to set up new GRE tunnels.

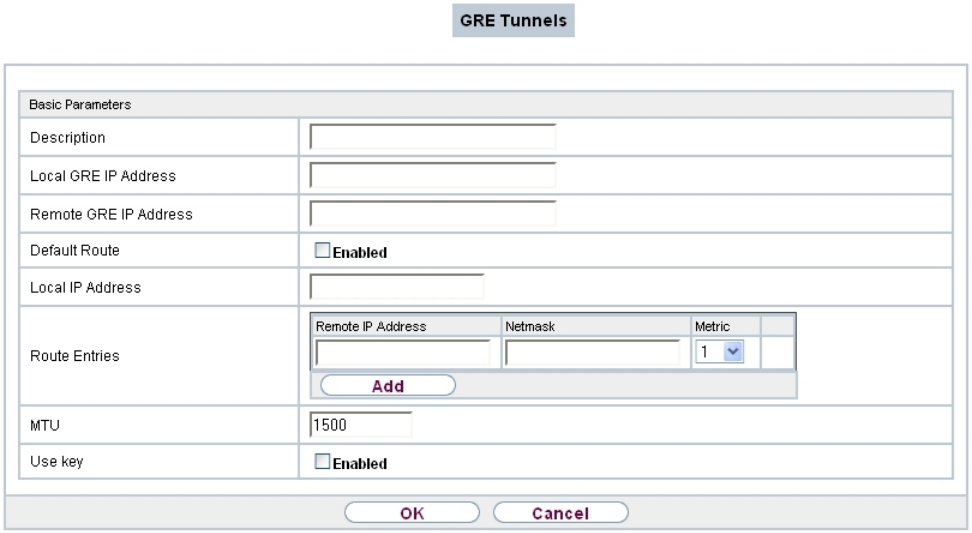


Fig. 134: **VPN**->**GRE**->**GRE Tunnels**->**New**

The **VPN**->**GRE**->**GRE Tunnels**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for the GRE tunnel.
Local GRE IP Address	Enter the source IP address of the GRE packets to the GRE partner. If no IP address is given (this corresponds to IP address 0.0.0.0), the source IP address of the GRE packets is selected automatically from one of the addresses of the interface via which the GRE partner is reached.
Remote GRE IP Address	Enter the target IP address of the GRE packets to the GRE partner.

Field	Description
Default Route	If you enable the **Default Route**, all data is automatically routed to one connection. The function is disabled by default.
Local IP Address	Here, enter the (LAN-side) IP address that is to be used as your device's source address for your own packets through the GRE tunnel.
Route Entries	Define other routing entries for this connection partner. Add new entries with **Add**. • *Remote IP Address*: IP address of the destination host or network. • *Netmask*: Netmask for **Remote IP Address** If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (range of values *0*... *15*). The default value is *1*.
MTU	Enter the maximum packet size (Maximum Transfer Unit, MTU) in bytes that is allowed for the GRE connection between the partners. Possible values are *1* to *8192*. The default value is *1500*.
Use key	Enable the key input for the GRE connection, which makes it possible to distinguish between several parallel GRE connections between two GRE partners (see RFC 1701). The identification is enabled with *Enabled* The function is disabled by default.
Key Value	Only if **Use key** is enabled. Enter the GRE connection key. Possible values are *0* to *2147483647*. The default value is *0*.

Chapter 17 Firewall

The Stateful Inspection Firewall (SIF) provided for bintec elmeg gateways is a powerful security feature.

The SIF with dynamic packet filtering has a decisive advantage over static packet filtering: The decision whether or not to send a packet cannot be made solely on the basis of source and destination addresses or ports but also using dynamic packet filtering based on the state of the connection to a partner.

This means packets that belong to an already active connection can also be forwarded. The SIF also accepts packets that belong to an "affiliated connection". The negotiation of an FTP connection takes place over port 21, for example, but the actual data exchange can take place over a completely different port.

SIF and other security features

The Stateful Inspection Firewall fits into the existing security architecture of bintec elmeg. The configuration work for the SIF is comparatively straightforward with systems like Network Address Translation (NAT) and IP Access Lists (IPAL).

As SIF, NAT and IPAL are active in the system simultaneously, attention must be given to possible interaction: If any packet is rejected by one of the security instances, this is done immediately. This is irrelevant whether another instance would accept it or not. Your need for security features should therefore be accurately analysed.

The essential difference between SIF and NAT/IPAL is that the rules for the SIF are generally applied globally, i.e. not restricted to one interface.

In principle, the same filter criteria are applied to the data traffic as those used in NAT and IPAL:

- Source and destination address of the packet (with an associated netmask)
- Service (preconfigured, e.g. Echo, FTP, HTTP)
- Protocol
- Port number(s)

To illustrate the differences in packet filtering, a list of the individual security instances and their method of operation is given below.

NAT

One of the basic functions of NAT is the translation of the local IP addresses of your LAN into the global IP addresses you are assigned by your ISP and vice versa. All connections initiated externally are first blocked, i.e. every packet your device cannot assign to an existing connection is rejected. This means that a connection can only be set up from inside to outside. Without explicit permission, NAT rejects every access from the WAN to the LAN.

IP Access Lists

Here, packets are allowed or rejected exclusively on the basis of the criteria listed above, i.e. the state of the connection is not considered (except for **Services** = *TCP*).

SIF

The SIF sorts out all packets that are not explicitly or implicitly allowed. The result can be a "deny", in which case no error message is sent to the sender of the rejected packet, or a "reject", where the sender is informed of the packet rejection.

The incoming packets are processed as follows:

- The SIF first checks if an incoming packet can be assigned to an existing connection. If so, it is forwarded. If the packet cannot be assigned to an existing connection, a check is made to see if a suitable connection is expected (e.g. as affiliated connection of an existing connection). If so, the packet is also accepted.
- If the packet cannot be assigned to any existing or expected connection, the SIF filter rules are applied: If a deny rule matches the packet, the packet is discarded without sending an error message to the sender of the packet; if a reject rule matches, the packet is discarded and an ICMP Host Unreachable message sent to the sender of the packet. The packet is only forwarded if an accept rule matches.
- All packets without matching rules are rejected without sending an error message to the sender when all the existing rules have been checked (=default behaviour).

17.1 Policies

17.1.1 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.

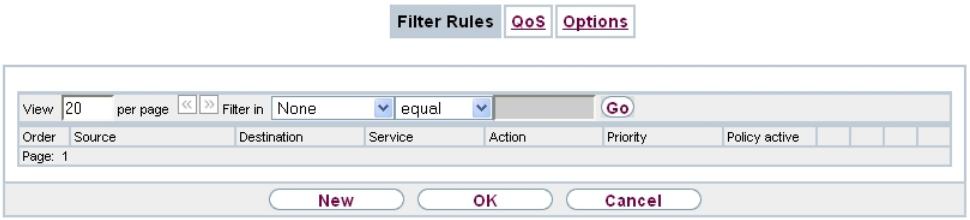


Fig. 135: **Firewall**->**Policies**->**Filter Rules**

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.

17.1.1.1 New

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

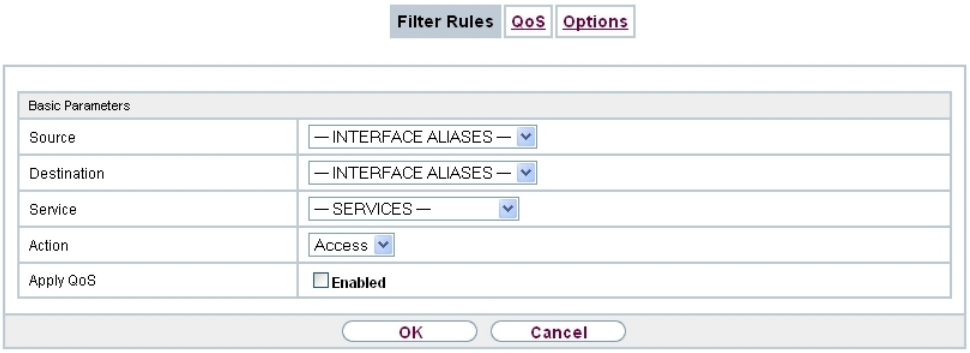


Fig. 136: **Firewall**->**Policies**->**Filter Rules**->**New**

The menu **Firewall**->**Policies**->**Filter Rules**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Source	Select one of the preconfigured aliases for the source of the packet. In the list, all WAN/LAN interfaces, interface groups (see **Firewall**->**Interfaces**->**Groups**), addresses (see **Firewall**->**Addresses**->**Address List**) and address groups (see **Firewall**->**Addresses**->**Groups**) are available. The value *Any* means that neither the source interface nor the source address is checked.
Destination	Select one of the preconfigured aliases for the destination of the packet. In the list, all WAN/LAN interfaces, interface groups (see **Firewall**->**Interfaces**->**Groups**), addresses (see **Firewall**->**Addresses**->**Address List**) and address groups (see **Firewall**->**Addresses**->**Groups**). The value *Any* means that neither the destination interface nor the destination address is checked.
Service	Select one of the preconfigured services to which the packet to be filtered must be assigned. The extensive range of services configured ex works includes the following: • *ftp* • *telnet* • *smtp* • *dns* • *http* • *nntp* • *Internet* • *Netmeeting* Additional services are created in **Firewall**->**Services**->**Service List**. In addition, the service groups configured in **Firewall**->**Services**->**Groups** can be selected.

Field	Description
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. 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 **Action** = *Access* and **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*

17.1.2 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.

17.1.2.1 New

Choose the **New** button to set up new QoS rules.

Fig. 137: **Firewall**->**Policies**->**QoS**->**New**

The **Firewall**->**Policies**->**QoS**->**New** menu consists of the following fields:

Fields in the Configure 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 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.

Field	Description
Filter Rules	This field contains a list of all configured firewall policies for which QoS was activated (**Apply QoS** = *Enabled* under **Firewall**->**Policies**->**Filter Rules**->**New**). 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.

17.1.3 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.

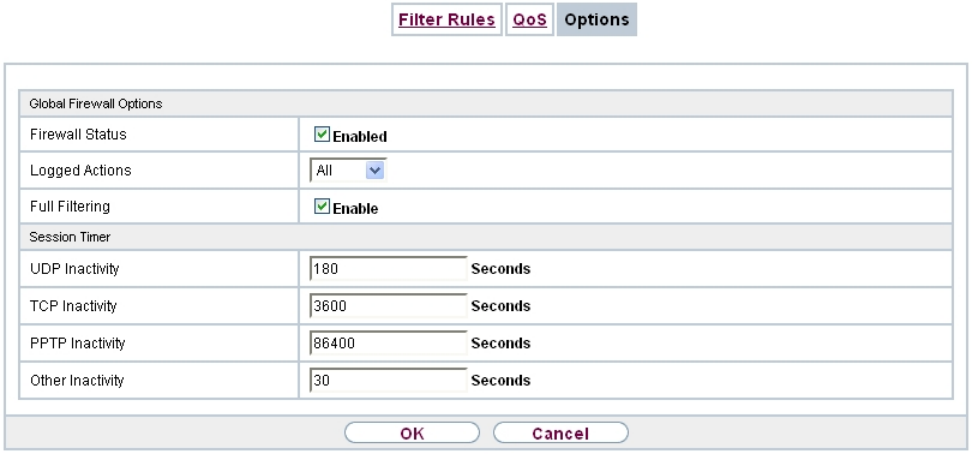


Fig. 138: **Firewall**->**Policies**->**Options**

The menu **Firewall**->**Policies**->**Options** consists of the following fields:

Fields in the Global 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.
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 define whether packets are only to be filtered if they are sent to an interface other than the interface that created the connection. With *Enable*, all the packets are filtered (default value).

Fields in the Session Timer menu.

Field	Description
UDP Inactivity	Enter the inactivity time after which a UDP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *180*.
TCP Inactivity	Enter the inactivity time after which a TCP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *3600*.
PPTP Inactivity	Enter the inactivity time after which a PPTP session is to be regarded as expired (in seconds).

Field	Description
	Possible values are *30* to *86400*. The default value is *86400*.
Other Inactivity	Enter the inactivity time after which a session of another type is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *30*.

17.2 Interfaces

17.2.1 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.

17.2.1.1 New

Choose the **New** button to set up new interface groups.

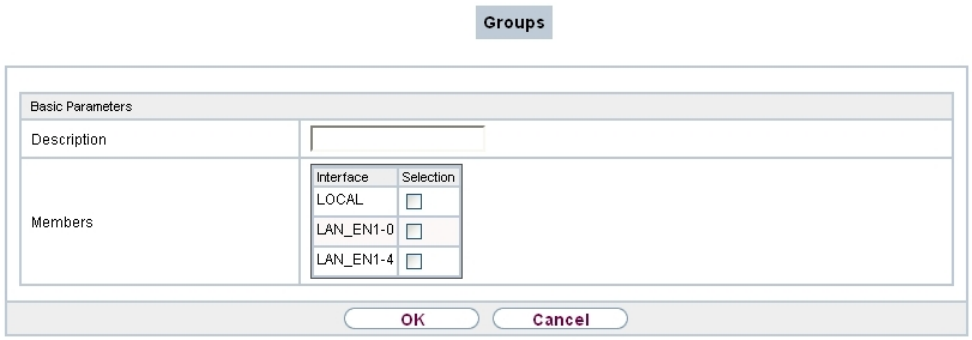


Fig. 139: **Firewall**->**Interfaces**->**Groups**->**New**

The menu **Firewall**->**Interfaces**->**Groups**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the interface group.
Members	Select the members of the group from the available interfaces. To do this, activate the field in the **Selection** column.

17.3 Addresses

17.3.1 Address List

A list of all configured addresses is displayed in the **Firewall**->**Addresses**->**Address List** menu.

17.3.1.1 New

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

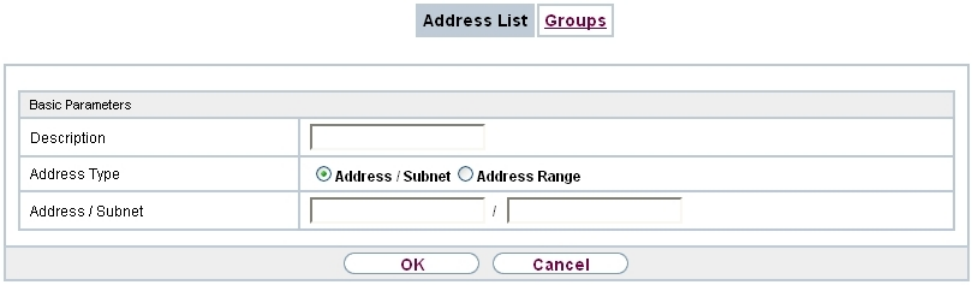


Fig. 140: **Firewall**->**Addresses**->**Address List**->**New**

The menu **Firewall**->**Addresses**->**Address List**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the address.
Address Type	Select the type of address you want to specify. Possible values: • *Address / Subnet* (default value): Enter an IP address with subnet mask.

Field	Description
	• *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.

17.3.2 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.

17.3.2.1 New

Choose the **New** button to set up additional address groups.

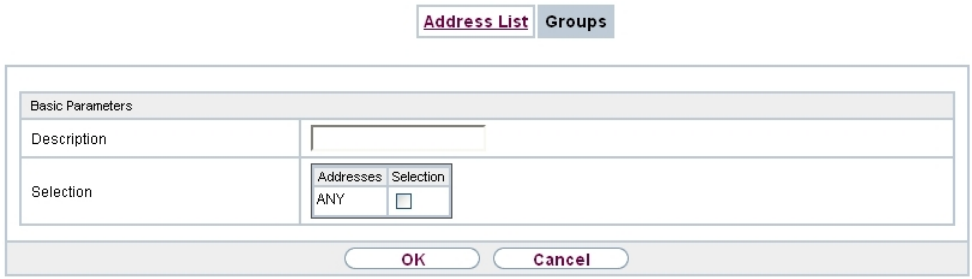


Fig. 141: **Firewall**->**Addresses**->**Groups**->**New**

The menu **Firewall**->**Addresses**->**Groups**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the address group.

Field	Description
Selection	Select the members of the group from the available **Addresses**. To do this, activate the Fields in the **Selection** column.

17.4 Services

17.4.1 Service List

In the **Firewall**->**Services**->**Service List** menu, a list of all available services is displayed.

17.4.1.1 New

Choose the **New** button to set up additional services.

Fig. 142: **Firewall**->**Services**->**Service List**->**New**

The menu **Firewall**->**Services**->**Service List**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter an alias for the service you want to configure.
Protocol	Select the protocol on which the service is to be based. The most important protocols are available for selection.
Destination Port Range	Only for **Protocol** = *TCP*, *UDP/TCP* or *UDP* In the first field, enter the destination port via which the service is to run. If a port number range is specified, in the second field enter the last port of the port range. By default the field does not contain an entry. If a value is displayed, this means that the previously

Field	Description
	specified port number is verified. If a port range is to be checked, enter the upper limit here. Possible values are *1* to *65535*.
Source Port Range	Only for **Protocol** = *TCP*, *UDP/TCP* or *UDP* In the first field, enter the source port to be checked, if applicable. If a port number range is specified, in the second field enter the last port of the port range. By default the field does not contain an entry. If a value is displayed, this means that the previously specified port number is verified. If a port range is to be checked, enter the upper limit here. Possible values are *1* to *65535*.
Type	Only for **Protocol** = *ICMP* The **Type** field shows the class of ICMP messages, the **Code** field specifies the type of message in greater detail. Possible values: • *Any* (default value) • *Echo Reply* • *Destination unreachable* • *Source Quench* • *Redirect* • *Echo* • *Time Exceeded* • *Parameter Problem* • *Timestamp* • *Timestamp Reply* • *Information Request* • *Information Reply* • *Address Mask Request* • *Address Mask Reply*

Field	Description
Code	Selection options for the ICMP codes are only available for **Type** = *Destination unreachable* Possible values: • *Any* (default value) • *Net Unreachable* • *Host Unreachable* • *Protocol Unreachable* • *Port Unreachable* • *Fragmentation Needed* • *Communication with Destination Network is Administratively Prohibited* • *Communication with Destination Host is Administratively Prohibited*

17.4.2 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.

17.4.2.1 New

Choose the **New** button to set up additional service groups.

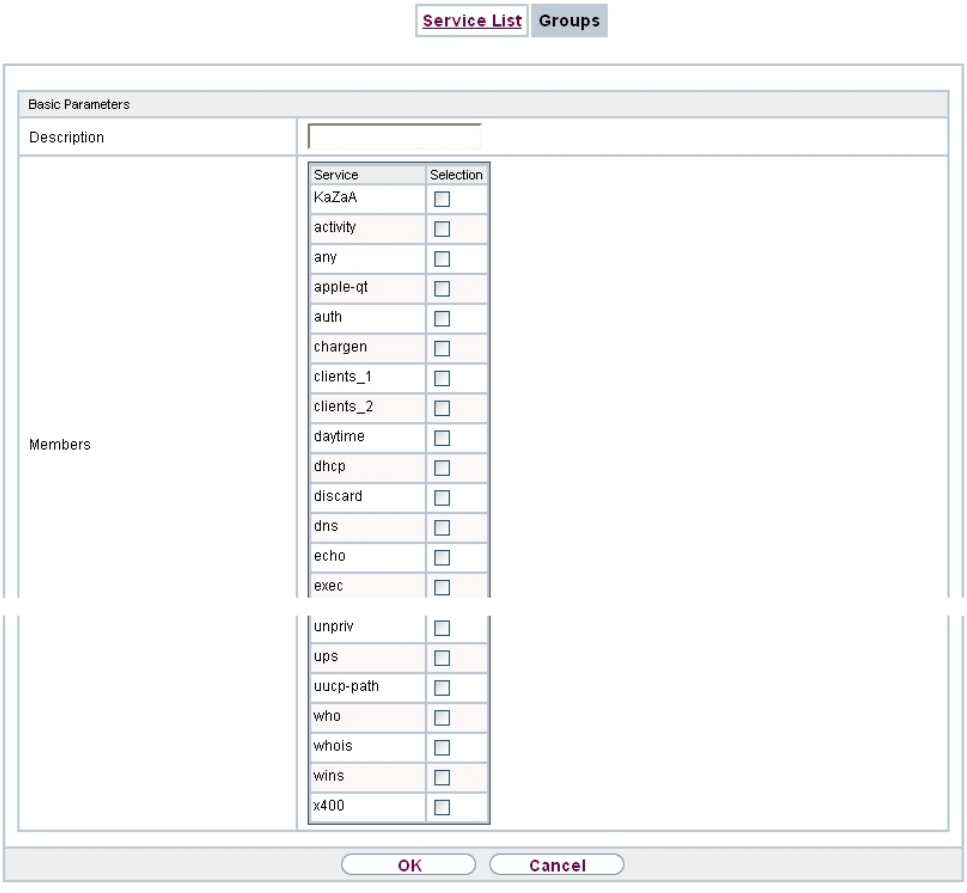


Fig. 143: **Firewall->Services->Groups->New**

The menu **Firewall->Services->Groups->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the service group.
Members	Select the members of the group from the available service aliases. To do this, activate the Fields in the **Selection** column.

Chapter 18 Local Services

This menu offers services for the following application areas:

- Name resolution (DNS)
- Configuration via web browser (HTTPS)
- Locating of dynamic IP addresses using a DynDNS provider
- Configuration of gateway as a DHCP server (assignment of IP addresses)
- Automation of tasks according to schedule (scheduling)
- Alive checks for hosts or interfaces, ping tests
- Automatic detection and configuration of bintec elmeg devices
- Provision of public Internet accesses (hotspot).
- Wake on LAN, um Netzwerkgeräte zu aktivieren, die aktuell ausgeschaltet sind.

18.1 DNS

Each device in a TCP/IP network is usually located by its IP address. Because host names are often used in networks to reach different devices, it is necessary for the associated IP address to be known. This task can be performed by a DNS server, which resolves the host names into IP addresses. Alternatively, name resolution can also take place over the HOSTS file, which is available on all PCs.

Your device offers the following options for name resolution:

- DNS Proxy, for forwarding DNS requests sent to your device to a suitable DNS server. This also includes specific forwarding of defined domains (Forwarded Domains).
- DNS cache, for saving the positive and negative results of DNS requests.
- Static entries (static hosts), to manually define or prevent assignments of IP addresses to names.
- DNS monitoring (statistics), to provide an overview of DNS requests on your device.

Name server

Under **Local Services**->**DNS**->**DNS Servers**->**New** you enter the IP addresses of name servers that are queried if your device cannot answer requests itself or by forwarding entries. Global name servers and name servers that are attached to an interface can both be entered.

Your device can also receive the global name servers dynamically via PPP or DHCP and transfer them dynamically if necessary.

Strategy for name resolution on your device

A DNS request is handled by your device as follows:

(1) If possible, the request is answered directly from the static or dynamic cache with IP address or negative response.

(2) Otherwise, if a suitable forwarding entry exists, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If the DNS server can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(3) Otherwise, if name servers have been entered, taking into account the priority configured and if the relevant interface status is "up", the primary DNS server is queried and then the secondary DNS server. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(4) Otherwise, if a suitable Internet or dialin connection is selected as the standard interface, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(5) Otherwise, if overwriting the addresses of the global name servers is allowed in the **WAN**->**Internet + Dialup** menu (**Interface Mode** = *Dynamic*), a connection is set up – if necessary at extra cost – to the first Internet or dialin connection configured to enable DNS server addresses to be requested from DNS servers (**DNS Negotiation** = *Enabled*), if this has not been already attempted. When the name servers have been negotiated successfully, these name servers are then available for more queries.

(6) Otherwise the initial request is answered with a server error.

If one of the DNS servers answers with `non-existent domain`, the initial request is immediately answered accordingly and a corresponding negative entry is made in the DNS cache of your device.

18.1.1 Global Settings

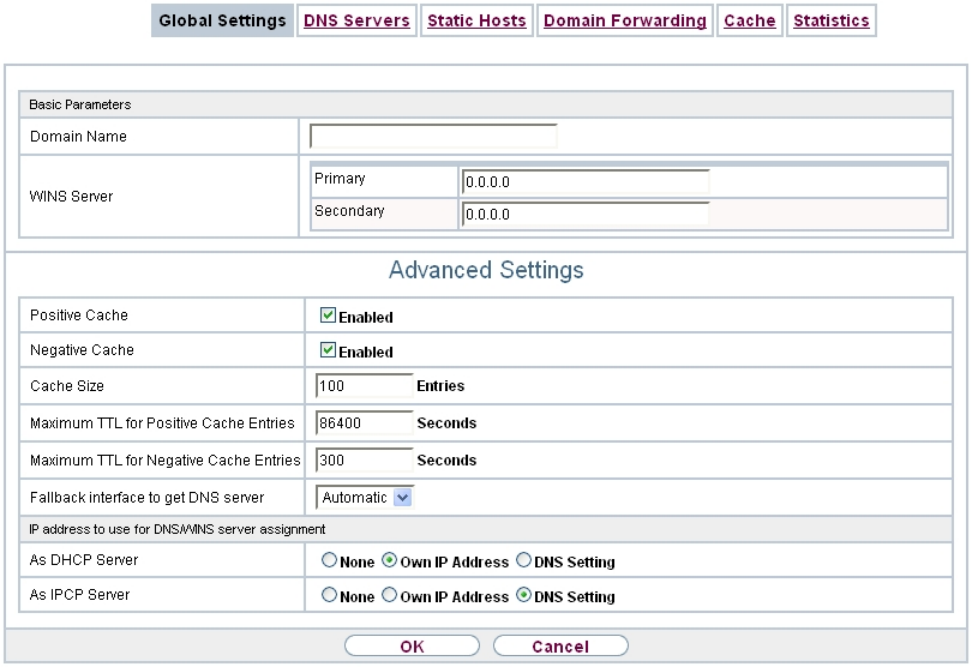


Fig. 144: **Local Services->DNS->Global Settings**

The menu **Local Services->DNS->Global Settings** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Domain Name	Enter the standard domain name of your device.
WINS Server **Primary** **Secondary**	Enter the IP address of the first and, if necessary, alternative global Windows Internet Name Server (=WINS) or NetBIOS Name Server (=NBNS).

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

Fields in the Advanced Settings menu

Field	Description
Positive Cache	Select whether the positive dynamic cache is to be activated,

Field	Description
	i.e. successfully resolved names and IP addresses are to be stored in the cache. The function is activated by selecting *Enabled*. The function is enabled by default.
Negative Cache	Select whether the negative dynamic cache is to be activated, i.e. whether queried names for which a DNS server has sent a negative response are stored as negative entries in the cache. The function is activated by selecting *Enabled*. The function is enabled by default.
Cache Size	Enter the maximum total number of static and dynamic entries. Once this value is reached, the dynamic entry not requested for the longest period of time is deleted when a new entry is added. **Cache Size** is reduced by the user, dynamic entries are deleted if necessary. Statistical entries are not deleted. **Cache Size** cannot be set to lower than the current number of static entries. Possible values: *0*.. *1000*. The default value is *100*.
Maximum TTL for Positive Cache Entries	Enter the value to which the TTL is to be set for a positive dynamic DNS entry in the cache if its TTL is *0* or its TTL exceeds the value for **Maximum TTL for Positive Cache Entries**. The default value is *86400*.
Maximum TTL for Negative Cache Entries	Enter the value set to which the TTL is to be set in the case of a negative dynamic entry in the cache. The default value is *86400*.
Fallback interface to get DNS server	Select the interface to which a connection is set up for name server negotiation if other name resolution attempts were not successful. The default value is *Automatic*, i.e. a one-time connection is set up to the first suitable connection partner configured in the system.

Fields in the IP address to use for DNS/WINS server assignment menu

Field	Description
As DHCP Server	Select which name server addresses are sent to the DHCP client if your device is used as DHCP server. Possible values: • *None*: No name server address is sent. • *Own IP Address* (default value): The address of your device is transferred as the name server address. • *DNS Setting*: The addresses of the global name servers entered on your device are sent.
As IPCP Server	Select which name server addresses are to be transmitted by your device in the event of dynamic server name negotiation if your device is used as the IPCP server for PPP connections. Possible values: • *None*: No name server address is sent. • *Own IP Address*: The address of your device is transferred as the name server address. • *DNS Setting* (default value): The addresses of the global name servers entered on your device are sent.

