Additional information on Release 10.1.9

IPSec - IKEv2 Initiator Mode

Starting with release 10.1.9 devices of the RS series support the IKEv2 initiator mode. When initiating Phase 1 they can now be used as initiator, too, and not only as responder. No specific configuration is required.

Release Notes

Copyright© Version 1.1, 2015 bintec elmeg GmbH

Rechtlicher Hinweis

Warranty

This publication is subject to change.

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

Copyright © bintec elmeg GmbH.

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

Inhaltsverzeichnis

Kapitel 1 Important Information

1.1 Preparation and update with the GUI

Updating the system software with the Graphical User Interface (GUI) is done using a BLUP (bintec Large Update) file so as to update all the necessary modules intelligently. All those elements that are newer in the BLUP than on your gateway are updated.

Hinweis

The result of an interrupted updating operation could be that your gateway no longer boots. Hence, do not turn your gateway off during the update.

To prepare and carry out any update to **Systemsoftware 10.1.4** using the Graphical User Interface, proceed as follows:

(1) For the update, you'll need the `XXXXX_bl1014.xxx`file, where `XXXXX` stands for you device. Ensure that the file that you require for the update is available on your PC. If the file is not available on your PC, enter *www.bintec-elmeg.com* in your browser. The bintec-elmeg homepage will open. You will find the required file in the download area for your gateway. Save it on your PC.

(2) Backup the current boot configuration before updating. Export the current boot configuration using the **Maintenance**->**Software &Configuration** menu in the Graphical User Interface. To do this, select: **Action** = *`Export configuration`*, **Current File Name in Flash** = *`boot`*, **Include certificates and keys** = *`enabled`*, **Configuration Encryption** = *`disabled.`* Confirm with **Start**. The **Open <name of gateway>.cf** window opens. Leave the selection *`Save file`* and click **OK** to save the configuration to your PC. The file `<name of gateway.cf>` is saved and the **Downloads** window shows the saved file.

(3) Update to **Systemsoftware 10.1.4** via the **Maintenance**->**Software &Configuration** menu. To do this, select: **Action** = *`Update system software`*, **Source Location** = *`Local File`*, **Filename** = *`XXXXX_bl9110.xxx`*. Confirm with **Start**. The message „System request. Please stand by. Operation in progress.“ or „System Maintenance. Please stand by. Operation in progress.“ shows that the selected file is being uploaded to the device. When the upload procedure is finished, you will see the message „System - Maintenance. Success. Operation completed successfully.“ Click **Reboot**. You will see the message „System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds.“ The device will start with the new system software, and the browser window will open.

1.2 Downgrade with the GUI

If you wish to carry out a downgrade, proceed as follows:

(1) Replace the current boot configuration with the previous backup version. You import the saved boot configuration using the **Maintenance**->**Software &Configuration** menu. To do this, select: **Action** = *Import configuration*, **Configuration Encryption** = *disabled*, **Filename** = *<name of the device>.cf*. Confirm with **Start**. The message „System request. Please stand by. Operation in progress.“ or „System Maintenance. Please stand by. Operation in progress.“ indicates that the selected configuration is being uploaded to the device. When the upload procedure is finished, you will see the message „System - Maintenance. Success. Operation completed successfully.“ Click **Reboot**. You will see the message „System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds.“ The device will start and the browser window will open. Log into your device.

(2) Downgrade to the software version you want using the **Maintenance**->**Software &Configuration** menu.
To do this, select: **Action** = *Update system software*, **Source Location** = *Local File*, **Filename** = *RXL_Series_bl9109.biq* (example). Confirm with **Start**. The message „System request. Please stand by. Operation in progress.“ or „System Maintenance. Please stand by. Operation in progress.“ shows that the selected file is being uploaded to the device. When the upload procedure is finished, you will see the message „System - Maintenance. Success. Operation completed successfully.“ Click **Reboot**. You will see the message „System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds.“ The device will start with the new system software, and the browser window will open.

You can log into your device and configure it.

1.3 Supported web browsers

The HTML GUI supports the use of the following browsers, each in their latest version:

- Microsoft Internet Explorer
- Mozilla Firefox

.

Wichtig

Ensure that you keep your browser updated to the latest version, since you need to do so to take advantage of new functions and security features. The HTML GUI does not support versions that are no longer supported by the manufacturer and supplied with software updates. If necessary, go to the software manufacturer's website to find out which versions they currently support.

Kapitel 2 New Functions

Systemsoftware 10.1.4 includes a number of new functions that significantly improve performance compared to the previous version of the system software.

Hinweis

Please note that not all the functions listed here are available for every device. Please refer, if necessary, to the current data sheet for your device or to the relevant manual.

2.1 IPv4 filter rules

Hinweis

From **Systemsoftware 10.1.4** onwards, the IPv4 filter rules concept has changed fundamentally.

In IPv4, trustworthy or non-trustworthy zones are available in a comparable manner, as in IPv6. In the SIF, at first all LAN interfaces are considered trustworthy, all WAN interfaces as non-trustworthy.

In the **Firewall**->**Guide lines**->**IPv4 Filter Rules** menu, you can display an IPv4 interface list using the button under **Trustworthy Interfaces** and identify which interfaces are trustworthy.

Furthermore, in IPv4 the following menus and fields are affected:

- in the **LAN**->**IP-configuration**->**Interfaces**-> menu, the **Security Policy field**
- the **WAN**->**Internet + Dialup**->**PPPoE**->**New**, **WAN**->**Internet + Dialup**->**PPTP**->**NEW**, **WAN**->**Internet +Dialup**->**PPPoA**->**New menus**
- the **VPN**->**IPSec**->**IPSec-Peers**->**New menu**

2.2 IPv6

Wichtig

The following functions can NOT be used with IPv6:

- Load balancing: The function is not applicable on IPv6 interfaces because the IPv6 data traffic is not recorded.
- Hotspot Gateway: IPv6 data traffic is not recorded by Hotspot Gateway and can therefore, not be controlled and restricted, if necessary.
- IPv6 tunnel mechanisms for transferring IPv6 data through IPv4 networks (6in4 Relay, SixXS, Hurricane Electric, 6to4 RFC) are no longer supported. Configurations making use of these mechanisms are incompatible with **Systemsoftware 10.1.4** .

With **Systemsoftware 10.1.4** IPv6 is available for selected bintec routers.

Configure IPv6 addresses

In addition to IPv4 addresses, you can use IPv6 addresses.

In the following, there is an example of an IPv6 address:

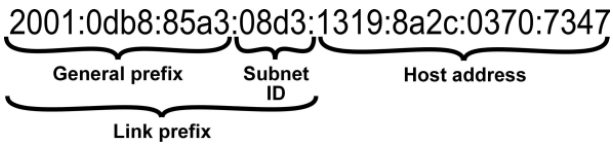

Abb. 1: IPv6 address (example)

On an interface, your device can either run as a router or host. On a LAN interface, it usually runs as a router and on WAN as well as PPP connections it runs as a host.

If your device runs as a router, its own IPv6 addresses can be formed as follows: a link-prefix can be derived from a general prefix (see **IPv6 General Prefixes** further below) or you can enter the static value. A host address can be generated via `Auto EUI-64`, you can enter static values for other host addresses.

If your device runs as a router, it usually distributes the configured link-prefix to hosts via router advertisements. Additional information, e.g., the time server address is transmitted to the hosts via the DHCP servers. The client can generate his/her host address either via Stateless Address Autoconfiguration (SLAAC) or have these addresses assigned by a DH-

CP server.

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

If your devices runs as a host, a link-prefix from another router is assigned to it via router advertisement. The host address is automatically generated via SLAAC. Additional information, e.g. general prefix of the provider or the address of a time server can be obtained via DHCP. To do so, in the **LAN**->**IP Configuration**->**Interfaces**->**New** menu, use the **IPv6 Mode** = *Client*, **Accept Router Advertisement** *Enabled* and **DHCP Client** = *Enabled* settings.

IPv6 General Prefixes

IPv6 General Prefixes are usually assigned by IPv6 providers. They can be statically assigned or obtained via DHCP. It usually has to do with /48- or /56- networks. You can generate /64-subnets from these general prefixes and have them redistributed in your network.

The general prefix concept has two decisive advantages:

- A single route is sufficient between the provider and client.
- If the provider assigns a new general prefix via DHCP or must change a statically assigned general prefix, you as the customer have little or no configuration expenditure. You will automatically receive the new general prefix via DHCP. In case of the statically assigned general prefix, you must enter this into your system once. All subnets and IPv6 addresses derived from this general prefix change automatically change if the general prefix is updated.

Menus

The following menus are provided for defining the IPv6 configuration:

- **Assistants**->**First Steps**->**Basic Settings**: Here you can define basic IPv6 settings using the **First steps** assistant. Explanations of the displayed IPv6 parameters can be found directly in the GUI in the right window.
- **Assistants**->**Internet Access**->**Internet Connections**: Here you can configure IPv6 settings for an internet connection using the **Internet Access** assistant. Explanations of the displayed IPv6 parameters can be found directly in the GUI in the right window.
- **LAN**->**IP Configuration**->**Interfaces**->**New**: Here you can configure the desired IPv6 interfaces (see *Interfaces* auf Seite 7).
- **LAN**->**IP Configuration**->**Interfaces**->: Here you can view all the IPv4 and IPv6 addresses of the corresponding interfaces.

- **Networking**->**Routes**->**IPv6 Route Configuration**: In this menu you can define new IPv6 routes or edit existing routes (see *IPv6 Route Configuration* auf Seite 16).
- **Networking**->**Routes**->**IPv6 Routing Table**: Here, a list of all IPv6 routes active in the system are displayed.
- **Networking**->**IPv6 General Prefixes**->**General Prefix Configuration**: Here you can create new general prefixes for IPv6 or change previously created general prefixes (see *General Prefix Configuration* auf Seite 19).
- **Networking**->**QoS**->**IPv4/IPv6 Filter**: Here you can configure IPv4 and IPv6 filters (see *IPv4/IPv6 Filter* auf Seite 21).
- **WAN**->**Internet + Dialup**->**PPPoE**->**New**: Here you can configure IPv6 for PPoE (see *PPPoE* auf Seite 22).
- **WAN**->**Internet + Dialup**->**PPPoA**->**New**: Here you can configure IPv6 for PPoE (see *PPPoA* auf Seite 24).
- **VPN**->**IPSec**->**IPSec Peers**->**New**: Here you can configure IPv6 for IPSec (see *IPSec Peers* auf Seite 27).
- **Firewall**->**Policies**->**IPv6 Filter Rules**->**New**: Here you can configure filter rules for IPv6 (see *IPv6 Filter Rules* auf Seite 30).
- **Firewall**->**Interfaces**->**IPv6 Groups**->**New**: You can combine IPv6 interfaces for groups (see *IPv6 Groups* auf Seite 33).
- **Firewall**->**Addresses**->**Address List**: Here, a list of all configured addresses is displayed. You can create new (IPv6) addresses (see *Address List* auf Seite 34).
- **Firewall**->**Addresses**->**Groups**->**New**: You can combine addresses for groups (see *Groups* auf Seite 35).
- **Local Services**->**DNS**->**DNS Servers**->**New**: Here you can create a DNS server for IPv6 (see *DNS Servers* auf Seite 35).
- **Local Services**->**DNS**->**Dynamic Hosts**: Here, the learned DNS entries are displayed via DHCPv6 (see *Dynamic Hosts* auf Seite 47). For example, you will see the IPv6 addresses assigned via DHCPv6.
- **Local Services**->**DHCPv6 server**: here, you can configure your device as a DHCPv6 server (see *DHCPv6-Server* auf Seite 37 and *DHCPv6 Global Options* auf Seite 40).
- **Maintenance**->**Diagnostics**->**Ping Test** (see *Ping Test* auf Seite 44)
- **Maintenance**->**Diagnostics**->**Traceroute Test** (see *Traceroute Test* auf Seite 45)

2.2.1 Interfaces

The existing IP interfaces are listed in the **LAN**->**IP Configuration**->**Interfaces** menu. You can see IPv6 address that have already been created for interfaces.

