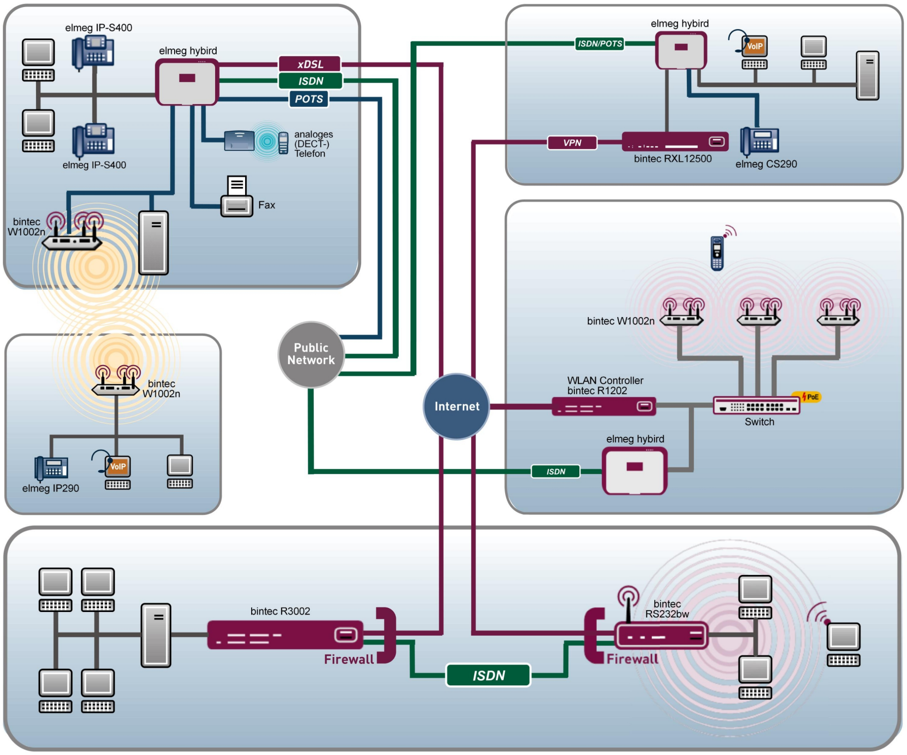

Manual
Release Notes

7.10.5

Copyright© Version 1.0, 2012 Teldat GmbH

Legal Notice

Aim and purpose
This document is part of the user manual for the installation and configuration of Teldat 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.teldat.de* .

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. Teldat Enterprise Communications GmbH is only liable within the terms of its conditions of sale and supply and accepts no liability for technical inaccuracies and/or omissions.

The information in this manual can be changed without notice. You will find additional information and also release notes for Teldat devices under *www.teldat.de* .

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

Trademarks
Teldat trademarks and the Teldat logo, bintec trademarks and the bintec logo, artem trademarks and the artem logo, elmeg trademarks and the elmeg logo are registered trademarks of Teldat Enterprise Communications GmbH.

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

Copyright
All rights reserved. No part of this manual may be reproduced or further processed in any way without the written consent of Teldat GmbH. The documentation may not be processed and, in particular, translated without the consent of Teldat Enterprise Communications GmbH.

You will find information on guidelines and standards in the declarations of conformity under *www.teldat.de* .

How to reach Teldat GmbH
Teldat 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.de*

Table of Contents

Chapter 1 Important Information

1.1 Preparation and update with the FCI

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

Note

Any interruption to the update process may result in your gateway no longer booting up. So do not turn your gateway off while it is updating.

To prepare and carry out any update to **Systemsoftware 7.10.5** using the Graphical Configuration Interface, proceed as follows:

(1) Updating requires the file `XXXXX_bl71005.xxx`, in which `XXXXX` stands for your device. Ensure that the file that you need for the update is available on your PC. If the file is not available on your PC, enter *www.teldat.de* in your browser. The Teldat homepage will open. You will find the required file in the download area for your gateway. Save it to your PC.

