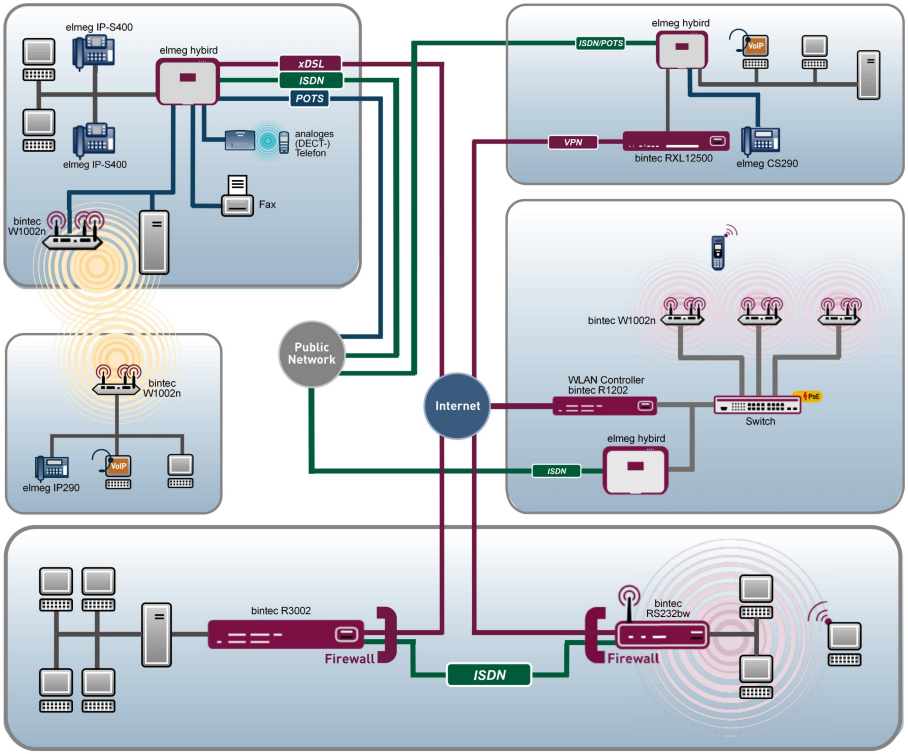

Manual
Release Notes

9.1.1

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 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 GmbH.

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

Copyright

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

Updating the system software with the Graphical User Interface 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.

Note

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 **System software 9.1.1** using the Graphical User Interface, proceed as follows:

(1) For the update, you'll need the `XXXXX_bl9101.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.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 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 **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) Carry out the update to **System software 9.1.1** via the **Maintenance**->**Software &Configuration** menu. To do this, select: **Action** = *`Update system software`*, **Source Location** = *`Local File`*, **Filename** = *`XXXXX_bl9101.xxx`*. Confirm by clicking **Go**. 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,0, 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. Import the backup boot configuration via the **Maintenance**->**Software &Configuration** menu. To do this, select: **Action** = *Import configuration* **Configuration Encryption** = *disabled*, **Filename** = *<Device name>.cf*. Confirm by clicking **Go**. 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) Carry out the downgrade to the required software version via the **Maintenance**->**Software &Configuration** menu.

To do this, select: **Action** = *Update system software*, **Source Location** = *Local File*, **Filename** = *R3000_bl9101.r3d* (example). Confirm by clicking **Go**. 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.

Chapter 2 New Functions

System software 9.1.1 includes a number of new functions that significantly extend the performance over 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 Telephone connection assistant

A new assistant has been incorporated into the user interface, providing assistance for the basic use of a telephone connection. External analogue ISDN and VoIP connections can be configured and created with the aid of this assistant.

The PBX assistants can be found under **Assistants** -> **PBX** -> **Trunks**. All of the existing connections are displayed in the overview. Delete the entries by clicking the  icon. Select the  icon to edit the existing connections.

A new connection can be created by pressing the **New** button. Using a selection field, define the **Connection Type** in the next configuration step. You are given the following options here:

- *ISDN*
- *ISDN P-P*
- *SIP provider*
- *SIP provider (extension)*
- *FXO*

By selecting *ISDN* as the **Connection Type**
and clicking **Next** to confirm, you are taken to the ISDN settings. Here, you can give the connection a **Name**, select the corresponding external **Ports** and **Single Number (MSN)** and define an **Class of Service**.

Instead of an individual number, a **P-P Base Number** is required for the *ISDN (P-P)* option. You can also configure an **P-P DDI Exception** in **Advanced Settings**.

When using an *SIP Provider,* in addition to the **Name**, you must also enter the **Sinle Number (MSN)** and the **Class of Service** as well as the **Authentication ID**, the

, the **User Name** and the **Registrar.** You can then enter the number of the **Registrar Port** to be used for the connection to the server in **Advanced Settings**. The default value is *5060*. Select the **Transport Protocol** for the connection. You can enter the **IP Address** and **Port** for a STUN server and generate a **National** or **International phone number**.

A **Base Number** must also be entered for an *SIP Provider (DDI)*.

If you are using a standard telephone connector (*FXO*), you will also need to select the corresponding **External Port** in addition to the **Name**, **Single Number** and the **Class of Service**.

2.2 IKEv2 - Support for certificates

Teldat GmbH IKEv2 implementation now supports certificate-based authentication.

In order to use this function, go to **VPN** -> **IPSec** -> **IPSec Peers**-> **New**.

Then, under **Internet Key Exchange**, select *IKEv2*. Along with *Preshared Keys*, you can also select the *RSA Signature* **Authentication Method** here. If you are using the RSA function, you can determine your own certificate for authentication under **Local Certificate**. The index number and the name of the certificate are displayed in the field.

Select the local ID type under **Local ID Type**. The following can be selected:

- *Fully Qualified Domain Name (FQDN)*
- *E-mail Address*
- *IPV4 Address*
- *ASN.1-DN (Distinguished Name)*
- *Key ID*

Enter the ID for your device in the **Local ID** field. The **Use Subject Name from certificate** option is displayed for the RSA signature authentication method. When you enable this option, the first alternative subject name indicated in the certificate is used, or, if none is specified, the subject name of the certificate is used.

2.3 IPSec: Directly defining the phase 2 selectors

If an IPSec tunnel has been created using the user interface, the phase 2 SAs are negotiated via configured or dynamically learned routes. However, this can sometimes lead to problems as a result of competing routes or default routes with a lack of granularity, as default routes do not allow for network traffic to be filtered at the level of the protocol or the port.

For this reason, selectors can now also be determined manually in order to derive the SAs.

To do this, go to **VPN** ->**IPSec** -> **IPSec Peers**-> **New**. You will then need to configure all of the VPN parameters required here. When doing so, do not use any IPSec routes. Instead, generate one or more default routes and enable the **Default Route** field. You can create a new filter under **Additional Traffic Filter** by clicking **Add**.