2.2.1.1 Edit or New

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

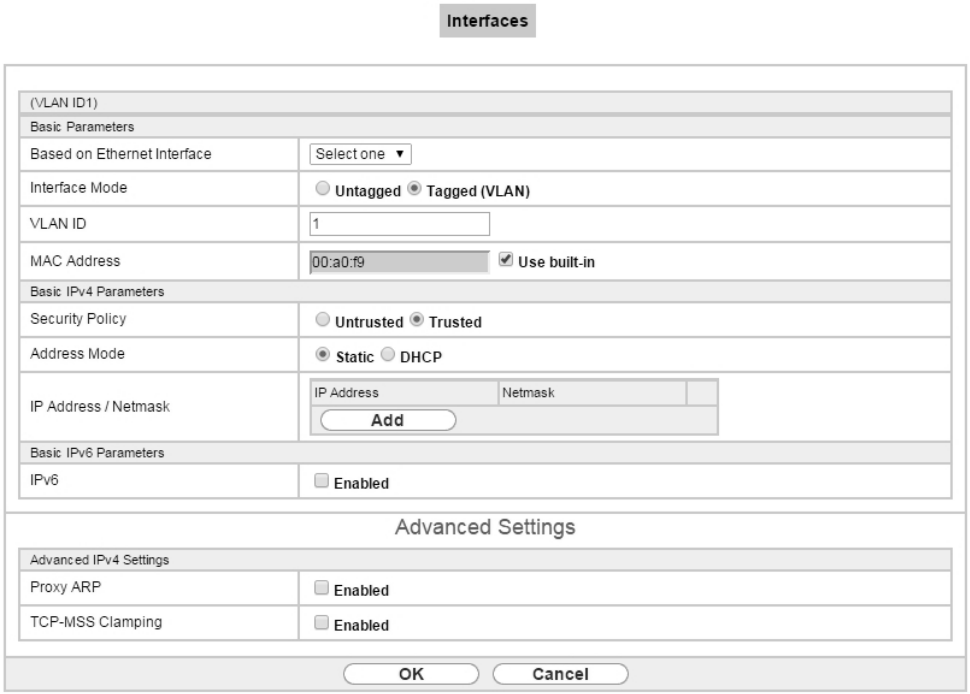

Abb. 2: **LAN->IP Configuration->Interfaces->New**

The **LAN->IP Configuration->Interfaces->New** menu contains the following fields relevant for IPv6:

Fields in the menu Basic IPv6 Parameters

Field	Description
IPv6	Select whether the selected interface is to use Internet Protocol version 6 (IPv6) for data transmission. The function is activated by selecting *Enabled*. The function is disabled by default.
Security Policy	Here only for **IPv6** = *Enabled* Select the security settings to be used with the interface.

Field	Description
	Possible values: • *Trusted* (default value): All IP packets are allowed through except for those which are explicitly prohibited. We recommend you use this setting if you want to use IPv6 on your LAN. • *Untrusted*: Only those IP packets that can be assigned to a connection, which were set-up from a trustworthy zone are allowed through. We recommend you use this setting if you want to use IPv6 outside of your LAN. You can configure exceptions for the selected setting in the Firewall menu.
IPv6 Mode	Only for **IPv6** = *Enabled* Select whether the interfaces are to be operated in the host or router mode. Depending on the selection made, different parameters are displayed, which you must configure. Possible values: • *Router (Transmit Router Advertisement)* (default value): The interface is operated in router mode. • *Host*: The interface is operated in host mode.
Transmit Router Advertisement	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Router (Transmit Router Advertisement)* Select whether router advertisements are to be sent via the selected interface. With the help of router advertisements, e.g., the prefix list is transmitted and the router is propagated as a standard gateway. The function is activated by selecting *Enabled*. The function is enabled by default.
DHCP Server	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Router (Transmit Router Advertisement)*

Field	Description
	Determine whether your device is to be run as a DHCP server, i.e., whether it is to send DHCP options to forward, e.g., information on the DNS servers to clients. Activate this option if hosts are to generate IPv6 addresses via SLAAC. The function is activated by selecting *Enabled*. The function is enabled by default.
IPv6 Addresses	Only for **IPv6** = *Enabled* You can allocate **IPv6 Addresses** to the selected interface. With **Add** you can create one or several address entries. An additional window is opened, where you can determine a IPv6 address comprising a link prefix and a host share. If your device works in the host mode (**IPv6 Mode** = *Host*, **Accept Router Advertisement** *Enabled* and **DHCP Client** *Enabled*), its IPv6 addresses are determined via SLAAC. You are not required to manually configure IPv6 addresses, but can key in additional addresses if desired. If your device works in the router mode (**IPv6 Mode** = *Router (Transmit Router Advertisement)*, **Transmit Router Advertisement** *Enabled* and **DHCP Server** *Enabled*), then you must also configure it IPv6 addresses.
Accept Router Advertisement	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Host* Select whether router advertisements are to be received via the selected interface. With the help of router advertisement, e.g., the prefix list is created. The function is activated by selecting *Enabled*. The function is enabled by default.
DHCP Client	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Host* Determine whether your device is to be run as a DHCP client, i.e., whether it is to receive DHCP options to forward, e.g., infor-

Field	Description
	mation on the DNS servers. The function is activated by selecting *Enabled*. The function is enabled by default.

If you click on **Add**, an additional window opens.

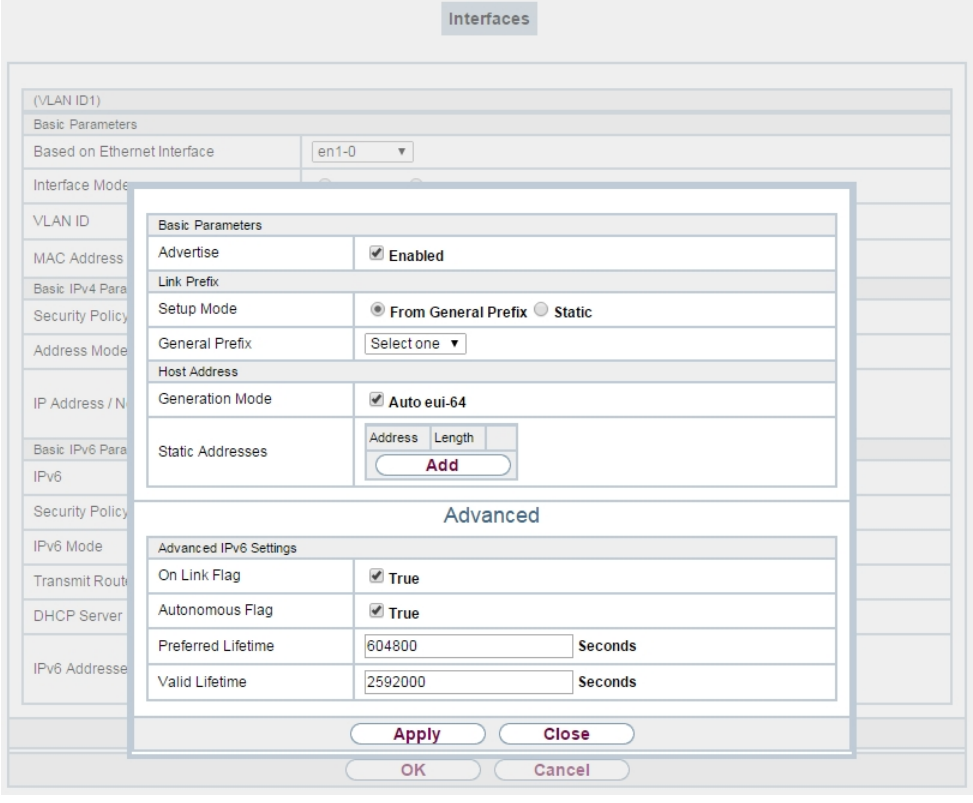

Abb. 3: **LAN->IP Configuration->Interfaces->New->Add**

Field in the menu Basic Parameters

Field	Description
Advertise	Only for **IPv6 Mode** = *Router (Transmit Router Advertisement)* Here, - with regard to the link prefix that is defined in the current window - you can define whether this prefix is to be sent via rou-

Field	Description
	ter advertisement via the selected interface. The function is activated by selecting *Enabled*. The function is enabled by default.

Fields in the menu Link Prefix

Field	Description
Type of set-up	Select how the link prefix is to be determined. Possible values: • *From General Prefix* (default value): The link prefix is derived from a general prefix. • *Static*: You can enter the link prefix.
General Prefix	Only for **type of set-up** = *From General Prefix* Select the general prefix which the link prefix is to be derived from. You can select among the general prefixes which are created under **Network**->**IPv6 General Prefixes**->**General Prefix Configuration**->**New** (see *General Prefix Configuration* auf Seite 19).
Auto Subnet Configuration	Only if **type of set-up** = *From General Prefix* and if a **General Prefix** is selected. Select whether the subnet is to be created automatically. In automatic subnet configuration, the ID *0* is used for the first subnet, the second subnet uses the subnet ID *1*, etc. Possible values for the **Subnet ID** are *0* to *65535*. The subnet ID describes the fourth of the four 16-bit fields of a link prefix. In subnet configuration, the decimal ID value is converted to a hexadecimal value. The function is activated by selecting *Enabled*. The function is enabled by default. If the function is not active, you can define a subnet by entering the subnet OD.

Field	Description
Subnet ID	Only if **Auto Subnet Configuration** is not enabled. Enter the subnet ID to define a subnet. The subnet ID describes the fourth of the four 16-bit fields of a link prefix. Possible values are *0* to *65535*. In subnet configuration, the entered decimal ID value is converted to a hexadecimal value.
Link Prefix	Only for **type of set-up** = *Static* You can enter the link prefix of a IPv6 address. This prefix must end with *::*. It's length is specified with *64*.

Fields in the menu Host Address

Field	Description
Generation method	Determine whether the host share of the IPv6 address is to be automatically generated from the MAC address using EUI-64. The function is activated by selecting *Enabled*. The function is enabled by default. EUI-64 starts up the following process. • The hexadecimal 48 bit MAX address is divided into 2 x 24 bit. • *FFFE* is entered in the gap created to maintain 64 bit. • The hexadecimal form of 64 bit is transformed into the dual form. • In the first 8 bit field, bit 7 is placed on *1*.
Static Addresses	Irrespective of the automatic generation that is specified under **Generation methods**, you can manually enter the host share of one or several IPv6 addresses using **Add**. It's length is specified with *64*. Start your entry with *::* .

The fields in the **Advanced** menu are a component of the prefix information which are sent in the router advertisement, if **Advertise** is enabled. The menu **Advanced** consists of the following fields:

Fields in the menu Advanced IPv6 Settings

Field	Description
On Link Flag	Select whether the On-Link Flag (L-Flag) should be set. This allows the host to enter the prefix from the prefix list. The function is activated by selecting *True*. The function is enabled by default.
Autonomous Flag	Select whether the Autonomous Address Configuration Flag (A-Flag) should be set. This allows the host to use the prefix and an interface ID, to derive its address. The function is activated by selecting *True*. The function is enabled by default.
Preferred Lifetime	Enter a time period in seconds. During this time, the addresses that are created with the help of the prefix via SLAAC, are used preferentially. The default value is *604800* seconds.
Valid Lifetime	Enter a time period in seconds, for which the prefix is valid. The default value is *2592000* seconds. **Hinweis** The value for the validity period should be lower than the value that is configured under **Advanced IPv6 Settings** for the **Router Lifetime** option.

The **Advanced Settings** menu contains the following fields relevant for IPv6:

Fields in the menu Advanced IPv6 Settings

Field	Description
Router Lifetime	Only for **IPv6** = *Enabled*, **IPv6 Mode** = *Router (Transmit Router Advertisement)* and **Transmit Router Advertisement** = *Enabled*

Field	Description
	Enter a time period in seconds. The router remains in the default router list throughout this interval. The default value is *600* seconds. The maximum value is *65520* seconds. A value of *0* means that the router is not a default router, and will not be entered in the default router list.  **Hinweis** The value for the **Router Lifetime** should be higher than the shortest link prefix validity period, which is configured under **Basic IPv6 Parameters** for the interface.
Router Preference	Only for **IPv6** = *Enabled*, **IPv6 Mode** = *Router (Transmit Router Advertisement)* and **Transmit Router Advertisement** = *Enabled* Select your router's preference for choice of default router. This is useful for cases where a node receives advertisements from multiple routers, or for back-up scenarios. Possible values: • *High* • *Medium* (default value) • *Low*
DHCP Mode	Only for **IPv6** = *Enabled*, **IPv6 Mode** = *Router (Transmit Router Advertisement)* and **Transmit Router Advertisement** = *Enabled* Select the information forwarded to the DHCP client.  **Hinweis** To achieve this, your router must not be set up as a DHCP server. By selecting *Other - DNS Servers, SIP Servers* (default value), no address-related information, such as i.e.,

Field	Description
	DNS, VoIP, etc., is passed through. Activate this option if the hosts in the network are to automatically set-up your IP address via SLAAC. In this case, the router only sends non-address-related data via DHCP. With the selection of *Managed - IPv6 Address Management* both the IPv6 address as well as all non-address-related data are derived from the host via DHCP.