(2) Backup the current boot configuration before updating. Export the current boot configuration using the **Maintenance**->**Software &Configuration** menu in the Graphical Configuration Interface. To do this, select: **Action** = *Export configuration*, **Current File Name in Flash** = *boot*, **Include certificates and keys** = *enabled*, **Configuration Encryption** = *disabled* Confirm this with **Go**. 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 system software 7.10.5 using the **Maintenance**->**Software &Configuration** menu. To do this, select: **Action** = *Update system software*, **Source Location** = *Local File*, **Filename** = *XXXXX_bl71005.xxx*. Confirm with **Go**. The message “System request. Please stand by. Your request is being processed.” 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 FCI

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 device>.cf*. Confirm with **Go**. The message “System request. Please stand by. Your request is being processed.” or “System maintenance. Please stand by. Operation in progress.”shows 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** = *R3000_bl71001.r3d*(example). Confirm with **Go**. The message “System request. Please stand by. Your request is being processed.” 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.

Chapter 2 New Functions

Systemsoftware 7.10.5 includes a number of new functions that significantly improve performance compared with the previous version of the system software.

Note

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 Drop In

The new menu **Network**->**Drop In** is available since **Systemsoftware 7.10.5** .

Drop In Mode enables you to separate a network into multiple segments without creating subnets inside the IP network. In order to achive this, multiple interfaces can be collected into a Drop In Group. All interfaces are then assigned to the same netweork and are configured with a single IP address.

The network components of a segment that are connected to one port can now, e.g., be protected by a single firewall configuration. Data traffic between network components of segments connected to different ports are controlled according to the configured firewall rules.

2.1.1 Drop In Groups

The **Networking**->**Drop In**->**Drop In Groups** menu displays a list of all the **Drop In Groups**. Each **Drop In** group represents a network.

2.1.1.1 New

Select the **New** button to set up other **Drop In Groups**.

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.

Field	Description
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 passed on transparently (unmodified). • *Proxy*: ARP packets and IP packets belonging to the Drop In network are passed on with the MAC address of the respective interface.
Network Configuration	Select how an IP address is assigned to the network components. 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 on your device that are a member of the Drop In group.

Field	Description
ARP Lifetime	Specifies how long an ARP entry is kept in the cache. The default value is *3600* seconds.
DNS assignment via DHCP	The gateway can modify packets passing the Drop In group and insert itself as offered DNS server. Possible values: • **Unchanged** (default value) • **Own IP Address** .
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*. The function is disabled by default.
Interface Selection	Select all the ports which are to be included in the **Drop In** group (in the network). Add new entries with **Add**.

2.2 Special Session Handling

With **system software 7.10.5** and later, the new menu **Network**->**Load Balancing**->**Special Session Handling** is provided.

2.2.1 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.

2.2.1.1 Edit or New

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

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

Fields in the Basic Parameters menu

Field	Description
Admin Status	Select whether the Special Session Handling should be activated. The function is activated by selecting *Enabled*. The function is enabled by default.
Description	Enter a name for the entry.
Service	Select one of the preconfigured services, if required. The extensive range of services configured ex works includes the following: • *activity* • *apple-qt* • *auth* • *charge*

Field	Description
	- *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. - *Network*: Enter the network address and the related netmask.
Source Port/Range	Enter, if required, a source port number or a range of source

Field	Description
	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.

2.3 Interface-specific DNS Server Concept

With **system software 7.10.5** and later, you can define interface-specific DNS serves in addition to the system-wide valid one. Configuring a DNS server for a particular interface can be useful, for example, if accounts with different providers have been set up and load balancing is being used.

2.3.1 DNS Servers

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

2.3.1.1 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.

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*.

Field	Description
Interface	Select the interface to which the DNS server pair is to be assigned. A global DNS server is created with the setting *None*.
Interface Mode	Select whether the IP addresses of name servers for resolving the names of Internet addresses are to be obtained automatically or whether up to two fixed DNS server addresses are to be entered, depending on the priority. Possible values: • *Static* • *Dynamic* (default value)
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.

2.4 Load Balancing - Route Selector and Tracking IP Address parameters added

In the **Network**->**Load Balancing**->**Load Balancing Groups**->**New** menu you can select the **Add** button to edit the interfaces for the **Load Balancing Groups**. Under **Advanced Settings**, the parameters **Route Selector** and **Tracking IP Address** have been added.