To begin, you should enter a **Description** of the filter in the newly opened window. Then specify the **Protocol** used. You will then need to enter the network and its corresponding netmask under **Source IP Address / Netmask** and **Destination IP Address / Netmask**. Save your settings by clicking **Apply**.

The extended procedure also offers the option to use NAT and PAT within a tunnel or to use routing protocols such as RIP or OSPF. It also offers the option to create VPN backup scenarios.

This feature also resolves a problem with VPN business access. For this purpose, the **Source IP address / Netmask** must be configured in the same way as your LAN connection. The setting **Any** can be kept for **Protocol** and *Target IP address / Netmask*.

2.4 Rogue access point management

2.4.1 Rogue access point overview

Rogue access points (rogue APs) use the SSID (service set identifier, i.e. the network name) of their own network. Although they are not part of the network, clients may accidentally log into these third party APs. Attackers can take advantage of this capacity to retrieve users' private data.

In the GUI, you can now initiate a search for adjacent APs in two menus. In addition to the **Wireless LAN Controller** -> **Monitoring** -> **Neighbor APs** GUI menu, this is also possible in the **Wireless LAN Controller** -> **Monitoring** ->**Rogue APs** menu.

When a search has been completed successfully, you are shown all of the available APs under **Wireless LAN Controller** -> **Monitoring** -> **Neighbor APs**. Rogues APs which are not managed by the WLAN controller but are using an SSID managed by this controller are highlighted in red.

The rogue APs are also displayed separately in the new submenu: **Wireless LAN Controller** -> **Monitoring** ->**Rogue APs**. All of the entries are also initially highlighted in red here. In the **Rogue APs** submenu, there is also a column entitled **Accepted**. If the administrator has enabled the corresponding selection field, the rogue AP is classed as trustworthy. Any alerts which have been specified are deleted and no longer sent. These APs are also no longer highlighted in red in the **Rogue APs**s and **Neighbor APs** menus.

2.4.2 Indicate new rogue APs with the aid of the alert service

If new rogue APs are found when searching for adjacent APs, notification can be given in an e-mail.

To do so, select *New Rogue AP found* as **Event** in **External Reporting**-> **Alert Service** -> **Alert Recipient** -> **New**.

2.5 Improved voicemail administration

2.5.1 Delete voicemail messages automatically

Voicemail messages are deleted after a set period of time. This time period is defined in the menu: **Applications** -> **Voice Mail System** ->**General** -> **Advanced Settings** under **Lifetime**. Possible values are 10 to 60 days. The default value is 60 days.

2.5.2 Delete voicemail message in user access

It is now possible to delete all or individual voicemail messages in user access. Individual messages can also be deleted by pressing the "1" key whilst listening to the message on the system telephone.

If you look in the **User Access** -> **Voice Mail System** -> **Messages** menu, you will find a new column **Select all** / **Deactivate all**.

Active number entries can be deleted here using the **Delete Selected** button. All of the entries can be added to the selection or removed using the corresponding reference in the column header,

2.5.3 Manage voicemail messages in user access

Voicemail messages can now be managed within user access. To do this, go to **Applications** -> **Voice Mail System** -> **Voice Mail Boxes** -> **New** and select *User Defined* under **E-Mail Notification**. The user can then define the type of **E-Mail Notification** in **User Access**->**Voice Mail System** ->  Settings. You can specify the *E-Mail Forwarding Behaviour* for the options *E-mail* and **E-Mail with Attachment**. This means you can define whether a voicemail message should be deleted after an e-mail alarm or forwarding (*Remove message after forwarding*) or whether the **Status** should be changed to "old" (*Change message status to "Old" after forwarding*) or "new" (*Keep message status as "New" after forwarding*).

2.5.4 Save or play back voicemail messages in user access

You can choose to play back voicemail messages or download these to your PC in the **User Access** -> **Voice Mail System** -> **Messages** menu. To save a message, click on the  icon. The download dialog then opens. To listen to a message, click on the  icon.

2.5.5 Specify the number of stored voicemail messages

You can now set the maximum number of voice mail messages yourself.

The previously hard-coded value of a maximum of 60 records for each user of the voice mail system is stored in the **vms** -> **vmsAccountTable** ->  -> **vmsAccountMaxMessages** MIB table and can be changed as needed via the SNMP browser.

2.6 Switch contacts

The **elmeg hybird 130j** and the **elmeg hybird 300** / **elmeg hybird 600** have one or two independent switch contacts which are already supported by hardware.

A switch contact can be used as an on/off switch or as a button, i.e. the electric circuit is closed, opened or closed for a set period of time. You can use this feature to operate a door opener or to turn the exterior light on and off.

These functions are controlled by dialling code numbers into telephones which are connected either internally or externally. To close the electric circuit, enter the sequence `* 531` for the first switch contact and `* 532` for the second contact.

To open the circuit, you will need to enter the following combination: `# 53n`. You can either replace the `n` with a 1 for the first switch contact or a 2 for the second switch contact here.

If you would like to close the electric circuit for a set amount of time, you must use the following sequence: `* 54n`, `n` stands for the first or second switch contact again here. In its ex works state, the period for which the electric circuit is closed is set at 3 seconds. You can change this value via the user interface. To do this, go to the GUI menu **Physical Interfaces** -> **Relay** -> **Relay Configuration**. Here, you can give a **Description** of **Contacts** 1 and 2 and define the time period under **Signalling Period**. The set switching time for the button can be anything between one and 999 seconds. The default value is `3` seconds.

2.7 NAT loopback

The NAT loopback function enables address translation for connectors whereby NAT is not activated. This is often used in order to interpret queries from the LAN as if they were coming from the WAN.

This could, for example, be used to test the services provided by the server in its own network. The client to be used for testing and the server are located in a common LAN. To set up a connection, the client sends a request to the router's WAN IP address together with its LAN IP address. If the NAT loopback function is enabled, the data packet is then forwarded to the server. It appears to the server that the data packet has come from the WAN rather than the LAN. If the NAT loopback function is not enabled, requests will not be forwarded to the server.

Go to the GUI menu **Networking** -> **NAT** -> **NAT Interfaces** to enable the NAT loopback function. The **Loopback** column on the overview page gives you the option to enable the function by activating the corresponding selection field.

2.8 SMS alert service

If you have a **bintec RS120wu**, **bintec RS230au+** or **bintec RS230bu+**, you can receive notification of system alerts in text messages. Here, text message implementation works in the same way as alerts delivered via e-mail.

If you wish to activate the function, go to the GUI menu **External Reporting** -> **Alert Service** ->**Alert Recipient**-> **New** and enable the function under **Alert Service**. Select *SMS* here and enter the SMS recipient's telephone number under **Recipient**.

You will then need to select the **SMS Device** to be used in the **External Reporting** ->**Alert Settings**-> **Alert Settings** menu.