DNS Propagation	Only for **IPv6 Mode** = *Router (Transmit Router Advertisement)* and **Transmit Router Advertisement** *Enabled*
	
	Select whether DNS server addresses are to be propagated via router advertisements and if yes, in which manner. A maximum of two DNS server addresses are propagated.
	
	Possible values:
	
	• *Off*: No name DNS server address is propagated.
	• *Self*: The personal IP address is propagated as the DNS server address. In case of several addresses, the addresses are propagated in the following order:
	  • Global addresses
	  • ULA (Unique Local Addresses)
	  • Link-local addresses
	• *Other*: The statically configured and dynamically learned DNS server entries are propagated according to their priority. If no entries are available, no addresses are propagated.

2.2.2 IPv6 Route Configuration

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

2.2.2.1 Edit or New

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

Routes without an icon have been created by the router automatically and cannot be edited.

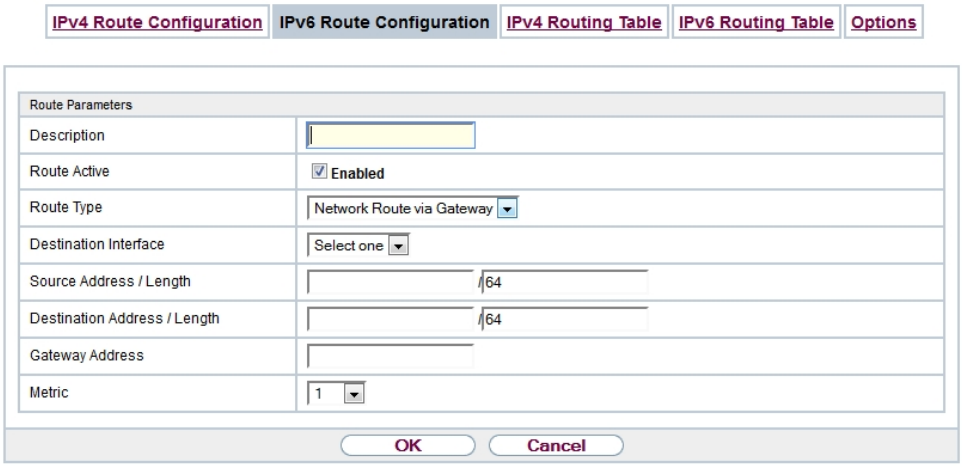

Abb. 4: **Network->Routes->IPv6 Route Configuration->New**

The **Network->Routes->IPv6 Route Configuration->New** menu consists of the following fields:

Fields in the menu Route Parameters

Field	Description
Description	Enter a description for the IPv6 route.
Route Active	Select if the route is to be active or inactive. With *Enabled* the status of the route will be set to active. The function is enabled by default.
Route Type	Select the type of route. Possible values: • *Default Route via Interface* : Route via a specific interface that is used if no other suitable routes are available. • *Default Route via Gateway*: Route via a specific gateway that is used if no other suitable routes are 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.

Field	Description
	• *Network Route via Interface*: Route to a network via a specific interface. • *Network Route via Gateway* (default value): Route to a network via a specific gateway.
Destination Interface	Select the IPv6 interface to be used for this route. You can select among the interfaces that are created under **LAN**->**IP Configuration**->**Interfaces**->**New** and for which the use of IPv6 is enabled.
Source Address / Length	Enter the IPv6 source address along with the corresponding prefix length. The entry *::* describes an unspecific address. By default the prefix length *64* is predefined.
Destination Address / Length	Enter the IPv6 target address along with the corresponding prefix length. The entry *::* describes an unspecific address. By default the prefix length *64* is predefined.
Gateway Address	Enter a the IPv6 address for the next hop.
Metric	Select the priority of the route. The lower the value, the higher the priority of the route. The valuation of *0*to *255*, the default value is *1*.

2.2.3 IPv6 Routing Table

In the **Network**->**Routes**->**IPv6 Routing Table** menu a list of all IPv6 routes active in the system are displayed.

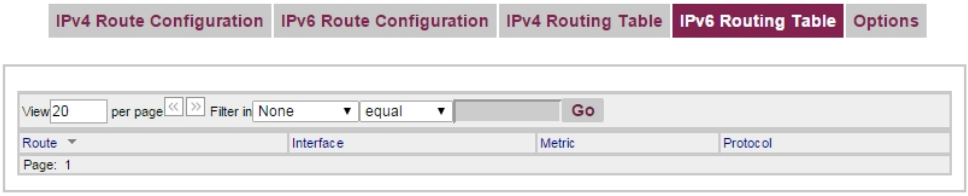

Abb. 5: **Network->Routes->IPv6 Routing Table**

Fields in the menu IPv6 Routing Table

Field	Description
Route	Displays the source and target address which is used for this route as well as the gateway IP address. In case of routes received via DHCP, nothing is displayed.
Interface	Displays the interface which is used for this route.
Metric	Displays the route priority. The lower the value, the higher the priority of the route
Protocol	Displays how the entry was generated, e.g., manual (`Local`) or via one of the available protocols.

2.2.4 General Prefix Configuration

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

2.2.4.1 Edit or New

Select the icon to edit existing entries. Choose the **New** button to configure additional operations.

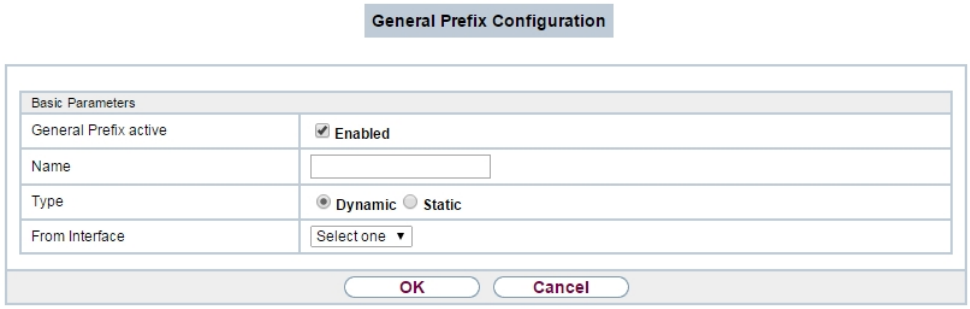

Abb. 6: **Networking->IPv6 General Prefixes->General Prefix Configuration->New**

Fields in the menu Basic Parameters

Field	Description
General Prefix active	Select if the prefix is to be active or inactive. With *Enabled* the status of the prefix will be set to active. By default, the prefix is enabled.
Name	Enter a name for the general prefix. A descriptive name is used to be able to easily select the general prefix from a prefix list.
Type	Specify how the address range is to be assigned. Possible values: • *Dynamic* (default value): The general prefix is determined dynamically using a DHCP transmission, e.g., from a provider. • *Static*: The prefix is fixed, e.g., by a provider.
From Interface	Only if **Type** = *Dynamic* Select the IPv6 interface from which a **General Prefix** is to be obtained. You can select among the interfaces that are created under **LAN->IP Configuration->Interfaces->New** and fulfil the following conditions: • **IPv6** is *Enabled*. • **IPv6 Mode** = *Host* • **DHCP Client** is *Enabled*.

Field	Description
Used Prefix / Length	Only if **Type** = *Static* Enter the prefix to be used. Enter the corresponding length. This prefix must end with ::. By default the prefix length *48* is predefined.

2.2.5 IPv4/IPv6 Filter

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

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

2.2.5.1 New

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

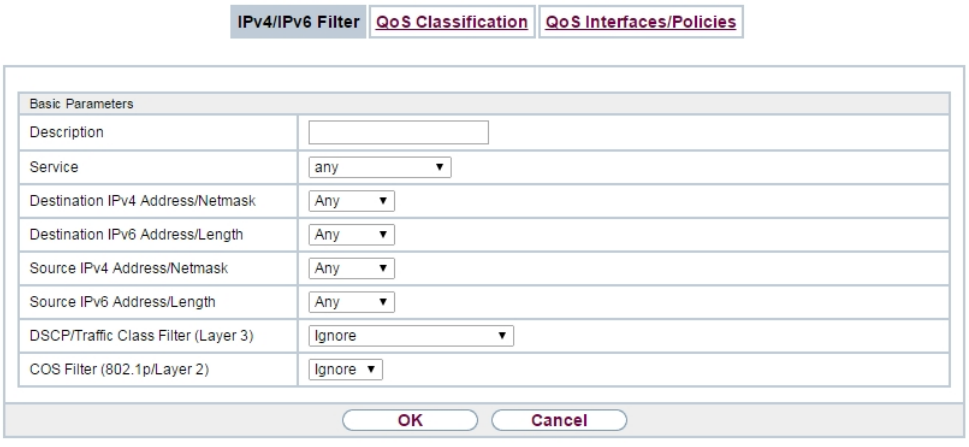

Abb. 7: **Networking**->**QoS**->**IPv4/IPv6 Filter**->**New**

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

Relevant fields in the menu Basic Parameters

Field	Description
Destination IPv6 Address/Length	Enter the IPv6 target address of the data packets and the prefix length. Possible values: • *Any* (default value): The target IP address/length are not spe-

Field	Description
	cified in detail. • *Host*: Enter the target IP address of the host. • *Network*: Enter the target network address and the prefix length.
Source IPv6 Address/ Length	Enter the IPv6 source address of the data packets and the prefix length. Possible values: • *Any* (default value): The source IP address/length are not specified in detail. • *Host*: Enter the source IP address of the host. • *Network*: Enter the source network address and the prefix length.

2.2.6 PPPoE

A list of all PPPoE interfaces are 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.

2.2.6.1 New

Choose the **New** button to set up new PPPoE interfaces.

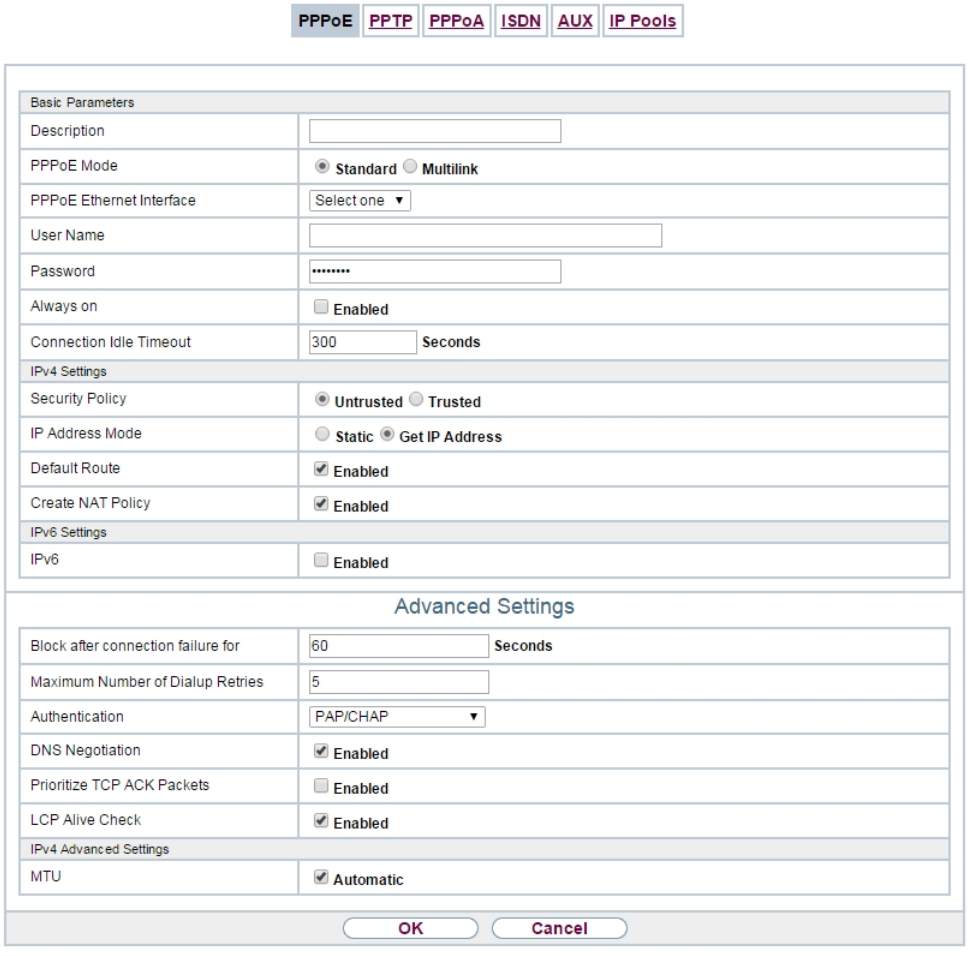

Abb. 8: **WAN->Internet + Dialup->PPPoE->New**

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

Fields in the menu IPv6 Settings

Field	Description
IPv6	Select whether the selected PPPoE interface is to use Internet Protocol version 6 (IPv6) for data transmission. The function is activated by selecting *Enabled*. The function is disabled by default.
Security Policy	Select the security settings to be used with the interface.