18.1.2 DNS Servers

A list of all configured DNS servers is displayed in the **Local Services**->**DNS**->**DNS Servers** menu.

18.1.2.1 Edit or New

Choose the icon to edit existing entries. Select the **New** button to set up additional DNS servers.

Here you can configure both global DNS servers and DNS servers that are to be assigned to a particular interface.

Configuring a DNS server for a particular interface can be useful, for example, if accounts with different providers have been set up via different interfaces and load balancing is being used.

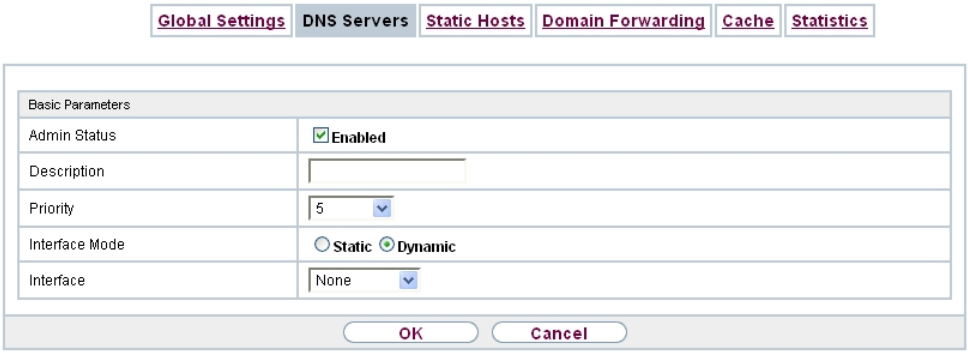


Fig. 145: **Local Services->DNS->DNS Servers->New**

The **Local Services->DNS->DNS Servers->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Admin Status	Select whether the DNS server should be enabled. The function is activated by selecting *Enabled*. The function is enabled by default.
Description	Enter a description for DNS server.
Priority	Assign a priority to the DNS server. You can assign more than one pair of DNS servers (**Primary DNS Server** and **Secondary DNS Server**) to an interface (i. e. for example, to an Ethernet port or a PPPoE WAN partner). The pair with the highest priority is used if the interface is "up". Possible values from *0* (highest priority) to *9* (lowest priority). The default value is *5*.
Interface Mode	Select whether the IP addresses of name servers for resolving the names of Internet addresses are to be obtained automatically or whether up to two fixed DNS server addresses are to be entered, depending on the priority. Possible values: • *Static*

Field	Description
	• *Dynamic* (default value)
Interface	Select the interface to which the DNS server pair is to be assigned. For **Interface Mode** = *Dynamic* A global DNS server is created with the setting *None*. For **Interface Mode** = *Static* A DNS server is configured for all interfaces with the *Any* setting.
Primary DNS Server	Only if **Interface Mode** = *Static* Enter the IP address of the first name server for Internet address name resolution.
Secondary DNS Server	Only if **Interface Mode** = *Static* Optionally, enter the IP address of an alternative name server.

18.1.3 Static Hosts

A list of all configured static hosts is displayed in the **Local Services**->**DNS**->**Static Hosts** menu.

18.1.3.1 New

Choose the **New** button to set up new static hosts.

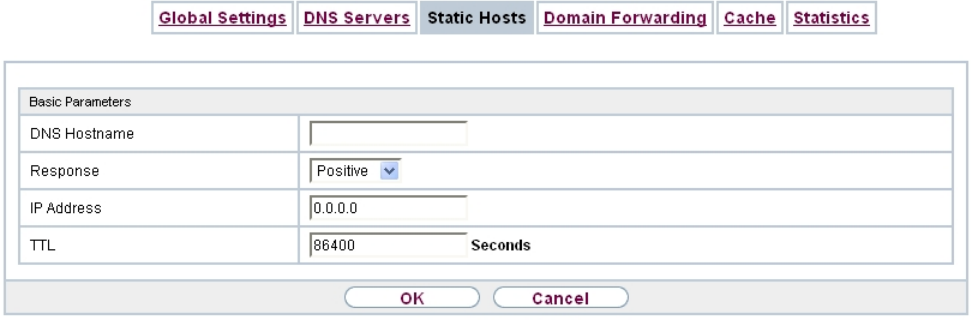


Fig. 146: **Local Services**->**DNS**->**Static Hosts**->**New**

The menu **Local Services**->**DNS**->**Static Hosts**->**New** consists of the following fields:

Fields in the Basic 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. *.bintec-elmeg.com. 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).

18.1.4 Domain Forwarding

In the **Local Services**->**DNS**->**Domain Forwarding** menu, a list of all configured forwardings for defined domains is displayed.

18.1.4.1 New

Choose the **New** button to set up additional forwardings.

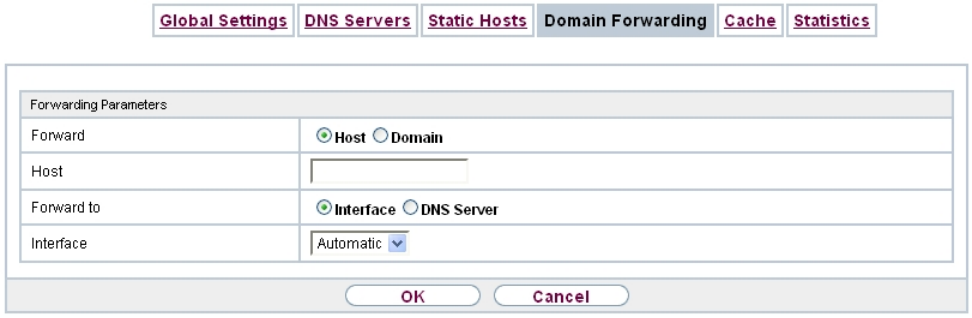


Fig. 147: **Local Services->DNS->Domain Forwarding->New**

The menu **Local Services->DNS->Domain Forwarding->New** consists of the following fields:

Fields in the Forwarding Parameters menu.

Field	Description
Forward	Select whether requests for a host or domain are to be forwarded. Possible values: • *Host* (default value) • *Domain*
Host	Only for **Forward** = *Host* Enter the name of the host for which requests are to be forwarded. If you enter a name without a ".", the entry is supplemented with the name supplied by the value specified in **Local Services->DNS->Global Settings** for **Domain Name** as soon as you confirm with **OK**.
Domain	Only for **Forward** = *Domain* Enter the name of the domain for which requests are to be forwarded.

Field	Description
	The entry can start with the wildcard "*", e.g. "*.bintec-elmeg.com". If you enter a name without a leading wildcard "*" a leading wildcard "*" is supplemented as soon as you confirm with **OK**.
Forward to	Select if matching DNS requests are to be forwarded to the DNS server of an **Interface** or to a manually specified **DNS Server**. Possible values: • *Interface* (default value): Requests are forwarded to the DNS server assigned to either an automatically selected or to a user-selected interface. • *DNS Server*: Requests are forwarded to the specified **DNS Server**.
Interface	Only for **Forward to** = *Interface* Select the interface that has the DNS server assinged which is to receive the DNS requests.
DNS Server	Only for **Forward to** = *DNS Server* Enter the IP address of the primary and secondary DNS server.

18.1.5 Cache

In the **Local Services**->**DNS**->**Cache** menu, a list of all available cache entries is displayed.

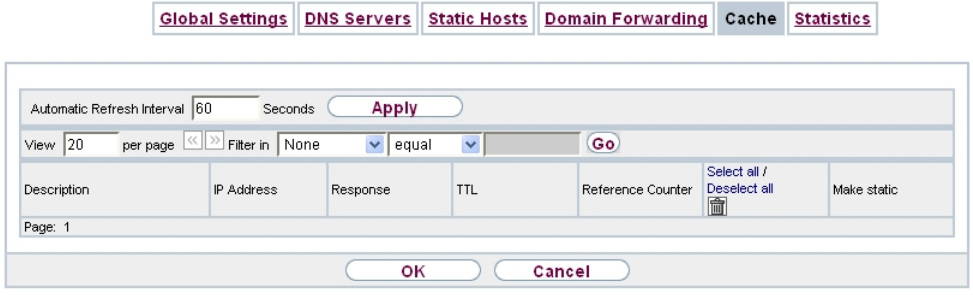


Fig. 148: **Local Services**->**DNS**->**Cache**

You can select individual entries using the checkbox in the corresponding line, or select them all using the **Select all** button.

A dynamic entry can be converted to a static entry by marking the entry and confirming with **Make static**. This corresponding entry disappears from the list and is displayed in the list in the **Static Hosts** menu. The TTL is transferred.

18.1.6 Statistics

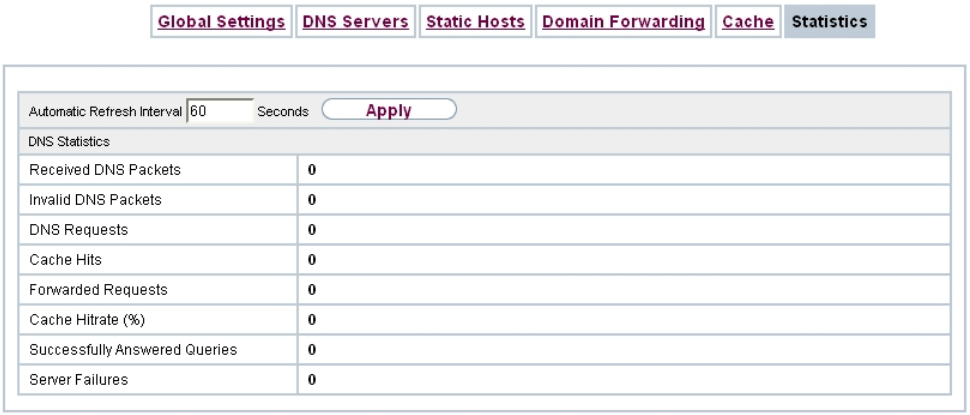


Fig. 149: **Local Services->DNS->Statistics**

In the **Local Services->DNS->Statistics** menu, the following statistical values are displayed:

Fields in the DNS Statistics menu.

Field	Description
Received DNS Packets	Shows the number of received DNS packets addressed direct to your device, including the response packets for forwarded requests.
Invalid DNS Packets	Shows the number of invalid DNS packets received and addressed direct to your device.
DNS Requests	Shows the number of valid DNS requests received and addressed direct to your device.
Cache Hits	Shows the number of requests that were answered with static or dynamic entries from the cache.
Forwarded Requests	Shows the number of requests forwarded to other name servers.
Cache Hitrate (%)	Indicates the number of **Cache Hits** pro DNS request in per-

Field	Description
	centage.
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).

18.2 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.

18.2.1 HTTPS Server

In the **Local Services**->**HTTPS**->**HTTPS Server** menu, configure the parameters of the backed up configuration connection via HTTPS.

Fig. 150: **Local Services->HTTPS->HTTPS Server**

The **Local Services**->**HTTPS**->**HTTPS Server** menu consists of the following fields:

Fields in the HTTPS Parameters menu.

Field	Description
HTTPS TCP Port	Enter the port via which the HTTPS connection is to be established. Possible values are *0* to *65535*. The default value is *443*.

Field	Description
Local Certificate	Select a certificate that you want to use for the HTTPS connection. Possible values: • *Internal* (default value): Select this option if you want to use the certificate built into the device. • *<Certificate name>*: Under **System Management**->**Certificates**->**Certificate List** select entered certificate.

18.3 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.

18.3.1 DynDNS Update

In the **Local Services**->**DynDNS Client**->**DynDNS Update** menu, a list of all configured DynDNS registrations for updating is displayed

18.3.1.1 New

Choose the **New** button to set up further DynDNS registrations to be updated.

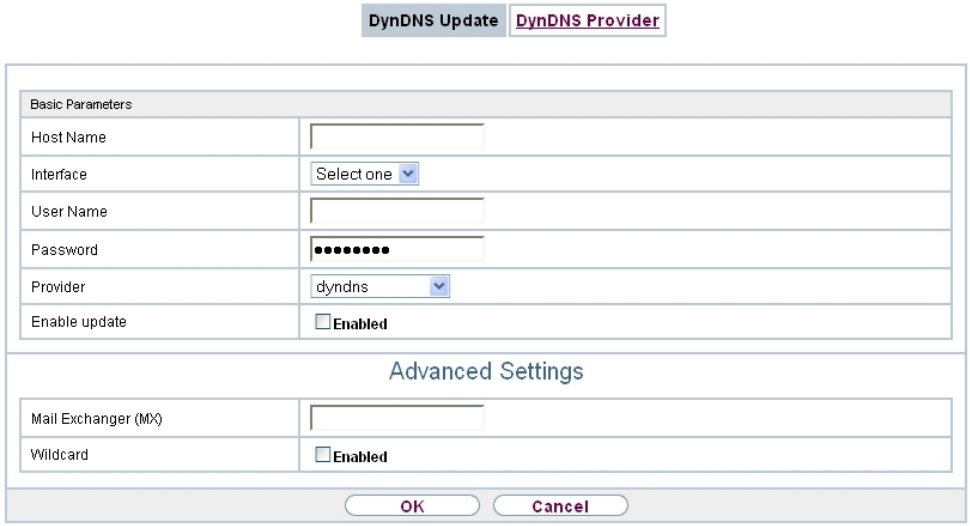


Fig. 151: **Local Services->DynDNS Client->DynDNS Update->New**

The menu **Local Services->DynDNS Client->DynDNS Update->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Host Name	Enter the complete host name as registered with the DynDNS provider.
Interface	Select the WAN interface whose IP address is to be propagated over the DynDNS service (e.g. the interface of the Internet Service Provider).
User Name	Enter the user name as registered with the DynDNS provider.
Password	Enter the password as registered with the DynDNS provider.
Provider	Select the DynDNS provider with which the above data is registered. A choice of DynDNS providers is already available in the uncon-

Field	Description
	figured state and their protocols are supported. Other DynDNS providers can be configured in the **Local Services**->**DynDNS Client**->**DynDNS Provider** menu. The default value is *DynDNS*.
Enable update	Select whether the DynDNS entry configured here is to be activated. The function is activated by selecting *Enabled*. The function is disabled by default.

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

Fields in the Advanced Settings menu.

Field	Description
Mail Exchanger (MX)	Enter the full host name of a mail server to which e-mails are to be forwarded if the host currently configured is not to receive mail. Ask your provider about this forwarding service and make sure e-mails can be received from the host entered as MX.
Wildcard	Select whether forwarding of all subdomains of the **Host Name** is to be enabled for the current IP address of the **Interface** (advanced name resolution). The function is activated by selecting *Enabled*. The function is disabled by default.

18.3.2 DynDNS Provider

A list of all configured DynDNS providers is displayed in the **Local Services**->**DynDNS Client**->**DynDNS Provider** menu.

18.3.2.1 New

Choose the **New** button to set up new DynDNS providers.

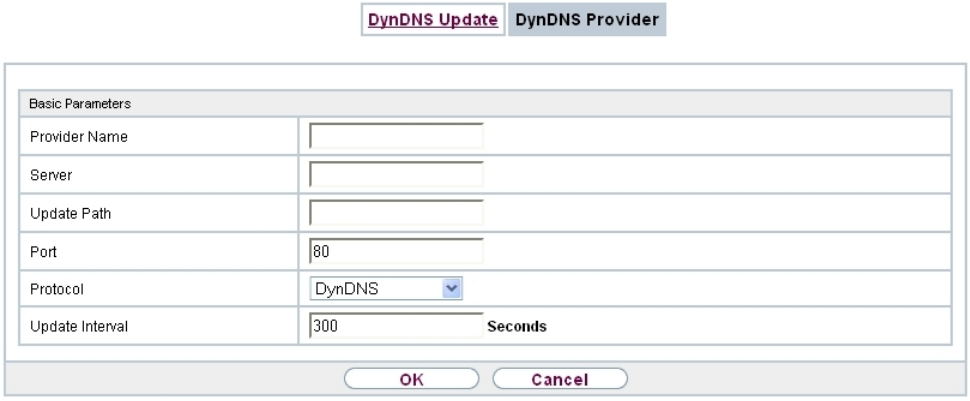


Fig. 152: **Local Services->DynDNS Client->DynDNS Provider->New**

The menu **Local Services->DynDNS Client->DynDNS Provider->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Provider Name	Enter a name for this entry.
Server	Enter the host name or IP address of the server on which the provider's DynDNS service runs.
Update Path	Enter the path on the provider's server that contains the script for managing the IP address of your device. Ask your provider for the path to be used.
Port	Enter the port at which your device is to reach your provider's server. Ask your provider for the relevant port. The default value is *80*.
Protocol	Select one of the protocols implemented. Possible values: • *DynDNS* (default value) • *Static DynDNS* • *ODS*

Field	Description
	• *HN* • *DYNS* • *GnuDIP-HTML* • *GnuDIP-TCP* • *Custom DynDNS* • *DnsExit*
Update Interval	Enter the minimum time (in seconds) that your device must wait before it is allowed to propagate its current IP address to the DynDNS provider again. The default value is *300* seconds.

18.4 DHCP Server

You can configure your device as a DHCP (Dynamic Host Configuration Protocol) server.

Your device and each PC in your LAN requires its own IP address. One option for allocating IP addresses in your LAN is the Dynamic Host Configuration Protocol (DHCP). If you configure your device as a DHCP server, the device automatically assigns IP addresses to requesting PCs in the LAN from a predefined IP address pool.

If a client requires an IP address for the first time, it sends a DHCP request (with its MAC address) to the available DHCP server as a network broadcast.* The client then receives its IP address from bintec elmeg (as part of a brief exchange).

You therefore do not need to allocate fixed IP addresses to PCs, which reduces the amount of configuration work in your network. To do this, you set up a pool of IP addresses, from which your device assigns IP addresses to hosts in the LAN for a defined period of time. A DHCP server also transfers the addresses of the domain name server entered statically or by PPP negotiation (DNS), NetBIOS name server (WINS) and default gateway.

18.4.1 IP Pool Configuration

The **Local Services**->**DHCP Server**->**IP Pool Configuration** menu displays a list of all the configured IP pools. This list is global and also displays pools configured in other menus.

18.4.1.1 Edit or New

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

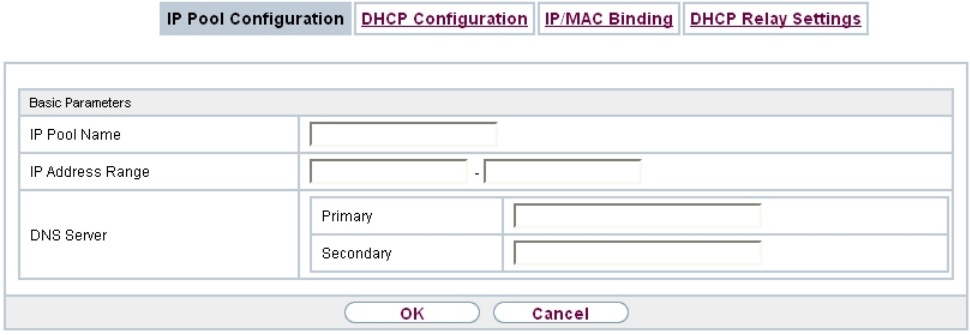


Fig. 153: **Local Services->DHCP Server->IP Pool Configuration->New**

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	**Primary**: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. **Secondary**: Optionally, enter the IP address of an alternative DNS server.

18.4.2 DHCP Configuration

To activate your device as a DHCP server, you must first define IP address pools from which the IP addresses are distributed to the requesting clients.

A list of all configured IP address pools is displayed in the **Local Services->DHCP Server->DHCP Configuration** menu.

In the list, for each entry, you have the possibility under **Status** of enabling or disabling the configured DHCP pools.

Note

In the ex works state the DHCP pool is preconfigured with the IP addresses 192.168.0.10 to 192.168.0.49 and is used if there is no other DHCP server available in the network.

18.4.2.1 Edit or New

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

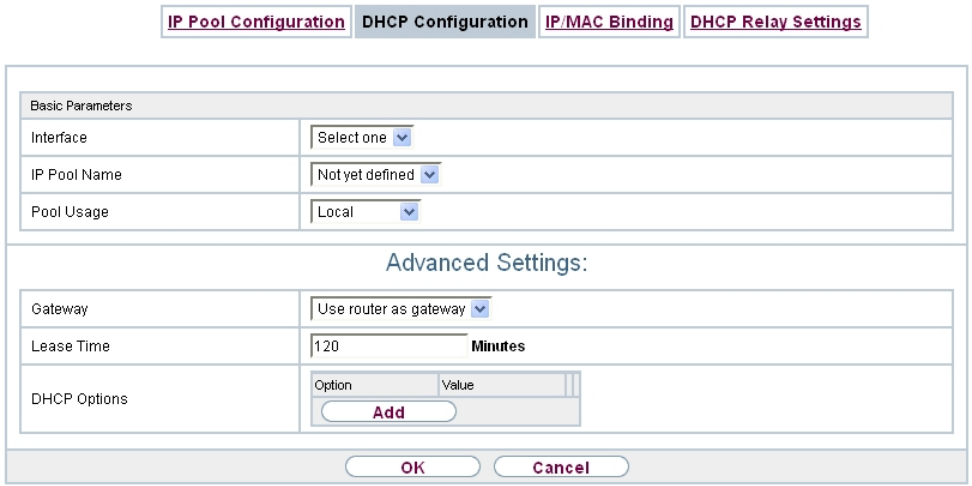


Fig. 154: **Local Services->DHCP Server->DHCP Configuration->New**

The **Local Services->DHCP Server->DHCP Configuration->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Select the interface over which the addresses defined in **IP Address Range** are to be assigned to DHCP clients. When a DHCP request is received over this **Interface**, one of the addresses from the address pool is assigned.
IP Pool Name	Select an IP pool name configured in the **Local Services->DHCP Server->IP Pool Configuration** menu.

Field	Description
Pool Usage	Specify whether the IP pool is used for DHCP requests in the same subnet or for DHCP requests that have been forwarded to your device from another subnet. In this case it is possible to define IP addresses from another network. Possible values: • *Local* (default value): The DHCP pool is only used for DHCP requests in the same subnet. • *Relay*: The DHCP pool is only used for DHCP requests forwarded from other subnets. • *Local/Relay*: The DHCP pool is used for DHCP requests in the same subnet and from other subnets.

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

Fields in the menu Advanced Settings

Field	Description
Gateway	Select which IP address is to be transferred to the DHCP client as gateway. Possible values: • *Use router as gateway* (default value): Here, the IP address defined for the **Interface** is transferred. • *No gateway*: No IP address is sent. • *Specify*: Enter the corresponding IP address.
Lease Time	Enter the length of time (in minutes) for which an address from the pool is to be assigned to a host. After the **Lease Time** expires, the address can be reassigned by the server. The default value is *120*.
DHCP Options	Specify which additional data is forwarded to the DHCP client. Possible values for **Option**: • *Time Server* (default value): Enter the IP address of the time server to be sent to the client.

Field	Description
	• *DNS Server*: Enter the IP address of the DNS server to be sent to the client. • *DNS Domain Name*: Enter the DNS domain to be sent to the client. • *WINS/NBNS Server*: Enter the IP address of the WINS/ NBNS server to be sent to the client. • *WINS/NBT Node Type*: Select the type of the WINS/NBT node to be sent to the client. • *TFTP Server*: Enter the IP address of the TFTP server to be sent to the client. • *CAPWAP Controller*: Enter the IP address of the CAPWAP controller to be sent to the client. • *URL (provisioning server)*: This option enables you to send a client any URL. Use this option to send querying **IP1x0** telephones the URL of the provisioning server if the telephones are to be provisioned automatically. The URL then needs to take the form *http://<IP address of the provisioning server>/eg_prov*. • *Vendor Group* (Vendor Specific Information): This enables you to send the client any manufacturer-specific information in any text string. Several entries are possible. Add additional entries with the **Add** button.

Edit

In the **Local Services**->**DHCP Server** ->**DHCP Configuration**->**Advanced Settings** menu you can edit an entry in the **DHCP Options** field, if **Option** = *Vendor Group* is selected.

Choose the  icon to edit an existing entry. In the popup menu, you configure manufacturer-specific settings in the DHCP server for specific telephones, for example.

Fields in the Basic Parameters menu

Field	Description
Select vendor	Here, you can select for which manufacturer specific values shall be transmitted for the DHCP server.

Field	Description
	Possible values: • *Siemens* (default value) • *Other*
Provisioning Server	Only für **Select vendor** = *Siemens* Enter which manufacturer value shall be transmitted. For the setting **Select vendor** = *Siemens*, the default value *sdlp* is displayed. You can complete the IP address of the desired server.
Vendor Description	Only für **Select vendor** = *Other* Type in the name of the manufacturer for which you want to transfer specific DHCP server settings.
Custom DHCP Options	Only für **Select vendor** = *Other* Use **Add** to add more entries. You can add custom DHCP options.

18.4.3 IP/MAC Binding

The **Local Services**->**DHCP Server**->**IP/MAC Binding** menu displays a list of all clients that received an IP address from your device via DHCP.

You can allocate an IP address from a defined IP address pool to specific MAC addresses. You can do this by selecting the **Static Binding** option in the list to convert a list entry as a fixed binding, or you manually create a fixed IP/MAC binding by configuring this in the **New** sub-menu.

Note

You can only create new static IP/MAC bindings if IP address ranges were configured in **Local Services**->**DHCP Server**->**DHCP Pool**, and in the **Local Services**->**DHCP Server**->**IP Pool Configuration** menu is assigned a valid IP Pool.

18.4.3.1 New

Choose the **New** button to set up new IP/MAC bindings.

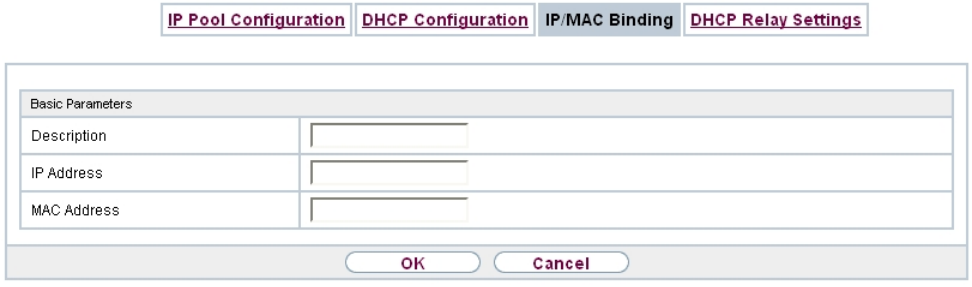


Fig. 155: **Local Services->DHCP Server->IP/MAC Binding->New**

The menu **Local Services->DHCP Server->IP/MAC Binding->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the host to which the **MAC Address** the **IP Address** is to be bound. A character string of up to 256 characters is possible.
IP Address	Enter the IP address to be assigned to the MAC address specified in **MAC Address** is to be assigned.
MAC Address	Enter the MAC address to which the IP address specified in **IP Address** is to be assigned.

18.4.4 DHCP Relay Settings

If your device for the local network does not distribute any IP addresses to the clients by DHCP, it can still forward the DHCP requests on behalf of the local network to a remote DHCP server. The DHCP server then assigns the your device an IP address from its pool, which in turn sends this to the client in the local network.

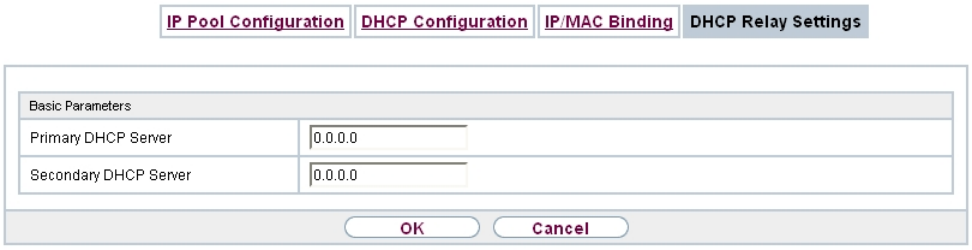


Fig. 156: **Local Services->DHCP Server->DHCP Relay Settings**

The menu **Local Services->DHCP Server->DHCP Relay Settings** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Primary DHCP Server	Enter the IP address of a server to which BootP or DHCP requests are to be forwarded. The default value is `0.0.0.0`.
Secondary DHCP Server	Enter the IP address of an alternative BootP or DHCP server. The default value is `0.0.0.0`.