2.9 IPSec: Support for the ISAKMP extended authentication method.

Up until **System software 9.1.1** , Teldat GmbH devices only supported the simple XAuth authentication method when using IPSec. Now, an extended two factor authentication method can be used. This is described in the RFC draft *Extended authentication within ISAKMP/Oakley (XAUTH)*. Here, a second identity test which uses another transmission channel acts an extension of the conventional authentication method. Specifically, following successful authentication with the user name and password, the security software then sends a text message containing an additional access key to the user's registered mobile number.

Most importantly, this enables **SMS passcode** software from *ProSoft Software Vertriebs GmbH* to be used. The program runs on a **Windows 2008 Radius Server** and offers an extended login procedure to provide extra security for remote applications in networks or on websites. The functionality has been tested using the NCP IPSec Client.

2.10 Physical Interfaces Menu - UMTS/LTE

System software 9.1.1 provides support for LTE USB sticks on the RS Series USB interface. The following sticks have been tested for compatibility by Teldat.

- Telekom Speedstick LTE (Huawei/E398)
- Vodafone SurfStick (Huawei K5005)

Note

At present, LTE connections do not support certain features such as SMS and incoming connection types such as ISDN login, PPP and IPSec callback.

The menus for configuring the physical interface and the WAN connections have been modified accordingly. In addition, the internet access configuration assistant also supports LTE connections.

In the **UMTS/LTE** menu, configure the connection for the integrated UMTS/HSDPA/LTE modem (for **bintec RS232j-4G**), UMTS/HSDPA modem (for **bintec RS120wu** and **bintec RS230au+**) or an optional plug-in UMTS/LTE USB stick.

A list of compatible UMTS/LTE USB sticks can be found at *www.teldat.de* under **Products**.

Select the following entry for the corresponding UMTS/LTE modem:

- *Slot6 Unit 0*: The integrated modem is to be configured.
- *Slot6 Unit 1*: The plug-in UMTS USB stick is to be configured.

Note

Please note that the technology used not only depends on availability and the setting in the **Preferred Network Type** field; rather it is also determined by the strength and quality of the signal.

The **Physical Interfaces**->**UMTS/LTE**->**UMTS/LTE**-> consists of the following fields:

Fields in the Basic Settings menu

Field	Description
UMTS/LTE Status	Select whether the chosen UMTS/LTE modem should be enabled or disabled. The function is activated with *Enabled*. The function is enabled by default.
Modem Status	Only for **UMTS/LTE Status** = *Enabled* Shows the status of the UMTS/LTE modem. Possible values: • *Up* • *Down* • *Init* • *Called* • *Calling* • *Connect* • *SIM insert required* • *PIN input required* • *Error* • *Disconnected*
Network Provider	Only for **UMTS/LTE Status** = *Enabled* This is only displayed if the status of the modem is "up".

Field	Description
	Displays the **Network Provider** currently connected.
Actual Network	Only for **UMTS/LTE Status** = *Enabled* Displays the current network, e.g. GSM or UMTS.
Network Quality	Only for **UMTS/LTE Status** = *Enabled* Displays the current quality of the UMTS/LTE connection. The value cannot be changed.
Preferred Network Type	Only for **UMTS/LTE Status** = *Enabled* Select which network type should preferably be used. Possible values: • *Automatic* (default value): GPRS, UMTS or LTE is automatically selected for the connection, depending on which network type is locally available. • *GPRS only*: Only GPRS is used; should GPRS be unavailable, no connection is established. • *UMTS only*: Only UMTS is used; should UMTS be unavailable, no connection is established. • *GPRS preferred*: GPRS is preferably used; should GPRS be unavailable, UMTS is used. • *UMTS preferred*: UMTS is preferably used; should UMTS be unavailable, GPRS is used. • *LTE only*: Only LTE is used; should LTE be unavailable, no connection is established. • *LTE preferred (Priority 4G/3G/2G)*: LTE is preferably used; should LTE be unavailable, UMTS is used, and if UMTS is unavailable, GPRS is used. • *LTE/UMTS (Priority 4G/3G)*: LTE is used. If the strength and quality of the signal are insufficient with LTE then UMTS is used. • *LTE/GPRS (Priority 4G/2G)*: LTE is used. If the strength and quality of the signal are insufficient with LTE then GPRS is used. • *LTE/GPRS/UMTS (Priority 4G/2G/3G)*: LTE is used. If the strength and quality of the signal are insufficient with LTE

Field	Description
	then GPRS is used. If the strength and quality of the signal are insufficient with GPRS then UMTS is used. • *UMTS/LTE (Priority 3G/4G)*: UMTS is used. If the strength and quality of the signal are insufficient with UMTS then LTE is used. • *UMTS/GPRS (Priority 3G/2G)*: UMTS is used. If the strength and quality of the signal are insufficient with UMTS then GPRS is used. • *UMTS/LTE/GPRS (Priority 3G/4G/2G)*: UMTS is used. If the strength and quality of the signal are insufficient with UMTS then LTE is used. If the strength and quality of the signal are insufficient with LTE then GPRS is used. • *GPRS/LTE (Priority 2G/4G)*: GPRS is used. If the strength and quality of the signal are insufficient with GPRS then LTE is used. • *GPRS/UMTS (Priority 2G/3G)*: GPRS is used. If the strength and quality of the signal are insufficient with GPRS then UMTS is used. • *GPRS/LTE/UMTS (Priority 2G/4G/3G)*: GPRS is used. If the strength and quality of the signal are insufficient with GPRS then LTE is used. If the strength and quality of the signal are insufficient with LTE then UMTS is used.  **Note** An incoming data call (PPP dialin or ISDN login via V.110) can generally only be set up via GSM. Setup for UMTS/LTE is generally only possible if the provider has activated this functionality on demand. When a modem is in the "up" state and the **Preferred Network Type** is not *UMTS only*, the modem normally logs in to the GMS network, so that incoming data calls can be signalled. If a connection to the Internet is then established, there occurs a switch to the UMTS network, provided that UMTS is currently available.
Incoming Service Type	Only for **UMTS/LTE Status** = *Enabled* Here you select the gateway subsystem to which an incoming

Field	Description
	call over the modem is to be assigned. Possible values: • *Disabled* : Call is not accepted (default value for LTE connections). • *ISDN Login*: The call is assigned to the ISDN Login subsystem (default value for UMTS connections). • *PPP Dialin*: The call is assigned to the PPP subsystem. • *IPSec*: The call is made via IPSec. Please note the following for the setting **Incoming Service Type** *IPSec*: IPSec callback is used to cause an IPSec peer to set up an Internet connection, thus allowing an IPSec tunnel over the Internet. You can make a direct call via the UMTS/LTE wireless network in order to signal to a peer that you are online and waiting for an IPSec tunnel to be set up over the Internet. If the called peer currently has no connection to the Internet, the mobile call causes a connection to be set up. You can also choose whether the IP address for IPSec tunnel setup should be transmitted with the UMTS/LTE callback call in the following menu: **VPN**->**IPSec**->**IPSec Peers**->  ->**Advanced Settings** under **Transfer own IP address over ISDN/GSM**. This may shorten and simplify tunnel setup.
PUK	This is only displayed if the device has made three failed attempts to establish a connection, e.g. if the PIN for the SIM card (see **SIM Card Uses PIN** field) has been entered incorrectly three times. Enter the PUK (personal unblocking key) for your SIM card to unblock the SIM card.
SIM Card Uses PIN	Only for **UMTS/LTE Status** = *Enabled* Enter the PIN for your UMTS/LTE modem card.