Field	Description
	Possible values: • *Untrusted* (default value): Only those IP packets that can be assigned to a connection, which were set-up from a trustworthy zone are allowed through. We recommend you use this setting if you want to use IPv6 outside of your LAN. • *Trusted*: All IP packets are allowed through except for those which are explicitly prohibited. We recommend you use this setting if you want to use IPv6 on your LAN. You can configure exceptions for the selected setting in the Firewall menu.
IPv6 Mode	Only for **IPv6** = *Enabled* The selected PPPoE interface is operated in host mode.
Accept Router Advertisement	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Host* Select whether router advertisements are to be received via the interface. The default router list and the prefix list are created by the router advertisements. The function is activated by selecting *Enabled*. The function is enabled by default.
DHCP Client	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Host* Define whether your device is to be run as a DHCP client. The function is activated by selecting *Enabled*. The function is enabled by default.

2.2.7 PPPoA

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

In this menu, you configure a xDSL connection used to set up PPPoA connections. With

PPPoA, the connection is configured so that the PPP data flow is transported directly over an ATM network (RFC 2364).

When using the internal DSL modem, a PPPoA interface must be configured with **Client Type** = *On Demand* for this connection in **WAN**->**ATM**->**Profiles**->**New**.

2.2.7.1 New

Choose the **New** button to set up new PPPoA interfaces.

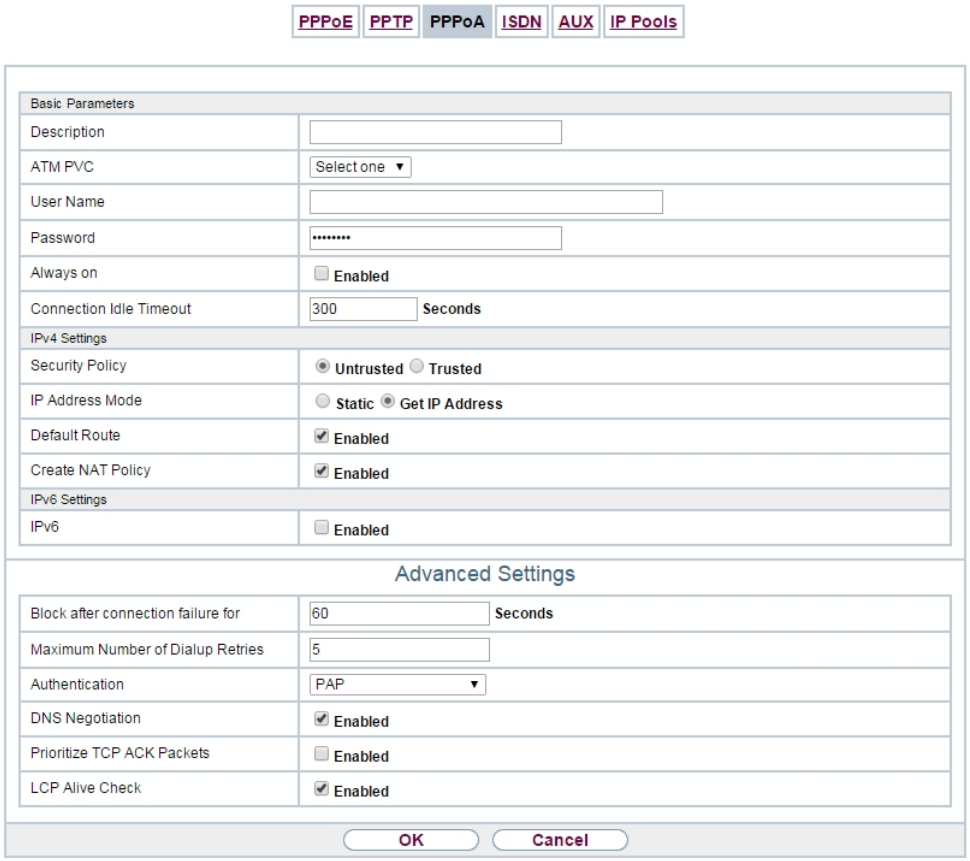

Abb. 9: **WAN**->**Internet + Dialup**->**PPPoA**->**New**

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

Fields in the menu IPv6 Settings

Field	Description
IPv6	Select whether the selected ATM profile is to use Internet Proto-

Field	Description
	col version 6 (IPv6) for data transmission. The function is activated by selecting *Enabled*. The function is disabled by default.
Security Policy	Select the security settings to be used with the selected ATM profile. Possible values: • *Untrusted* (default value): Only those IP packets that can be assigned to a connection, which were set-up from a trustworthy zone are allowed through. We recommend you use this setting if you want to use IPv6 outside of your LAN. • *Trusted*: All IP packets are allowed through except for those which are explicitly prohibited. We recommend you use this setting if you want to use IPv6 on your LAN. You can configure exceptions for the selected setting in the **Firewall** menu.
IPv6 Mode	Only for **IPv6** = *Enabled* The selected ATM profile is operated in host mode.
Accept Router Advertisement	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Host* Select whether router advertisements are to be received via the ATM profile. The default router list and the prefix list are created by the router advertisements. The function is activated by selecting *Enabled*. The function is enabled by default.
DHCP Client	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Host* Define whether your device is to be run as a DHCP client. The function is activated by selecting *Enabled*.

Field	Description
	The function is enabled by default.

2.2.8 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 are displayed according to priority in the **VPN**->**IPSec**->**IPSec Peers** menu.

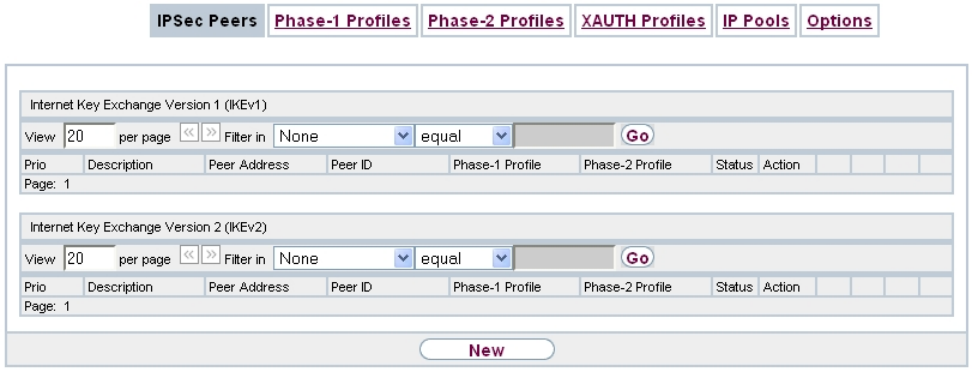

Abb. 10: **VPN**->**IPSec**->**IPSec Peers**

2.2.8.1 New

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

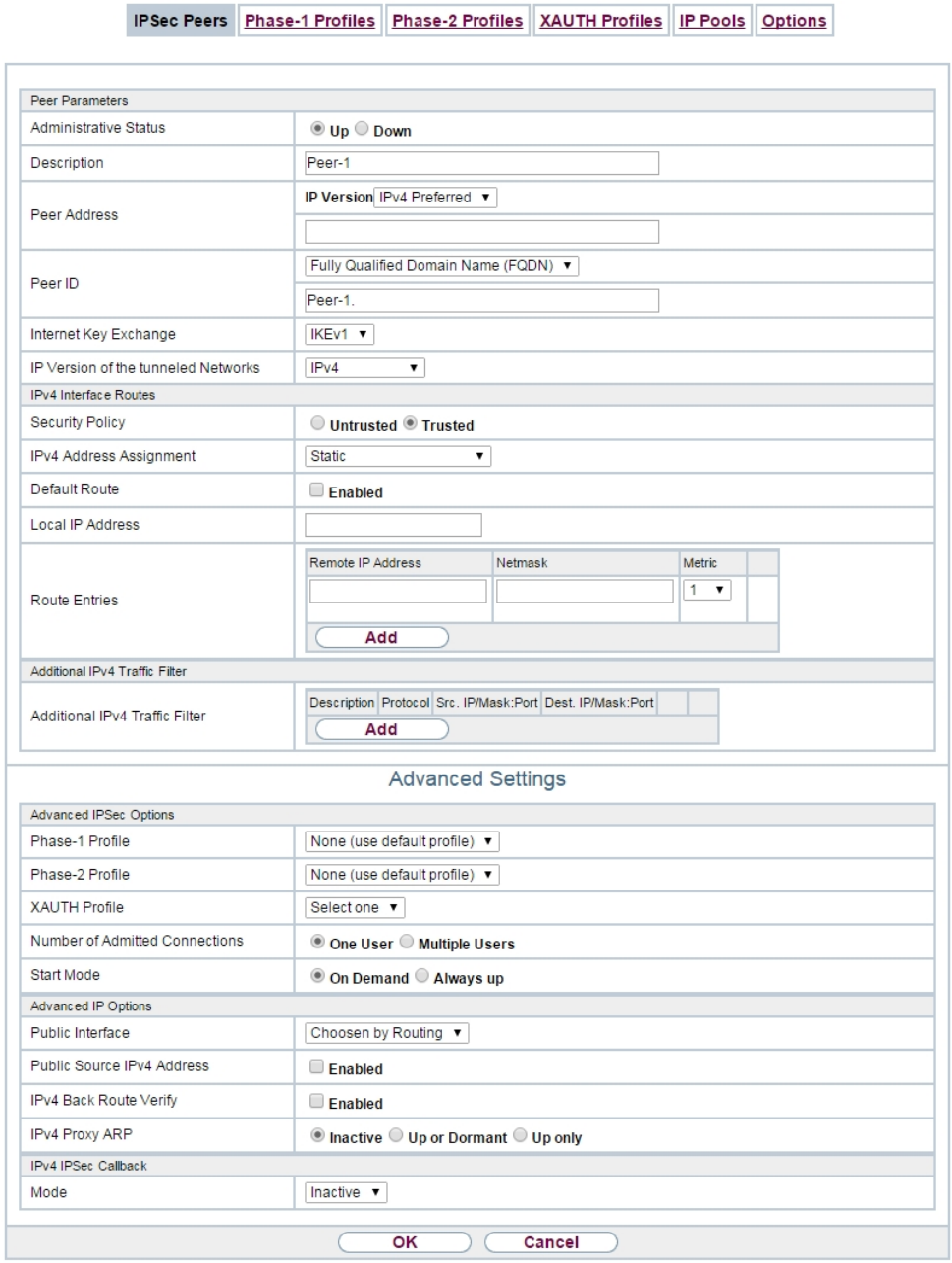

Abb. 11: **VPN->IPSec->IPSec Peers->New**

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

Relevant fields in the menu Peer Parameters

Field	Description
Peer Address	Select the **IP Version**. You can select whether IPv4 or IPv6 is to be used or whether only one of the two IP versions is to be allowed. **Hinweis** This selection is only relevant if a host name is entered as a peer address. Possible values: • *IPv4 Preferred* • *IPv6 Preferred* • *IPv4 Only* • *IPv6 Only* 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.
IP Version of the tunneled Networks	Select whether IPv4 or IPv6 or both versions are to be applicable for the VPN tunnel. Possible values: • *IPv4* • *IPv6* • *IPv4 and IPv6*

Fields in the menu IPv6 Interface Routes

Field	Description
Security Policy	Select the security settings to be used with the interface. Possible values: • *Untrusted*: Only those IP packets that can be assigned to a connection, which were set-up from a trustworthy zone are allowed through.