18.5 Scheduling

Your device has a event scheduler, which enables certain standard actions (for example, activating and deactivating interfaces) to be carried out. Moreover, every existing MIB variable can be configured with any value.

You specify the **Actions** you want and define the **Trigger** that control when and under which conditions the **Actions** are to be carried out. A **Trigger** may be a single event or a sequence of events which are combined into an **Event List**. You also create an event list for a single event, but it only contains one event.

Actions can be initiated on a time-controlled basis. Moreover, the status or accessibility of interfaces or their data traffic may lead to execution of the configured actions, or also the validity of licences. Here also, it is possible to set up every MIB variable as initiator with any value.

To take the event scheduler live, enable the **Schedule Interval** under **Options**. This interval species the time gap in which the system checks whether at least one event has occurred. This event is used as the initiator for a configured action.

Caution

The configuration of actions that are not available as defaults requires extensive knowledge of the method of operation of bintec elmeg gateways. An incorrect configuration can cause considerable disruption during operation. If applicable, save the original configuration on your PC.

Note

To run the event scheduler, the date configured on your device must be 1.1.2000 or later.

18.5.1 Trigger

The **Local Services**->**Scheduling**->**Trigger** menu displays all the event lists that have been configured. Every event list contains at least one event which is intended to be the initiator for an action.

18.5.1.1 New

Choose the **New** button to create more event lists.

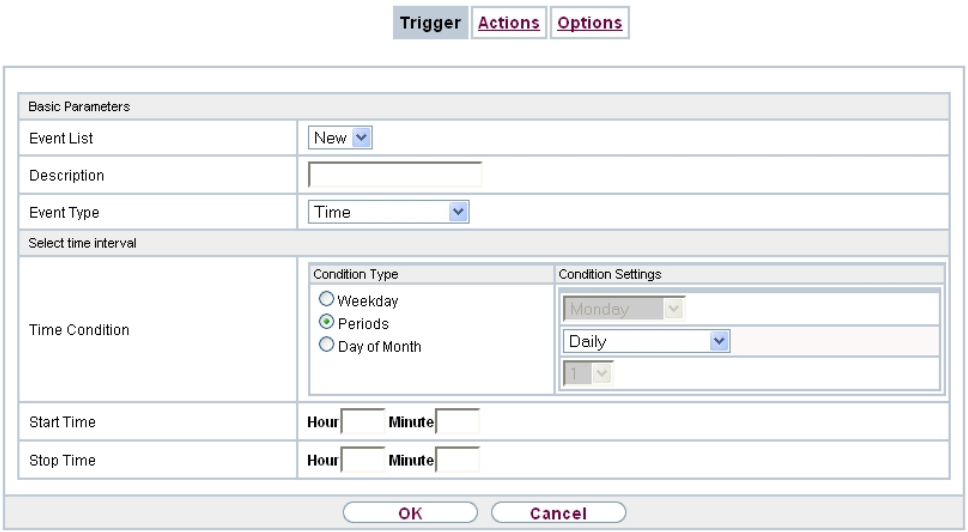


Fig. 157: **Local Services->Scheduling->Trigger->New**

The menu **Local Services**->**Scheduling**->**Trigger**->**New** consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Event List	You can create a new event list with *New* (default value). You give this list a name with **Description**. You use the remaining parameters to create the first event in the list. If you want to add to an existing event list, select the event list you want and add at least one more event to it. You can use event lists to create complex conditions for initiating an action. The events are processed in the same order in which they are created in the list.
Description	Only for **Event List** = *New* Enter your chosen designation for the event list.
Event Type	Select the type of event. Possible values: • *Time* (default value): The operations configured and assigned in **Actions** are initiated at specific points in time. • *MIB/SNMP*: The actions configured and assigned in **Actions** are initiated when the defined MIB variables assumes the assigned values. • *Interface Status*: Operations configured and assigned in **Actions** are initiated, when the defined interfaces take on a specified status. • *Interface Traffic*: The operations configured and assigned in **Actions** are triggered if the data traffic on the specified interfaces falls below or exceed the defined value. • *Ping Test*: the operations configured and assigned in **Actions** are triggered if the defined IP address is accessible or not accessible. • *Certificate Lifetime*: Operations configured and assigned in **Actions** are initiated when the defined period of validity is reached. • *GEO Zone Status* : Operations configured and assigned in **Actions** are initiated, when the defined **GEO Zones** take on a

Field	Description
	specified status.
Monitored GEO Zone	Only for **Event Type** *GEO Zone Status* Select a GEO zone configured in the **Physical Interfaces** menu.
GEO Zone Status	Only for **Event Type** *GEO Zone Status* Select the **GEO Zone Status**. Possible values: • *True*: The current position lies within the defined zone. • *False*: The current position lies outside the defined zone.
Monitored Variable	Only for **Event Type** *MIB/SNMP* Select the MIB variable whose defined value is to be configured as initiator. First, select the **System** in which the MIB variable is saved, then the **MIB Table** and finally the **MIB Variable** itself. Only the MIB tables and MIB variables present in the respective area are displayed.
Compare Condition	Only for **Event Type** *MIB/SNMP* Select whether the MIB variable *Greater* (default value), *Equal*, *Less*, *Not Equal*, must have the value given in *Compare Value* or must lie within *Range* to initiate the operation.
Compare Value	Only for **Event Type** *MIB/SNMP* Enter the value of the MIB variable.
Index Variables	Only for **Event Type** *MIB/SNMP* Where required, select MIB variables to uniquely identify a specific data set in the **MIB Table**, e.g. *ConnIfIndex*. The unique identification of a particular table entry is derived from the combination of **Index Variable** (usually an index variable which is flagged with *) and **Index Value**. Use **Index Variables** to create more entries with **Add**.
Monitored Interface	Only for **Event Type** *Interface Status* and *Interface*

Field	Description
	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 have in order to initiate the intended operation. Possible values: • *Up* (default value): The function is enabled. • *Down*: The interface is disabled.
Traffic Direction	Only for **Event Type** *Interface Traffic* Select the direction of the data traffic whose values should be monitored as initiating an operation. Possible values: • *RX* (default value): Incoming data traffic is monitored. • *TX*: Outgoing data traffic is monitored.
Interface Traffic Condition	Only for **Event Type** *Interface Traffic* Select whether the value for data traffic must be *Greater* (default value) or *Less* the value specified in *Transferred Traffic* in order to initiate the operation.
Transferred Traffic	Only for **Event Type** *Interface Traffic* Enter the desired value in **kBytes** for the data traffic to serve as comparison. The default value is *0*.
Destination IP Address	Only for **Event Type** *Ping Test* Enter the IP address whose accessibility is to be checked.
Source IP Address	Only for **Event Type** *Ping Test* Enter an IP address to be used as sender address for the ping test.

Field	Description
	Possible values: • *Automatic* (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address. • *Specific*: Enter the desired IP address in the input field.
Status	Only for **Event Type** *Ping Test* Select whether **Destination IP Address** *Reacheable* must be (default value) or *Unreacheable* in order to initiate the operation.
Interval	Only for **Event Type** *Ping Test* Enter the time in **Seconds** after which a ping must be resent. The default value is *60* seconds.
Trials	Only for **Event Type** *Ping Test* Enter the number of ping tests to be performed until **Destination IP Address** as *Unreacheable* applies. The default value is *3*.
Monitored Certificate	Only for **Event Type** *Certificate Lifetime* Select the certificate whose validity should be checked.
Remaining Validity	Only for **Event Type** *Certificate Lifetime* Enter the desired value for the remaining validity of the certificate in percentage.

Fields in the menu Select time interval

Field	Description
Time Condition	For **Event Type** *Time* only First select the type of time entry in **Condition Type**. Possible values: • *Weekday*: Select a weekday in **Condition Settings**.

Field	Description
	• *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. Deactivation is carried on the next scheduling interval. If you do not enter a **Stop Time** or set a **Stop Time** = **Start Time**, the initiator is activated, and deactivated after 10 seconds.

18.5.2 Actions

In the **Local Services**->**Scheduling**->**Actions** menu is displayed a list of all operations to be initiated by events or event chains configured in **Local Services**->**Scheduling**->**Trigger**.

18.5.2.1 New

Choose the **New** button to configure additional operations.

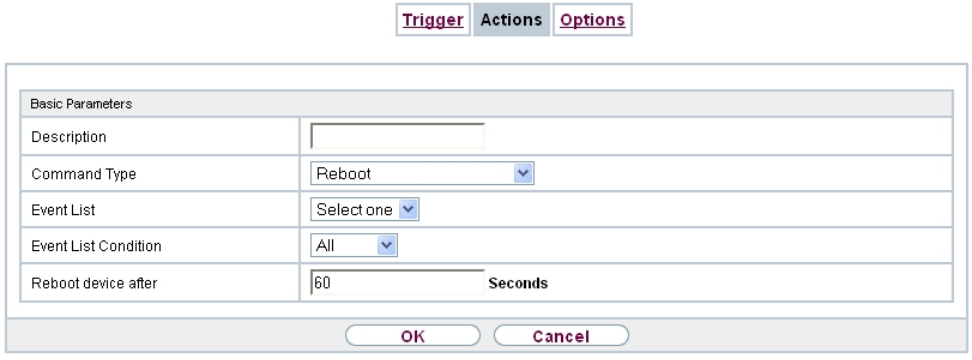


Fig. 158: **Local Services->Scheduling->Actions->New**

The menu **Local Services->Scheduling->Actions->New** consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter your chosen designation for the action.
Command Type	Select the desired action. Possible values: • *Reboot* (default value): Your device is rebooted. • *MIB/SNMP*: The desired value is entered for a MIB variable. • *Interface Status*: The status of an interface is modified. • *Wlan Status*: Only for devices with a wireless LAN. The status of a WLAN-SSID is modified. • *Software Update*: A software update is initiated. • *Configuration Management*: A configuration file is loaded onto your device or backed up by your device. • *Ping Test*: Accessibility of an IP address is checked. • *Certificate Management*: A certificate is to be renewed, deleted or entered. • *5 GHz WLAN Bandscan*: Only for devices with a wireless LAN. A scan of the 5 GHz frequency band is performed.

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

Field	Description
	Possible settings: • *Change existing entry* (default value): An existing entry shall be modified. • *Create new MIB entry*: A new entry shall be created.
Index Variables	Only if **Command Type** = *MIB/SNMP* Where required, select MIB variables to uniquely identify a specific data set in **MIB Table**, e.g. *ConnIfIndex*. The unique identification of a particular table entry is derived from the combination of **Index Variable** (usually an index variable which is flagged with *) and **Index Value**. Use **Index Variables** to create more entries with **Add**.
Trigger Status	Only if **Command Type** = *MIB/SNMP* Select what status the event must have in order to modify the MIB variable as defined. Possible values: • *Active* (default value): The value of the MIB variable is modified if the initiator is active. • *Inactive*: The value of the MIB variable is modified if the initiator is inactive. • *Both*: The value of the MIB variable is differentially modified if the initiator status changes.
MIB Variables	Only if **Command Type** = *MIB/SNMP* Select the MIB variable whose value is to be configured as dependent upon initiator status. If the initiator is active (**Trigger Status** *Active*), the MIB variable is described with the value entered in **Active Value**. If the initiator is inactive (**Trigger Status** *Inactive*), the MIB variable is described with the value entered in **Inactive Value**. 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**

Field	Description
	Value and with an inactive initiator with the value in **Inactive Value**. Use **Add** to create more entries.
Interface	Only if **Command Type** = *Interface Status* Select the interface whose status should be changed.
Set interface status	Only if **Command Type** = *Interface Status* Select the status to be set for the interface. Possible values: • *Up* (default value) • *Down* • *Reset*
Local WLAN SSID	Only if **Command Type** = *Wlan Status* Select the desired wireless network whose status shall be changed.
Set status	Only if **Command Type** = *Wlan Status* or *WLC: VSS State* Select the status for the wireless network. Possible values: • *Activate* (default value) • *Deactivate*
Source Location	Only if **Command Type** = *Software Update* Select the source for the software update. Possible values: • *Current Software from Update Server* (default value): The latest software will be downloaded from the update server. • *HTTP Server*: The latest software will be downloaded from an HTTP server that you define in *Server URL*. • *HTTPS Server*: The latest software will be downloaded from

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

Field	Description
	Possible values: • *Import certificate* (default value) • *Delete certificate* • *SCEP*
Protocol	Only for **Command Type** = *Certificate Management* and *Configuration Management* if **Action** = *Import configuration* Select the protocol for the data transfer. Possible values: • *HTTP* (default value) • *HTTPS* • *TFTP*
CSV File Format	Only where **Command Type** = *Configuration Management* and **Action** = *Import configuration* or *Export configuration* Select whether the file is to be sent in the CSV format. The CSV format can easily be read and modified. In addition, you can view the corresponding file clearly using Microsoft Excel for example. The function is enabled by default.
Remote File Name	Only if **Command Type** = *Configuration Management* For **Action** = *Import configuration* Enter the name of the file under which it is saved on the server from which it is to be retrieved. For **Action** = *Export configuration* Enter the file name under which it should be saved on the server.
Local File Name	Only where **Command Type** = *Configuration Management* and **Action** = *Import configuration*, *Re-*

Field	Description
	name configuration or *Copy configuration* At import, renaming or copying enter a name for the configuration file under which to save it locally on the device.
File Name in Flash	Where **Command Type** = *Configuration Management* and **Action** = *Export configuration* Select the file to be exported. Where **Command Type** = *Configuration Management* and **Action** = *Rename configuration* Select the file to be renamed. Where **Command Type** = *Configuration Management* and **Action** = *Delete configuration* Select the file to be deleted. Where **Command Type** = *Configuration Management* and **Action** = *Copy configuration* Select the file to be copied.
Configuration contains certificates/keys	Only where **Command Type** = *Configuration Management* and **Action** = *Import configuration* or *Export configuration* Select whether the certificates and keys contained in the configuration are to be imported or exported. The function is disabled by default.
Encrypt configuration	Only where **Command Type** = *Configuration Management* and **Action** = *Import configuration* or *Export configuration* Define whether the data of the selected **Action** are to be encrypted.. The function is disabled by default.
Reboot after execution	Only if **Command Type** = *Configuration Management* Select whether your device should restart after the intended **Ac-**

Field	Description
	tion. The function is disabled by default.
Version Check	Only where **Command Type** = *Configuration Management* and **Action** = *Import configuration* Select whether, when importing a configuration file, to check on the server for the presence of a more current version of the already loaded configuration. If not, the file import is interrupted. The function is disabled by default.
Destination IP Address	Only if **Command Type** = *Ping Test* Enter the IP address whose accessibility is to be checked.
Source IP Address	Only if **Command Type** = *Ping Test* Enter an IP address to be used as sender address for the ping test. Possible values: • *Automatic* (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address. • *Specific*: Enter the desired IP address in the input field.
Interval	Only if **Command Type** = *Ping Test* Enter the time in **Seconds** after which a ping must be resent. The default value is *1* second.
Count	Only if **Command Type** = *Ping Test* Enter the number of ping tests to be performed until **Destination IP Address** is considered unreachable. The default value is *3*.
Server Address	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Enter the URL of the server from which a certificate file is to be

Field	Description
	retrieved.
Local Certificate Description	Where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Enter a description for the certificate under which to save it on the device. Where **Command Type** = *Certificate Management* and **Action** = *Delete certificate* Select the certificate to be deleted.
Password for protected Certificate	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Select whether to use a secure certificate requiring a password and enter it into the entry field. The function is disabled by default.
Overwrite similar certificate	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Select whether to overwrite a certificate already present on the your device with the new one. The function is disabled by default.
Write certificate in configuration	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Select whether to integrate the certificate in a configuration file; and if so, select the desired configuration file. The function is disabled by default.
Certificate Request Description	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Enter a description under which the SCEP certificate on your device is to be saved.
URL SCEP Server URL	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP*

Field	Description
	Enter the URL of the SCEP server, e.g. *http://scep.bintec-elmeg.com:8080/scep/scep.dll* Your CA administrator can provide you with the necessary data.
Subject Name	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Enter a subject name with attributes. Example: *"CN=VPNServer, DC=mydomain, DC=com, c=DE"*
CA Name	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Enter the name of the CA certificate of the certification authority (CA) from which you wish to request your certificate, e.g. *cawindows*. Your CA administrator can provide you with the necessary data.
Password	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* To obtain certificates, you may need a password from the certification authority. Enter the password you received from the certification authority here.
Key Size	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Select the length of the key to be created. Possible values are *1024* (default value), *2048* and *4096*.
Autosave Mode	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Select whether your device automatically stores the various steps of the enrolment internally. This is an advantage if enrolment cannot be concluded immediately. If the status has not been saved, the incomplete registration cannot be completed. As soon as the enrolment is completed and the certificate has been downloaded from the CA server, it is automatically saved in the device configuration.

Field	Description
	The function is enabled by default.
Use CRL	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Define the extent to which certificate revocation lists (CRLs) are to be included in the validation of certificates issued by the owner of this certificate. Possible values: • *Auto* (default value): In case there is an entry for a CDP, CRL distribution point this should be evaluated in addition to the CRLs globally configured in the device. • *Yes*: CRLs are always checked. • *No*: No checking of CRLs.
Select radio	Only where **Command Type** = *5 GHz WLAN Bandscan*, *5.8 GHz WLAN Bandscan* or *WLAN: Operation Mode* Select the WLAN module on which to perform the frequency band scan.
WLC SSID	Only where **Command Type** = *WLC: VSS State* Select the wireless network administered over the WLAN controller whose status should be changed.
Operation Mode (**Active**)	Only where **Command Type** = *WLAN: Operation Mode* Select the required operating mode for the selected radio module if it currently has the status *Active*. You may select from any of the operating modes that your device supports. So the choice may vary from device to device.
Operation Mode (**Inactive**)	Only where **Command Type** = *WLAN: Operation Mode* Select the required operating mode for the selected radio module if it currently has the status *Down*. You may select from any of the operating modes that your device supports. So the choice may vary from device to device.

18.5.3 Options

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

Fig. 159: **Local Services**->**Scheduling**->**Options**

The **Local Services**->**Scheduling**->**Options** menu consists of the following fields:

Fields in the Scheduling Options menu.

Field	Description
Schedule Interval	Select whether the schedule interval is to be enabled for the interface. The schedule interval is disabled by default. Enter the period of time in seconds after which the system checks whether configured events have occurred. Possible values are *0* to *65535*. The value *300* is recommended (5 minute accuracy).

18.6 Surveillance

In this menu, you can configure an automatic availability check for hosts or interfaces and automatic ping tests.

You can monitor temperature with devices from the **bintec WI** series.

Note

This function cannot be configured on your device for connections that are authenticated via a RADIUS server.

18.6.1 Hosts

A list of all monitored hosts is displayed in the **Local Services**->**Surveillance**->**Hosts** menu.

18.6.1.1 Edit or New

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

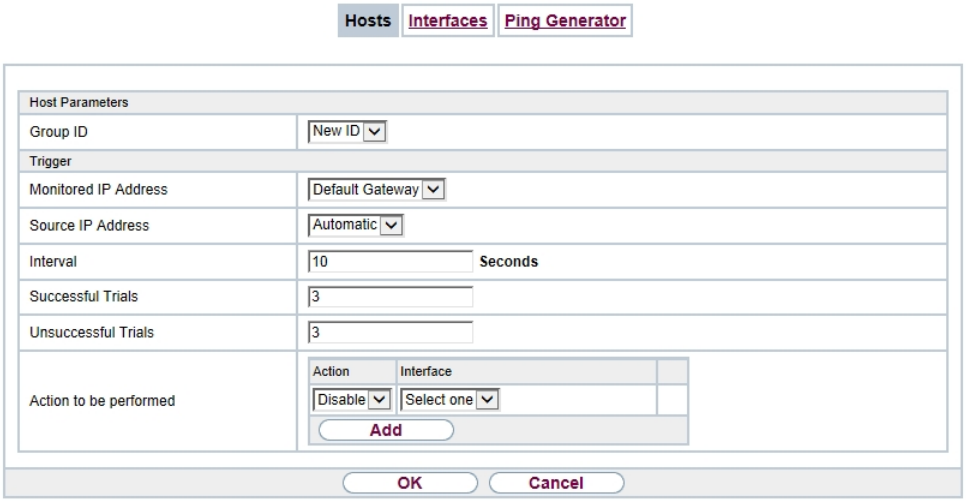


Fig. 160: **Local Services**->**Surveillance**->**Hosts**->**New**

The menu **Local Services**->**Surveillance**->**Hosts**->**New** consists of the following fields:

Fields in the Host Parameters menu

Field	Description
Group ID	If the availability of a group of hosts or the default gateway is to be monitored by your device, select an ID for the group or the default gateway. The group IDs are automatically created from *0* to *255*. If an entry has not yet been created, a new group is created using the *New ID* option. If entries have been created, you can select one from the list of created groups. Each host to be monitored must be assigned to a group.

Field	Description
	The operation configured in **Interface** is only executed if no group member can be reached.

Fields in the Trigger menu.

Field	Description
Monitored IP Address	Enter the IP address of the host to be monitored. Possible values: • *Default Gateway* (default value): The default gateway is monitored. • *Specific*: Enter the IP address of the host to be monitored manually in the adjacent input field.
Source IP Address	Select how the IP address is to be determined that your device uses as the source address of the packet sent to the host to be monitored. Possible values: • *Automatic* (default value): The IP address is determined automatically. • *Specific*; Enter the IP address in the adjacent input field.
Interval	Enter the time interval (in seconds) to be used for checking the availability of hosts. Possible values are *1* to *65536*. The default value is *10*. Within a group, the smallest **Interval** of the group members is used.
Successful Trials	Specify how many pings need to be answered for the host to be regarded as accessible. You can use this setting to specify, for example, when a host is deemed to be accessible once more, and used again, instead of a backup device. Possible values are *1* to *65536*.

Field	Description
	The default value is *3*.
Unsuccessful Trials	Specify how many pings need to be unanswered for the host to be regarded as inaccessible. You can use this setting to specify, for example, when a host is deemed to be inaccessible, and that a backup device should be used. Possible values are *1* to *65536*. The default value is *3*.
Action to be performed	Select which **Action** should be run. For most actions, you select an **Interface** to which the **Action** relates. All physical and virtual interfaces can be selected. For each interface, select whether it is to be enabled (*Enable*), disabled (*Disable* default value), reset (*Reset*), or the connection restablished (*Redial*). With **Action** = *Monitor* you can monitor the IP address that is specified under **Monitored IP Address**. This information can be used for other functions, such as the **Tracking IP Address** .

18.6.2 Interfaces

A list of all monitored hosts is displayed in the **Local Services**->**Surveillance**->**Interfaces** menu.

18.6.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to set up monitoring for other interfaces.

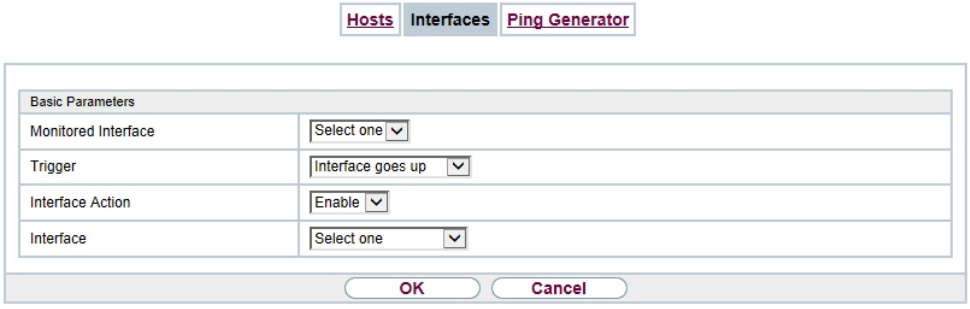


Fig. 161: **Local Services->Surveillance->Interfaces->New**

The menu **Local Services->Surveillance->Interfaces->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Monitored Interface	Select the interface on your device that is to be monitored.
Trigger	Select the state or state transition of **Monitored Interface** that is to trigger a particular **Interface Action**. Possible values: • *Interface goes up* (default value) • *Interface goes down*
Interface Action	Select the action that is to follow the state or state transition defined in **Trigger**. The action is applied to the Interface(s) selected in **Interface**. Possible values: • *Enable* (default value): Activation of interface(s) • *Disable*: Deactivation of interface(s)
Interface	Select the interface(s) for which the action defined in **Interface** is to be performed. You can choose all physical and virtual interfaces as well as options *All PPP Interfaces* and *All IPSec Interfaces*.

18.6.3 Ping Generator

In the **Local Services**->**Surveillance**->**Ping Generator** menu, a list of all configured, automatically generated pings is displayed.

18.6.3.1 Edit or New

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

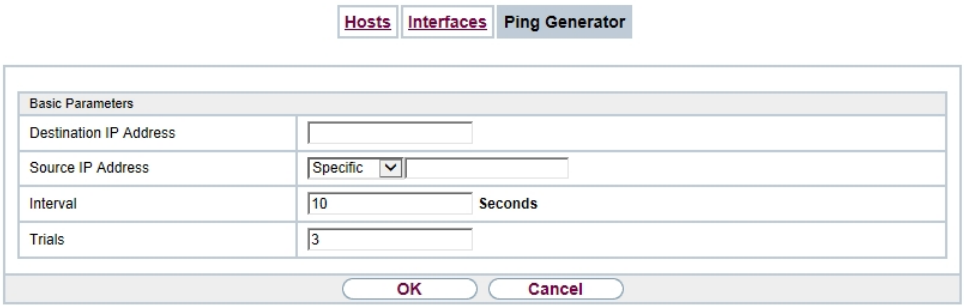


Fig. 162: **Local Services**->**Surveillance**->**Ping Generator**->**New**

The menu **Local Services**->**Surveillance**->**Ping Generator**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Destination IP Address	Enter the IP address to which the ping is automatically sent.
Source IP Address	Enter the source IP address of the outgoing ICMP echo request packets. Possible values: • *Automatic*: The IP address is determined automatically. • *Specific* (default value): Enter the IP address in the adjacent input field e.g. to test a particular extended route.
Interval	Enter the interval in seconds during which the ping is sent to the address specified in **Remote IP Address**. Possible values are *1* to *65536*.

Field	Description
	The default value is *10*.
Trials	Enter the number of ping tests to be performed until **Destination IP Address** as *Unreacheable* applies. The default value is *3*.

18.7 HotSpot Gateway

The **HotSpot Solution** allows provision of public Internet accesses (using WLAN or wired Ethernet). The solution is adapted to setup of smaller and larger Hotspot solutions for cafes, hotels, companies, communal residences, campgrounds, etc.

The **HotSpot Solution** consists of a bintec elmeg gateway installed onsite (with its own WLAN access point or additional connected WLAN device or wired LAN) and of the Hotspot server, centrally located at a computing centre. The operator account is administered on the server via an administration terminal (e.g., a hotel reception PC); this includes functions such as registration entry, generating tickets, statistical analysis, etc.

Login sequence at the Hotspot server

- When a new user connects with the Hotspot, he/she is automatically assigned an IP address via DHCP.
- As soon as he attempts to access any Internet site with a browser, the user is redirected to the home/login page.
- After the user has entered the registration data (user/password), these are sent to the central RADIUS server (Hotspot server) as RADIUS registration.
- Following successful registration, the gateway opens Internet access.
- For each user, the gateway sends regular additional information to the RADIUS server for recording accounting data.
- When the ticket expires, the user is automatically logged off and again redirected to the home/login page.

Requirements

To operate a Hotspot, the customer requires:

- a bintec elmeg device as hotspot gateway with active Internet access and configured hotspot server entries for login and accounting (see menu **System Management**->**Remote**

Authentication->**RADIUS**->**New** with **Group Description** *default group 0*)

- bintec elmeg Hotspot hosting (article number 5510000198)
- Access data
- Documentation
- Software licensing

Please note that you must first activate the licence.