Field	Description
	Note Entering a wrong PIN blocks communication until the entry is corrected.
	Note If the device has made three failed attempts to establish a connection, e.g. because the PIN has been entered incorrectly three times, you will need to enter the **PUK** in order to unblock the SIM card.
Fallback Number	Only for **UMTS/LTE Status** = *Enabled* Enter the call number for the GSM fallback function. When a voice calls goes in on this number, any active connection is immediately disconnected and the operating mode of the modem reset to GSM, where the modem remains until another data call (PPP, ISDN login, IPSec callback) comes in. If flat-rate mode is enabled for the WAN connection (option **Always active** enabled in **WAN**->**Internet + Dialup**->**UMTS/LTE**->), this means that the connection will be re-established immediately.
	Note Please note that the SIM card must support this function, and that not all mobile telephony providers relay voice calls over data SIM cards.
APN (Access Point Name)	Only for **UMTS/LTE Status** = *Enabled* If GPRS/UMTS/LTE is to be used, you must enter the so-called Access Point Name that you received from your provider here. A maximum of 80 characters can be entered. If no APN or an incorrect APN has been entered, a configured GPRS/UMTS/LTE connection will not function.

2.11 WAN menu - UMTS/LTE

Note

Please note that the **UMTS/LTE** menu is only available with **bintec RS120wu** and **bintec RS230au+** (integrated UMTS/HSDPA modem) and **bintec RS232j-4G** (integrated UMTS/HSDPA/LTE modem), or if you are using a UMTS/HSDPA/LTE USB stick!

A list of all configured GPRS/UMTS/LTE connections is shown in the **WAN**->**Internet + Dialup**->**UMTS/LTE** menu.

With mobile standards GPRS, UMTS and LTE, you can establish an internet connection via the mobile network.

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

Fields in the Basic Parameters menu

Field	Description
Description	Enter a name for uniquely identifying the internet connection. The first character in this field must not be a number No special characters or umlauts must be used.
UMTS/LTE Interface	Select the UMTS/LTE interface. In **bintec RS120wu** the integrated modem with slot 6 unit 0 UMTS is preselected; for devices with an optional plug-in UMTS/LTE stick the USB port of the device is preselected.
User Name	Enter the user name.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is activated with *Enabled*. The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle	Only if **Always on** is disabled.

Field	Description
Timeout	Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the short hold. The default value is *300*.

Fields in the menu IP Mode and Routes

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Get IP Address*(default value): Your device is dynamically assigned an IP address. • *Static*: You enter a static IP address.
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is activated with *Enabled*. The function is enabled by default.
Create NAT Policy	Specify whether Network Address Translation (NAT) is to be activated. The function is activated with *Enabled*. The function is enabled by default.
Local IP Address	Only if **IP Address Mode** = *Static* Enter the static IP address of the connection partner.
Route Entries	Only if **IP Address Mode** = *Static* Define other routing entries for this connection partner. Add a new entry with **Add**.

Field	Description
	• *Remote IP Address*: IP address of the destination host or network. • *Netmask*: Netmask of **Remote IP Address**. If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (possible values *0*... *15*). The default value is *1*.

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

Fields in the menu Advanced Settings

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *60*.
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are *0* to *100*. The default value is *5*.
Authentication	Select the authentication protocol for this connection partner. Select the authentication specified by your provider. Possible values: • *PAP* (default value) Run *PAP* only (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Run *CHAP* only (PPP Challenge Handshake Authentication Protocol as per RFC 1994); the password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Run MS-CHAP version 1 only (PPP Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP*: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.

Field	Description
DNS Negotiation	Select whether your device receives IP addresses for the **DNS Server Primary** and the **DNS Server Secondary** from the connection partner or sends these to the connection partner. The function is activated with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is activated with *Enabled*. The function is disabled by default.
LCP Alive Check	Select whether the availability of the remote terminal is to be checked by sending LCP echo requests or replies. This makes it possible to switch to a backup connection more quickly in the event of line faults. The function is activated with *Enabled*. The function is disabled by default.

2.12 Temperature menu

Devices from the **bintec WI** series are fitted with a temperature sensor. This is located on the main board, under the first WLAN card.

The sensor measures the current temperature. Its measurement range is from -55 to +125 °C, with an accuracy of less than 1 °C.

In addition, the minimum and maximum temperatures reached are shown, together with the times at which they were reached. These values are cleared and refilled upon rebooting the device.

Lower and upper limits are set for the temperature by default; overstepping these sets an alert variable and generates a syslog message. The values are updated every 10 seconds.

The temperature limits are configured in the **Local Services**->**Surveillance**->**Temperature** menu. You can link the overstepping of a limit value with an action.

Fields in the Basic Parameters menu

Field	Description
Trigger	Enter the temperature limit value here (min/max). Possible values: • *Temperature above* • *Temperature below*
Action	Select the desired action. Possible values: • *Enable* (default value) • *Disable*
Interface	Select the interface to be used to perform the action. Possible values: • *Relay* (default value): The overstepping of the limit is coupled with the relay (see **Physical Interfaces**->**Relay**->**Relay Configuration** menu). • <Interface>: The selected interface is turned off if the temperature limit is exceeded.

Chapter 3 Changes

The following modifications have been performed in **System software 9.1.1** .

3.1 New information fields for WLAN monitoring

Three new columns have been added to **Wireless LAN Controller** -> **Monitoring** -> **Active Clients**: **Name**, **Client IP Address** and **Signal : Noise (dBm)** have been added in order to improve information and error searches.

A new column has been added under **Status** -> **Wireless LAN Controller** -> **Monitoring Wireless Networks (VSS)**. This shows whether the access point is managed by the WLAN controller () or not ().

3.2 Signalling new voicemail messages on the system telephone

When a new voicemail message has been recorded, an alert appears on the system telephone's display.

3.3 Voicemail announcements in French

Voicemail announcements are now available in French. You can enable these in the **Applications** -> **Voice Mail System** -> **Voice Mail Boxes** menu under **Voice Mail Language**.