Route Selector

The **Route Selector** parameter is an additional criterion used for a more precise definition of load balancing groups. The interface entry within a load balancing group is extended by a routing information. The Route Selector is required in certain applications in order to unambiguously assign the router managed IP sessions to the load balacing groups. The following rules apply to the usage of this parameter:

- If an interface is assigned only to one load balancing group, configuration of the Route Selector is not required.

- If an interface is assigned to several load balancing groups, configuration of the Route Selector is mandatory.
- Within a given load balancing group, the Route Selector has to be identical for all interface entries.

> **Important**
>
> The configuration of the Route Selector requires that all routes required for load balancing have already been configured.

Tracking IP Address

The parameter **Tracking IP Address** serves to monitor a specific route by modifying the load balancing status of he respective interface or the routes connected with the interface. This means that routes can be activated or deactivated independently from the opreation status of the interface. The interface is monitored by means of the host surveillance function of the gateway. Therefore, the configuration of host surveillance entries is mandatory. This is done in the menu **Local Services**->**Surveillance**->**Hosts**. It is vital to keep in mind that only entries with the action **Surveillance** are respected. The host surveillance is then linked to the load balancing function by configuring **Tracking IP Address** in the menu **Load Balancing**->**Load Balancing Groups**->**Advanced Settings**. The load balancing status now changes acording to the status of the assigned host surveillance entry.

2.5 IPSec over TCP

The IPSec configuration now offers the new option **IPSec over TCP** within the **VPN**->**IPSec**->**Options**->**Advanced Settings** menu. This function is based on the NPC Pathfinder technology and encapsulates all IPSec data traffic into a pseudo HTTPS session. This allows the use of IPSec even in situations where it would not be possible otherwise (e.g. if a firewall blocks IPSec traffic).

2.6 Wireless LAN Controller - Slave AP Location parameter added

The **Wireless LAN Controller**->**Controller Configuration**->**General** has had the parameter **Slave AP location** added.

You can use this parameter to select whether the APs that the wireless LAN controller is to manage are located in the LAN or the 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.

Chapter 3 Changes

The following changes have been made in **Systemsoftware 7.10.5** .

3.1 FCI - DNS server configuration - changed

Global DNS servers are no longer created in the FCI menu **Local Services**->**DNS**->**Global Settings** but in the menu **Local Services**->**DNS**->**DNS Servers**->**New**.

So the parameter **DNS server configuration**, with the options *Dynamic* and *Static*, has been removed under **Local Services**->**DNS**->**Global Settings**. The parameters **DNS servers** *Primary* and *Secondary* have been removed for the same reason.

To create a new global DNS server in the new menu **Local Services**->**DNS**->**DNS Servers**->**New**, leave the default setting **Interface** *None*.

3.2 FCI - Monitoring - Hosts changed

In the FCI menu **Local Services**->**Surveillance**->**Hosts**->**New** the field **Trials** has been removed and, in its place, the fields **Successful Trials** and **Unsuccessful Trials** have been added.

With **Unsuccessful Trials**, you can 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.

With **Successful Trials** you can 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.

The **Controlled Interfaces** field has been renamed to **Action to be performed**. The order of **Interface** and **Interface Action** was reversed. **Interface Action** has been renamed to **Action**. The new value *Monitor* is provided under **Action**.

If you select **Action** *Monitor*, you can monitor the IP address that has been specified under **Monitored IP Address**.

3.3 UMTS Stick Vodafone K3806 supported

From system software 7.10.1 on, the UMTS Stick Vodafone K3806 (Huawei) is supported.

⚠ **Caution**

Do not remove or plug in an UMTS stick during operation. This may lead to a malfunction of your device.

Chapter 4 Bugfixes

The following bugs have been fixed in **Systemsoftware 7.10.5** :

Note

Please note that the changes described below do not cover the complete extent of the corrections made. Likewise, they need not apply to all products. Even if the changes described are not relevant for your specific device, it will benefit from the overall enhancements of the patch.

4.1 WLAN Controller - Discovered APs not removed

(ID 15923)

APs discovered by the WLAN Controller were not removed from the overview page under **Wireless LAN Controller**->**Slave AP configuraton**->**Slave Access Points** if they were no longer manged by the WLAN Controller.

The problem has been solved.

4.2 RADIUS - Panic and Reboot

(ID 15843)

A Radius reload caused a panic and a reboot of the system.

The problem has been solved.