Go to *www.bintec-elmeg.com* then **Service/Support** -> **Services** -> **Online Services**.

- Enter the required data (please note the relevant explanations on the license sheet), and follow the instructions of the online licensing.

- You then receive the Hotspot server's login data.

Note

Activation may require 2-3 business days.

Access data for gateway configuration

RADIUS Server IP	62.245.165.180
RADIUS Server Password	Set by bintec elmeg GmbH
Domain	Individually set for customers by customer/dealer
Walled Garden Network	Individually set for customers by customer/dealer
Walled Garden Server URL	Individually set for customers by customer/dealer
Terms & Conditions URL	Individually set for customers by customer/dealer

Access data for configuration of the Hotspot server

Admin URL	https://hotspot.bintec-elmeg.com/
Username	Individually set by bintec elmeg
Password	Individually set by bintec elmeg

Note

Also refer to the WLAN Hotspot Workshop that is available to download from *www.bintec-elmeg.com*

18.7.1 HotSpot Gateway

In the **HotSpot Gateway** menu, you can configure the bintec elmeg gateway installed onsite for the **Hotspot Solution**.

A list of all configured hotspot networks is displayed in the **Local Services**->**HotSpot Gateway**->**HotSpot Gateway** menu.

Fig. 163: **Local Services**->**HotSpot Gateway**->**HotSpot Gateway**

You can use the **Enabled** option to enable or disable the corresponding entry.

18.7.1.1 Edit or New

You configure the hotspot networks in the **Local Services**->**HotSpot Gateway**->**HotSpot Gateway**->[icon] menu. Choose the **New** button to set up additional Hotspot networks.

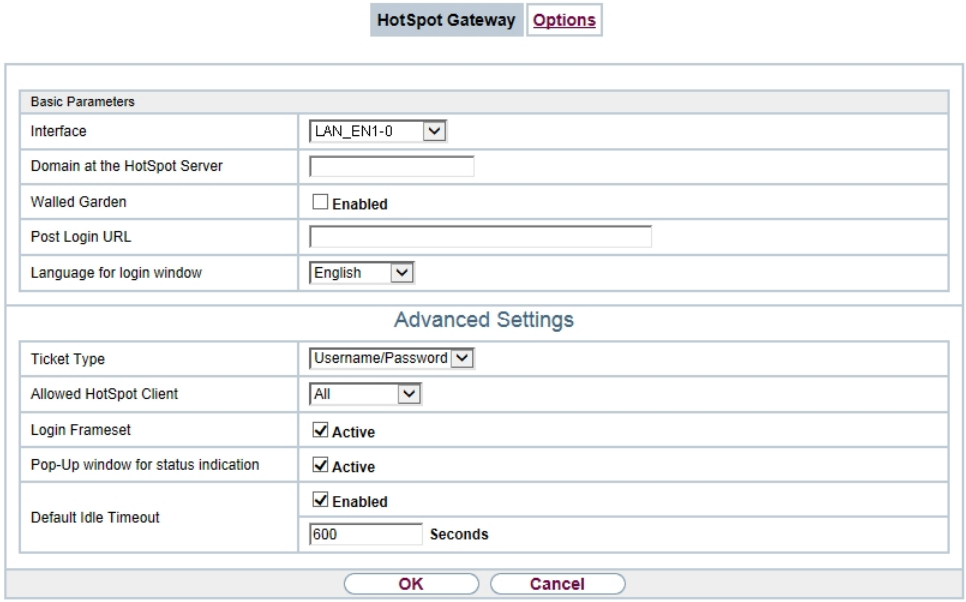


Fig. 164: **Local Services->HotSpot Gateway->HotSpot Gateway->**

The **Local Services->HotSpot Gateway->HotSpot Gateway->** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Choose the interface to which the Hotspot LAN or WLAN is connected. When operating over LAN, enter the Ethernet interface here (e. g. en1-0). If operating over WLAN, the WLAN interface to which the access point is connected must be selected. **Caution** For security reasons you cannot configure your device over an interface that is configured for the Hotspot. Therefore take care when selecting the interface you want to use for the Hotspot. If you select the interface over which the current configuration session is running, the current connection will be lost. You must then log in again over a reachable interface that is not configured for the Hotspot to configure your device.

Field	Description
Domain at the HotSpot Server	Enter the domain name that you used when setting up the HotSpot server for this customer. The domain name is required so that the Hotspot server can distinguish between the different clients (customers).
Walled Garden	Enable this function if you want to define a limited and free area of websites (intranet). The function is not activated by default.
Walled Network / **Netmask**	Only if **Walled Garden** is enabled. Enter the network address of the **Walled Network** and the corresponding **Netmask** of the intranet server. For the address range resulting from **Walled Network** / **Netmask**, clients require no authentication. Example: Enter 192.168.0.0 / 255.255.255.0, if all IP addresses from 192.168.0.0 to 19.168.0.255 are free. Enter 192.168.0.1 / 255.255.255.255, if only the IP address 192.168.0.1 is free.
Walled Garden URL	Only if **Walled Garden** is enabled. Enter the **Walled Garden URL** of the intranet server. Freely accessible websites must be reachable over this address.
Terms &Conditions	Only if **Walled Garden** is enabled. In the **Terms &Conditions** input field, enter the address of the general terms and conditions on the intranet server, or public server, e.g., http://www.webserver.de/agb.htm. The page must lie within the address range of the walled garden network.
Additional freely accessible Domain Names	Only if **Walled Garden** is enabled. Add further URLs or IP addresses with **Add**. The web pages can be accessed via these additional freely accessible addresses.
Post Login URL	Here you can specify the URL a user is redirected to after logging in to the Hotspot Solution.
Language for login window	Here you can choose the language for the start/login page.

Field	Description
	The following languages are supported: *English*, *Deutsch*, *Italiano*, *Français*, *Español*, *Português* and *Nederlands*. The language can be changed on the start/login page at any time.

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

Fields in the menu Advanced Settings

Field	Description
Ticket Type	Select the ticket type. Possible values: • *Voucher*: Only the user name must be entered. Define a default password in the input field. • *Username/Password* (default value): User name and password must be entered.
Allowed HotSpot Client	Here you can define which type of users can log in to the Hotspot. Possible values: • *All*: All clients are approved. • *DHCP Client*: Prevents users who have not received an IP address from DHCP from logging in.
Login Frameset	Enable or disable the login window. The login window on the HTML homepage consists of two frames. When the function is enabled, the login form displays on the left-hand side. When the function is disabled, only the website with information, advertising and/or links to freely accessible websites is displayed. The function is enabled by default.

Field	Description
Pop-Up window for status indication	Specify whether the device uses pop-up windows to display the status. The function is enabled by default.
Default Idle Timeout	Enable or disable the **Default Idle Timeout**. If a hotspot user does not trigger any data traffic for a configurable length of time, they are logged out of the hotspot. The function is enabled by default. The default value is *600* seconds.

18.7.2 Options

In the **Local Services**->**HotSpot Gateway**->**Options** menu, general settings are performed for the hotspot.

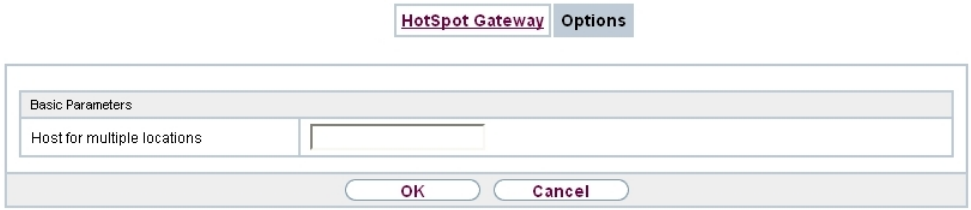


Fig. 165: **Local Services**->**HotSpot Gateway**->**Options**

The **Local Services**->**HotSpot Gateway**->**Options** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Host for multiple locations	If several locations (branches) are set up on the Hotspot server, enter the value of the NAS identifier (RADIUS server parameter) that has been registered for this location on the Hotspot server.

18.8 Wake-On-LAN

With the function **Wake-On-LAN** you can start network devices that are switched off via an integrated network card. The network card also needs a power supply, even when the computer is switched off. You can use filters and rule chains to define the conditions that need to be met to send the so-called magic packet, and select the interfaces that are to be monitored for the defined rule chains. Configuring the filters and rule chains is largely like configuring filters and rule chains in the menu **Access Rules**.

18.8.1 Wake-On-LAN Filter

The menu **Local Services**->**Wake-On-LAN**->**Wake-On-LAN Filter** displays a list of all the WOL filters that have been configured.

18.8.1.1 Edit or New

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

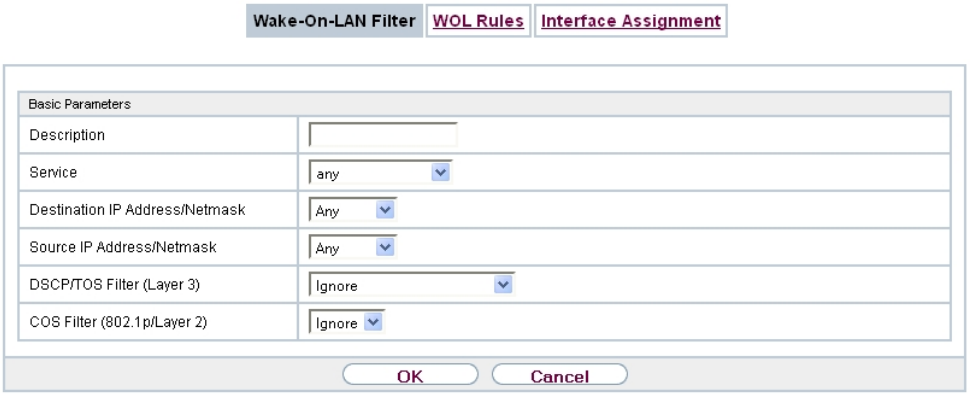


Fig. 166: **Local Services->Wake-On-LAN->Wake-On-LAN Filter->New**

The **Local Services->Wake-On-LAN->Wake-On-LAN Filter->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter the name of the filter.

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

Field	Description
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)	Select the Type of Service (TOS). Possible values: • *Ignore* (default value): The type of service is ignored. • *DSCP Binary Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63.

Field	Description
	• *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*. Value range *0* to *7*. The default value is *Ignore*.

18.8.2 WOL Rules

The menu **Local Services**->**Wake-On-LAN**->**WOL Rules** displays a list of all the WOL rules that have been configured.

18.8.2.1 Edit or New

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

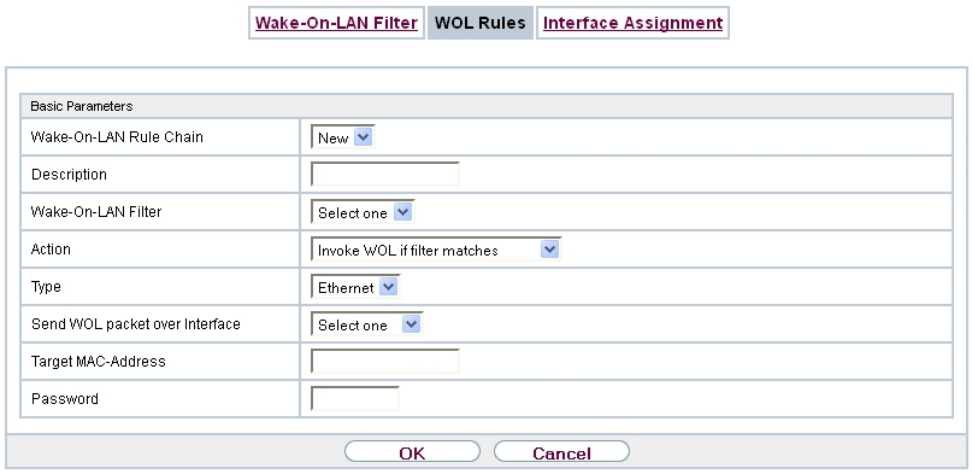


Fig. 167: **Local Services**->**Wake-On-LAN**->**WOL Rules**->**New**

The **Local Services**->**Wake-On-LAN**->**WOL Rules**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Wake-On-LAN Rule Chain	Select whether to create a new rule chain or to edit an existing one. Possible values: • *New* (default value): You can create a new rule chain with this setting. • *<Name of the rule chain>*: Shows a rule chain that has already been created, which you can select and edit.
Description	Only where **Wake-On-LAN Rule Chain** = *New* Enter the name of the rule chain.
Wake-On-LAN Filter	Select a WOL filter. If the rule chain is new, select the filter to be set at the first point of the rule chain. If the rule chain already exists, select the filter to be attached to the rule chain. To select a filter, at least one filter must be configured in the **Local Services**->**Wake-On-LAN**->**WOL Rules** menu.
Action	Define the action to be taken for a filtered data packet. Possible values: • *Invoke WOL if filter matches*: Run WOL if the filter matches. • *Invoke if filter does not match*: Run WOL if the filter does not match. • *Deny WOL if filter matches*: Do not run WOL if the filter matches. • *Deny WOL if filter does not match*: Do not run WOL if the filter does not match. • *Ignore rule and skip to next rule*: This rule is ignored and the next one in the chain is examined.
Type	Select whether the Wake on LAN magic packet is to be sent as a UDP packet or as an Ethernet frame via the interface specified in **Send WOL packet over Interface**.

Field	Description
Send WOL packet over Interface	Select the interface which is to be used to send the Wake on LAN magic packet.
Target MAC-Address	Only where **Action** = *Invoke WOL if filter matches* and *Invoke if filter does not match* Enter the MAC address of the network device that is to be enabled using WOL.
Password	Only where **Action** = *Invoke WOL if filter matches* and *Invoke if filter does not match* If the network device that is to be enabled supports the "SecureOn" function, enter the corresponding password for this device here. The device is only enabled if the MAC address and password are correct.

18.8.3 Interface Assignment

In this menu, the configured rule chains are assigned to individual interfaces which are then monitored for these rule chains.

A list of all configured interface assignments is displayed in the **Local Services**->**Wake-On-LAN**->**Interface Assignment** menu.

18.8.3.1 Edit or New

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

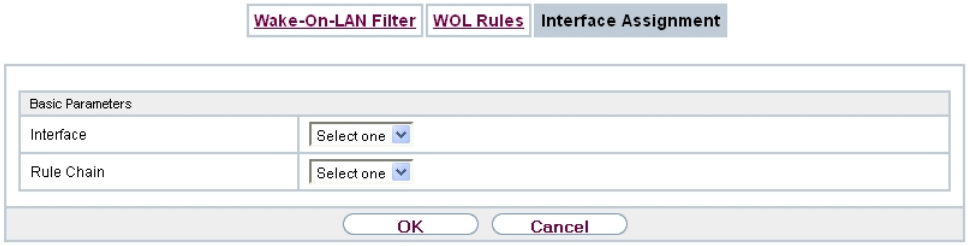


Fig. 168: **Local Services**->**Wake-On-LAN**->**Interface Assignment**->**New**

The **Local Services**->**Wake-On-LAN**->**Interface Assignment**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Select the interface for which a configured rule chain is to be assigned.
Rule Chain	Select a rule chain.

Chapter 19 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.

19.1 Diagnostics

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

19.1.1 Ping Test

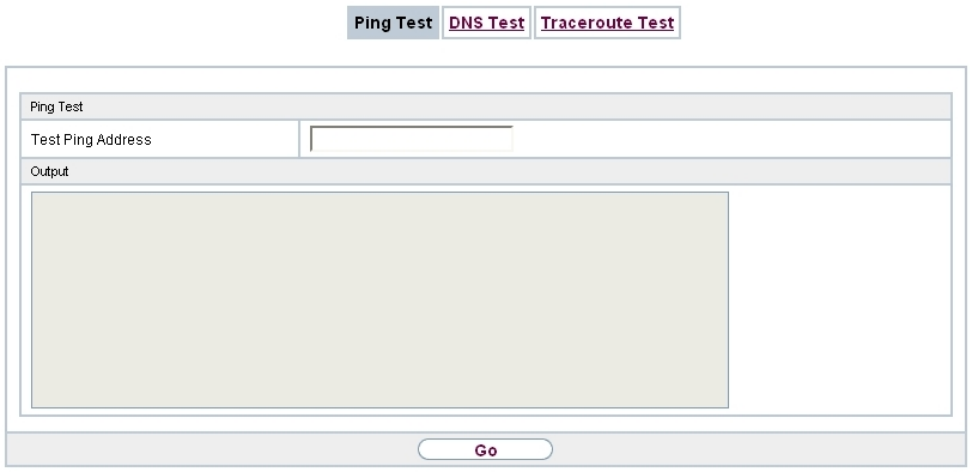


Fig. 169: **Maintenance**->**Diagnostics**->**Ping Test**

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.

19.1.2 DNS Test

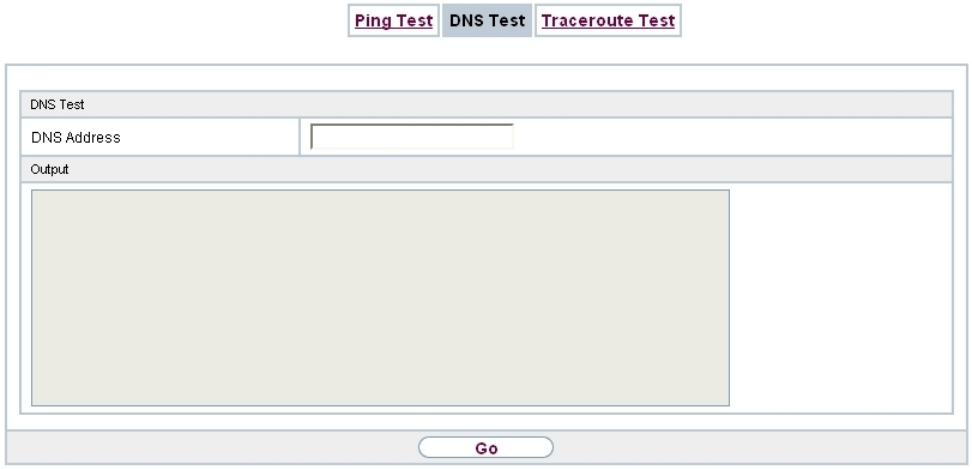


Fig. 170: **Maintenance->Diagnostics->DNS Test**

The DNS test is used to check whether the domain name of a particular host is correctly resolved. The **Output**field displays the DSN test messages. The ping test is launched by entering the domain name to be tested in **DNS Address** and clicking the **Go** button.

19.1.3 Traceroute Test

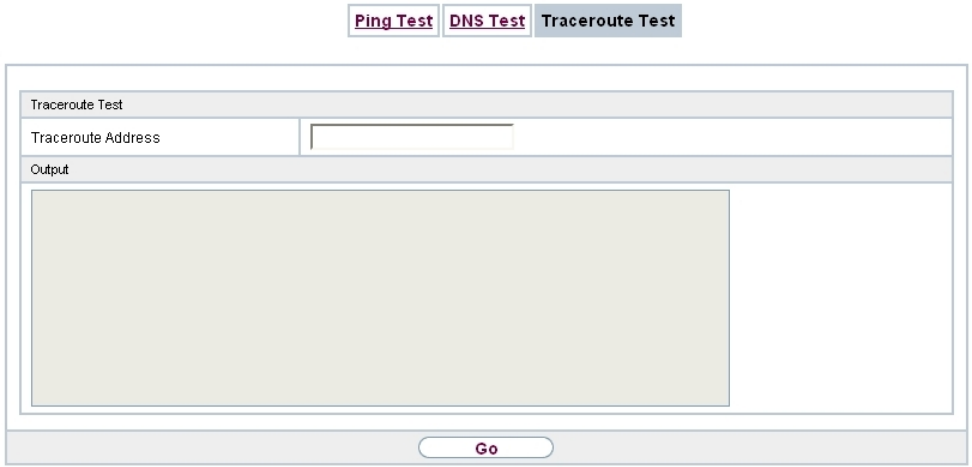


Fig. 171: **Maintenance->Diagnostics->Traceroute Test**

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 ping test is launched by entering the IP address to be tested in **Traceroute Address** and clicking the **Go** button.

19.2 Software &Configuration

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

19.2.1 Options

Your device contains the version of the system software available at the time of production. More recent versions may have since been released. You may therefore need to carry out a software update.

Every new system software includes new features, better performance and any necessary bugfixes from the previous version. You can find the current system software at *www.bintec-elmeg.com* . The current documentation is also available here.

Important

If you want to update your software, make sure you consider the corresponding release notes. These describe the changes implemented in the new system software.

The result of an interrupted update (e.g. power failure during the update) could be that your gateway no longer boots. Do not turn your device off during the update.

An update of BOOTmonitor and/or Logic is recommended in a few cases. In this case, the release notes refer expressly to this fact. Only update BOOTmonitor or Logic if bintec elmeg GmbH explicitly recommends this.

Flash

Your device saves its configuration in configuration files in the flash EEPROM (Electrically Erasable Programmable Read Only Memory). The data even remains stored in the flash when your device is switched off.

RAM

The current configuration and all changes you set on your device during operation are

stored in the working memory (RAM). The contents of the RAM are lost if the device is switched off. So if you modify your configuration and want to keep these changes for the next time you start your device, you must save the modified configuration in the flash memory before switching off: The **Save configuration** button over the navigation area of the **GUI**. This configuration is then saved in the flash in a file with the name `boot`. When you start your device, the `boot` configuration file is used by default.

Actions

The files in the flash memory can be copied, moved, erased and newly created. It is also possible to transfer configuration files between your device and a host via HTTP.

Configuration file format

The file format of the configuration file allows encryption and ensures compatibility when restoring the configuration on the gateway in various system software versions. This is a CSV format, which can be read and modified easily. In addition, you can view the corresponding file clearly using Microsoft Excel for example. The administrator can store encrypted backup files for the configuration. When the configuration is sent by e-mail (e.g for support purposes) confidential configuration data can be protected fully if required. You can save or import files with the actions "Export configuration", "Export configuration with status information" and "Load configuration". If you want to save a configuration file with the action ""Export configuration" or "Export configuration with status information", you can choose whether the configuration file is saved encrypted or without encryption.

Caution

If you have saved a configuration file in an old format via the SNMP shell with the `put` command, there is no guarantee that it can be reloaded to the device. As a result, the old format is no longer recommended.

Fig. 172: **Maintenance->Software &Configuration->Options**

The **Maintenance**->**Software &Configuration**->**Options** menu consists of the following fields:

Fields in the Currently Installed Software menu.

Field	Description
BOSS	Shows the current software version loaded on your device.
System Logic	Shows the current system logic loaded on your device.
ADSL Logic	Shows the current version of the ADSL logic loaded on your device.

Fields in the Software and Configuration Options menu.

Field	Description
Action	Select the action you wish to execute. After each task, a window is displayed showing the other steps that are required. Possible values: • *No Action* (default value): • *Export configuration*: The configuration file **Current File Name in Flash** is transferred to your local host. If you click the **Go** button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name. • *Import configuration*: Under **Filename** select a configuration file you want to import. Please note: Click **Go** to first load the file under the name *boot* in the flash memory for the device. You must restart the device to enable it. Please note: The files to be imported must be in CSV format! • *Copy configuration*: The configuration file in the **Source File Name** field is saved as**Destination File Name**. • *Delete configuration*: The configuration in the **Select file** field is deleted. • *Rename configuration*: The configuration file in the **Select file** field is renamed to **New File Name**. • *Restore backup configuration*: Only if, under **Save configuration** with the setting *Save configuration and*

Field	Description
	back up previous boot configuration the current configuration was saved as boot configuration and the previous boot configuration was also archived. You can load back the archived boot configuration. • *Delete software/firmware*: The file in the **Select file** field is deleted. • *Import language*: You can import additional language versions of the **GUI** into your device. You can download the files to your PC from the download area at *www.bintec-elmeg.com* and from there import them to your device • *Update system software*: You can launch an update of the system software, the ADSL logic and the BOOTmonitor. • *Import Voice Mail Wave Files*: (Only displayed if an SD card is inserted.) In **file name**, select the *vms_wavfiles.zip* file that you wish to import. • *Export configuration with state information*: The active configuration from the RAM is transferred to your local host. If you click the **Go** button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name.
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*

Field	Description
	Select the source of the update. Possible values: • *Local File* (default value): The system software file is stored locally on your PC. • *HTTP Server*: The file is stored on a remote server specified in the **URL**. • *Current Software from Update Server*: The file is on the official update server.
URL	Only for **Source Location** = *HTTP Server* Enter the URL of the update server from which the system software file is loaded.
Current File Name in Flash	For **Action** = *Export configuration* Select the configuration file to be exported.
Include certificates and keys	For **Action** = *Export configuration*, *Export configuration with state information* Define whether the selected **Action** should also be applied for certificates and keys. The function is activated by selecting *Enabled*. The function is enabled by default.
Source File Name	Only for **Action** = *Copy configuration* Select the source file to be copied.
Destination File Name	Only for **Action** = *Copy configuration* Enter the name of the copy.
Select file	Only for **Action** = *Rename configuration*, *Delete configuration* or *Delete software/firmware* Select the file or configuration to be renamed or deleted.
New File Name	Only for **Action** = *Rename configuration*

Field	Description
	Enter the new name of the configuration file.

19.3 Reboot

19.3.1 System Reboot

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

Pay attention to the LEDs on your device. For information on the meaning of the LEDs, see the **Technical Data** chapter of the manual.

Note

Before a reboot, make sure you confirm your configuration changes by clicking the **Save configuration** button, so that these are not lost when you reboot.

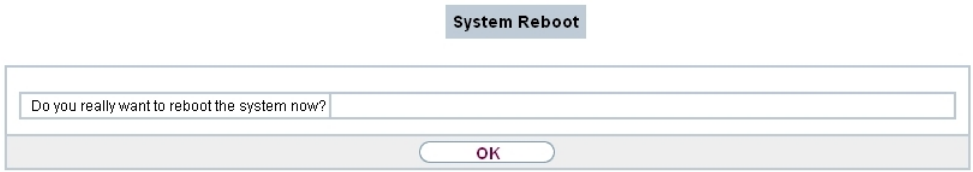


Fig. 173: **Maintenance->Reboot->System Reboot**

If you wish to restart your device, click the **OK** button. The device will reboot.

Chapter 20 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.

20.1 Syslog

Events in various subsystems of your device (e.g. PPP) are logged in the form of syslog messages (system logging messages). The number of messages visible depends on the level set (eight steps from *Emergency* over *Information* to *Debug*).

In addition to the data logged internally on your device, all information can and should be transmitted to one or more external PCs for storage and processing, e.g. to the system administrator's PC. The syslog messages saved internally on your device are lost when you reboot.

Warning

Make sure you only pass syslog messages to a safe computer. Check the data regularly and ensure that there is always enough spare capacity available on the hard disk of your PC.

Syslog Daemon

All Unix operating systems support the recording of syslog messages. For Windows PCs, the Syslog Demon included in the **DIME Tools** can record the data and distribute to various files depending on the contents (can be called in the download area at *www.bintec-elmeg.com*).

20.1.1 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.

20.1.1.1 New

Select the **New** button to set up additional syslog servers.

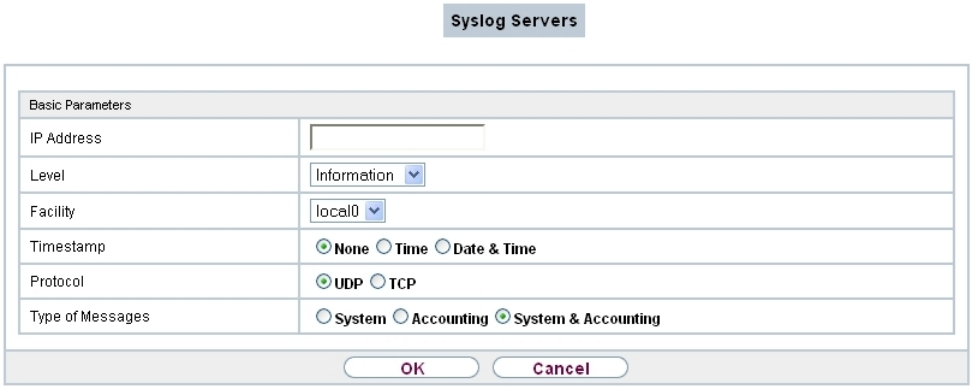


Fig. 174: **External Reporting->Syslog->Syslog Servers->New**

The menu **External Reporting->Syslog->Syslog Servers->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
IP Address	Enter the IP address of the host to which syslog messages are passed.
Level	Select the priority of the syslog messages that are to be sent to the host. Possible values: • *Emergency* (highest priority) • *Alert* • *Critical* • *Error* • *Warning* • *Notice* • *Information* (default value)

Field	Description
	• *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*.
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*

20.2 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).