3.4 Expansion of the Mini Call Center

The mini call center has been expanded to make way for multiple self-contained solutions with their own user interfaces and personal access to these. Previously, the call center could be divided into several areas, however these were not displayed. Now, each new mini call center has its own lines and agents.

New call centres are set up together with lines. A new dialog box was added to the following menu for this purpose: **Applications** -> **Mini Call Center** -> **Lines** -> **New**. The option under **Call Center Description** should be left as *New*. You can enter a name for the mini call center in the field behind this. If a call center has been set up successfully, new lines can be added to it by selecting the **Call Center Description** selection field.

The call center status display in the **Applications** -> **Mini Call Center** -> **Status** menu has been changed so that lines assigned to a call center and subscribers assigned to lines are grouped in a block.

A new column has been added to the list view for lines in the **Applications** -> **Mini Call Center** -> **Lines** menu. This column is entitled **Assigned To** and contains the name of the call center.

In order to improve the overview for line selection, the name of the corresponding call center has been added when new agents are generated in the **Applications** -> **Mini Call Center** -> **Agents**-> **New** menu.

3.5 Increasing the number of private phone book entries

The number of private phone book entries for each user has increased from 20 to 50.

3.6 Transfer the function key to another system telephone

You can now transfer a configured function key from one system telephone to another.

Go to **Numbering** -> **Terminal Assignment** -> **System Phone** ->  -> **Keys**. Select the  icon to move any configured function key. You can check the **Key name**, the **Key Type** and the **Settings** again in the pop-up menu. Then select the **Phone** (telephone system), the **Module** (telephone or key extension) and the **Key** (new function key number on the other telephone) to which the functionality is to be transferred.

You can also transfer the function in user access by going to **User Access** -> **System Phones** -> **Assigned System Phones** ->  -> **Keys**. Here you can move buttons only within your own phone system.

3.7 New profiles for internet access assistants – Telekom VDSL and Telekom Entertain VDSL

Standard profiles have been created for the **VDSL** and **Entertain VDSL** services from Deutsche Telekom AG. This enables you to set up connections with ease using the assistants. To do this, go to the GUI menu and select **Assistants** -> **Internet Access** -> **New**. In the dialog box, select *External xDSL Modem* and click **Next** to confirm. Use the appropriate **Physical Ethernet Port**, leave the **Type** as *Predefined* and select **Germany** under *Country*. You can now set *Telekom VDSL*, *Telekom Entertain VDSL* or others as internet access options under *Internet Service Provider*.

3.8 BRRP: BRRP status display with the aid of the status LED

With **System software 9.1.1** , it is now possible to determine the status of the router in BRRP operation. If the status LED lights up, the device is functioning as a master router. If the status LED does not light up, it is functioning as a backup router. The status LED flashes if the router is being initialised.

BRRP status	LED display
Master router	LEDs on
Backup router	LEDs off
Init	LED flashes

3.9 Surveillance of the default gateway

The default gateway can be monitored using Keep Alive Monitoring. Another interface can be used if this is no longer accessible.

To set up this function, go to the configuration menu and select **Local services** -> **Surveillance** -> **Hosts** -> **New**. This set-up menu has been re-structured. Create a new entry with *New ID*. If a group already exists, you can select and edit this under **Group ID**.

For **Monitored IP Address,** select *Default Gateway*. You can configure the remaining settings for **Source IP Address**, **Interval**, **Successful Trials** and **Unsuccessful Trials** as you require. Under **Action to be performed**, select *Redial* then specify the interface to be used to set up the connection following a loss of the default gateway.

3.10 Changes to the WLAN controller

3.10.1 Changes to the Adjacent APs menu

The **Beighbor APs** menu under **Wireless LAN Controller** -> **Monitoring** has been re-structured. In order to reduce the number of table entries displayed, APs are now grouped to networks according to their SSID and BSSID.

The individual table columns are now divided in the following format:

Column	Label	Description
1	**SSID**	All of the SSIDs found are arranged in alphabetical order.
2	**MAC Address**	MAC address or basic service set identifier (BSSID)
3	**Signal dBm**	Signal strength in dBm
4	**Channel**	Channel used
5	**Security**	Security settings of the AP
6	**Last Seen**	Time passed since the AP was last detected
7	**Strongest signal received by**	Location and name of the Slave AP which has received the strongest signal
8	**Total detections**	Number of detections with the same BSSID

The most decisive factor in terms of error searches and network optimisation is the strength of the signal received. The security settings provide information about the creation of an insecure network within your own WLAN infrastructure.

3.10.2 Reconfiguring the buttons in the Wireless LAN Controller Wizard

The order of the **Next** and **Cancel** buttons has been reversed in all stages of the **Wireless LAN Controller Wizard** and modified to fit the general style of the GUI.

3.10.3 Changes to the set-up options in the Wireless LAN Controller Wizard

The **WPA Cipher** option has been removed from the third configuration step in the WLAN Controller assistant.

If **WPA** is selected under *WPA Mode*, the **WPA Cipher** *TKIP* is automatically enabled. If **WPA 2** is selected under *WPA Mode*, the **WPA Cipher** *AES* is automatically enabled.

The **Operating Mode** option has been removed from the fourth configuration step. The setting now automatically matches the *Default* value.

3.10.4 Changing the DHCP server name in the Wireless LAN Controller Wizard

It is now possible to select **External or static**or **Internal** for the *DHCP Server* in the first configuration step of the *Wireless LAN Controller Wizard*. By enabling the first option, the IP addresses are either statically assigned to APs or dynamic assignment take place via an external DHCP server. If *Internal* has been selected, the device itself acts as a DHCP server. In this case, the CAPWAP option 138 must be selected in order for communication between the controller and the APs to take place.

Note

The CAPWAP option 138 must be enabled if an external DHCP server is being used.

3.10.5 Naming a Slave Access Point

You can now enter a **Name** as well as a **Location** for a Slave AP. The device name is used as a preset value.

The name can be configured in the last step of the assistant in the **Wireless LAN Controller** -> **Wizard** menu. The value in the **Name** field can be changed on the **Slave Access Points** overview. Alternatively, another name can be entered in the **Wireless LAN Controller** -> **Slave AP configuration** -> **Slave Access Points** ->  menu under **Name**.

3.10.6 Simplification of firmware maintenance

An option which allows you to select all of the Access Points at once and remove the selected items has been created in the **Wireless LAN Controller** -> **Maintenance** -> **Firmware Maintenance** menu. By clicking the link **Select all** and **Deselect all**, all of the APs are selected and removed. This makes it easier to manage a large number of access points.

3.10.7 Warning in the event of a change to the settings on the DHCP server.

If the DHCP server is already being executed on the desired LAN interface when a user opens the **Wireless LAN Controller Wizard**, it is only possible to update the DHCP server if the DHCP option **CAPWAP Address** is enabled. However, access points that are already connected do not receive new CAPWAP addresses here so they are not displayed in the fourth step of the configuration process either. As there is no technical solution for this problem, any access points which have already been connected to the WLAN controller will need to be reset. A suitable warning message has been added to the first configuration step of the **Wireless LAN Controller Wizard**.