4.3 Routing - Problems with an Extended Route

(ID 16251)

When saving the settings **Extended Route** *`Enabled`*, **Route Type** = *`Network Route`* and **Network Type** = *`Direct`* in the **Networking**-> **Routes**->**IP Routes**->‹**New** menu, the message "Input Error. Network type must be set to "Indirect" was displayed.

The problem has been solved.

4.4 Keepalive Monitoring - Entries deleted by mistake

(ID 15976)

When saving a configuration and rebooting the system in the Setup Tool the MIB table *ipHostsAliveTable* contained only eleven entries, even if more entries had been created.

The problem has been solved.

4.5 Qos - Entries not correctly displayed

(ID 16116)

In the **Networking**->**QoS**->**QoS Filter** menu the filter for displaying the entries did not work correctly.

The problem has been solved.

4.6 QoS - Dispensable message displayed

(ID 16095)

If entries were created with **Add** in the field **Queues/Policies** under **Networking**->**QoS**->**QoS Interfaces/Policies**->**New** and such an entry was opened by clicking on the Edit symbol, the message "Operation in progress" was displayed.

The problem has been solved.

4.7 WLAN Controller - Wrong channels used

(ID 16026)

If in the **Wireless LAN Controller**->**Slave AP configuration**->**Radio Profiles**->**New**->**Advanced Settings** menu, the field **Channel Plan** = *User defined* was set and under **Wireless LAN Controller**->**Slave AP configuration**->**Radio Profiles**->**New** the setting in the **Operation Band** field was changed, the values in the *User defined* **Channel Plan** field were not adapted.

The problem has been solved, the values will be preset according to the setting in **Channel Plan** = *Auto*.

4.8 IPSec - Wrong value saved

(ID 15990)

If in the **VPN**->**IPSec**->**Phase-1 Profiles**->**New** menu the field **Local ID Type** = *ASN.1-DN (Distinguished Name)* was set, the field **Local ID Value** was left empty and this configuration was saved, the entry **Local ID Type** = *Fully Qualified Domain Name (FQDN)* was displayed when calling up the menu again.

The problem has been solved.

4.9 Script Error with Service Tool

(ID 15804)

Using the ISDN service dial-in tool **SvcCfgMgr**, it could happen that a script error occured.

The problem has been solved.

4.10 IPSec - Setting up a peer failed

(ID 16271)

Setting up a peer could cause a stacktrace on the system.

The problem has been solved.

4.11 Filter - Setting up a new filter failed

(ID 16180)

If **Service** = *any* in the **Networking**->**QoS**->**QoS Filter**->**New** menu was set, creating a new filter failed and the message "Input Error. Invalid value for Attribute" was displayed serval times.

The problem has been solved.

4.12 IPSec - Error Messages displayed

(ID 15708)

After setting up an IPSec connection the error message "NCI Alert ... failed to add attrib for ipsecStatPeerDPD" was displayed several times.

The problem has been solved.

4.13 ISDN - Error Message during booting the system

(ID 18973)

The message "!!!no masterenable for [2:0] !!!" could be displayed during booting a system with only one ISDN BRI port.

The problem has been solved.

4.14 Scheduler - No action performed

ID 15997

When the configured timer range expired, no action was performed for the command type *`Interface Status`*.

The problem has been solved.

4.15 Configuration Interface - Change not properly applied

ID 15970

Changing the net mask of an existing IP address did not properly change the destination network IP address.

The problem has been solved.

Chapter 5 Known Issues

The follwoing problems have not been solved at the time of publishing this release:

5.1 HTML Configuration - Route Selector not correctly configured

ID 16536

Using the graphical configuration interface leads to an error in the configuration of the route selector in the menu **Network**->**Load Balancing**->**Load Balancing Groups**->**New** When writing the configuration, there is no proper distinction between normal and extended routes. This may lead to a non-functional configuration. Configuration via the Setup Tool avoids this problem.

5.2 Drop In - DHCP Relay

ID n/a

DHCP Relay is not functional for interfaces assigned to more than one Drop In group.

5.3 Setup Tool - IP address change not activated

ID 16290

When changing the IP address of an interface via the Setup Tool, the change is not activated before the configuration has not been saved and the gateway rebooted. Configuration via the graphical user interface avoids this problem.