20.2.1 Interfaces

In this menu, you can configure the IP Accounting function individually for each interface.

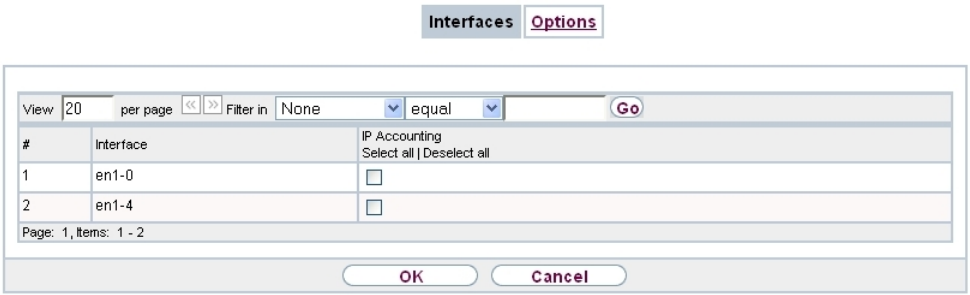


Fig. 175: **External Reporting->IP Accounting->Interfaces**

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.

20.2.2 Options

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

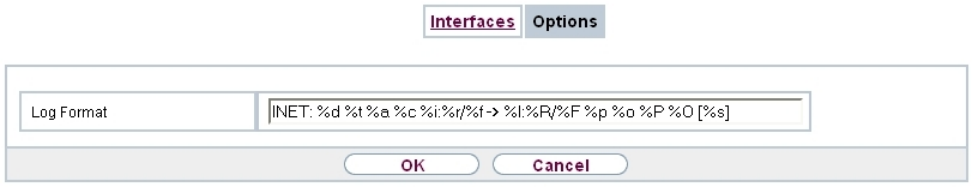


Fig. 176: **External Reporting->IP Accounting->Options**

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]*

20.3 Alert Service

It was previously possible to send syslog messages from the router to any syslog host. Depending on the configuration, e-mail alerts are sent to the administrator as soon as relevant syslog messages appear.

20.3.1 Alert Recipient

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

20.3.1.1 New

Select the **New** to create additional alert recipients.

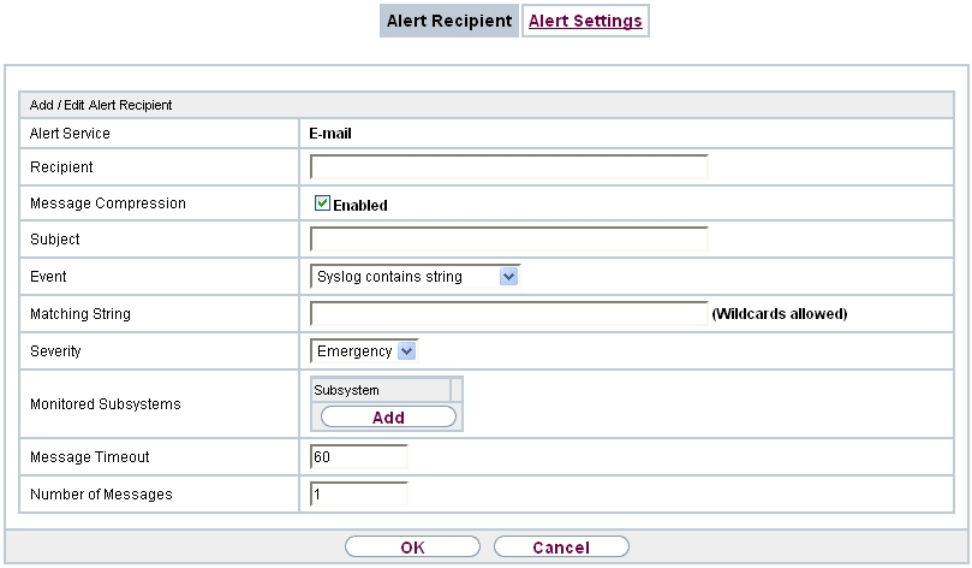


Fig. 177: **External Reporting->Alert Service->Alert Recipient->New**

The menu **External Reporting->Alert Service->Alert Recipient->New** consists of the following fields:

Fields in the Add / Edit Alert Recipient menu.

Field	Description
Alert Service	Displays the alert service. You can select an alert service for devices with UMTS.

Field	Description
	Possible values: • E-mail • SMS
Recipient	Enter the recipient's e-mail address. The entry is limited to 40 characters.
Message Compression	Select whether the text in the alert E-mail is to be shortened. The e-mail then contains the syslog message only once plus the number of relevant events. Enable or disable the field. The function is enabled by default.
Subject	You can enter a subject.
Event	This feature is available only for devices with Wireless LAN Controller. Select the event to trigger an email notification. Possible values: • *Syslog contains string* (default value): A Syslog message includes a specific string. • *New Neighbor AP found*: A new adjacent AP has been found. • *New Rogue AP found*: A new Rough AP has been found, i.e. an AP using an SSID of its own network, yet is not a component of this network. • *New Slave AP (WTP) found*: A new unconfigured AP has reported to the WLAN. • *Managed AP offline*: A managed AP is no longer accessible.
Matching String	You must enter a "Matching String". This must occur in a syslog message as a necessary condition for triggering an alert. The entry is limited to 55 characters. Bear in mind that without the use of wildcards (e.g. "*"), only those strings that correspond exactly to the entry fulfil the condition. The "Matching String"

Field	Description
	entered therefore usually contains wildcards. To be informed of all syslog messages of the selected level, just enter "*".
Severity	Select the severity level which the string configured in the **Matching String** field must reach to trigger an e-mail alert. Possible values: *Emergency* (default value), *Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Information*, *Debug*
Monitored Subsystems	Select the subsystems to be monitored. Add new subsystems with **Add**.
Message Timeout	Enter how long the router must wait after a relevant event before it is forced to send the alert mail. Possible values are *0* to *86400*. The value *0* disables the timeout. The default value is *60*.
Number of Messages	Enter the number of syslog messages that must be reached before an E-mail can be sent for this case. If timeout is configured, the mail is sent when this expires, even if the number of messages has not been reached. Possible values are *0* to *99*; the default value is *1*.

20.3.2 Alert Settings

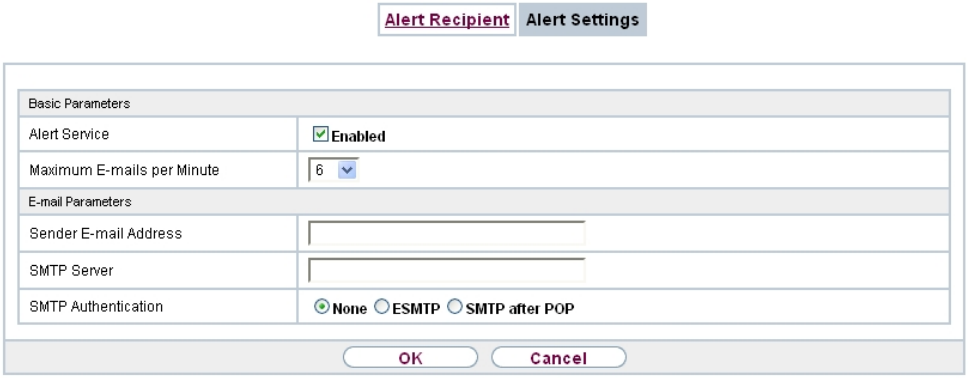


Fig. 178: **External Reporting->Alert Service->Alert Settings**

The menu **External Reporting->Alert Service->Alert Settings** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Alert Service	Select whether the alert service is to be enabled for the interface. The function is enabled with *Enabled*. The function is enabled by default.
Maximum E-mails per Minute	Limit the number of outgoing mails per minute. Possible values are *1* to *15*, the default value is *6*.

Fields in the E-mail Parameters menu.

Field	Description
Sender E-mail Address	Enter the mail address to be entered in the sender field of the E-mail.
SMTP Server	Enter the address (IP address or valid DNS name) of the mail server to be used for sending the mails. The entry is limited to 40 characters.
SMTP Authentication	Authentication expected by the SMTP server.

Field	Description
	Possible values: • *None* (default value): The server accepts and send emails without further authentication. • *ESMTP*: The server only accepts e-mails if the router logs in with the correct user name and password. • *SMTP after POP*: The server requires that e-mails are called via POP3 by the sending IP with the correct POP3 user name and password before sending an e-mail.
User Name	Only if **SMTP Authentication** = *ESMTP* or *SMTP after POP* Enter the user name for the POP3 or SMTP server.
Password	Only if **SMTP Authentication** = *ESMTP* or *SMTP after POP* Enter the password of this user.
POP3 Server	Only if **SMTP Authentication** = *SMTP after POP* Enter the address of the server from which the e-mails are to be retrieved.
POP3 Timeout	Only if **SMTP Authentication** = *SMTP after POP* Enter how long the router must wait after the POP3 call before it is forced to send the alert mail. The default value is *600* seconds.

Fields in the SMS Parameters menu (for devices with UMTS only)

Field	Description
SMS Device	You can receive notification of system alerts in text messages. Select the device to be used to send the text message.
Maximum SMS per Day	Limit the maximum number of SMS sent during a single day. Activating *No Limitation* allows any number of SMS to be sent. The defualt value is 10 SMS per day. Note: Entering a value of *0* is equivalent to activating *No Limitation*.

20.4 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

20.4.1 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.

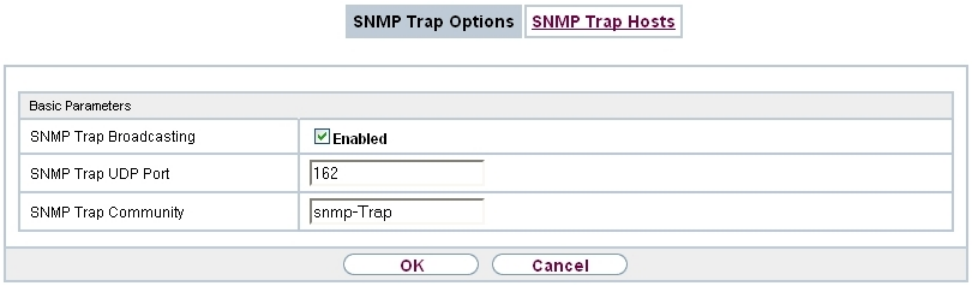


Fig. 179: **External Reporting->SNMP->SNMP Trap Options**

The menu **External Reporting**->**SNMP**->**SNMP Trap Options** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
SNMP Trap Broadcast-	Select whether the transfer of SNMP traps is to be activated.

Field	Description
ing	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 device. A character string of between *0* and *255* characters is possible. The default value is *SNMP Trap*.

20.4.2 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.

20.4.2.1 New

Select the **New**button to create additional SNMP trap hosts.

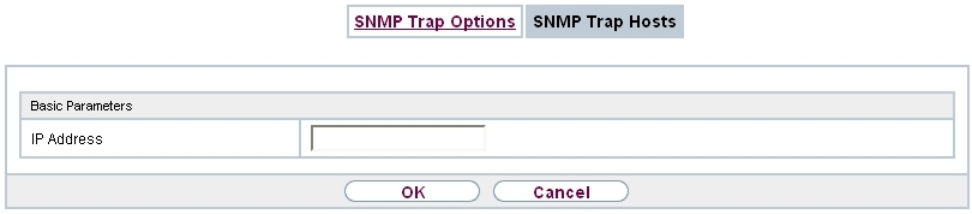


Fig. 180: **External Reporting->SNMP->SNMP Trap Hosts->New**

The menu **External Reporting->SNMP->SNMP Trap Hosts->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
IP Address	Enter the IP address of the SNMP trap host.

20.5 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 a single 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.bintec-elmeg.com* and from there import it to your device).

20.5.1 Options

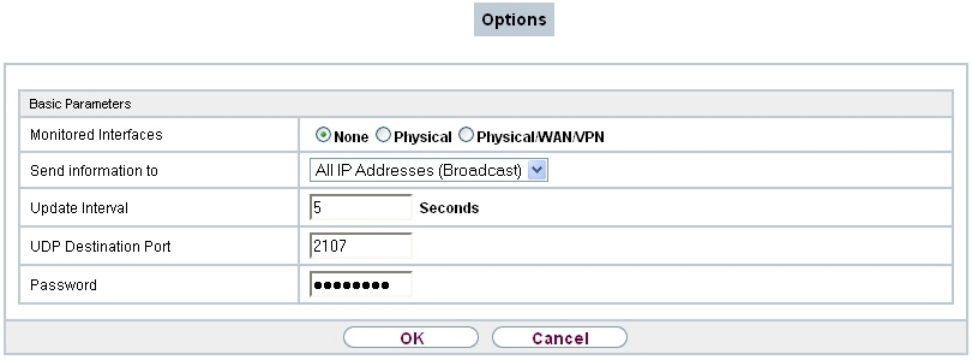


Fig. 181: **External Reporting->Activity Monitor->Options**

The menu **External Reporting->Activity Monitor->Options** consists of the following fields:

Fields in the Basic 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.

Field	Description
	• *Single Host*: The UDP packets are sent to the IP address 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 21 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.

21.1 Internal Log

21.1.1 System Messages

In the **Monitoring**->**Internal Log**->**System Messages** menu, a list of all internally stored system messages is displayed. Above the table you will find the configured vales for the **Maximum Number of Syslog Entries** and **Maximum Message Level of Syslog Entries** fields. These values can be changed in the **System Management**->**Global Settings**->**System** menu.

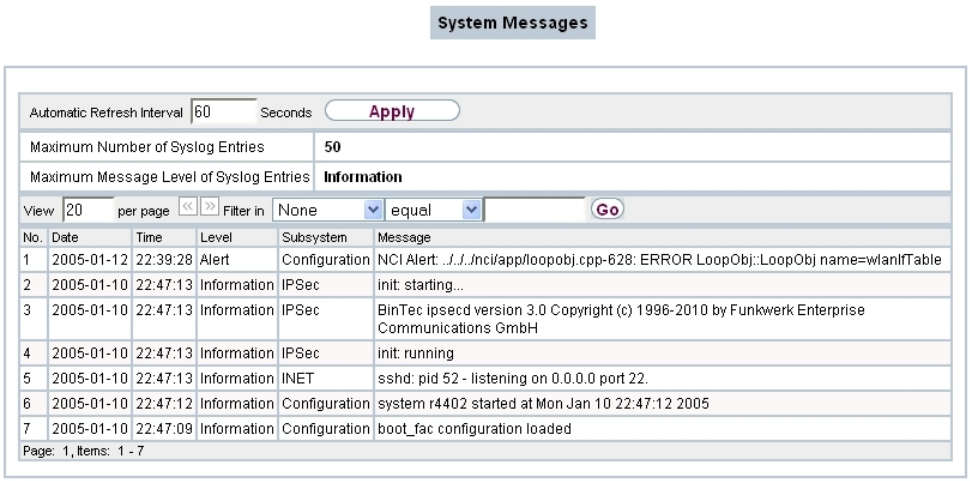


Fig. 182: **Monitoring->Internal Log->System Messages**

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.

Field	Description
Subsystem	Displays which subsystem of the device generated the message.
Message	Displays the message text.

21.2 IPSec

21.2.1 IPSec Tunnels

A list of all configured IPSec tunnel providers is displayed in the **Monitoring**->**IPSec**->**IPSec Tunnels** menu.

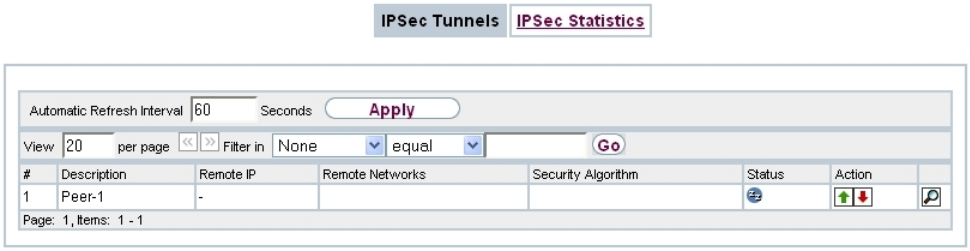


Fig. 183: **Monitoring**->**IPSec**->**IPSec Tunnels**

Values in the IPSec Tunnels list

Field	Description
Description	Displays the name of the IPSec tunnel.
Remote IP	Displays the IP address of the remote IPSec Peers.
Remote Networks	Displays the currently negotiated subnets of the remote terminal.
Security Algorithm	Displays the encryption algorithm of the IPSec tunnel.
Status	Displays the operating status of the IPSec tunnel.
Action	Enables you to change the status of the IPSec tunnel as displayed.
Details	Opens a detailed statistics window.

You change the status of the IPSec tunnel by clicking the button or the button in the **Action** column.

By clicking the button, you display detailed statistics on the IPSec connection.

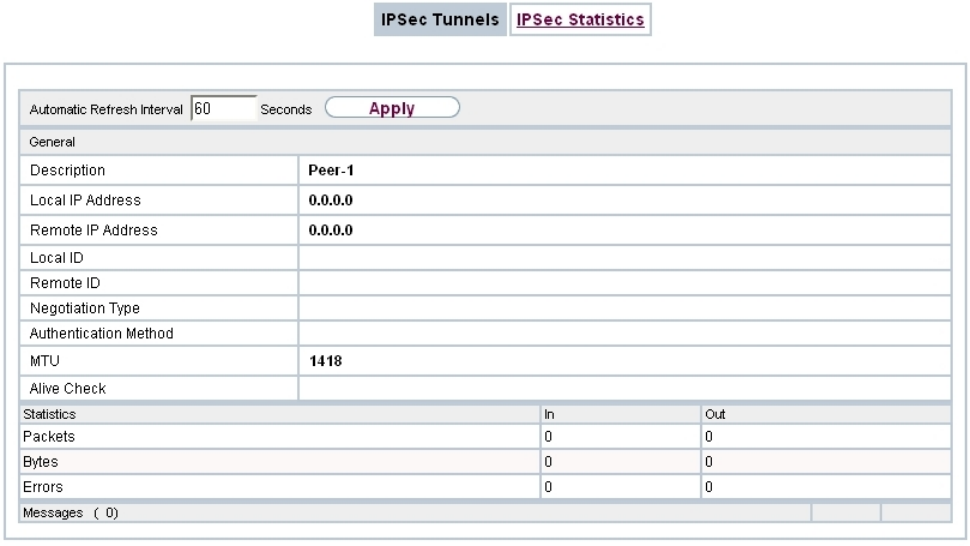


Fig. 184: **Monitoring->IPSec->IPSec Tunnels->**

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)	The parameters of the IKE (Phase 1) SAs are displayed here.

Field	Description
Role / **Algorithm** / **Lifetime remaining** / **Status**	
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.

21.2.2 IPSec Statistics

In the **Monitoring**->**IPSec**->**IPSec Statistics** menu, statistical values for all IPSec connections are displayed.

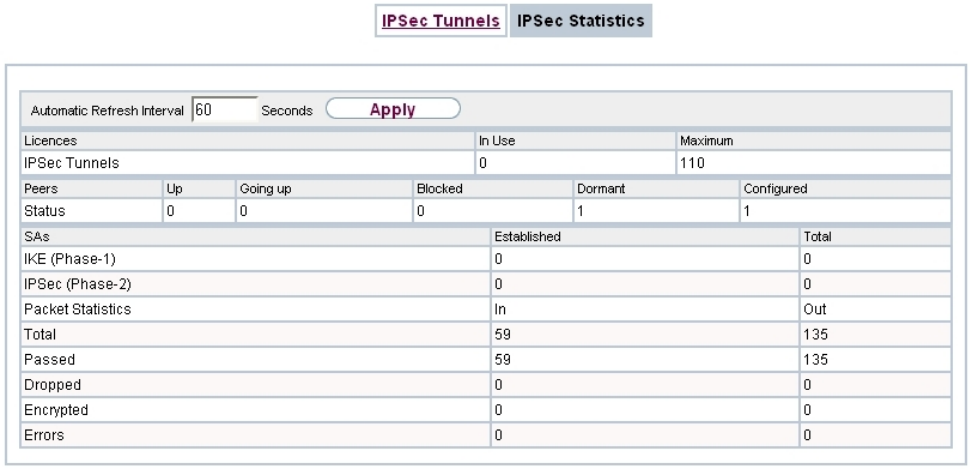


Fig. 185: **Monitoring**->**IPSec**->**IPSec Statistics**

The **Monitoring**->**IPSec**->**IPSec Statistics** menu consists of the following fields:

Fields in the Licences menu

Field	Description
IPSec Tunnels	Shows the IPSec licences currently in use (**In Use**) and the maximum number of licenses usable (**Maximum**).

Fields in the Peers menu

Field	Description
Status	Displays the number of IPSec tunnels by their current status. • **Up**: Currently active IPSec tunnels. • **Going up**: IPSec tunnels currently in the tunnel setup phase. • **Blocked**: IPSec tunnels that are blocked. • **Dormant**: Currently inactive IPSec tunnels. • **Configured**: Configured IPSec tunnels.

Fields in the SAs menu.

Field	Description
IKE (Phase-1)	Shows the number of active phase 1 SAs (**Established**) from the total number of phase 1 SAs (**Total**).
IPSec (Phase-2)	Shows the number of active phase 2 SAs (**Established**) from the total number of phase 2 SAs (**Total**).

Fields in the Packet Statistics menu.

Field	Description
Total	Shows the number of all processed incoming (**In**) or outgoing (**Out**) packets.
Passed	Shows the number of incoming (**In**) or outgoing (**Out**) packets forwarded in plain text.
Dropped	Shows the number of all rejected incoming (**In**) or outgoing (**Out**) packets.
Encrypted	Shows the number of all incoming (**In**) or outgoing (**Out**) packets protected by IPSec.
Errors	Shows the number of incoming (**In**) or outgoing (**Out**) packets for which processing led to errors.

21.3 Interfaces

21.3.1 Statistics

In the **Monitoring**->**Interfaces**->**Statistics** menu, current values and activities of all device interfaces are displayed.

With the filter bar, you can select whether to display **Transfer Totals** or **Transfer Throughput**. The values per second are shown on the **Transfer Throughput** display.

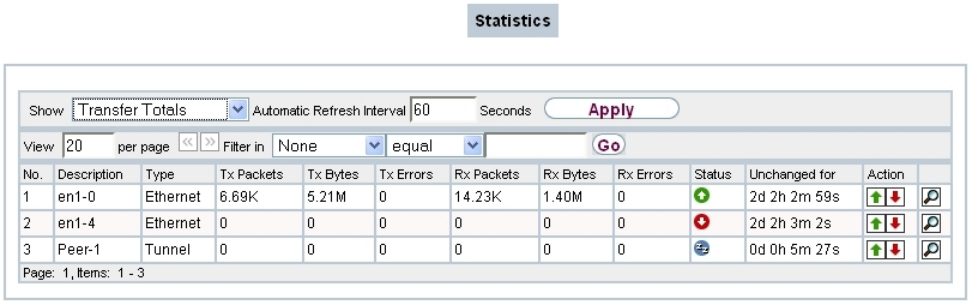


Fig. 186: **Monitoring->Interfaces->Statistics**

Change the status of the interface by clicking the or the button in the **Action** column.

Values in the Statistics list

Field	Description
No.	Shows the serial number of the interface.
Description	Displays the name of the interface.
Type	Displays the interface text.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Tx Errors	Shows the total number of errors sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.
Rx Errors	Shows the total number of errors received.
Status	Shows the operating status of the selected interface.
Unchanged for	Shows the length of time for which the operating status of the interface has not changed.
Action	Enables you to change the status of the interface as displayed.

Click the button to display the statistical data for the individual interfaces in detail.

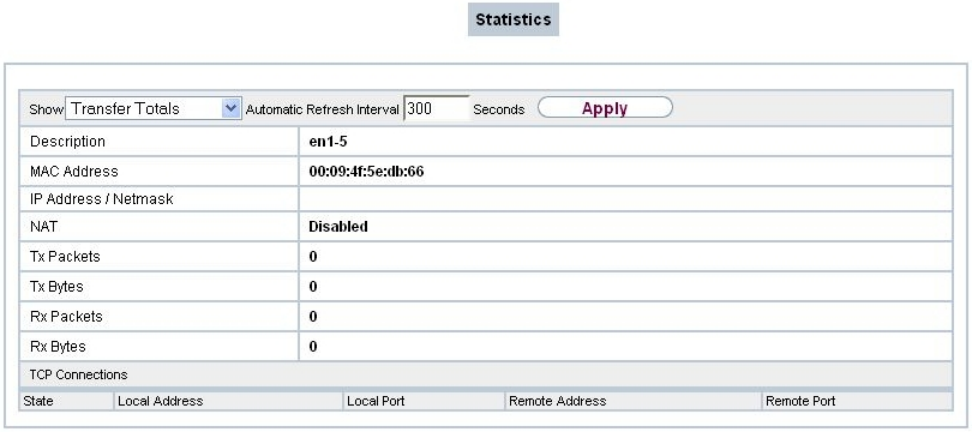


Fig. 187: **Monitoring->Interfaces->Statistics->**

Values in the Statistics list

Field	Description
Description	Displays the name of the interface.
MAC Address	Displays the interface text.
IP Address / Netmask	Shows the IP address and the netmask.
NAT	Indicates if NAT is activated for this interface.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.

Fields in the TCP Connections menu

Field	Description
Status	Displays the status of an active TCP connection.
Local Address	Displays the local IP address of the interface for an active TCP connection.
Local Port	Displays the local port of the IP address for an active TCP connection.
Remote Address	Displays the IP address to which an active TCP connection exists.
Remote Port	Displays the port to which an active TCP connection exists.

21.4 WLAN

21.4.1 WLANx

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

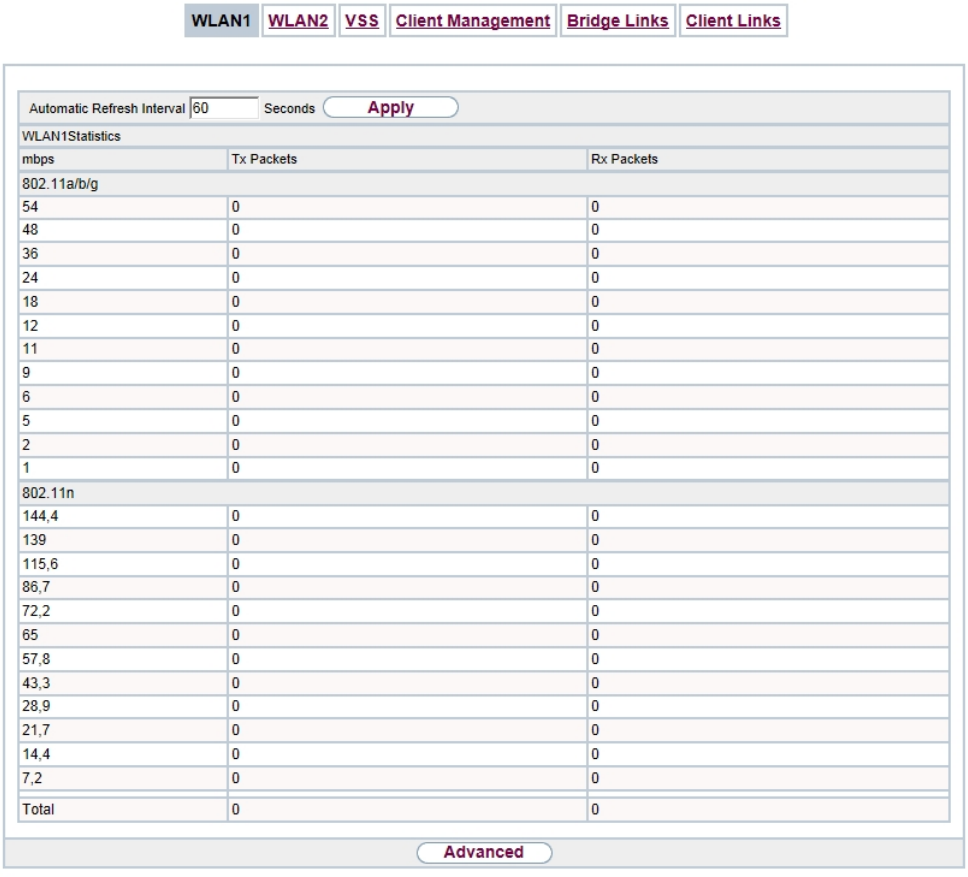


Fig. 188: **Monitoring->WLAN->WLAN**

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**.