3.10.8 E-mail notification assistant

When you have finished the fourth configuration step in the WLAN controller assistant, you can then go on to set up e-mail alerts straight away. Pressing the **START** button next to **Configure alert service for WLAN monitoring** takes you to the following menu: **External Reporting** -> **Alert Service** ->**Alert Recipient**, where you can configure the reporting process for WLAN events.

3.10.9 Slave AP LEDs

You can now set the lighting behavior of the slave APs.

Go to the **Wireless LAN Controller** -> **Controller Configuration** -> **General** menu. Here you can configure the **Slave AP LED mode**. If the default *Status* has been selected, the status LED blinks only once per second. If *Flashing* has been selected, the AP LEDs show their previous default behavior. When set to *Off*, you can turn off all LEDs.

3.11 HotSpot: Walled garden pages from different IP address ranges

HotSpot users can now allow access to websites from various freely accessible IP address ranges. To do this, enable **Walled Garden** under **Local Services** -> **Hotspot Gateway** -> **Hotspot Gateway** -> **New**. Enter the **Walled Garden URL** of the intranet server. You can now access websites via these addresses and all addresses which have been entered under **Additional freely accessible Domain Names** with the aid of **Add**.

3.12 VoIP dialling behaviour

When using VoIP, the dialling process is either completed after a set period of time or by pressing #. The **elmeg hybird** now deals with both dialling methods in the same way. The # sign is no longer used internally. In doing so, this prevents conflict between the databases managed by the **elmeg hybird** (phone book, call lists, etc.).

Note: The system telephone also needs to be modified.

3.13 Enable announcements and simplex operations in the user interface

The announcement and simplex operation functions can now be activated directly in the **elmeg hybird** user interface. You no longer need to configure the "allow announcement" and "allow simplex operation" function keys on the system telephone.

In order to allow announcements and simplex operations to be automatically accepted, go to the following menu: **Numbering** -> **Terminal Assignment** -> **System Phone** ->  -> **Settings** -> **Advanced Settings**. You can authorise **Receive System Intercom Call** or **Receive Announcement Calls** separately for each device here.

If a system telephone has more than one number then the settings are only applied to the first MSN.

If a function key has already been programmed on the system telephone, the LED is also controlled according to the GUI status.

The setting can also be applied in user access in the **User Access** -> **System Phones** -> **Assigned System Phones** ->  -> **Settings** -> **Advanced Settings** menu.

3.14 Team log in/out

Only system telephones allow you to log out of a team using the "Team log in/out" function key. With standard telephones, you can only carry out this function in **User Access**.

Here, you will need to go to the new **User Access** -> **Settings** ->**Feature Settings** ->  ->**Log on / Log off** menu in the user interface. You can the log in or out by enabling or disabling the selection field in the **Status** column for the various teams. You must then confirm the changes again by clicking **Apply**.

The function keys on a connected system telephone are synchronised accordingly.

3.15 Line key function key

A channel for an external POTS/ISDN/VoIP connection is set up under the the "line key" function key. Hands free mode is switched on automatically if this key is pressed on the system telephone and the first free channel of the connection is assigned. Four line keys have been configured. If the third key has been set to idle, the status is signalled on the first line key. You then hear the external dial tone and the LED for the line key for the corresponding channel starts flashing.

The LED for the next free line key flashes on your phone if an external call is signalled on another internal system telephone. You can pick up this call by pressing the line key.

A line key can be assigned to a system telephone as often as desired and configured on several keys.

Note: A current firmware version of the system telephone is required for the new principle of line key control.

3.16 Extension of call variants

Until **System software 9.1.1** , it was only possible to change the call variants 1 to 4 for all of the teams at once. This was achieved by entering the sequence `* 91 n` into the telephone. `n` stands for a number from 1 to 4 here. This represents the call variants. It is now possible to change the call variants separately for each team. To do so, the number sequence just needs to be extended to include the corresponding team number (MSN). The sequence takes the following format: `* 91 tm n tm` refers to the team number here (MSN).

This new code procedure can only be used by subscribers who are authorised to do so according to their user-assigned authorisation class.

3.17 Improved display notification with the following models: elmeg CS 4x0x and elmeg IP-S 400.

The following models displayed the exchange name and the call number name alternatively for exchange calls: **elmeg CS 4x0x** and **elmeg IP-S 400**.

This behaviour can now be configured more precisely. The field **Additional Info for Extern Call** in **Numbering** -> **User Settings** -> **Class of Service** ->  -> **Basic Settings** -> **Advanced Settings** allows you to choose from the following display types: `, Number Name Only` (default value), `Trunk and Number Name`, `Trunk Name Only` and `None`.

3.18 Switch off hold on external S_0 connection.

There is now the option to disable "hold" ISDN information on the external S_0 connection. This is necessary because a number providers either mute the connection or record their own melody (usually sound or text only) depending on the "hold" ISDN information.

Enable or disable this function in the **Numbering** -> **Trunk Settings** -> **Trunks** ->  -> **Advanced Settings** menu under **Call Hold inside the PBX system**. By default, this function is not enabled.

3.19 Play back Wave file and copy from the the SD card to the PC.

You can listen to Wave files from voice applications (such as "announcement before query", MoH, information messages, wake-up messages, etc.) as well as voicemail announcements, recordings and voice messages or copy these to your PC from the SD card and play them back there.

To do this, go to **Applications** -> **Voice Applications** -> **Wave Files**. To save a message, click on the  icon. The download dialog then opens. To listen to a message, click on the  icon.

3.20 Display authorisation classes both under Monitoring and in User Access

You now have the option to view the authorisation classes assigned to a user in the monitoring display.

You will need to go to **Monitoring** -> **Status Information** -> **User** ->  . All of the classes which have been assigned are displayed under **Current Class of Service**. The class which is currently enabled is labelled accordingly ( ).

The **Current Class of Service** is also displayed in user access under **User Access** -> **Status**.

3.21 Alerts in the event of forwarded e-mails

Whilst listening to a voice message on the telephone, you can forward it to an e-mail address by pressing the "5" button. Until now, messages were played back to the end without notification. With the new firmware version, pressing "5" ends playback of the message and forwards it by e-mail. A confirmation message tells you if the message was forwarded successfully or not.. These new announcements are available in German, English and French.

3.22 DSP usage display on the GUI status page

The DSP channels currently in use (in use / available) are displayed in the **System Management** -> **Status** menu under **Modules** next to the DSP modules being used.

3.23 TAPI: Call number display for an external call

The caller's telephone number (caller ID) is now transferred using the "connected ID" TAPI field. This means that the number can be registered before the call is accepted or in the event of forward calls.