Field	Description
	We recommend you use this setting if you want to use IPv6 outside of your LAN. • *Trusted* (default value): All IP packets are allowed through except for those which are explicitly prohibited. We recommend you use this setting if you want to use IPv6 on your LAN. You can configure exceptions for the selected setting in the **Firewall** menu.
Local IPv6 Network	Select a network. You can select among the link prefixes which are created under **LAN**->**IP Configuration**->**Interfaces**->**New**. Enter the local IPv6 address along with the corresponding prefix length. This prefix must end with ::. By default the prefix length / 64 is predefined.
Remote IPv6 Network	Add a new **Prefix** with **Add**. Enter the address of the tunnel remote terminal. By default a **Length** of *64* and a **Priority** of *1* is predefined. The lower the value of the priority, the higher the priority of the route.

2.2.9 IPv6 Filter Rules

A list of all configured IPv6 filter rules is displayed in the **Firewall**->**Policies**->**IPv6 Filter Rules** menu.

Hinweis

Please not that - in comparison to IPv4 firewall - the IPv6 firewall is always switched on and cannot be switched off.

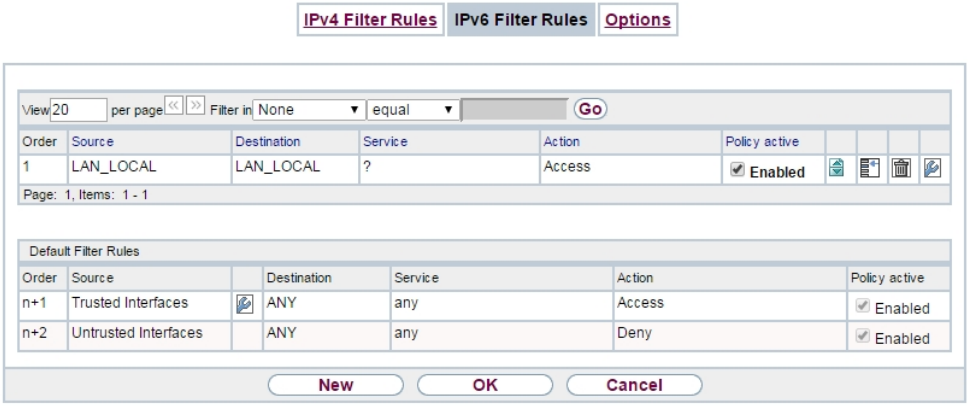

Abb. 12: **Firewall->Policies->IPv6 Filter Rules**

With the button in the **Trusted Interfaces** line, you can determined which are **Trusted** interfaces. A new window with a interface list appears. You can mark the individual interfaces as trustworthy.

Hinweis

Please note that the interface list for IPv6 is empty as long as IPv6 is not enabled for any interface.

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 dialogue box opens, in which you can select the position to which the policy is to be moved.

2.2.9.1 New

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

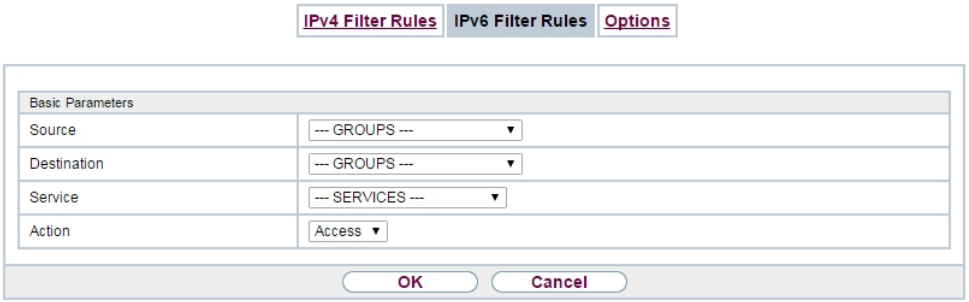

Abb. 13: **Firewall->Policies->IPv6 Filter Rules->New**

The **Firewall->Policies->IPv6 Filter Rules->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Source	Select one of the preconfigured aliases for the source of the packet. In the list all WAN/LAN interfaces, interface groups (see **Firewall->Interfaces->IPv6 Groups**), addresses (see **Firewall->Addresses->Address List**) and address groups (see **Firewall->Addresses->Groups**) are available for selection for which the IPv6 is enabled.
Destination	Select one of the preconfigured aliases for the destination of the packet. In the list all WAN/LAN interfaces, interface groups (see **Firewall->Interfaces->IPv6 Groups**), addresses (see **Firewall->Addresses->Address List**) and address groups (see **Firewall->Addresses->Groups**) are available for selection for which the IPv6 is enabled.
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*

Field	Description
	• *http* • *nntp* Additional services are created in **Firewall**->**Services**->**Service List**. In addition, the service groups configured in **Firewall**->**Services**->**Groups** can be selected
Action	Select the action to be applied to a filtered packet. Possible values: • *Access* (default value): The packets are forwarded on the basis of the entries. • *Deny* : The packets are rejected. • *Reject* : The packets are rejected. An error message is issued to the sender of the packet.

2.2.10 IPv6 Groups

A list of all configured IPv6 interface routes is displayed in the **Firewall**->**Interfaces**->**IPv6 Groups** menu.

You can group together the interfaces of your device. This makes it easier to configure firewall rules.

2.2.10.1 New

Choose the **New** button to set up new IPv6 interface groups.

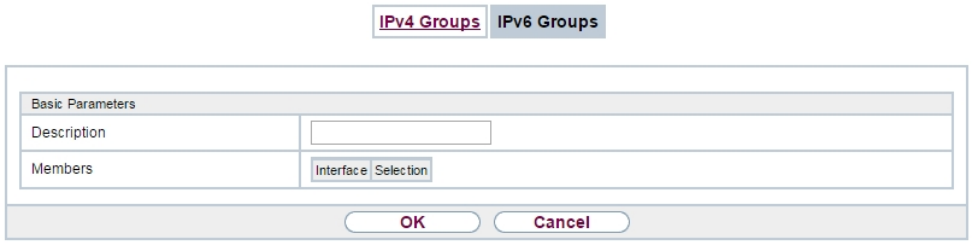

Abb. 14: **Firewall**->**Interfaces**->**IPv6 Groups**->**New**

The **Firewall**->**Interfaces**->**IPv6 Groups**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter the desired description of the IPv6 interface group.
Members	Select the members of the group from the available interfaces. To do this, activate the field in the **Selection** column.

2.2.11 Address List

A list of all configured addresses is displayed in the **Firewall**->**Addresses**->**Address List** menu.

2.2.11.1 New

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

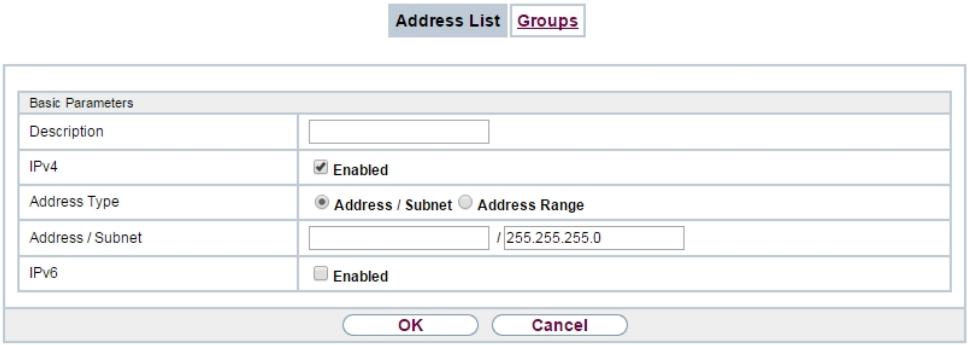

Abb. 15: **Firewall**->**Addresses**->**Address List**->**New**

The **Firewall**->**Addresses**->**Address List**->**New** menu consists of the following fields:

Relevant fields in the menu Basic Parameters

Field	Description
IPv6	Allows configuration of IPv6 address lists. The function is enabled with *Enabled*. The function is disabled by default.
Address / Prefix	Only for **IPv6** = *Enabled* Enter IPv6 address and the related prefix.

2.2.12 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.

2.2.12.1 New

Choose the **New** button to set up additional address groups.

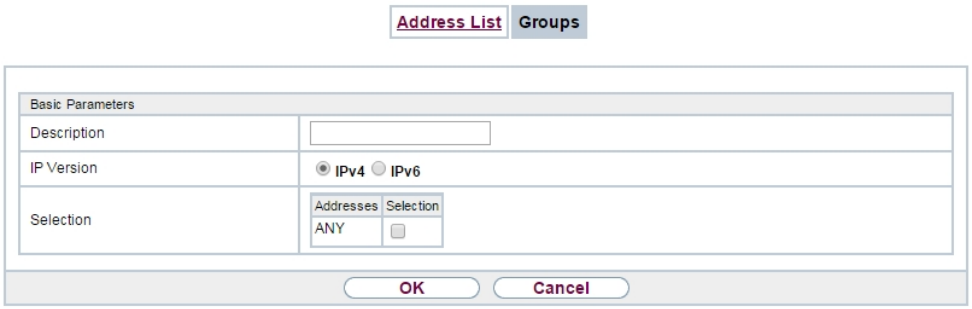

Abb. 16: **Firewall**->**Addresses**->**Groups**->**New**

The **Firewall**->**Addresses**->**Groups**->**New** menu consists of the following fields:

Relevant field in the menu Basic Parameters

Field	Description
IP Version	Select the IP version used. Possible values: • *IPv4* • *IPv6* *IPv4* is selected by default.

2.2.13 DNS Servers

A list of all configured DNS servers is displayed in the **Local Services**->**DNS**->**DNS Servers** menu.

2.2.13.1 Edit or New

Select 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.

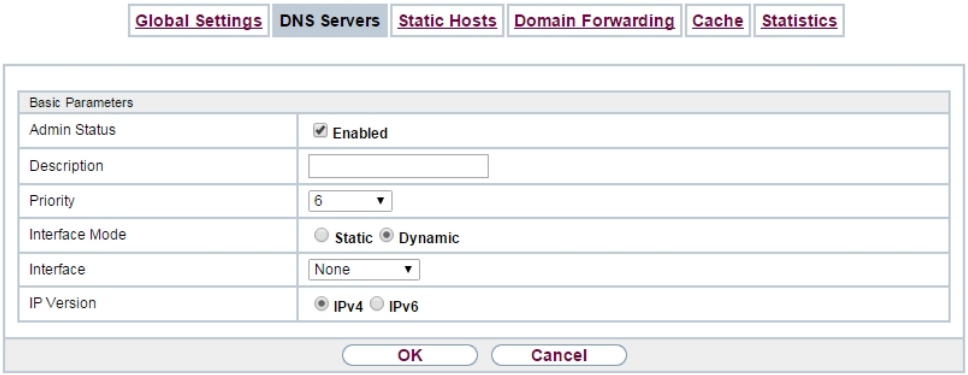

Abb. 17: **Local Services->DNS->DNS Servers->New**

The **Local Services->DNS->DNS Servers->New** menu consists of the following fields:

Relevant fields in the menu Basic Parameters

Field	Description
IP Version	Select the IP version used. Possible values: • *IPv4* • *IPv6* *IPv4* is selected by default.
Primary IPv6 DNS Server	Only if **Interface Mode** = *Static* Enter the IPv6 address of the first name server for Internet address name resolution.

Field	Description
Secondary IPv6 DNS Server	Only if **Interface Mode** = *Static* Optionally, enter the IPv6 address of an alternative name server.

2.2.14 DHCPv6-Server

Alternatively, you can use your device as a DHCPv6 server. This DHCPv6 server can distribute IP addresses and DHCP options to clients or just DHCP options without addresses. These parameters are summarised in a so-called "Option Set". An option set can be linked to an interface (see under **Local Services**->**DHCPv6 server**->**DHCPv6 server**->**New**) or it can be globally configured (see under **Local Services**->**DHCPv6 server**->**DHCPv6 server global options**->**New**). DHCP options can, for example, contain information on DNS servers or time servers.

Hinweis

An IPv6 address pool occurs by allocating an IPv6 link prefix (subnet with the length / 64) to a DHCPv6 option set. The definition of a separate section of IPv6 addresses, e.g., fc00:1:2:3::1..fc00:1:2:3::100, unlike in DHCPv6, is not provided.

For the configuration of an IPv6 address pools, the following system requirements must be met:

(a) IPv6 must be enabled on the relevant interface.

(b) An IPv6 link prefix (subnet) with the length /64 must be configured on the desired interface. An IPv6 link prefix can be defined on two types:

- The IPv6 link prefix is derived from a general IPv6 prefix (prefix with a length of, for example /56 or /48). In this case, the general IPv6 prefix must be configured in the **Networking**->**General IPv6 prefixes**->**General Prefix Configuration** menu.
- The IPv6 link prefix with the length /64 is manually configured on the corresponding interface and not derived from a general IPv6 prefix.