Field	Description
Rx Packets	Shows the total number of received packets for the data rate shown in **mbps**.

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

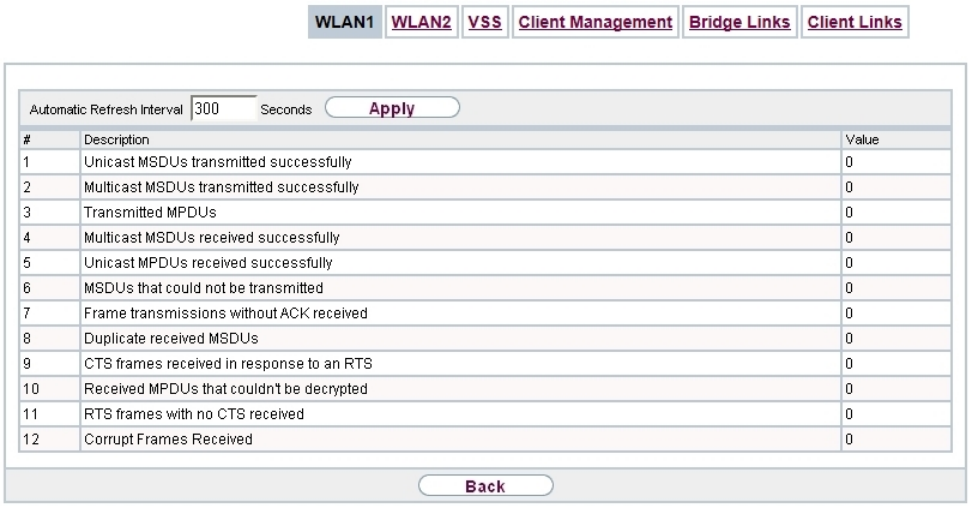


Fig. 189: **Monitoring->WLAN->WLAN->Advanced**

Values in the Advanced list

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

Meaning of the list entries

Description	Meaning
Unicast MSDUs transmitted successfully	Displays the number of MSDUs successfully sent to unicast addresses since the last reset. An acknowledgement was received for each of these packets.
Multicast MSDUs transmitted successfully	Displays the number of MSDUs successfully sent to multicast addresses (including the broadcast MAC address).
Transmitted MPDUs	Displays the number of MPDUs received successfully.
Multicast MSDUs received successfully	Displays the number of successfully received MSDUs that were sent with a multicast address.
Unicast MPDUs re-	Displays the number of successfully received MSDUs that were

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

21.4.2 VSS

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

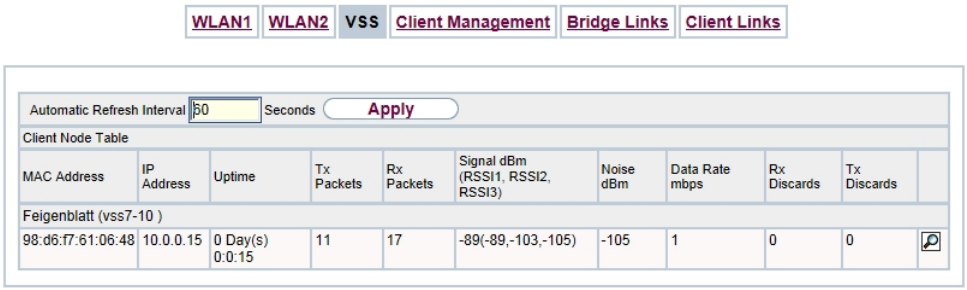


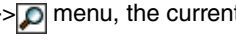
Fig. 190: **Monitoring**->**WLAN**->**VSS**

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.
Uptime	Shows the time in hours, minutes and seconds for which the cli-

Field	Description
	ent is logged in.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.
Signal dBm (RSSI1, RSSI2, 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.
Rx Discards	Displays the number of received data packets that have been discarded if the bandwidth for receive traffic has been limited in the **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)**->  menu using the field **Rx Shaping**
Tx Discards	Displays the number of data packets that were queued for transmission and have been discarded if the bandwidth for transmit traffic has been limited in the **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)**-> menu using the field **Rx Shaping**.

VSS - Details for Connected Clients

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

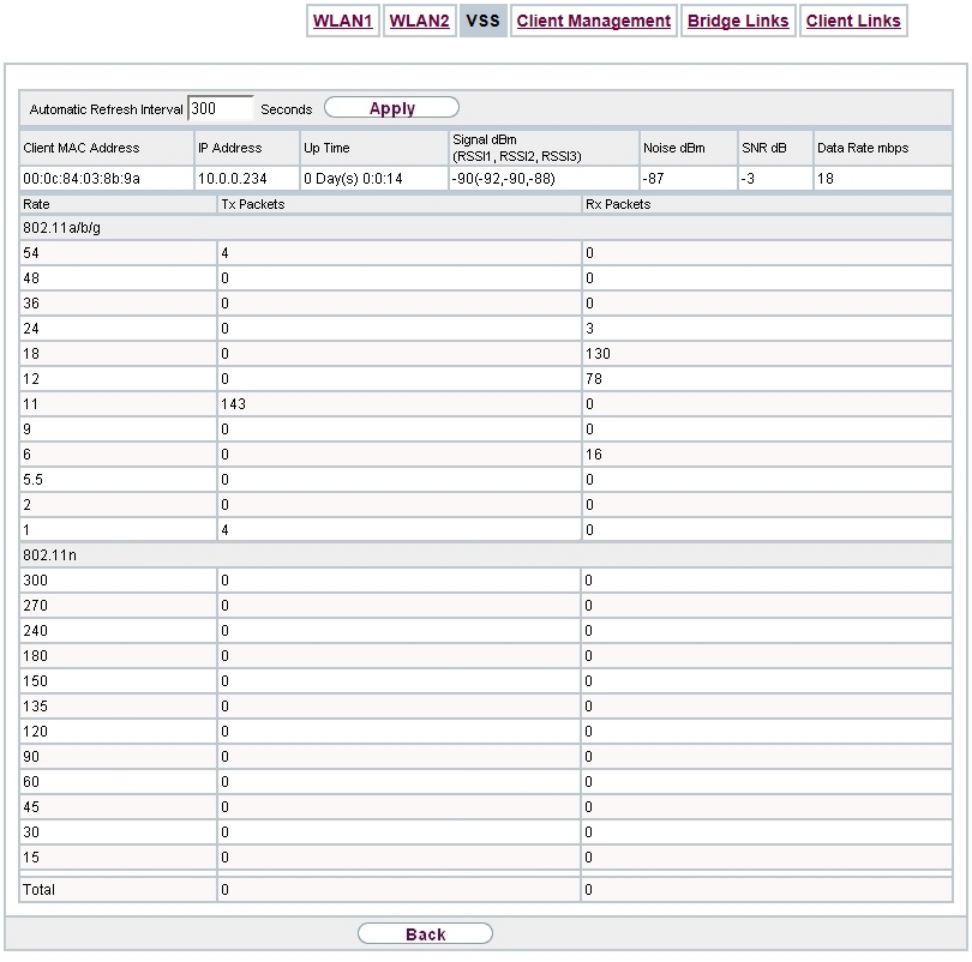


Fig. 191: **Monitoring->WLAN->VSS-><connected client>->**

Values in the list <Connected Client>

Field	Description
Client MAC Address	Shows the MAC address of the associated client.
IP Address	Shows the IP address of the client.
Uptime	Shows the time in hours, minutes and seconds for which the client is logged in.
Signal dBm(RSSI1, RSSI2, RSSI3)	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
SNR dB	Signal-to-Noise Ratio in dB is an indicator of the quality of the

Field	Description
	wireless connection. Values: • > 25 dB excellent • 15 – 25 dB good • 2 – 15 dB borderline • 0 – 2 dB bad.
Data Rate mbps	Shows the current transmission rate of data received by this client in mbps. The following clock rates are possible: IEEE 802.11b: 11, 5.5, 2 and 1 mbps; IEEE 802.11g/a: 54, 48, 36, 24, 18, 12, 9.6 Mbps. If the 5-GHz frequency band is used, the indication of 11, 5.5, 2 and 1 Mbps is suppressed for IEEE 802.11b.
Rate	Displays the possible data rates on the wireless module.
Tx Packets	Shows the number of sent packets for the data rate.
Rx Packets	Shows the number of received packets for the data rate.

21.4.3 Client Management

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

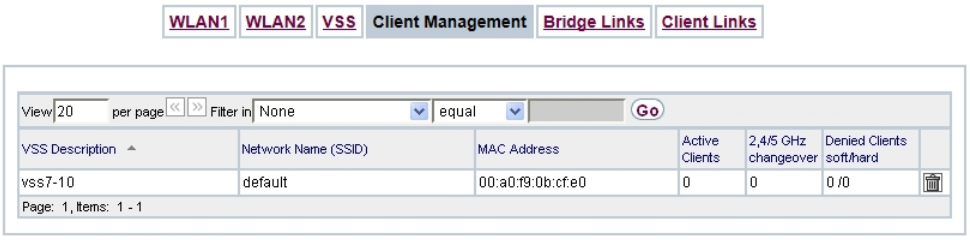


Fig. 192: **Monitoring->WLAN->Client Management**

Values in the list Client Management

Field	Description
VSS Description	Displays the unique description of the wireless network (VSS).
Network Name (SSID)	Displays the name of the wireless network (SSID).

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

21.4.4 Bridge Links

In the **Monitoring**->**WLAN**->**Bridge Links** menu, current values and activities of the bridge links are displayed.

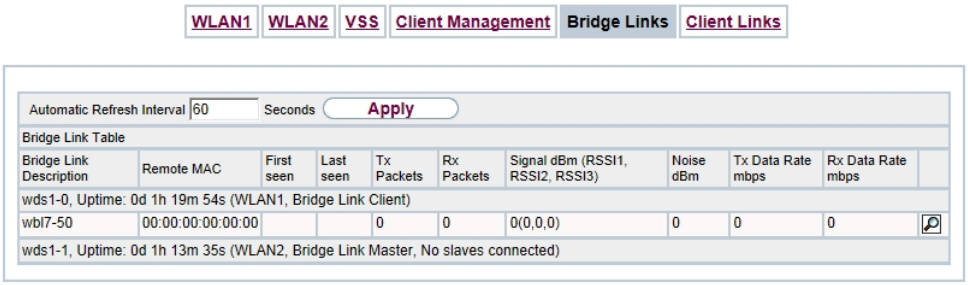


Fig. 193: **Monitoring**->**WLAN**->**Bridge Links**

Values in the Bridge Links list

Field	Description
Bridge Link Description	Shows the name of the bridge link.
Remote MAC	Shows the MAC address of the bridge link partner.
First seen	Displays the time of the first registered attempted contact of the bridge link partner.
Last seen	Displays the time of the last registered attempted contact of the bridge link partner.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.
Signal dBm (RSSI1, RSSI2, RSSI3)	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
Tx **Data Rate mbps**	Shows the current clock rate of data sent on this bridge link in

Field	Description
	Mbps.
Rx **Data Rate mbps**	Shows the current clock rate of data received on this bridge link in Mbps.
Uptime	Shows the time in hours, minutes and seconds for which the bridge link in question is active.

Bridge link details

You can use the icon to open an overview of further details of the bridge links.

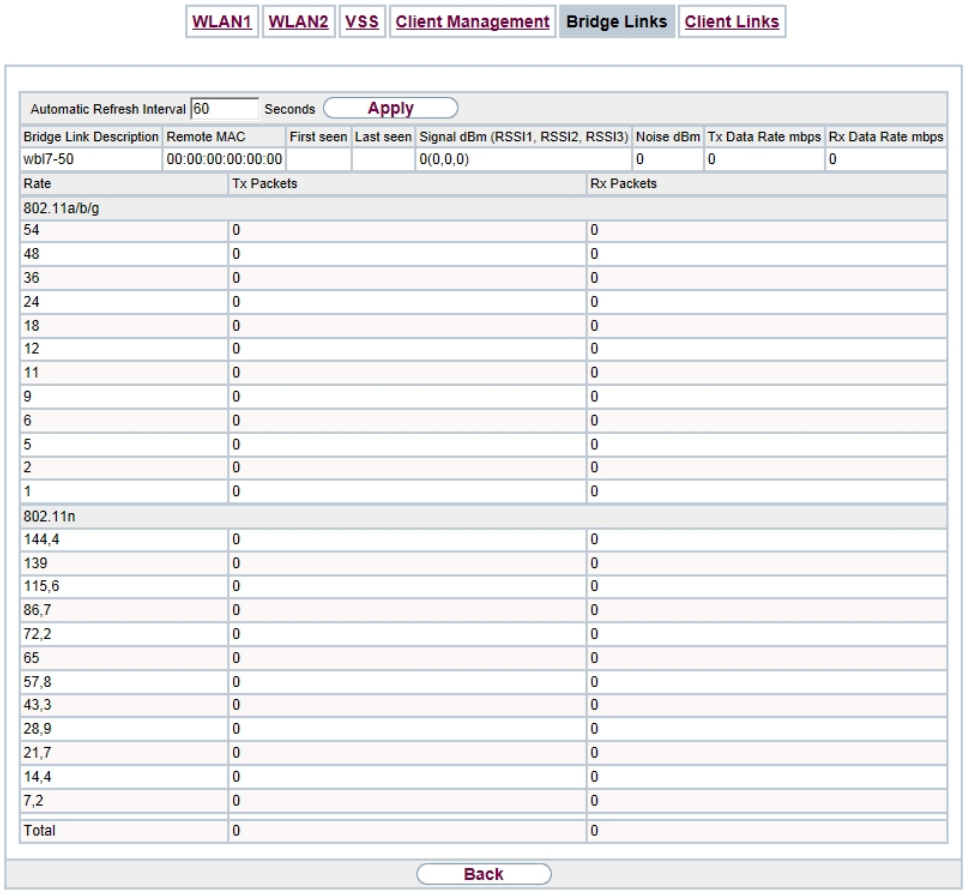


Fig. 194: **Monitoring->WLAN->Bridge Links->**

Values in the Bridge Links list

Field	Description
Bridge Link Description	Shows the name of the bridge link.
Remote MAC	Shows the MAC address of the bridge link partner.
First seen	Displays the time of the first registered attempted contact of the bridge link partner.
Last seen	Displays the time of the last registered attempted contact of the bridge link partner.
Signal dBm (RSSI1, RSSI2, RSSI3)	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
Tx **Data Rate mbps**	Shows the current clock rate of data sent on this bridge link in Mbps.
Rx **Data Rate mbps**	Shows the current clock rate of data received on this bridge link in Mbps.
Rate	For each of the specified data rates, displays the values for **Tx Packets** and **Rx Packets**.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.

21.4.5 Client Links

In the **Monitoring**->**WLAN**->**Client Links** menu, current values and activities of the configured client links are displayed.

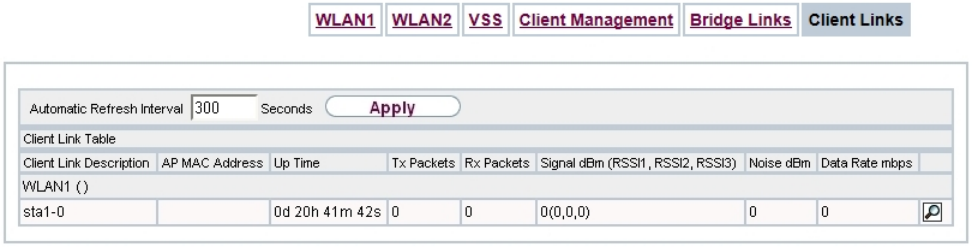


Fig. 195: **Monitoring**->**WLAN**->**Client Links**

Values in the Client Links list

Field	Description
Client Link Description	Shows the name of the client link.
AP MAC Address	Shows the MAC address of the client link partner.

Field	Description
Uptime	Shows the time in hours, minutes and seconds for which the client link in question is active.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.
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 clock rate of data received on this client link in Mbps.

Client Link Details

You can use the  icon to open an overview of further details of the client links.

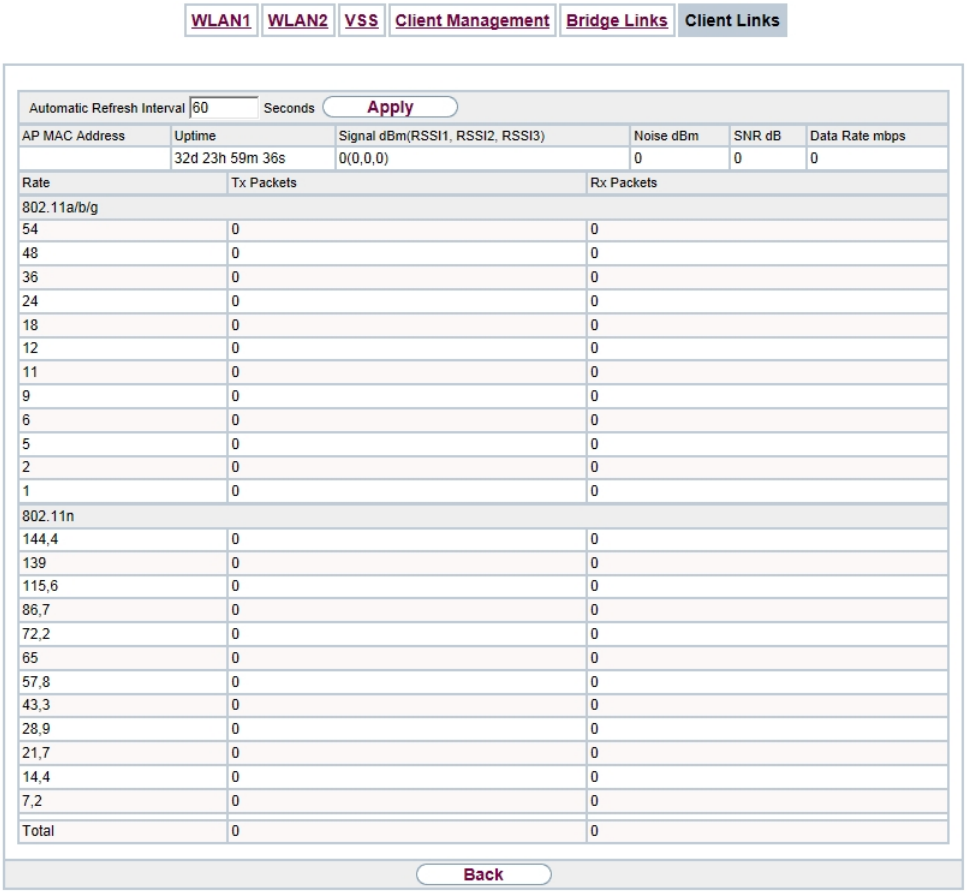


Fig. 196: **Monitoring->WLAN->Client Links->**

Values in the Client Links list

Field	Description
AP MAC Address	Shows the MAC address of the client link partner.
Uptime	Shows the time in hours, minutes and seconds for which the client link in question is active.
Signal dBm (RSSI1, RSSI2, RSSI3)	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
SNR dB	Shows the signal quality in dB.
Data Rate mbps	Shows the current clock rate of data received on this client link in Mbps.
Rate	For each of the specified data rates, displays the values for **Tx**

Field	Description
	Packets and **Rx Packets**.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.

21.5 Bridges

21.5.1 br<x>

In the **Monitoring**->**Bridges**-> **br<x>** menu, the current values of the configured bridges are shown.

Fig. 197: **Monitoring**->**Bridges**

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.

21.6 HotSpot Gateway

21.6.1 HotSpot Gateway

A list of all linked hotspot users is displayed in the **Monitoring**->**HotSpot Gateway**->**HotSpot Gateway** menu.

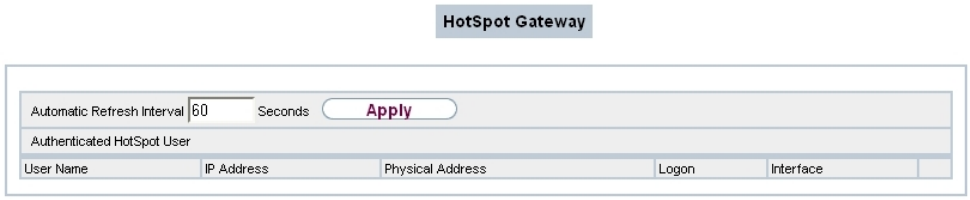


Fig. 198: **Monitoring->HotSpot Gateway->HotSpot Gateway**

Values in the HotSpot Gateway list

Field	Description
User Name	Displays the user's name.
IP Address	Shows the IP address of the user.
Physical Address	Shows the physical address of the user.
Logon	Displays the time of the notification.
Interface	Shows the interface used.

21.7 QoS

In the **Monitoring->QoS** menu, statistics are displayed for interfaces on which QoS has been configured.

21.7.1 QoS

A list of all interfaces for which QoS was configured is displayed in the **Monitoring->QoS->QoS** menu.

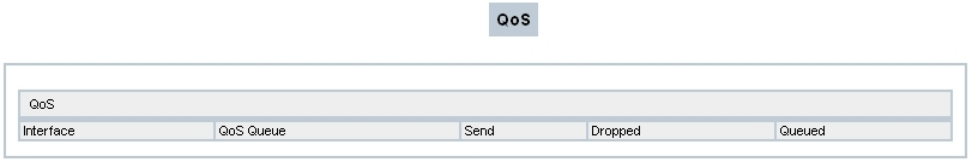


Fig. 199: **Monitoring->QoS->QoS**

Values in the QoS list

Field	Description
Interface	Shows the interface for which QoS has been configured.

Field	Description
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.

21.8 PIM

21.8.1 Global Status

The status of all configured PIM components is displayed in the **Monitoring**->**PIM**->**Global Status** menu.

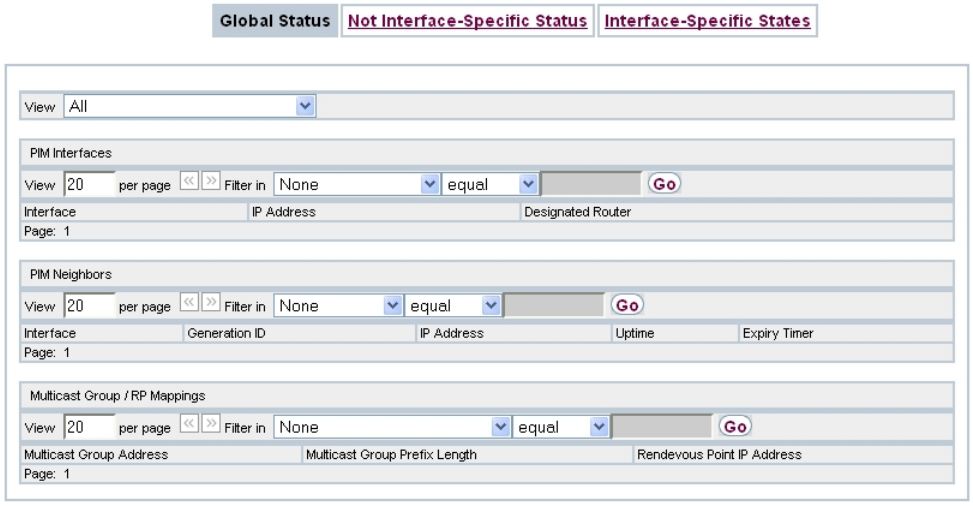


Fig. 200: **Monitoring**->**PIM**->**Global Status**

Values in the Global Status list

Field	Description
View	Select the desired view from the dropdown menu. Are available: *All*, *PIM Interfaces*, *PIM Neighbors* and

Field	Description
	Multicast Group / RP Mappings

Values in the PIM Interfaces list

Field	Description
Interface	Displays the name of the PIM interface.
IP Address	Displays the primary IP address of the PIM interface.
Designated Router	Displays the primary IP address of the designated router on this PIM interface.

Values in the PIM Neighbors list

Field	Description
Interface	Displays the interface via which the PIM Neighbor is reached.
Generation ID	Displays the ID of the neighbor gateway.
IP Address	Displays the primary IP address of the PIM Neighbor.
Uptime	Indicates how long the last PIM Neighbor is a neighbor of the local router.
Expiry Timer	Indicates when the PIM Neighbor is no longer entered as neighbor. If the value *0* is displayed, the PIM Neighbor always remains entered as neighbor.

Values in the Multicast Group / RP Mappings list

Field	Description
Multicast Group Address	Displays the multicast group address.
Multicast Group Prefix Length	Displays the related network mask.
Rendezvous Point IP Address	Displays the IP address of the Rendezvous point.

21.8.2 Not Interface-Specific Status

The menu **Monitoring**->**PIM**->**Not Interface-Specific Status** includes status information for all PIM interfaces.

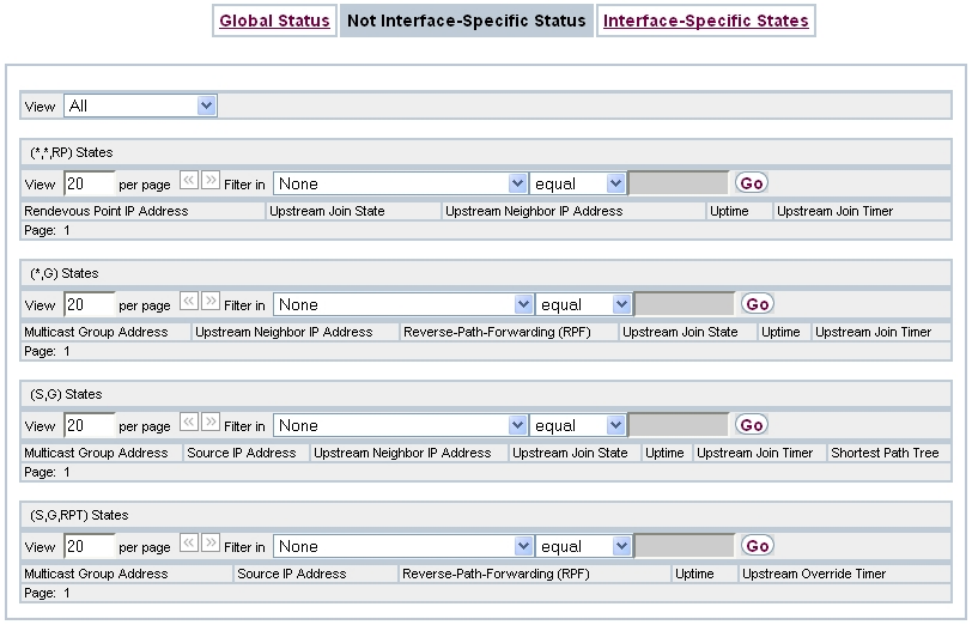


Fig. 201: **Monitoring->PIM->Not Interface-Specific Status**

Values in the Not Interface-Specific Status list

Field	Description
View	Select the desired view from the dropdown menu. Are available: *All*, *(*,*,RP) States*, *(*,G) States*, *(S,G) States* and *(S,G,RPT) States*

Values in the (*,*,RP) States list

Field	Description
Rendezvous Point IP Address	Displays the IP address of the Rendezvous Point (RP) for the group.
Upstream Join State	The Upstream (*,*,RP) Join/Prune Status indicates the status of the Upstream (*,*,RP) State Machine in the PIM-SM Specification.
Upstream Neighbor IP Address	Displays the primary IP address of the Upstream Neighbors, or unknown (0) if the Upstream Neighbor IP address is not known, or if it is not a PIM Neighbor.
Uptime	Indicates the timespan of the RP's existence.