3.24 Change to the default settings

The default settings for several values have been changed.

In **Numbering** -> **User Settings** -> **Users** -> **New** -> **Basic Settings**, the pre-defined values for **Class of Service Standard**, **Optional** and **Night** have been changed from *Not allowed* to *Default CoS*.

In **Numbering** -> **User Settings** -> **Users** -> **New** -> **Numbers**, the **System phonebook** and **Busy Lamp Field** are now enabled by default.

In **Numbering** -> **User Settings** -> **Class of Services** ->  , the following selection fields are enabled by default on the **Features** and **Applications** tabs:

- **Call Waiting**
- **Call Through**
- **Receive System Intercom Call**
- **Receive Announcement Calls**
- **Receive MWI Information**
- **Save call data records**

- **Transmit charge information**

In the **Numbering** -> **Terminal Assignment** -> **Analogue** menu, the **Show incoming Number (CLIP)** and **Show new Messages (MWI)** functions under **Advanced Settings** are enabled by default. Meanwhile, the default value for **FXS Ringing Frequency** is `50 Hz`.

3.25 Filter users according to internal call numbers

In the **Numbering** -> **User Settings** -> **Users** menu, it is now also possible to filter according to **Internal Numbers** under **Filter in**.

3.26 Change to the ISDN slot sort order

In the **Numbering** -> **Terminal Assignment** -> **ISDN** menu, the slots are now sorted by number under **Interface**.

3.27 Delete system phone book

3.27.1 Delete system phone book

In order to delete the system phone book completely, go to **Applications** -> **System Phonebook** -> **General**. Now press the **Delete Phonebook** button under **Delete Phonebook**. A security warning message then appears: Click **OK** to confirm your decision.

3.27.2 Share system phone book using LDAP

The **elmeg hybird** now supports LDAP (Lightweight Directory Access Protocol). System phone book entries are provided to other devices or installations, e.g. OpenStage 40/60. Name, calling number, mobile and home phone number can be transferred this way.

LDAP is pre-enabled in the works state and requires no configuration. The client connects with the telephone system anonymously or using user name and password.

The LDAB parameters for name, calling number, mobile and home phone number (sn, telephoneNumber, mobile, homePhone) are stored in the two MIB tables **mpsPhonebookTable** and **mpsExtensionAdmin**.

mpsPhonebookTable

LDAP	MIB
sn	mpsPhonebookName

LDAP	MIB
telephoneNumber	mpsPhonebookNumber
mobile	-
homePhone	-

mpsExtensionAdmin

LDAP	MIB
sn	mpsUserName
telephoneNumber	mpsExtensionNumber
mobile	mpsUserMobileNumber
homePhone	mpsUserHomeNumber

You can get detailed information from the debug ldap mechanism.

3.28 Sort holidays on the calendar by date

Holidays in the **Applications** -> **Calendar** -> **Public Holidays** menu are no longer sorted in alpahabetical order; rather they are organised by date.

3.29 Open hold for SIP telephones

Code procedures now authorised for standard SIP telephones when connecting an "open hold for enquiry".

3.30 Telephone blocks / Permission to make external calls using PIN

Using a special code procedure, any telephone can be temporarily used to make an external call with its own personal authorisations. To do so, the user will need to enter their MSN and their corresponding PIN.

Proceed as follows for an individual call:

(1) Dial the following sequence on any telephone: *5*

(2) Enter your own MSN.

(3) Press the star button.

(4) Enter your 4-digit PIN.

(5) You will hear the external dialling tone.

(6) Enter the external call number.

The following user-specific features are then used temporarily for this individual call:

- Type of subscriber
- Exchange access right (CoS)
- Exchange access sequence (CoS)
- External MSN / DDI signal
- Further identification from the authorisation class

Performance features and restrictions have certain correlations which should be taken into consideration for this type of external call.

- The "busy" status of a monitored (previous) MSN must be changed after a new MSN has been entered.
- The busy lamp field on the system telephone also needs to be updated.
- The line status does change whenever TAPI monitoring is enabled, however this is not signalled to the PC application.
- The user MSN previously entered must also be indicated when initiating a hold for enquiry connection.
- If a "hold for enquiry" connection has been terminated by the receiver being replaced whilst dialling, no return call will be made because the user MSN entered does not match the device.
- No "return call after time" is made if a hold for enquiry connection is transferred via a blind transfer (transfer without notification).
- The same restrictions outlined above apply to return calls to teams.
- A "return call after time" for an "open hold for enquiry" is signalled on the original device.
- Automatic callbacks (CCBS and CCNR) are not allowed.
- The phone unblocking procedure can not be selected in a normal hold for enquiry connection.

3.31 Combination of the ADSL and VDSL menus

The menus **ADSL** / **VDSL Modem** under **Physical Interfaces** no longer exist in the devices **bintec R3002**, **bintec RT3002** or **bintec R3502**. The have been unified into a single **DSL** menu.

3.32 Alphabetical sorting of the maintenance func-

tions

The **Aktion** parameters are sorted alphabetically in the **Maintanance** ->**Software & Configuration** -> **Options** menu.

3.33 biboAdmConfig: Changed syntax

The syntax or configuring biboAdmConfigHostUrl has changed. Below the commands for SNMP and configd are listed:

SNMP:

```
cmd=put hosturl="xmodem:1k"
```

configd:

```
configd put all xmodem:1k
```

3.34 hybird 120 / 130 - ISDN LED

The signaling behavior of ISDN LEDs has been extended: the B channel usage is now displayed.

ISDN LED display

Farbe	Status	Information
yellow	on	layer 1 active
yellow	off	idle or non-operating
yellow	flashing slowly (once per second)	1 B channel active
yellow	rapidly flashing (twice per second)	2 B channels active

Chapter 4 Bugfixes

Note

Please note that the changes specifically mentioned in the following do not represent the full scope of bugfixes. In particular, the changes do not necessarily apply to all products. Even if the following corrections are not relevant to your device, it will still benefit from the general improvements to the patch.

The following bugs have been eliminated in **System software 9.1.1** :

4.1 System - Validating the software version

(ID 12594)

In order to avoid unnecessary downloads, the firmware version number is now checked before the file is downloaded. Until now, the version number was only checked after being downloaded from the server and following the final CRC verification.

This resolves the problem with updates for Telekom VPN business connections.

4.2 : GUI - Internet Assistant

(ID 14701)

The internet access assistant for **bintec R3502** was not capable of setting up an ADSL or ADSL2 connection.

The problem has been solved.

4.3 Telephony - Initiating a conference call

(ID 14230)

Initiating a conference call from an IP system telephone to an ISDN system telephone was not possible.

The problem has been solved.

4.4 Telephony - Erroneous conference call initiation

(ID 14229)

A three party conference call was initiated after being put on hold or when recording from an ESTOS application.

The problem has been solved.