(c) The **DHCP Server** option must be enabled for the interface.

Furthermore, the following settings are recommended:

- The values for the **Preferred Lifetime** and **Valid Lifetime** options should be set to values that are bigger than the value for **Router Lifetime**.

  In the case of a **Router Lifetime** of 600 seconds, e.g., a **Preferred Lifetime** if 900 seconds and a **Valid Lifetime** of 1800 are recommended.

- The **DHCP Mode** option is to be enabled.

To set the aforementioned options, select the **LAN**->**IP configuration**->**Interfaces** menu. Using the symbol, select the desired interface. Enable IPv6 and set **IPv6 Mode** to *Router (Transmit Router Advertisement)*. In the **IPv6 Addresses** field click on **Add** and configure the link prefix. Press **Apply** to confirm your configuration. The configuration of the recommended settings then takes place in the following menus:

- **Router Lifetime**: **LAN**->**IP configuration**->**Interfaces**->**New**->**Advanced Settings**->**Advanced IPv6 Settings**
- **Preferred Lifetime** and **Valid Lifetime**: **LAN**->**IP configuration**->**Interfaces**->**New**->**Basic IPv6 Parameters**->**Add**->**Advanced**

Here - with regard to an interface - you can create address pools in an option set and define DHCP options.

2.2.14.1 Edit or New

Select the **New** button to create a option set. Select the icon to edit existing entries.

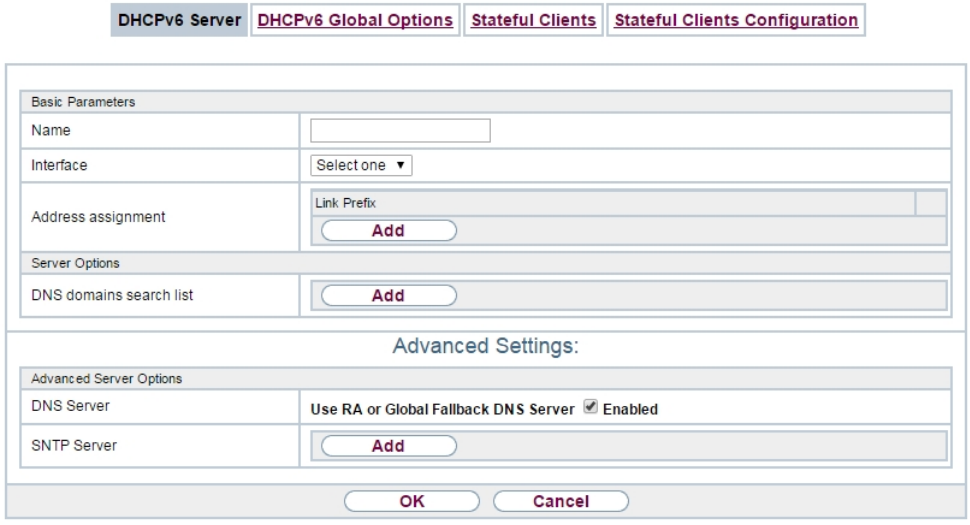

Abb. 18: **Local Services**->**DHCPv6 Server**->**DHCPv6 Server**->**New**

The menu **New** consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Name	Enter a name for the option set.
Interface	Select the IPv6 interface to which the option set should be linked. Interfaces with the following configuration are available for selection: • IPv6 is activated. • The **DHCP Server** option is enabled. In the ex works state, IPv6 is deactivated for all interfaces. If the desired interface is not available for selection, you can configure it in the **LAN**->**IP Configuration**->**Interfaces** menu according to the instructions of the mentioned policies.
Address assignment	The definition of an IPv6 address pool occurs through the allocation of an IPv6 link prefix (subnet with the length /64) to a DHCPv6 option set. The IPv6 address pool always includes the complete 64 bit address range of the selected IPv6 link prefix. The address assignment takes place randomly. With **Add** you can assign one or several IPv6 link prefixes to the IPv6 option set.  **Hinweis** Please note that the only IPv6 link prefixes that are assigned to selected interfaces are available for selection.

Fields in the menu Server options

Field	Description
DNS domains search list	Using **Add** you can create a list of domain names which are to be used on the client page as domain search lists for name resolution (DHCPv6 option 24 "Domain Search List"). The domain names are transmitted to clients according to the sequence specified by the lists.

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

Fields in the Advanced Server Options menu

Field	Description
DNS Server	Here, you can configure the DNS servers that are to be propagated via DHCPv6 (DHCPv6 option 23 "DNS Recursive Name Server"). In the default setting, the global DNS servers of the system are propagated. (The global DNS servers are configured in the **DNS Propagation** field in the **LAN**->**IP Configuration**->**Interfaces**->->**Advanced Settings** menu with **IPv6** = *Enabled*.) However, DNS servers can be manually specified and transmitted to clients. To do so, deactivate the **Use RA or Global Fallback DNS Server** option and using **Add** create the desired DNS server entries.
SNTP server	Here, you can configure the time servers that are to be propagated via DHCPv6 (DHCPv6 option 31 "Simple Network Time Protocol Server"). Using **Add** you can create the desired time server entries.

2.2.15 DHCPv6 Global Options

In this menu, you can configure the globally valid DHCPv6 options for the DHCPv6 server. An option configured here is always propagated if there is no exact definition (e.g., not interface-specific or vendor ID-specific definition) for this option.

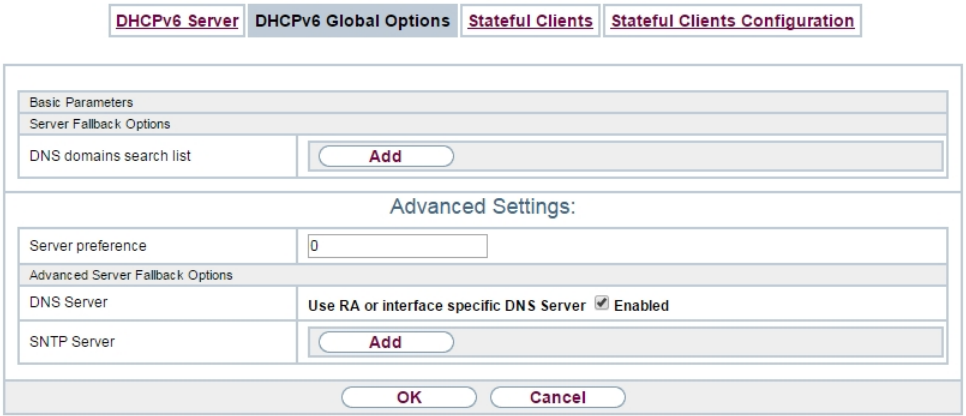

Abb. 19: **Local Services**->**DHCPv6 Server**->**DHCPv6 Global Options**

The menu **New** consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
DNS domains search list	Using **Add** you can create a list of domain names which are to be used on the client page as domain search lists for name resolution (DHCPv6 option 24 "Domain Search List"). The domain names are transmitted to clients according to the sequence specified by the lists. The domain name (e.g., dev.bintec.de) must end with a dot (.).

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

Fields in the menu Server preference

Field	Description
Server preference	The DHCPv6 option 7 preference may be included in the DHCPv6 advertisement sent to the clients from the DHCPv6 servers. Possible values are *0...255*. In a network with several DHCPv6 servers, this option controls which DHCPv6 servers have the highest priority in the network. If a client receives DHCPv6 advertisements with different priorities from different servers, the client usually takes over the values of the server with the highest priority. However, the client can accept DHCPv6 advertisement with a lower priority, if the parameter set included in the DHCPv6 advertisement corresponds to more of the options requested by the client. The *0* value means "not specified" (lowest priority), *255* means the highest priority.

Fields in the menu Advanced Server Options

Field	Description
DNS Server	Here, you can configure the DNS servers that are to be propagated via DHCPv6 (DHCPv6 option 23 "DNS Recursive Name Server"). In the default setting, the global DNS servers of the system are propagated. (The global DNS servers are configured in the **DNS Propagation** field in the **LAN**->**IP Configuration**->**Interfaces**->  ->**Advanced Settings** menu with **IPv6** = *Enabled*.)

Field	Description
	However, DNS servers can be manually specified and transmitted to clients. To do so, deactivate the **Use RA or Global Fallback DNS Server** option and using **Add** create the desired DNS server entries.
SNTP server	Here, you can configure the time servers that are to be propagated via DHCPv6 (DHCPv6 option 31 "Simple Network Time Protocol Server"). Using **Add** you can create the desired time server entries.

2.2.16 Stateful Clients

Here you will find information on stateful clients as soon as these have obtained an IPv6 address.

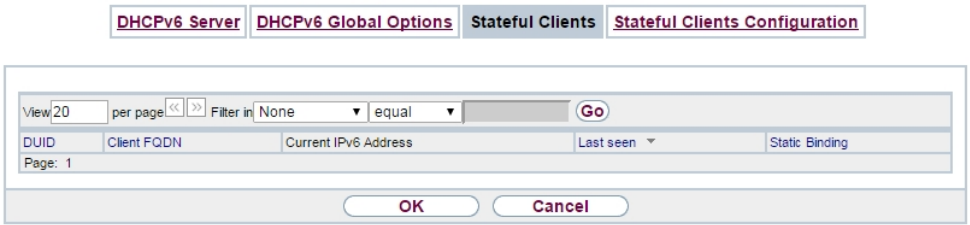

Abb. 20: **Local Services->DHCPv6 Server->Stateful Clients**

2.2.17 Stateful Clients Configuration

In a stateful configuration of IPv6 clients, the client will be transmitted the IPv6 prefix in addition to the DHCP options.

2.2.17.1 Edit or New

select the **New** button to create stateful clients. Usually you do not need to create any entries. Choose the icon to edit existing entries. You should open each automatically created entry to check the content and adapt it if necessary.

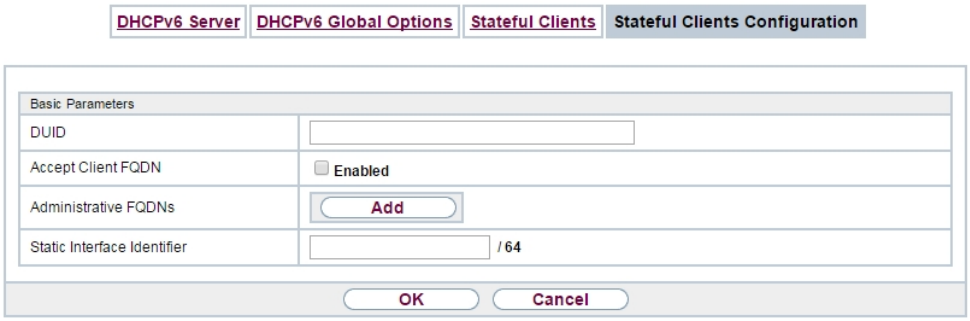

Abb. 21: **Local Services->DHCPv6 Server->Stateful Clients Configuration+New**

The menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
DUID	A client uses the **DUID** (DHCP unique identifier) field to identify themselves and to obtain an IP address from DHCPv6 servers. If you create an entry with the **New** button, you can enter the **DUID** as a 16- to 20- digit HEX number. You can enter it with the minus separator as in Windows or as a block without a separator as in Linux.
Accept Client FQDN	If **Accept Client FQDN** is enabled, the client will enter the domain name server with the parameter FQDN (Fully Qualified Domain Name) in the cache.
Administrative FQDNs	Even in automatically created entries, you can enter the parameter FQDN (Fully Qualified Domain Name) using **Add**.
Static Interface Identifier	The **Static Interface Identifier** field is the host share of the IPv6 address, i.e., the last 64 bit of the IPv6 address. This prefix must start with ::.