Field	Description
Upstream Join Timer	Join/Prune Timer is used to periodically send Join(*,*,RP) messages, and to correct Prune(*,*,RP) messages from peers on an Upstream LAN interface.

Values in the (*,G) States list

Field	Description
Multicast Group Address	Displays the multicast group address.
Upstream Neighbor IP Address	Displays the primary IP address of the Neighbor on pimStarGRPFIfIndex, to which the local router periodically (*,G) sends Join messages. The InetAddressType is defined through the pimStarGUpstreamNeighborType. In the PIM-SM specification, this address is named RPF'(*,G).
Reverse-Path-Forwarding (RPF)	Indicates the address type of the RPF Next Hop to the RP, or unknown(0), if the Next Hop is not known.
Upstream Join State	Indicates whether the local router should join the group's RP Tree. This corresponds to the status of the Upstream (*,G) State Machine in the PIM-SM specification.
Uptime	Indicates the timespan since the entry was generated by the local router.
Upstream Join Timer	Indicates the remaining time until the local router sends out the next periodic (*,G) Join message on pimStarGRPFIfIndex. In the PIM-SM specification, this address is named (*,G) Upstream Join Timer. If the timer is deactivated, it has the value `0`.

Values in the (S,G) States list

Field	Description
Multicast Group Address	Displays the multicast group address. InetAddressType is defined in the pimSGAddressType object.
Source IP Address	Displays the source IP address. InetAddressType is defined in the pimSGAddressType object.
Upstream Neighbor IP Address	Displays the primary IP address of the Neighbor on pimSGRPFIfIndex, to which the router periodically (S,G) sends Join messages. The value is `0`, if the RPF Next Hop is unknown or is no PM Neighbor. InetAddressType is defined in the pimSGAddressType object. In the PIM-SM specification, this address is named RPF'(S,G).
Upstream Join State	Indicates whether the local router should join the Shortest-Path-Tree for the source and the group represented by this

Field	Description
	entry. This corresponds to the status of the Upstream (S,G) State Machine in the PIM-SM specification.
Uptime	Indicates the timespan since the entry was generated by the local router.
Upstream Join Timer	Indicates the remaining time until the local router sends out the next periodic (S,G) Join message on pimSGRPFIfIndex. In the PIM-SM specification, this timer is named (S,G) Upstream Join Timer. If the timer is deactivated, it has the value *0*.
Shortest Path Tree	Indicates whether the Shortest Path Tree Bit is set, i.e. whether forwarding via the Shortest Path Tree should take place.

Values in the (S,G,RPT) States list

Field	Description
Multicast Group Address	Displays the multicast group address. InetAddressType is defined in the pimStarGAddressType object.
Source IP Address	Displays the source IP address. InetAddressType is defined in the pimStarGAddressType object.
Reverse-Path-Forwarding (RPF)	Indicates the address type of the RPF Next Hop to the RP, or unknown(0), if the RPF Next Hop is not known.
Uptime	Indicates the timespan since the entry was generated by the local router.
Upstream Override Timer	Indicates the remaining time until the local router sends out the next Triggered (S,G, rpt) Join message on pimSGRPFIfIndex. In the PIM-SM specification, this timer is named (S,G, rpt) Upstream Override Join Timer. If the timer is deactivated, it has the value *0*.

21.8.3 Interface-Specific States

The menu **Monitoring**->**PIM**->**Interface-Specific States** includes interface-specific status information.

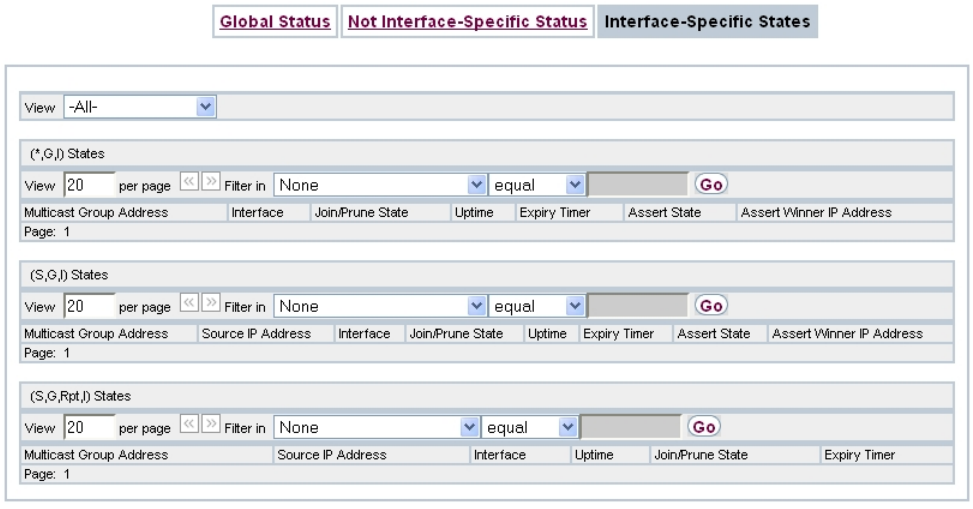


Fig. 202: **Monitoring->PIM->Interface-Specific States**

Values in the Interface-Specific States list

Field	Description
View	Select the desired view from the dropdown menu. Are available: `All`, `(*,G,I) States`, `(S,G,I) States` and `(S,G,RPT) States`

Values in the (*,G,I) States list

Field	Description
Multicast Group Address	Displays the multicast group address. InetAddressType is defined in the pimStarGAddressType object.
Interface	Displays the name of the interface.
Join/Prune State	Indicates the status that results from the (*,G) Join/Prune messages received on this interface. This corresponds to the status of the Downstream Per-Interface (*,G) State Machine in the PIM-SM specification.
Uptime	Indicates the timespan since the entry was generated by the local router.
Expiry Timer	Displays the remaining time until the (*,G) Join State becomes invalid for this interface. In the PIM-SM specification, this address is named (*,G) Join Expiry Timer. If the timer is deactivated, it has the value `0`. The value 'FFFFFFFF'h stands for infinite.

Field	Description
Assert State	Displays the (*,G) Assert State for this interface. This corresponds to the status of the Per-Interface (*,G) Assert State Machinen in the PIM-SM specification. If pimStarGPimMode is 'bidir', this object must 'noInfo' be.
Assert Winner IP Address	Indicates the address of Assert Winner, if pimStarGIAssertState runs 'iAmAssertLoser'. InetAddressType is defined through the object pimStarGIAssertWinnerAddressType.

Values in the (S,G) States list

Field	Description
Multicast Group Address	Displays the multicast IP address. InetAddressType is defined through the object pimSGAddressType.
Source IP Address	Displays the source IP address. InetAddressType is defined through the object pimSGAddressType.
Interface	Displays the name of the interface.
Join/Prune State	Indicates the status that results from the (S,G) Join/Prune messages received on this interface. This corresponds to the status of the Downstream Per-Interface (S,G) State Machine in the PIM-SM and PIM-DM.
Uptime	Indicates the time remaining before the local router reacts to an (S,G) Prune message received on this interface. The router waits this period to check whether another downstream router corrects the Prune message. In the PIM-SM specification, this timer is named (S,G) Prune-Pending Timer. If the timer is deactivated, it has the value `0`.
Expiry Timer	Displays the remaining time until the (S,G) Join State becomes invalid for this interface. In the PIM-SM specification, this timer is named (S,G) Join Expiry Timer . If the timer is deactivated, it has the value `0`. The value 'FFFFFFFF'h stands for infinite. In the PIM-DM specification, this timer is named (S,G) Prune Timer.
Assert State	Displays the (S,G) Assert State for this interface. This corresponds to the status of the Per-Interface (S,G) Assert State Machine in der PIM-SM Specification See "I-D.ietf-pim-sm-v2-new section 4.6.1"
Assert Winner IP Address	Indicates the address of Assert Winner, if pimStarGIAssertState runs 'iAmAssertLoser. InetAddressType is defined through the object pimSGIAssertWinnerAddressType.

Values in the (S,G,RPT) States list

Field	Description
Multicast Group Address	Displays the multicast IP address. InetAddressType is defined through the object pimSGAddressType.
Source IP Address	Displays the source IP address. InetAddressType is defined through the object pimStarGAddressType.
Interface	Displays the name of the interface.
Uptime	Indicates the timespan since the entry was generated by the local router.
Join/Prune State	Indicates whether the local router should sever the source of the RP tree. This corresponds in the PIM-SM specification to the status of the Upstream (S,G,rpt) State Machine for Triggered Messages.
Expiry Timer	Displays the remaining time until the (S,G, rpt) Prune State becomes invalid for this interface. In the PIM-SM specification, this timer is named (S,G, rpt) Prune Expiry Timer. If the timer is deactivated, it has the value `0`. The value 'FFFFFFFF'h stands for infinite. In the PIM-DM specification, this timer is named (S,G) Prune Timer.

Glossary

2G See GSM.

3DES See DES.

3G See UMTS.

4G See LTE.

802.11 The 802.11 norm describes wireless LAN (WLAN). There are a variety of amendments: 802.11a: Gross data transfer rates: 54 Mbit/s, frequency band: 5 GHz, 802.11b/g: Gross data transfer rates: 11 Mbit/s, frequency band: 2.4 GHz, 802.11g: Gross data transfer rates: 54 Mbit/s, frequency band: 2.4 GHz, 802.11n: Gross data transfer rates: 600 Mbit/s, frequency band: 2.4 GHz (optional: 5 GHz)

Access client Client mode is an operating mode of a wireless access point (AP) in which the latter behaves like a wireless adapter vis-a-vis the higher level AP. With an AP run in client mode, individual computers or entire sub-networks can be connected to higher level networks.

Access point An access point (AP) is a device for wirelessly connecting clients (computers). The AP thus serves to create a wireless network (WLAN) and connect that WLAN to a wired Ethernet network (bridging).

Accounting Accounting refers to the recording of connection data, e.g. date, time, connection duration, charging information and number of data packets transferred.

Activity monitor The activity monitor is used to oversee the status of physical and virtual device interfaces.

Ad-hoc network In an ad-hoc network, individual clients connect to an independent wireless LAN via a wireless adapter. Ad-hoc networks work independently, with no access point on a peer-to-peer basis. The ad-hoc mode is also referred to as IBSS (Independent Basic Service Set) mode and is useful in very small networks, e. g. when linking two notebooks with no access point.

ADSL Asymmetric digital subscriber line. See DSL.

AES Advanced Encryption Standard (AES, Rijndael) is an encryption method (see Cipher). AES uses a fixed block length of 128 bits. The

key length is 128, 192 or 256 bits. AES is a very fast and secure algorithm.

Aggressive mode When an IPSec connection is being established, aggressive mode is used to implement a phase 1 exchange. Aggressive mode offers no identity protection for negotiating nodes, since they have to transmit their identity before they can establish a secure channel. See also Main mode.

AH The authentication header (AH) is used with IPSec to ensure the authenticity and integrity of the packets transmitted and to authenticate the sender.

Annex A Annex A is a DSL variant which occurs in connection with analogue telephone connections, e. g. in France.

Annex B Annex B is a DSL variant which occurs in connection with ISDN, e. g. in Germany.

Annex J Annex J is a DSL variant purely for data transmission, with no voice data (unbundled connection). Annex J is an extension of specification G.992. These DSL connections require no splitter and have a greater range and faster transmission speed.

Annex L Annex L is an extension of Annex A. The range is increased at the expense of the data transmission rate.

Annex M Annex M is an extension of Annex A. The upstream is increased at the expense of the downstream.

ANSI T1.413 ANSI T1.413 is an ADSL variant.

ARP The Address Resolution Protocol (ARP) supplies the associated MAC addresses to IPv4 addresses. The information required is shared between the network nodes, stored in the device's cache, and deleted again after the ARP lifetime has expired. For IPv6 this functionality is provided by the Neighbor Discovery Protocol (NDP).

ATM Asynchronous Transfer Mode (ATM) is a data transmission technology in which the data traffic is coded in small packets – called cells or slots – with a fixed length and is transmitted via asynchronous time multiplexing.

Authentication Check on the user's identify.

Authorisation Based on their identity (authentication), the user can access certain services and resources.

AUX AUX is a signal input for external devices, e. g. analogue or GSM modems.

B channel See Basic Rate Interface and Primary Rate Interface.

Back Route Verify If a Back Route Verify is activated for an interface, incoming data packets are only accepted over this interface if outgoing response packets are routed over the same interface.

Backbone area The core area of a network which connects all the sub-networks (areas) with one another is known as the backbone.

Basic Rate Interface The Basic Rate Interface is a network connection to the ISDN. This type of connection is often abbreviated to BRI. A basic rate interface includes two basic channels (B channels) each with 64 kbps and one control and signalling channel (D channel) with 16 kbps. There are two operating modes for the Basic Rate Interface: Point-to-point ISDN and Point-to-multipoint The Primary Rate Interface (PRI) is used with larger installations.

Beacon The central access point sends beacons to create a wireless LAN in infrastructure mode. These messages contain the network name (SSID), a list of the supported transmission rates and the type of encryption.

Bit A binary digit (bit) is the smallest unit of data in computing technology. Signals are represented in the logical states "0" and "1".

Black / White List Entries in the Black List are blocked, entries in the White List are allowed through. (Example: Any telephone number beginning with 01234 is blocked in the Black List. The number 01234987 can nonetheless be approved in the White List.)

Blowfish Blowfish is an encryption method (see Cipher). Blowfish uses a fixed block length of 64 bits. The key length can be between 32 and 448 bits.

BootP The Bootstrap Protocol (BootP) is used to automatically issue an IP address.

Bps Bits per second. A unit of measure for the transmission rate.

BRI See Basic Rate Interface

Bridge A bridge is a network component for connecting the same types of network at Level 2 of the OSI model. Data packets are transmitted using MAC addresses. The use of bridges divides up the network

	and reduces the load.
Broadcast	In a broadcast, data packets are sent from one point to all the subscribers in a network, e. g. if the recipient is not yet known. Examples of this are the ARP and DHCP protocols. The communication is via broadcast addresses: MAC networks: FF:FF:FF:FF:FF:FF, IPv4 networks: 255.255.255.255, IPv6 networks: ff00::/8
BRRP	BRRP is an implementation of the Virtual Router Redundancy Protocol (VRRP). The aim of the method is to compensate for the failure of the default gateway. Multiple routers are combined to form one virtual router. If one of these routers falls over, the others are able to replace it.
CA	Certificate Authority. See Certificate.
Cache	The device temporarily stores data used in name resolution in the cache. See also ARP.
Called party number	The number of the party being phoned.
Calling party number	The number of the calling terminal.
CAPI	The Common ISDN Application Programming Interface (CAPI) is a programming interface for ISDN. It enables application programs to access ISDN hardware from a PC. See also TAPI.
CAPWAP	Control And Provisioning of Wireless Access Points Protocol (CAPWAP) is used to have wireless access points (slaves) monitored by a WLAN controller (master). It uses UDP port 5246 for monitoring and 5247 to send data.
CAST	CAST is an encryption method (see Cipher). CAST uses a fixed block length of 64 bits. The key length can be between 40 and 128 bits. Alternative names are CAST-128 and CAST5.
Certificate	A certificate identifies a person, an institution, a device or an application. A public key certificate is a digital certificate and it creates a connection between the identity and a public key. Certificates with public keys are issued by a certification authority (CA). Certificates that can no longer be trusted may be revoked using certificate revocation lists (CRLs)
Channel	A wireless channel is a frequency band used for wireless LAN. Devices that send on adjacent channels disrupt one another.

Channel bundling When channels are bundled, the B channels in an ISDN connection are combined to increase data throughput.

CHAP The Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol for PPP connections. As well as the standard CHAP, Microsoft also has the variants MS-CHAPv1 and MS-CHAPv2. You dial into a network via PPP and you authenticate yourself with a username and password. The username and password are transmitted encrypted. See also PAP.

Cipher A block cipher is an encryption algorithm. In this encryption method, a data block of a fixed size (normally 64 bit) is rewritten to a block of the same size using a so-called key. The longer the key, the more secure the algorithm.

Client A client uses the services provided by a server. Clients are usually workstations.

Configuration The configuration refers to all of a device's settings. It is stored internally, in MIB tables. This data can be backed up, loaded and deleted externally. The configuration is edited using the HTTP(S) user interface, an SNMP client or connected telephones.

CoS The term Class of Service (CoS) means different things depending on the area in which it is applied. In telecommunications CoS refers to the permission class assigned to the user. The permission class defines the user's rights, e. g. exchange access right, features that can be used, access to applications, ... In network technology CoS refers to the classification of certain services as per IEEE 802.1p. CoS enables priorities to be set in a targeted way, while Quality of Service (QoS) is used to set up explicit bandwidth guarantees or restrictions. Data packets are classified using a DSCP (Differentiated Services Code Point) value.

CRC Cyclic Redundancy Check (CRC) is a method of detecting errors in the data transmission.

CRL See Certificate.

D channel See Basic Rate Interface and Primary Rate Interface.

Daemon A daemon refers to a program that runs in the background and provides certain services.

Data compression Data compression is a method of reducing the data volume transmitted. See STAC and MPPC.

Datagram A datagram is a self-contained data entity with user and control data. It generally stands for the terms data frame, data packet and data segment.

DCN DCN stands for data communication network.

Dead Peer Detection In IPSec, Dead Peer Detection is used to identify IKE peers that can no longer be accessed.

Default gateway All the data traffic which is not intended for one's own network is sent to the default gateway (default router).

Default route See Standard route

Default route The default route is used when no other suitable route is available.

Default router See Default gateway.

Deffie-Hellman Diffie-Hellman is a public key algorithm for negotiating and establishing keys. Because data is neither encrypted nor signed, the method is only secure if the connecting partners authenticate themselves using other mechanisms such as RSA and DSA.

Denial-Of-Service Attack In a Denial-Of-Service Attack (DoS), a network component is flooded with queries so that it becomes totally overloaded. As a result, the system or a particular service can no longer function.

DES The Data Encryption Standard (DES) is an encryption method (see Cipher). DES uses a fixed block length of 64 bits. The key length is 56 bits. Triple DES or 3DES is based on using DES three times (three different, independent keys).

DHCP The Dynamic Host Configuration Protocol (DHCP) allows IP addresses to be assigned dynamically. A DHCP server allocates each client in a network an IP address from a defined address pool. The clients need to be configured accordingly.

Dialup connection When required, a dialup connection is established by dialling a phone number, in contrast to a fixed connection (see Leased line) which is permanently enabled.

DIME Desktop Internetworking Management Environment (DIME) is used to configure and monitor gateways.

Direct dial exception See Point-to-point ISDN access and Direct dial-in (VoIP).

Direct dial-in (VoIP) Direct dial-in is a VoIP connection that is also known as point-

	to-point. It is used to connect a PBX. A main phone number and a number block are issued. Each of the numbers in the number block is called a direct dial exception. (Example: Main number 1234, number block: 1 - 99, numbers of the individual extensions: 1234-1, 1234-2, 1234-3, …)
Direct dialling range	See number block in Point-to-point ISDN access and Direct dial-in (VoIP)
DNS	The Domain Name System (DNS) is used to convert the domain name (e. g. www.example.org) to an IP address (name resolution).
Domain	A domain is a contiguous sub-set of the DNS (e. g. example.org).
Downstream	The gateway receives the data from a higher-level network and forwards it to its connected network.
DSA	The Digital Signature Algorithm (DSA) is used to create digital signatures and encrypt data packets. Signatures can be used to verify changes made to the information in the data packet. DSA is used for public-key cryptography (IPSec). See also RSA. Key generation is quicker with DSA than with RSA, but key processing is slower.
DSCP	Data packets can be marked with a Differentiated Services Codepoint (DSCP). DSCP values classify data packets in such a way that important packets can be routed through the network more quickly. See also QoS.
DSL modem	See Modem.
DSS1	Digital Subscriber Signalling System No. 1 (DSS1) is a signalling protocol for the D channel in the ISDN. It is also known as Euro ISDN.
DTIM	A Delivery Traffic Indication Message informs the clients that multicast or broadcast data is available at the access point.
Dynamic IP address	In contrast to a static IP address, a dynamic IP address is assigned temporarily by DHCP. Network components such as the web server or printer usually have static IP address, while clients such as notebooks or workstations usually have dynamic IP addresses.
DynDNS	A DynDNS provider can be used to link a domain name with a dynamically changing IP address.
Encapsulation	Encapsulation of data packets is a particular protocol to transmit the data packets in a network. See also VPN.

Encryption Refers to the encryption of data, e.g. using MPPE.

ESP Encapsulating Security Payload (ESP) is a protocol for IPSec. It uses protocol number 50 and supports data encryption and authentication.

Ethernet Ethernet is a specification for cable data networks. Ethernet works on the first and second layer of the OSI model.

Euro ISDN Standard ISDN in Europe, based on the DSS1 signalling protocol.

Eurofile transfer Eurofile transfer (EFT) is a protocol for sharing files over ISDN.

Extension number See Point-to-point ISDN access and Direct dial-in (VoIP).

Filter A filter comprises a number of criteria (e.g. protocol, port number, source and destination address). If these criteria match a data packet, the data packet can be subjected to a particular action (forward, reject, ...). This creates a filter rule.

Filter rule A rule that defines which data packets should or should not be transmitted by the gateway.

Firmware The firmware (system software) is programming code that is permanently embedded in the device. It provides the device's functions.

Fragmentation If the overall length of the data packet is greater than the Maximum Transmission Unit (MTU) of the network interface, the data packet has to be broken down into multiple physical data blocks using IP fragmentation. The reverse process is known as reassembly.

Frame A data frame is an information unit (Protocol Data Unit) in the data link layer in the OSI model.

Frame relay Frame relay is a data transmission technology and upgrade of X.25 (smaller packets, less error checking). Frame relay is primarily used for GSM networks.

FTP The File Transfer Protocol (FTP) regulates data transmission in IP networks. It regulates the exchange between FTP server and client.

Full-duplex With full-duplex, data can be sent and received simultaneously over a line.

G.991.1 Data transmission recommendation for HDSL.

G.991.2 Data transmission recommendation for SHDSL.

G.992.1 Data transmission recommendation for ADSL. There are two country-specific versions: G.992.1 Annex A and G.992.1 Annex B. Data transfer rates: 12 Mbit/s (downstream), 1.3 Mbit/s (upstream)

G.992.2 Data transmission recommendation for ADSL (G.LITE / ADSL-Lite). There are two versions: G.992.2 Annex A and G.992.2 Annex B. Data transfer rates: 12 Mbit/s (downstream), 1.3 Mbit/s (upstream)

G.992.3 Data transmission recommendation for xDSL2. There are three variants: G.992.3 Annex A/B (G.DMT to ADSL2) with data transmission rates of 12 Mbit/s in the downstream and 1.0 Mbit/s in the upstream, G.992.3 Annex L (RE-ADSL2) with data transmission rates of 5 Mbit/s in the downstream and 0.8 Mbit/s in the upstream and G.992.3 Annex M (ADSL2) with data transmission rates of 12 Mbit/s in the downstream and 2.5 Mbit/s in the upstream.

G.992.4 Data transmission recommendation for ADSL2 with Annex A/B. Data transmission rates: 12 Mbit/s (downstream), 1.0 Mbit/s (upstream)

G.992.5 Data transmission recommendation for xDSL2+. There are three variants: G.992.5 Annex A/B (ADSL2+) with data transmission rates of 25 Mbit/s in the downstream and 1.0 Mbit/s in the upstream, G.992.5 Annex L (RE-ADSL2+) with data transmission rates of 25 Mbit/s in the downstream and 1.0 Mbit/s in the upstream and G.992.5 Annex M (ADSL2+) with data transmission rates of 25 Mbit/s in the downstream and 3.5 Mbit/s in the upstream.

G.993.1 Data transmission recommendation for VDSL. Data transmission rates: 52 Mbit/s (downstream), 16 Mbit/s (upstream)

G.993.2 Data transmission recommendation for VDSL2. Data transmission rates: 200 Mbit/s (downstream), 200 Mbit/s (upstream)

G.DMT See F.992.1.

G.Lite See F.992.2.

G.SHDSL See G.991.2.

Gateway The gateway is a network component for connecting different types of network.

GPRS General Packet Radio Service (GPRS) is the name for the packet-oriented service for transmitting data in GSM networks.

GRE Generic Routing Encapsulation (GRE) is a network protocol for en-

capsulating other protocols so that they can be transported via the Internet Protocol (IP) in the form of a tunnel (VPN). GRE uses protocol number 47.

GSM The Global System for Mobile Communications (GSM), also known as 2G, is a mobile communications standard. It achieves, along with GPRS, a specified max. data transmission rate of 171.2 kbit/s.

Half-duplex With half-duplex, data can only be sent and received back-to-back over a line.

Hash To ensure data integrity, the information needs to be protected from unauthorised manipulation while it is being transmitted. To ensure that this happens, every item of communication received has to match the information originally sent. Therefore erratic mathematical value functions (hash functions) are used to calculate checksums (hash values). These are encrypted and sent as a digital signature with the message. The recipient, in turn, checks the signature before opening the packet. If the signature and, thus, the content of the data packet has changed, the packet is discarded. The hash algorithms used most frequently are Message Digest Version 5 (MD5) and Secure Hash Algorithm (SHA1).

HDSL High Data Rate Digital Subscriber Line. See DSL.

Heartbeat A network's subscribers use heartbeats to signal that they are ready to receive.

Hop Hop is the term for the connection from one network node to the next.

Host A host is a computer system that provides its services to the network.

Host name The domain name of a host. See DNS.

Host route A host route is the name for the route to a single host.

Hotspot A hotspot is a public internet access point via WLAN or wired Ethernet.

HSDPA High Speed Downlink Packet Access (HSDPA, 3.5G, 3G+ or UMTS broadband) is a data transmission method in the UMTS mobile communications standard.

HTTP The HyperText Transfer Protocol (HTTP) is a protocol for transmitting HTML pages (web pages) between server and client. By default

it uses port 80.

HTTPS The HyperText Transfer Protocol Secure (HTTPS) is a protocol which protects against eavesdropping when transmitting HTML pages (web pages) between server and client. HTTPS is schematically identical to HTTP. SSL / TLS is used for additional data encryption. The standard port for HTTPS connections is 443.

Hyperchannel With a hyperchannel, multiple subscribers have access to the transmission medium. A subscriber can only transmit their data if no other subscriber is using the medium. A hyperchannel network is mainly used for short-range operation with top data rates.

ICMP The Internet Control Message Protocol (ICMP) is used to exchange information and error messages over IPv4. The version ICMPv6 exists for IPv6.

IGMP The Internet Group Management Protocol (IGMP) is used in IPv4 networks to organise multicast groups.

IKE The Internet Key Exchange Protocol (IKE) is used for automatic key management with IPSec connections. The IKE process runs in two phases. During phase 1, the IKE subscribers authenticate themselves to one another and establish a secure channel. In phase 2, the two IPSec subscribers negotiate the SAs. There are two versions of the IKE mechanism.

Infrastructure network In an infrastructure network the individual terminals (clients) form a wireless LAN via a central access point. This central access point may also be an agent in other networks.

IP The Internet Protocol (IP) is a network protocol and it is the basis for the Internet. It works on the network layer of the OSI model. The TCP and UDP protocols are based on IP. There are two versions, Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).

IP address IP addresses are used to navigate in an IP network, to unambiguously identify the source and destination. IPv4 addresses consist of 32 bits, IPv6 addresses of 128 bits. So, with IPv4 232, i.e. 4.294.967.296 addresses can be represented, with IPv6 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 addresses. Dotted decimal notation, e. g. 192.168.0.250, is used for IPv4. Hexadecimal notation, e. g. 2001:db8:85a3::8a2e:370:7344, is used for IPv6. See also netmask.

IPCP The Internet Protocol Control Protocol (IPCP) is used, in a similar way to DHCP, to configure a host with an IP address, gateway and DNS server, when a PPP network connection is being used. With the extension Robust Header Compression over PPP, the header can be compressed for faster data transmission. Similarly, in IPv6 networks, the functionality is provided by the Internet Protocol version 6 Control Protocol (IPV6CP).