4.5 System - Tracing of GSM/UMTS/LTE interfaces

(ID 16957)

Tracing did not work on GSM / UMTS / LTE based PPP interfaces.

The problem has been solved.

4.6 IPSec - Panic at Openswan or strongSwan

(ID 12125)

If the IPSec implementations for Linux Openswan or strongSwan initialized an IPSec tunnel and neither a local nor a remote subnet was configured for phase 2, the gateway panicked.

The problem has been solved.

4.7 IP - Stack trace

(ID 16970)

If the IP Address of the LOCAL interface and the destination address of an IP packet were in the same subnet, the system panicked with a stack trace.

The problem has been solved.

4.8 IPSec - Dormant IPSec peers

(ID 14518)

An IPSec peer created by a RADIUS server should be deleted with all dependent entries if its status changes to "down", "blocked" or "dormant". But dormant peers were not always removed.

The problem has been solved.

4.9 DNS - Initial timeout

(ID 16909)

Processing an DNS request took up to 5 seconds if there was no matching entry in the DNS cache. This also affected the DynDNS service.

The problem has been solved.

4.10 GUI - Configuration backup

(ID 16037, 16771, 16776, 16782, 16871)

A backup of the configuration during a scan for neighboring APs resulted in corrupted MIB tables.

The configuration saving mechanism has been adapted. The results of the scanning process are included in the saved tables.

4.11 IPSec - Panic with Shrew Soft VPN Client

(ID 16823)

Initialization of a tunnel to a Teldat gateway by the Shrew Soft VPN Client caused a panic if the **IKE Config Mode** of the Shrew Soft Client was set to *Auto Configuration* and WINS or DNS were activated or the IKE config mode reply message contained two addresses for the WINS / DNS server.

The problem has been solved.

4.12 DHCP - Error in the relay mechanism

(ID 15915)

If multiple interfaces were configured on a single physical Ethernet port of the DHCP client, the DHCP relay service failed if the broadcast flag had not been set.

The problem has been solved.

4.13 QoS - Automatic policy generation

(ID 16561)

When creating a new QoS policy under **Queues/Policies** in the **Networking** -> **QoS** -> **QoS Interfaces/Policies** -> **New** menu, a default entry with the lowest priority (= 255) is created. This policy is already created upon clicking the **Add** button but the change does not be come visible until clicking the **OK** button..

A corresponding notice is now shown in the GUI.

4.14 Load Balancing - Error in the configuration of the Route Selector

(ID 16536)

By creating a new load balancing group in **Networking** -> **Load Balancing** -> **Load Balancing Groups** -> **New**, the configuration of the **Route Selector** under **Interface Selection for Distribution** -> **Add** -> **Advanced Settings** caused corrupt MIB entries.

The problem has been solved.

4.15 DHCP - Panic

(ID 16567)

If there were no more unassigned IP addresses in the dynamic IP Address Pool, the DHCP server panicked.

The problem has been solved.

4.16 hybird - Switch the TFE call variants

(ID 16787)

For all door intercoms only the call variants 1 and 2 can be simoultaneously switched by the sequence **92x* (x = 1, 2).

4.17 SIP - Suppress calling-line identification

(ID 19709)

It was not possible to initiate an anonymous call from a SIP telephone.

The problem has been solved.

4.18 UMTS - Reactivation of the UMTS modem

(ID 16758)

If the UMTS modem was deactivated and the configuration was saved, it was not possible to reactivate the modem over the graphical user interface.

The problem has been solved: You can now activate and deactivate the modem under **Action** in the **Physical interfaces** -> **UMTS/LTE** menu.

4.19 Licenses - Generation of standard system licenses

(ID 13960)

To restore the standard licenses for a device, the **Default Licenses** button (standard licenses) has to be clicked in the **System Management** -> **Global Settings** -> **System Li-**

censes menu. Up to now it was not checked whether the licenses had already been created and multiple entries for each license could be created.

The problem has been solved.

4.20 Disable SNMP service

(ID 16173)

If **snmpAdminPort** = *0*, the SNMP service was not disabled as expected.

The problem has been solved.

4.21 PPTP - Panic with MPPE

(ID 16662)

Using PPTP with MPPE caused a panic.

The problem has been solved.

4.22 bintec R3802- SHDSL interface status

(ID 11187)

On the **bintec R3802** the status page at **System Management** -> **Status**, the SHDSL did not properly display the SHDL interfaces and its possible configurations (e.g. wire modes).

The problem has been solved: The **Description** of the interface is now displayed as it is in the menu **Physical Interfaces** -> **SHDSL** ->**SHDSL Configuration**. Also the configuration state is properly displayed.

4.23 System - Tracing of PPP interfaces

(ID 14607)

It was not possible to perform tracing on all PPP interfaces.

The problem has been solved.

4.24 DynDNS - Recursive loop

(ID 9899)

If the system time changed, a loop was created in the DynDNS service that generated a high number of syslog messages.

The problem has been solved.

4.25 System phone book - Display issue

(ID 15132)

If you called the system phone book in the system telephone without any filter of the initial letter, only the first entry was displayed and it was not possible to search for further entries.

The problem has been solved.

4.26 OSPF - Routes not propagated

(ID 14333)

The direct routes of the LOCAL interface were not propagated.

The problem has been solved: You can now activate this function in the Setup Tool. Set the parameter **Propagate Routes bound on local interfaces** to *yes* in the **IP** -> **Routing Protocols** -> **OSPF** -> **OSPF Static Settings** menu.

4.27 IPSec - Wrong proposals

(ID 15148)

If you created an IKE profile in **VPN** -> **IPSec** -> **Phase-1 Profiles** -> **New**, the profile could contain non-selected proposals.

The problem has been solved.

4.28 CAPI - T.30 fax support

(ID 14810)

T.30 faxes over CAPI were not registered and the corresponding LEDs were not working.

The problem has been solved.

4.29 Loss of phase-2 heartbeats

(ID 14380)

Phase-2 heartbeats were lost under high CPU load. This problem was self-reinforcing, because the reinitialization of the heartbeats increased the system load.

The problem has been solved.

Chapter 5 Known issues

5.1 UMTS sticks Huawei E372 and Huawei E367u-2

(ID 16951)

Since **System software 9.1.1** the UMTS sticks **Huawei E372** and **Huawei E367u-2** do not support ISDN login, PPP dial-up and SMS.

5.2 Gigabit Ethernet configuration

(ID 19990)

If you configure a Gigabit-Ethernet connection, you should set the **Configured Speed / Mode** to *`Full Autonegotiation`* in the **Physial Interfaces** -> **Ethernet Ports** -> **Port Configuration** menu.

If you have manually configured the Ethernet interfaces, there may be problems after an update to system softwarw 9.1.1 if the gateway is connected to a switch and both the gateway and the switch act as clock master. In this case, set the gateway to automatic negotiation.