2.2.18 Ping Test

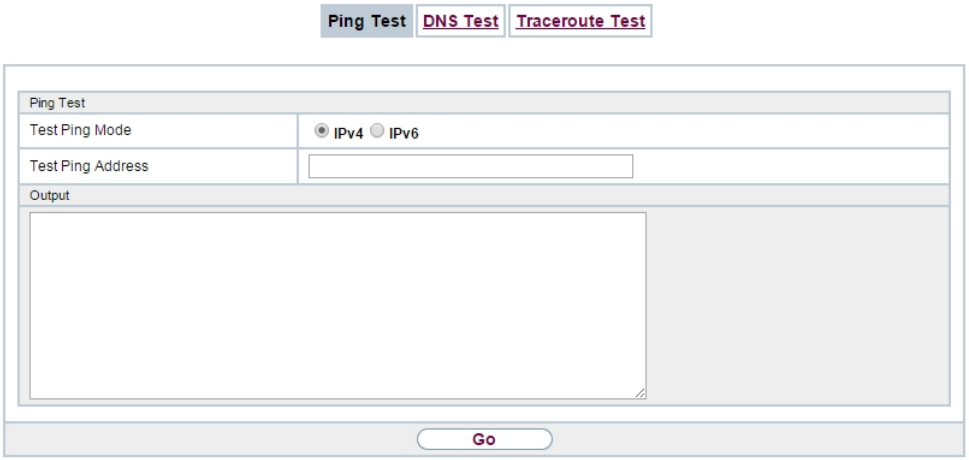

Abb. 22: **Maintenance->Diagnostics->Ping Test**

You can use the ping test to check whether a certain host in the LAN or an internet address can be reached.

Relevant fields in the menu Ping Test

Field	Description
Test Ping Mode	Select the IP version to be used for the ping test. Possible values: • *IPv4* • *IPv6*
Use Interface	Only for **Test Ping Mode** = *IPv6* For link local addresses select the interface to be used for the ping test. *Default* can be used for global addresses.

Pressing the **Go** button starts the ping test. The **Output** field displays the ping test messages.

2.2.19 Traceroute Test

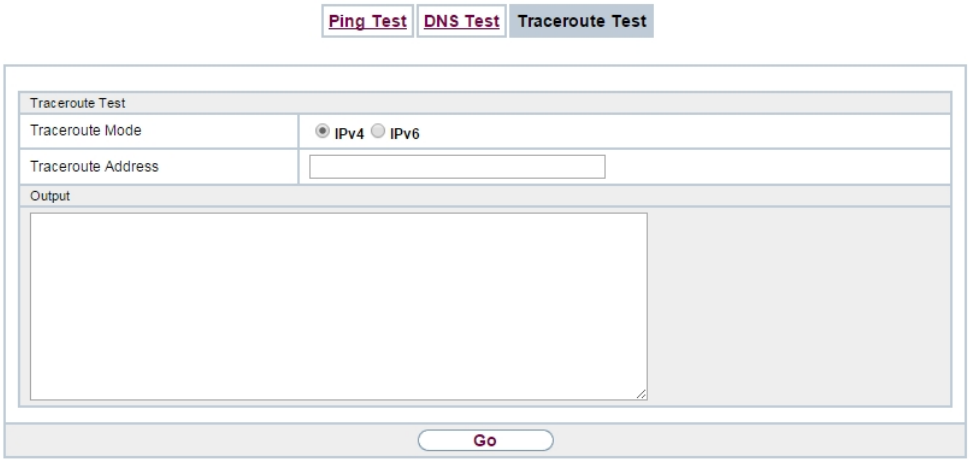

Abb. 23: **Maintenance->Diagnostics->Traceroute Test**

You use the Traceroute test to display the route to a particular address (IP address or domain name), if this can be reached.

Relevant field in the menu Traceroute Test

Field	Description
Traceroute Mode	Select the IP version to be used for the Traceroute test. Possible values: • *IPv4* • *IPv6*

Pressing the **Go** button starts the Traceroute test. The **Output** field displays the traceroute test messages.

2.3 IPSec - New algorithms

From **Systemsoftware 10.1** onwards, there are new algorithms available for IPSec. In the **VPN->IPSec->Phase-1 Profiles->Create new IKEv1 profile or Create new IKEv2 profile->New** or **VPN->IPSec->Phase-2 Profiles->New** menu, the new hash algorithms *SHA2-256*, *SHA2-384* and *SHA2-512* are available under **Proposals**. They can be selected in the GUI under the designation **Authentication**.

SHA2 is the successor of SHA1. The number that follows "SHA2" states the respective length of the hash value. In contrast to SHA1, the hash algorithm SHA2 is currently reliable.

In the **VPN**->**IPSec**->**Phase-1 Profiles**->**Create new IKEv2 profile**->**New** the new Diffie-Hellman groups *14 (2048 Bit)*, *15 (3072 Bit)* and *16 (4096 Bit)* are available under **Proposals**.

The Diffie-Hellman groups determine the strength of the key. Larger group numbers mean more security but require a greater computing effort for the calculation of the key.

Hinweis

Please observe the following information on this expansion:

The new algorithms - particularly those for the generation of long keys for the Diffie-Hellman exchange - require significant computing effort. The following device will support these new algorithms:

- bintec RS3xx- and RS123x series
- be.IP series
- bintec RXL series.

Depending on the number of active IPSec tunnels, a partially significant influence on the device's performance must be expected in all devices. In a later release, the bintec RXL series will have hardware support of the algorithms added which will lead to a significant increase in performance compared to the merely software-based solutions.

The devices of Rxx02- and RTxx02 series do NOT support the new algorithms due to their older hardware equipment.

2.4 IKEv2 Routing

From **Systemsoftware 10.1.4** onwards, the so-called "IKEv2 routing" will be available for the set-up of a tunnel with a Cisco FlexVPN server as a remote terminal. You bintec router as a client communicates its networks to the FlexVPN server which enters it into its routing table.

2.5 WLAN Several bridge links available

From **Systemsoftware 10.1.4** onwards, several entries for bridge links can be created in the slave mode in the **Wireless LAN**->**WLAN**->**Bridge Links** menu.

2.6 Maintenance - new options (hybrid)

From **Systemsoftware 10.1.4** onwards, the new *Import Additional Files (to usb storage)* and *Format MMC/SD Card* options will be available in the **Maintenance**->**Software &Configuration**->**Options** menu in the **Action** field for all devices of the hybird series which contain an inserted SD card.

2.7 SIA

From **Systemsoftware 10.1.4** onwards, in the **External Reporting**->**SIE**->**SIA** menu, a file can be created that delivers support with comprehensive information on the status of the device, e.g., the current configuration, available storage, running time of the device etc.

2.8 Factory reset

From **Systemsoftware 10.1.4** onwards, you can reset your device via the GUI in the **Maintenance**->**Factory Reset** menu in the ex works state.

2.9 Display manufacturer via MAC address

From **Systemsoftware 10.1.4** onwards, you can switch the display of the manufacturer in the MAC address on or off in the **System Management**->**Global Settings**->**System** menu. Up to eight characters are used at the beginning of the MAC address for the manufacturer name (usually an abbreviation thereof). Instead of *00:a0:f9:37:12:c9* the manufacturer display will display, for example, *BintecCo_37:12:c9*.

2.10 New DNS menu

2.10.1 Dynamic Hosts

In the **Local Services**->**DNS**->**Dynamic Hosts** you can see the relevant information on the dynamic DNS entries.

Abb. 24: **Local Services->DNS->Dynamic Hosts**

2.11 Log out Users

It may happen that the functions of the configuration interface are impaired due to an incompletely set-up configuration session. In this case, all existing connections for the GUI can be viewed and ended in this menu, if necessary.

2.11.1 Log out Users

This menu first shows a list of all the active configuration connections.

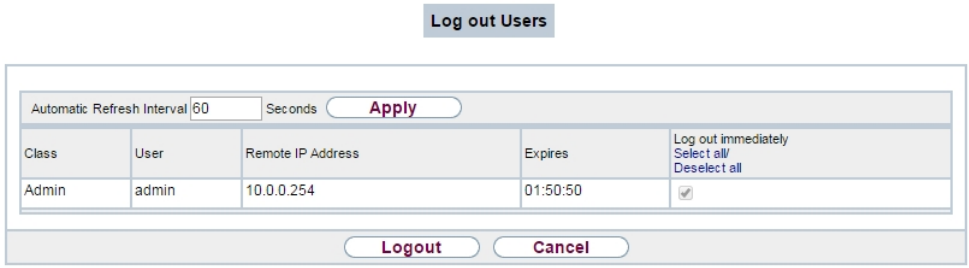

Abb. 25: **Maintenance->Log out Users->Log out Users**

Fields in the menu Log out Users

Field	Description
Class	Displays the user class that the registered used belongs to.
User	Displays the user name.
Remote IP Address	Displays the IP address from which the connection was set-up. This can be the address of a PC but also the address of an intermediately stored router.
Expires	Displays when the connection will be automatically disconnected.

Field	Description
Log out immediately	If you activate the control boxes, the user will be logged out of the system **Logout** with one click.

2.11.1.1 Logout Options

Once you have confirmed the selection of ending the connect with logging off, you can select whether and which configurations that are linked to the session in questions, are saved prior to logging of the user.

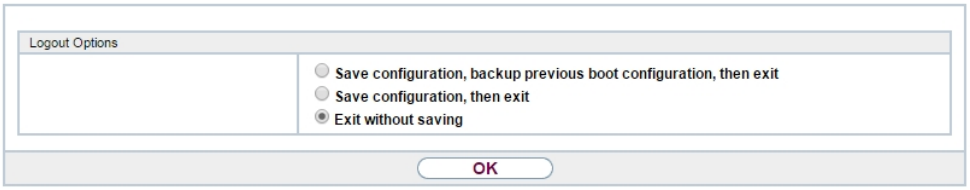

Abb. 26: **Maintenance->Log out Users->Logout**

2.12 Automatic VDSL/ADSL mode

In the **WAN->Internet + Dialup->PPPoE->New** menu in the **PPPoE Ethernet Interface** field, the `Automatic` value is available to support the automatic VDSL/ADLS mode which was already available in the assistants. In this mode, the interface for internet access is selected automatically. Please note that an interface must be created for an ADLS access in the ATM menu; this is not necessary for a VDSL access.

2.13 Firewall - Reset

From **Systemsoftware 10.1.4** onwards, you can reset the firewall on your ex works setting in the **Firewall->Policies->Options** menu.

2.14 Emergency calls

From **Systemsoftware 10.1.4** onwards, the emergency call will be prioritised. If all available channels (even SIP channels are considered) are busy, an current call will be ended to be able to send the emergency call.

2.15 elmeg IP680 available

The IP telephone **elmeg IP680** is available from **Systemsoftware 10.1.4** onwards. It is automatically recognised by the elmeg hybrid systems and displayed as a terminal under **Terminal**->**elmeg system phones**->**elmeg IP**.

2.16 Telephones in teams

If teams are used, from **Systemsoftware 10.1.4** onwards, the *On No Reply* and *On Busy* functions can be used because inactive telephones are automatically logged out of the teams.

Kapitel 3 Changes

The following changes have been made in **Systemsoftware 10.1.4** .

Hinweis

Please note that a change for different devices may be available at time different times.

3.1 Password change when you first log on.

From **Systemsoftware 10.1.4** onwards, the page to change the password will be opened as long as the Admin password has not been changed and the login page is not displayed as before. The administrator now no longer has to be logged in to change his/her password.

3.2 PBX assistant upgraded

In the **Assistants**->**PBS** menu, the PBS-assistant was expanded by the tabs **First Steps**, **Terminals** and **Call Distribution**.

3.3 Designation adjusted

Due to the introduction of IPv6, a few designations under IPv4 were adjusted for improved distinctness, e.g., in the **Firewall**->**Policies**->**Options** menu, the field **Firewall Status** was renamed **Status of the IPv4 Firewall**.

3.4 Menu description changed

The menu description **Terminals**->**elmeg System Phones**->**elmeg IP1x** was changed in **Terminals**->**elmeg System Phones**->**elmeg IP**.

3.5 Domain forwarding changed

In the **Local Services**->**DNS**->**Domain Forwarding**->**New** menu, the entry possibilities were expanded with **Forwarding** = *Domains* in the **Domains** field.

Until now, for example, **Domains** could be entered as **.qa.bintec.de* in order to use **.qa.bintec.de*.

From **Systemsoftware 10.1.4** onwards, a leading wild card is automatically entered during input without the *** leading wild card and after confirming with **OK**. For example, you can enter *.qa.bintec.de* or *qa.bintec.de* and use **.qa.bintec.de* after automatically confirming with **OK**.

3.6 VDSL - TCP Upstream Performance improved

In VDSL-connections, the TCP Upstream Performance was significantly improved by reducing the packet loss and it now moves in the same area as comparable devices of other manufacturers.

3.7 LEDs for bintec RS353jv-4G changed

From **Systemsoftware 10.1.4** onwards, the LEDS *LTE* and *USB* in the **bintec RS353jv-4G** device show the following behaviour:

LED status display

LED	Colour	Status	Information
LTE	green	flashing in a 1-second interval	Mobile connection is initialised
	green	on	WAV-connection established.
	green	flashing in overhaul interval	Data traffic via 3G/4G
	green	flashing in a 3-second interval	An error has occurred
		off	So SIM card in device
USB	green	on	USB0LTE stick installed
	green	flashing	Data traffic via USB
		off	No USB connection.