IPSec IPSec (Internet Protocol Security) is a network protocol for encapsulating other protocols so that they can be transported via the Internet Protocol (IP) in the form of a tunnel (VPN). The protocol number for IPSec depends on the protocol used. The Authentification Header (AH) uses protocol number 51, while the Encapsulating Security Payload (ESP) uses number 50.

IPv6 See IP.

ISDN Integrated Services Digital Network (ISDN) is a data transmission standard that includes telephony, fax and data transmission. There are two ISDN connection variants: Basic Rate Interface and Primary Rate Interface.

ISDN address The ISDN address of an ISDN device comprises an ISDN number followed by other numbers that relate to the specific terminal.

ISDN login The ISDN login is used to remotely configure the device via SNMP. To do so, it needs to have a configured ISDN or wireless connection.

ISDN number The ISDN number is the network address of the ISDN interface.

ISDN router See Router.

ISP Internet Service Providers (ISPs) supply technical services for using the Internet.

ITU The International Telecommunication Union (ITU) coordinates the setting up and operating of telecommunications networks and services.

Keepalive Keepalive packets are used to check that the communication partner can be contacted.

Keepalive Keepalive is a mechanism for maintaining the network connection and for checking that the communication partner can be reached. Specific packets are usually sent to the network for this purpose.

L2TP The Layer 2 Tunneling Protocol (L2TP) is a network protocol for encapsulating other protocols so that they can be transported via the Internet Protocol (IP) in the form of a tunnel (VPN). By default, L2TP uses protocol number 1701. The architecture in an L2TP network consists of an L2TP access concentrator (LAC) which may also be permanently integrated into the client, and the L2TP network server (LNS). The LAC establishes the connections to the LNS and manages them. The authorisation is regulated using a network access server (NAS), which can be implemented in the LAC or LNS. The LNS is responsible for routing and controlling the packets received from the LAC. The user data itself is exchanged unencrypted, while control messages for maintaining the accessibility of the tunnel endpoints are transmitted securely.

LAC See L2TP.

LAN A Local Area Network (LAN) refers to a network that is geographically very limited and normally spans one building or a company head office.

Layer A layer refers to a layer in the OSI model.

LCP The Link Control Protocol (LCP) is used in PPP connections to automatically negotiate encapsulation, process limits for varying packet sizes, authenticate the connection partner, determine faulty links, identify connection faults and terminate the connection.

LDAP The Lightweight Directory Access Protocol (LDAP) regulates the communication between a client and the directory server. LDAP is used for sharing and updating directories, e. g. a phone book.

Lease time The lease time refers to the validity period of a dynamic IP address that a client has been given by a DHCP server.

Leased line See Leased line

Leased line A leased line is a permanent connection of two communication partners via telecommunications network.

LLC The Link Layer Control (LLC) regulates the media allocation at MAC level.

LNS See L2TP.

Load balancing With load balancing, data is sent via different interfaces in order to increase the overall bandwidth available. In contrast to Multilink, load balancing also functions with accounts with different providers.

Loopback In a loopback switch the sender and recipient are identical.

LTE Long Term Evolution (LTE), also known as 4G, is a mobile communications standard with a standardised maximum data transmission rate of 300 Mbit/s.

MAC address The Media Access Control address (MAC address) is the hardware address of the network adapter and is used to identify the device at the hardware level.

Main Mode When establishing an IPSec connection, main mode is used to implement a phase 1 exchange by setting up a secure channel. See also Aggressive mode.

Man-in-the-Middle attack In a Man-in-the-Middle attack, the attacker is physically or logically between the two communication partners and so is able to view, and even manipulate, the data traffic.

MD5 Message Digest Algorithm 5 (MD5) is a hash function that generates a 128 bit hash value (checksum). See also Hash.

Media gateway A media gateway converts the network type of digital voice, audio or image information. For example, the signals from an ISDN network can be converted to an IP network.

Metric The metric is a measure for the properties of the route. The fastest route has the lowest metric (costs). Simplified, this is connecting with the smallest number of node points (routers).

MIB The Management Information Base (MIB) describes the data that can be queried or modified via a network management protocol (e. g. SNMP). The MIB is a database that describes all the devices and functions in the network.

MLP The Multicast Listener Discovery (MLD) is used in IPv6 networks to organise multicast groups.

Modem A modem is an electronic device that converts digital signals to frequency signals in order to distribute data in a wired or wireless network.

MPDU The MAC Protocol Data Unit (MPDU) refers to a data packet, including management frames and fragmented MSDUs, exchanged wirelessly.

MPPC Microsoft Point-to-Point Compression (MPPC) is a method of data compression.

MPPE Microsoft Point-To-Point Encryption (MPPE) is used to encrypt data transmitted via PPP. It was developed by Microsoft and Cisco and specified as RFC 3078.

MS-CHAP The Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is a method of authentication. MS-CHAPv1 is intended for authenticating DCN connections and is largely the same as the standard CHAP. MS-CHAPv2 is an authentication method for PPTP connections (VPN).

MSDU A MAC Service Data Unit (MSDU) is a data packet that is exchanged at LLC level.

MSN See Multiple subscriber number

MSS The Maximum Segment Size (MSS) defines the maximum number of bytes that can be used as user data in a TCP segment. The MSS must be smaller than the Maximum Transmission Unit (MTU) to avoid fragmenting the IP packets.

MSS clamping MSS clamping reduces the Maximum Segment Size (MSS) in order to connect networks with different Maximum Transmission Units (MTU).

MTU The Maximum Transmission Unit (MTU) is the largest possible data unit that can be transmitted over a physical line.

Multicast With a multicast, data packets are sent from one point to particular subscribers in a network. In IPv4 this is controlled via the address range 224.0.0.0 to 239.255.255.255 and the IGMP protocol, while in IPv6 it is controlled by ff00::/8 addresses and ICMPv6.

Multilink With multilink, multiple interfaces (PPP, PPPoE, ...) are combined into a single virtual connection in order to increase the total bandwidth available.

Multiple subscriber number Multiple subscriber numbers are the individual phone numbers in the ISDN point-to-multipoint connection.

NAPT Network Address Port Translation (NAPT) is another term for PAT. See PAT.

NAT Network Address Translation (NAT) is used to replace the source and destination IP addresses of a data packet with others. This enables different networks to be connected to one another. See also PAT.

NBNS Like DNS, NetBIOS Name Service (NBSN) is used in centralised name resolution. See also WINS and DNS.

Netmask With IPv4 in connection with the IP address, the netmask, also network mask and subnet mask, defines the network by dividing the IP address into network and device parts and thus determining which addresses need to be routed. Example of a netmask: 255.255.255.0. With IPv6 one refers to prefix length.

Network address A network address is the address of the network as a whole. The network mask and prefix length divide the IP address into the network address and host address (device address). Example of a network address: 192.168.0.250/24

Network route The network route refers to the route to a particular network.

Network termination Network termination (NT) refers to a connection or operating type. A terminal is given access to a communication network at the NT interface (connection socket). The connector is called a TAE with an analogue connection, an NTBA with the basic ISDN connection, and NTPMGF with the ISDN Primary Rate Interface. In the NT operation, the gateway is connected to the PABX's external S0 and is an external exchange connection for it. See also TE.

NT See Network termination.

NTP The Network Time Protocol (NTP) is used to synchronise the time of day.

OAM OAM is a service for monitoring ATM connections.

OSI model The OSI model divides the flow of communication between the physical medium and the user level into layers. The requirements at each layer are met by relevant protocols.

OSPF OSPF is a dynamic routing protocol which is usually used in larger network installations as an alternative to RIP.

PAP The Password Authentication Protocol (PAP) is an authentication method for connections via PPP. Unlike with CHAP, the username and password are not sent encrypted.

PAT Port and Address Translation (NAT) is used to replace the source and destination IP addresses and source and destination ports of a data packet with others. This enables different networks to be connected to one another. See also NAT.

Peer A peer is the endpoint of a communication in the network.

Phase 1/2 See IKE.

PIM The Protocol Independent Multicast (PIM) enables the dynamic routing of multicast packets on the Internet.

Ping Ping is a diagnostic tool that can be used to check whether a particular host in an IP network can be contacted. A measurement is taken of the time interval between sending a data packet (ICMP(v6) echo request packet) and receiving a response packet sent back immediately. This enables the connection quality to be determined.

PKCS The Public-Key Cryptography Standards (PKCS) are standards for public key cryptography. The PKCS are designed for binary and ASCII data and are compatible with the X.509 standard. The public standards are PKCS #1, #3, #5, #7, #8, #9, #10, #11, #12 and #15. PKCS #10 describes the syntax for certification inquiries.

PKI A public key infrastructure (PKI) is used to issue, distribute and verify digital certificates for an encryption procedure.

PMTU The Path MTU (PMTU) describes the maximum packet size that can be transmitted along the entire connection route without needing to be fragmented.

Point-to-multipoint Point-to-multipoint connection is an ISDNB connection. It is used to connect ISDN terminals. Multiple subscriber numbers (MSNs) are provided. See also Point-to-point ISDN access

Point-to-multipoint See Single phone number (VoIP).

Point-to-point See Point-to-point ISDN access and Direct dial-in (VoIP).

Point-to-point connection number: See Point-to-point ISDN access

Point-to-point ISDN access Point-to-point ISDN access refers to an ISDN connection that is also called point-to-point. It is used to connect a PBX. A point-to-point number and a number block are issued. Each of the numbers in the number block is called a direct dial exception. (Example: Point-to-point connection number: 1234, number block: 1 - 99, numbers of the individual extensions: 1234-1, 1234-2, 1234-3, …) See also Point-to-multipoint connection.

Pool An address pool is a collection of IP addresses that can be assigned to the connected clients, e. g. by DHCP.

POP3 The Post Office Protocol Version 3 (POP3) is a transmission protocol which controls how a client accesses emails from an email server.

Port The port number is used to decide the service (telnet, FTP, ...) to which an incoming data packet should be sent.

PPP The Point-to-Point Protocol (PPP) is a standardised technology for setting up a direct connection between the network nodes via dial-up lines.

PPPoA The Point-to-Point-over-ATM Protocol (PPPoA) enables PPP data packets to be transported directly over an ATM network.

PPPoE The Point-to-Point-over-Ethernet Protocol (PPPoE) enables PPP data packets to be transported directly over an Ethernet network.

PPTP The Point-to-Point Tunneling Protocol (PPTP) is a network protocol for encapsulating other protocols so that they can be transported via the Internet Protocol (IP) in the form of a tunnel (VPN). PPTP uses protocol number 1723. The PPTP architecture is divided into two logical systems. The PPTP Access Concentrator (PAC) and the PPTP Network Server (PNS). The PAC is usually integrated into the Windows client. It establishes the connection to the PNS and manages it. The PNS is responsible for routing and controlling the packets received by the PNS.

Pre-shared key A pre-shared key (PSK) is a key for an encryption procedure. The parties shared the key's value beforehand.

Prefix See Network address

Prefix delegation In IPv6 networks, prefix delegation is used to assign the network address (prefix) to the router.

Prefix length See netmask.

PRI See Primary Rate Interface.

Primary Rate Interface The Primary Rate Interface is a network connection to the ISDN. This type of connection is often also called a PRI or S2Minterface. A Primary Rate Interface offers 30 user channels (B channels), each with 64 kbits/s, in Europe and 23 in the USA, one control channel (D channel) with 64 kbits/s and one synchronisation channel with 64 kbits/s in Europe and 8 64 kbits/s in the USA. See also Basic Rate Interface.

Proposal When an IPSec connection is being established, the initiator of the connection makes proposals with relation to the authentication and encryption methods to be used.

Protocol Protocols regulate the flow of a data communication on different levels of the OSI model. Protocols control addressing, coding, authentication, formatting, etc. Examples: Ethernet, IP, TCP, HTTP

Proxy A proxy is a network component. The proxy is an agent. It routes a query from the source with its own IP address to the destination.

PVID The Port VLAN Identifier (PVID) is the standard VLAN ID for the port concerned. A packet that reaches this port without a VLAN tag is assigned this ID.

Q-SIG Q-Interface Signalling Protocol (Q-SIG) is an ISDN-based signalling protocol for linking PABX systems.

QoS Quality of Service (QoS) describes the properties of the communication service. It is defined using bandwidth, delay, packet losses and jitter. To transmit time-critical data packets for VoIP or video streaming as quickly as possible, QoS is used to sort all the data packets into groups and forward them on in the network either more quickly or slowly, depending on their priority.

Queue The data packets accumulate in a queue before they are sent.

RADIUS Remote Authentication Dial-In User Service (RADIUS) is a client-server protocol for authenticating, authorising and accounting for users with dial-in connections. The RADIUS server authenticates the client, e. g. by checking the username and password. See also TACACS+.

RE-ADSL2 See G.992.5.

Real Time Jitter Control Real Time Jitter Control is used, where necessary, to reduce the size of data packets during a telephone conversation so that voice packets are not blocked.

Registrar The SIP server (registrar) needs to be used in case the subscribers to a VoIP call are not using static IP addresses The SIP server registers the clients' IP addresses and sends this data to the SIP proxy, which connects the calls. The SIP proxy and SIP registrar are usually identical.

Repeater A repeater is a device that strengthens electric or optical signals and thus increases the range of the network.

Reset	This returns the device to its unconfigured state.
RFC	A Request For Comments (RFC) is a document that describes the standards and guidelines for the Internet.
Rijndael	See AES.
RIP	The Routing Information Protocol (RIP) is a routing protocol. It is restricted to small networks. See also OSPF.
RipeMD 160	RACE Integrity Primitives Evaluation Message Digest (RipeMD 160) is a hash function that generates a 160 bit hash value (checksum). See also Hash.
RJ45	RJ45 refers to a jack or connector with a maximum of eight wires to the digital terminals' connection.
Roaming	With roaming, a client moves through a WLAN logging on and off at different access points in the same network.
Router	A router is a network component for connecting different types of network at the network layer of the OSI model. Data packets are transmitted using IP addresses. Routing tables are used to identify the best routes through the network. In order to keep the routing tables up to date, the routers exchange information via routing protocols (e.g. OSPF, RIP).
Router advertisement	Router advertisements are messages that the router sends to the network. They announce the presence of the router in the network. Router announcements are also used to issue prefixes, organise the autoconfiguration and specify the standard router.
Routing	Routing refers to the identifying of routes for sending messages.
RSA	The RSA algorithm (named after its inventors, Rivest, Shamir and Adleman) is used to create digital signatures and encrypt data packets. The signature can be used to verify changes made to the information in the data packet. RSA is used for public-key cryptography (IPSec). See also DSA. Key generation is slower with RSA than with DSA, but key processing is faster.
RTP	The Real-Time Transport Protocol (RTP) is used to transmit audio and video data (streams) via IP-based networks.
RTS threshold	Once the number of frames in the data packet exceeds the RTS threshold, a connection check (RTS/CTS handshake) is run before a data packet is sent.

RTSP The Real-Time Streaming Protocol (RTSP) controls the transmission of audio and video data (streams) via IP-based networks. While the Real-Time Transport Protocol (RTP) is used to transmit user data, the main function of RTSP lies in controlling the data streams.

Rule chain A rule chain contains a combination of different filter rules. A filter rule selects part of the data traffic based on particular features, e. g. the source IP address, and applies an action, e. g. block, on this part.

S2M interface See Primary Rate Interface.

SA So-called security associations (SA) receive information about the measures to secure the communication connection. One SA, at least, is a prerequisite for establishing a secure connection. An SA receives the subscriber's IP address, the authentication protocol used, the encryption algorithm used, the security parameter index (SPI), the selector and the period of validity.

SAD All the parameters that are set while configuring IPSec are stored in the router in the form of databases. These are the Security Policy Database (SPD) and the Security Association Database (SAD). The SAD receives information about every security connection. That is, which encryption algorithms, keys, protocols, session numbers or periods of validity are to be used. For an outgoing connection, an SPD entry displays an SAD entry. In this way, the SPD can specify which SA is to be used for a particular packet. With an incoming connection, the SAD is addressed in order to specify how the packet is to be processed.

SCEP The Simple Certificate Enrollment Protocol (SCEP) is used to manage digital certificates.

Scheduling Scheduling refers to the planning of tasks. Particular actions (e. g. deactivating an interface) are triggered by events (e. g. time or changing a MIB variable).

Serial interface The serial interface is used to exchange data between computers and peripheral devices. It can be used to configure the device or to transmit data via an IP infrastructure (Serial over IP).

Server A server offers services used by clients.

SFP Small Form-factor Pluggable (SFP) is a plug-in connector that was developed for extremely fast Ethernet.

SHA1 Secure Hash Algorithm version 1 (SHA1) is a hash function that generates a 160 bit hash value (checksum). See also Hash.

SHDSL Symmetrical High-bit-rate Digital Subscriber Line. See DSL.

Shell The shell is an input interface (e. g. command line or graphic user interface) between computer and user.

Short hold The short hold is the defined amount of time after which a network connection is automatically cleared if no more data is transmitted.

SIF With a Stateful Inspection Firewall (SIF), the routing of a data packet is not determined only by source and destination addresses but also using dynamic packet filtering based on the connection status.

Single phone number (VoIP) Single phone number access is a VoIP connection that is also known as a point-to-multipoint connection. It is used to connect VoIP terminals. Multiple subscriber numbers (MSNs) are provided. See also Direct dial-in (VoIP)

SIP The Session Initiation Protocol is a network protocol for setting up a communication session between two or more subscribers. The protocol is used for IP telephony (VoIP).

SIP provider A SIP provider does the switching between a SIP connection and other analogue, ISDN and VoIP connections.

SNMP The Simple Network Management Protocol (SNMP) is used to configure, control and monitor different network components (e. g. routers, servers, etc.) from a single, central system. The network component settings that can be changed are stored in a database – the Management Information Base (MIB). SNMP uses UDP. The network component receives requests to port 161 while the managing system receives confirmation messages (TRAPs) at port 162.

Spatial streams Spatial streams are data streams that are sent out at the same time on the same frequency in the wireless LAN. The transmission rate is multiplied as a result.

SPD All the parameters that are set while configuring IPSec are stored in the router in the form of databases. These are the Security Policy Database (SPD) and the Security Association Database (SAD). The Security Policy Database lists the forms of data traffic that are to be secured. Factors such as the source and destination address of the data packet are used to do this.

SRTP The Secure Real-Time Transport Protocol (SRTP) is the variant of

	the Real-Time Transport Protocol (RTP) that is encrypted using AES.
SSH	Secure Shell (SSH) is a network protocol that can be used to establish an encrypted connection to a device's shell.
SSID	The Service Set Identifier (SSID) defines a wireless network that is based on IEEE 802.11. The SSID is the network name of the wireless LAN. All the access points and clients that belong to the same network use the same SSID. The SSID string can be up to 32 characters long and is placed, unencrypted, in front of all packets. A client uses SSID ANY to contact all the accessible access points. The user is then shown all the available WLANs and he can select the appropriate network. If an access point is used for different networks, each wireless network is given a separate MSSID (Multi Service Set Identifier).
SSL	Secure Sockets Layer (SSL) is a protocol for data encryption. Since version 3.1, the new term Transport Layer Security (TLS) has been used. SSL is mainly used for HTTPS to encrypt the data transmission between web server and web browser.
STAC	STAC is used to reduce the data volume transmitted (data compression).
Static IP Address	In contrast to a dynamic IP address, the static IP address is assigned permanently by the user. Network components such as the web server or printer usually have static IP address, while clients such as notebooks or workstations usually have dynamic IP addresses.
STUN Server	Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). A STUN server enables VoIP devices behind an active NAT to access the network.
Sub-addressing	As well as the ISDN telephone number, a sub-address can also be sent when establishing the connection. This sub-address can transmit any additional information. It can be used, e. g., to systematically address multiple ISDN terminals that can be reached under one telephone number, or to open particular programs on a PC.
Subnet	A sub-network in an IP network is known as a subnet. A subnet is defined like a normal network, via an IP address and (sub-)netmask (IPv4) and prefix length (IPv6). Example: 192.168.1.250/24 (192.168.1.250/255.255.255.0, 256 possible IP addresses) is a subnet of 192.168.1.250/16 (192.168.1.250/255.255.0.0, 65536 pos-

sible IP addresses).

Switch A switch is a network component that connects individual network segments to one another. On the one hand, a switch can be operated as a bridge to the data link layer in the OSI model. Unlike the bridge, however, a switch has more than one input and output. On the other hand, the switch can be operated as a gateway to the network layer in the OSI model. The device comparable to the switch in the physical layer is known as the hub.

SWYX SwyxWare is a software-based communication solution for VoIP.

Syslog The syslog protocol is used to transmit status messages in an IP network. In this way, different network components can be monitored from a single, central system. Syslog messages are sent as unencrypted text messages over the UDP port 514.

T.38 T.38 or Fax over IP (FoIP) refers to fax transmission via an IP network.

TACACS+ The Terminal Access Controller Access Control System Plus (TACACS+) is a client-server protocol for authenticating, authorising and accounting for users. The TACACS+ server authenticates the client by checking, e. g., the username and password. In contrast to the UDP-based RADIUS protocol, TACACS+ uses TCP on port 49 and transmits the entire communication encrypted.

TAPI The Telephony Applications Programming Interface (TAPI) is a programming interface for ISDN. It enables application programs to access ISDN hardware from a PC. See also CAPI.

TCP The Transmission Control Protocol (TCP) is a connection-oriented protocol. It works on the transport layer of the OSI model. With a connection-oriented protocol, a logical connection is established before transmission and maintained. This enables data to be transmitted reliably. Nonetheless, control information is constantly being sent alongside the actual data packets. This causes the data volume sent to increase. See also UDP.

TCP-ACK packet An ACK (acknowledgement) signal is used when transmitting data to confirm the receipt or the processing of data or commands. TCP uses ACK signals for communication.

TE Terminal equipment (TE) refers to a connection or operating type. The TE connector is a terminal's connector. In TE operation, the gateway is connected to the PABX's internal S0 and thus constitutes

	an ISDN terminal. See also NT.
Telnet	Telecommunication Network (Telnet) is a network protocol. It enables communication with another, remote device in the network, e. g. PCs, routers, etc.
TFTP	The Trivial File Transfer Protocol (TFTP) regulates the transmission of files. Compared with FTP, there is no option to display data, issue permissions or authenticate users.
Tiger 192	Tiger 192 is a hash function that generates a 192 bit hash value (checksum). See also Hash.
Time slot	A time slot is a period of time which is permanently assigned within a transmission frame, and is usually equivalent to one transmission channel.
TLS	See SSL.
TOS	Type of Service (TOS) is a field in the header of IP data packets. It specifies the priority of the data packet. See also QoS.
Traceroute	Traceroute is used to determine which routers will be used to route data packets to the queried destination host.
Trigger	This refers to a trigger impulse.
Triple DES	See DES.
TTL	The Time to live (TTL) is the configured period of validity of a data packet. With the Internet Protocol (IP), TTL specifies how many hops a data packet may pass. The maximum value is 255 hops. The TTL is reduced by 1 with each hop. If a data packet has not yet reached its destination when its TTL expires, it is discarded.
Twofish	Twofish is an encryption method (see Cipher). Twofish uses a fixed block length of 128 bits. The key length is 128, 192 or 256 bits.
U-ADSL	Universal Asymmetric Digital Subscriber Line (UADSL) is a DSL variant. It was developed as ANSI T1.413 and standardised as G.992.2. U-ADSL enables different communication technologies to be used in parallel, e. g. ISDN and POTS, and does not require a splitter.
UDP	The User Datagram Protocol (UDP) is a connectionless protocol. It works on the transport layer of the OSI model. With a connectionless protocol, no control is integrated for delivering the packet. The

control must take place in the application layer. Conversely, UDP is faster than connection-oriented protocols.

ULA Unique Local Addresses (ULA) are IPv6 addresses that are not routed. They can be used in private networks (e. g. a LAN). ULAs begin with the prefix fd.

UMTS The Universal Mobile Telecommunications System (UMTS), also known as 3G, is a mobile communications standard with a specified max. data transmission rate of 384 kbit/s and 21 Mbit/s in association with HSPA+.

Unicast With Unicast, data packets are transmitted from a sender to a single recipient.

UPnP Universal Plug and Play (UPnP) is used to control devices (audio devices, routers, printers, etc.) from any manufacturer via an IP-based network.

Upstream The gateway forwards the data from its own network.

URL A Uniform Resource Locator (URL) identifies a file's storage location. Example: http://www.example.org/index.htp (Internet website)

V.110 V.110 describes a method of aligning bitsteams with 0.6, 1.2, 2.4, 2.8, 7.2, 9.6, 12, 14.4, 19.2 and 38.4 kbit/s with the ISDN bitstream of 64 kbit/s.

VDSL Very High Speed Digital Subscriber Line. See DSL.

VID See VLAN.

VLAN A network can be divided up into one or more logical sub-networks– so-called Virtual Local Area Networks (VLAN) – by the network components no longer forwarding the data packet of a defined sub-network to other sub-networks. Each VLAN is assigned a unique number, This number is called a VLAN ID (VID) and assigned to the data packets in the VLAN tag.

VoIP Voice over IP (VoIP), also known as IP telephony, refers to the transmitting of voice via an IP network. The telephone is connected and disconnected using signalling protocols, e. g. SIP.

VPN A virtual private network (VPN) is used to transport private data packets through a public network. The data is separated from the publicly accessible data by being encapsulated in new protocols so that they can be routed to the intended recipient. In this context, one

	also refers to a tunnel that is established between the private networks of the two connected parties. VPN protocols are IPSec, PPTP, L2TP and GRE.
VSS	The Virtual Service Set (VSS) refers to a prefix for wireless LAN interfaces.
Walled garden	In the context of hotspots, a walled garden refers to the area of the website which is available to users free of charge and without logging in.
WAN	A Wide Area Network (WAN) refers to a network that is spread over a large geographic area. Global WAN networks provide access to the Internet.
WDS	The Wireless Distribution System (WDS) is used to establish a wireless connection between access points.
Web server	A web server provides HTML documents (web pages).
WEP	Wired Equivalent Privacy (WEP) is an encryption protocol for WLANs. The key length is 40 or 104 bits.
WINS	The Windows Internet Name Service (WINS) is a translation of the NetBIOS over TCP/IP network protocol by Microsoft. Like DNS, WINS is used for centralised name resolution. See also DNS.
WLAN	Wireless Local Area Network (Wireless LAN, WLAN) refers to a local wireless network based on the 802.11 standard.
WMM	Wi-Fi Multimedia (WMM) prioritises the data packets from different applications, thus improving the transmission of voice, music and video data in WLAN networks. To do this, WMM provides quality-of-service features (QoS) for IEEE 802.11-based networks.
WPA	Wi-Fi-Protected Access (WPA) is an encryption protocol for WLANs. WPA uses dynamic keys that are based on the Temporal Key Integrity Protocol (TKIP).
WPA 2	Wi-Fi Protected Access (WPA) is an encryption protocol for WLANs. WPA 2 uses AES.
WPA Enterprise	With WPA 1 / 2, WPA Enterprise enables subscribers to be authenticated using the Extensible Authentication Protocol (EAP). After successful authentication, the server transfers a shared key to the client and the access point for data transfer in the WLAN.

WPA-PSK With WPA 1 / 2, WPA-PSK enables subscribers to be authenticated using pre-shared keys. The access point and the client use the same string for the key calculation in the WLAN. This string needs to be configured by the users.

X.25 X.25 is a standardised series of protocols for wide area networks (WANs) via the telephone network.

X.31 The X.31 standard describes the connecting of ISDN and X.25 systems. It is a standard for connecting card terminals.

X.500 The X.500 standard describes the setting up of a directory service. See also LDAP.

X.509 The X.509 standard describes the generating of certificates for a public key insfrastructure (PKI).

X.75 X.75 is a standardised series of protocols for ISDN networks with a transmission rate of 64 kbit/s.

XAuth XAUTH (Extended Authentication) is used to add further authentication mechanisms to IKE. After a successful phase 1 authentication, the user can be separately identified again. The identifying is done using the username and password, PAP, CHAP or hardware-based systems.

Index

B

C

D

E

F

G

N

O

P

S

T

U

V

W

X

Z