Wireless standard

Via the **biboadmledmeter** MIB-variable, you can activate an additional LED mode, which

enables you to determine the state of the mobile connection. With **biboadmledmeter**= *1* you activate the mode, with **biboadmledmeter**= *2* you deactivate it. If you do not want to save the state of the LED mode, you can also activate it by pressing the reset-button three times in a row for approx. 1 second. By briefly pressing the button once more, the mode is deactivated again.

The following link exists between the lights of an LED and the wireless standard in use:

LED	**Wireless standard**
BRI	GSM
USB	UMTS
LTE	LTE

Furthermore, you can read the signal quality from the eight Ethernet LEDs. If all eight LEDS are on, this presents an almost perfect connection. If the signal quality if low, fewer LEDS will be illuminated.

3.8 WLAN - configuration possibilities

Depending on the configuration, there are different numbers of masters and slaves available in the WLAN:

Operation Mode	Channel	Supports
Off		
Access Client	Auto/fixed value	1 Client
Bridge Link Client	Auto	1 Slave (with several of the first in the list)
Bridge Link Client	Fixed value	x Slaves
Access Point / Bridge Link Master	Auto	x Access Points + x Masters
Access Point / Bridge Link Master	Fixed value	x Access Points + x Masters + x Slaves

3.9 SIP connections improved

SIP interruptions are recognised quicker and rectified

Kapitel 4 Troubleshooting

The following bugs have been fixed in **Systemsoftware 10.1.4** :

Hinweis

Please note that a troubleshooting for different devices may be available at time different times.

4.1 Stacktrace:

ID 19229

If an Ethernet interface, e.g., *en1-0* and a WLAN interface, e.g., *vss7-10* were assigned to the same bridge group *br0* a sporadic stracktrace would occur.

4.2 Panic (hybird 600)

ID 19574

It can happen that a *hybird 600*parameter> restarts every day. In a few of the connected phones, there were problems with the call connection.

4.3 Assistants - Internet assistant incorrect

ID 19394

If the Internet assistant was used, the **connection type** = *UMTS/LTE* was set and **Always active** was *activated* the assistant created two default routes.

4.4 Internet assistant - Incorrect parameter

ID n/a

Under specific conditions, *t-online-com/* was added in the Internet assistant by mistake by the system with a correctly entered user name.

4.5 Problems with Telekom Speedstick LTE V

ID 19147

The Telekom Speedstick LTE V (Huawei E3372) does not work correctly.

4.6 Internet connection down

ID n/a

If an interface was clicked, it may happen that an Internet connection was capped that was already set-up.

4.7 Bad performance

n/a

In a bridging scenario where the data traffic from the Ethernet was forwarded in a WLAN, it may happen that the CPU was operating to almost 100% capacity.

4.8 The same icon for different actions

ID n/a

The same  symbol was used start and reset the actions by mistake. From **Systemsoftware 10.1.4** onwards, the  symbol is available to reset the actions. For example, you can reset the profiles in ex works state under **System administration**->**Configuration access**->**Access profile**.

4.9 Error message incorrect

ID 19420

When entering the **country code** it may happen that an incorrect error message was displayed.

4.10 Entries cannot be deleted

ID 19638

It was not possible to delete entries in the **Physical Interfaces**->**ISDN Ports**->**MSN Configuration** menu using the  symbol.

4.11 Unintentional separation of a connection (hybird)

ID 19334

It can happen that a connection selected by elmeg was disconnected after external transfer.

4.12 Firmware update failed

ID 19327

A firmware update was not possible without an IPv6 connection.

4.13 LTE - Echo request packets did not reach their destination

ID 19333

Echo request packets that were generated on a router with in integrated LTE(4G) modem using Keepalive Monitoring did not reach the target host.

4.14 Roaming problems

ID n/a

In M2M cards problems with data roaming may occur.

4.15 SSH - Connection failed

ID 19213

After a proper router operation of approximately 2 days, the SSH connection suddenly failed.

4.16 Wrong page

ID 19506

It can happen that a wrong page is loaded after logging in.

4.17 Configuration session incomplete

ID 19493

It can happen that a configuration session could not be ended and TR069 could not be configured if the user just closed the browser - instead of logging off.

4.18 Windows 10 Edge Browser - Unwanted line breaks

ID n/a

The unwanted line breaks in the output of the browser window edge (Spartan) was removed by a Microsoft fix. The internal fix was removed because it was no longer required.

4.19 Connection failures (hybird)

ID 19334

Under specific circumstances it could result in connection failures.

4.20 System - LED mode displayed incorrectly (RS series)

19074

In the **System Management**->**Global Settings**->**System** menu, the **LED mode** field was incorrectly displayed in the RS series devices. This field is exclusively provided for WLAN devices.

4.21 SSL - No transmission of configuration files.

ID 19219

No configuration files could be transmitted via a SSL connection.

4.22 FAX not working correctly

ID 19098

When attempting to send a fax, it can happen that a system blockage occurs and the router no longer terminated the connection.

4.23 VoIP - No voice transmission

ID 19184

If a team of an analogue or a ISDN telephone was used, although an incoming call was signalled correctly, there was no voice transmission when the call was received.

4.24 VoIP - Account not usable

ID 19551

When using VoIP clients (e.g. a smart phone with VoIP client or a VoIP telephone) the VoIP account was not usable due to a NAT conflict.

4.25 VoIP - Provider problems

ID n/a

It can happen that providers with specific profiles are not displayed and/or cannot be edited or deleted.

4.26 WLAN - stacktrace

ID 19496

If several SSIDs were created via wireless module and a VSS interface was activated via GUI, a panic occurred at the access point.

4.27 WLAN - Panic

ID 19678

At access points in the slave mode, it can happen that a panic occurs several times a day.

4.28 WLAN - Access Point

ID 19530

If different types of access points were used together, it can happen that the GUI displays strange errors during the configuration of a slave access point or that the slave access point no longer works.

4.29 WLAN - LED mode missing

ID n/a

In the **System Management**->**Global Settings**->**System** menu the **LED mode** parameter was missing in WLAN devices.

4.30 WLAN - Automatic channel selection incorrect

ID 18836

When using a wireless LAN controller with a user-defined channel plan, it can happen that the channel selection does not work correctly with access points from Qualcomm Atheros.

4.31 WLAN - Active wireless module profile not selectable

ID 19198

If at least one access point was managed by the wireless LAN controller, in the **Wireless LAN Controller**->**Slave AP Configuration**->**Slave Access Points**->  menu it was not possible to select a wireless module profile under **Active wireless module profile**.

4.32 Wireless module - Profile displayed incorrectly

ID 19320

In the **Wireless LAN Controller**->**Slave AP Configuration**->**Slave Access Points**->  menu, it was possible to select the `1` value by mistake in the **Active wireless module profile**.

4.33 WLAN Controller - WTP does not work correctly

ID 19553

If several WTPs are managed by one WLAN controller, after switching a WTP on and off it can happen that another WTP is in the wrong state.

4.34 WLAN controller - Stacktrace

19698

If slave access points were managed by one wireless LAN controller, it can happen that a stackrace occured in a few access points.

4.35 Network - Reboots

ID 19484

When using a drop-in group, it resulted in two or three reboots per day.

4.36 QoS - no classification of high priority packets

ID 19527

The internal classification of the high priority packets was interrupted by an active firewall.

4.37 QoS - Configuration incorrect

19366

When using the **First steps** assistants, the QoS configuration was incorrect.

4.38 QoS - 1TR112 requirements not met

ID 19296

The QoS signalisation did not correspond to the 1TR112 requirements.

4.39 Codec problems

ID 19471

If the codec, which was named "Clearmode" according to RFC4040, was up for selection with other codecs, no data could be transmitted.

4.40 Codec problems (hybird 600)

ID 19606

There were problems in the negotiation of the codec between a polycom sound station IP 6000 and a **hybird 600**.

4.41 SIP - connection terminated

19587

It can happen that a connection was terminated after call forwarding.

4.42 SIP - Calls rejected

ID 19486

It can happen that incoming calls were rejected with the 480 status message (Temporarily not available). In doing so, the system issued the debug message "No matching codecs, call rejected".

4.43 SIP - Incoming calls ignored

ID 19432

It can happen that incoming SIP calls were ignored.

4.44 SIP - Incorrect format

ID 19447

Under specific condition, it can happen that an incorrect number format was used.

4.45 Telephony - Calls not possible

ID 19373

It can happen that no calls were possible from the main MSN.

4.46 Telephony - Incorrect connection data

ID 19422

Incorrect connection data was displayed during longer telephone calls.

4.47 Telephony - Provisioning problems

19449

When provisioning individual telephone, it can happen that the provisioning process only worked once and no updates were possible.

4.48 Telephony - Voice connections incorrect (hybird)

ID 19002

It can happen that voice connections were only usable to one side.

4.49 PBS - registration process delayed

ID 19417

Under specific condition, it can happen that numbers are registered with a great deal of delay in a telephone system.

4.50 DISA problem (hybird)

17964

The selection via DISA does not work with SIP connections and DTMF inband.

4.51 Network - Full cone NAT

ID n/a

If the **NAT method** = *full-cone* setting was using the **Network**->**NAT**->**NAT Configuration**->**New** menu, certain problems must have occurred and the NAT session was terminated.

4.52 PPP - No dialin

ID 19156

The PPP dialin via GPRS/GSM does not work.

4.53 ISDN - Call terminated

ID 19080

A short deactivation of ISDN results in a termination of the call.

4.54 IPSec - No data traffic

ID 19538

It can happen that no data was transmitted via IPSec as soon as the underlying PPPoE connection was briefly interrupted.

4.55 SIF - Alias problems

19502

Under specific circumstances the interface alias for the *ANY* interface does not exist for either IPv4 nor IPv6. The interface alias for the *LAN_Local* interface does not exist for IPv4.

4.56 DNS not working

ID 19363

The DNS service is not working because the port was preallocated with an incorrect value when configuring the SIP provider.

4.57 HTTPS - Certificate selection possible by mistake

ID 19511

Although the device family **hybird 300/600** does not support certificates, it was possible to configure certificates in the **System Management**->**Certificates** menu and these certificates can be selected in the **Local Services**->**HTTPS** menu.

4.58 DynDNS-Client - Input option incorrect

ID 19464

In the **Local Services**->**DynDNS Client**->**DynDNS Provider**->**New** menu, the **Update Path** field must not be left empty although it is not useful for each configuration.

4.59 Local services - Scheduling incorrect

ID 18745

If the **Schedule Interval** was set to `0`, configured scheduling actions were carried out by mistake.

4.60 Incorrect alert message

ID 18979

A syslog-message which occurs in each hotspot user-authentication ("HACC: Got IPC-reply: ..."), was displayed as an alert message although it had to do with an incorrect condition.

4.61 Hotspot-Gateway - Storage problem

ID 19274

When using the hotspot gateway together with RADIUS it can happen that a memory overflow occurs.

4.62 Hotspot gateway - Timeout cannot be switched off

ID 19290

In the **Local Services**->**Hotspot Gateway**->**Hotspot Gateway**->**New**->**Advanced Settings** menu it was not possible to enter the `0` value in the **Standard timeout during inactivity** field although this value is permitted to switch off the function.

4.63 BRRP - problems with the virtual router

ID 19252

In BRRP the changes of a virtual router deleted the VLAN ID of the corresponding advertisement interface.

4.64 BRRP - Panics (RXL)

ID 19399

When using BRRP, approx. 6 - 8 reboots per month occurred.

4.65 External reporting - alert service not working correctly

ID 19291

The **Alert Service** in the **External Reporting** menu does not work correct with the *mail.selfhost.de* provider.

4.66 Monitoring - Keepalive Monitoring incorrect

ID 19313

Keepalive Monitoring does not work if the number of the **Successful Attempts** was greater than the number of **Failed Attempts** in the **Local Services**->**Monitoring**->**Hosts**->**New** menu.

4.67 Setup Tool - Incorrect display

ID 18789

When using a **MC7710** type modem, the parameter **LTE Signal Level** = *n/a* was displayed in the setup tool.

4.68 MIB-Tabelle ipsecPeerTable not changable

ID 19222

In the GUI in the **SNMP Browser** view, it was not possible to change the entries in the MIB table **ipsecPeerTable**.