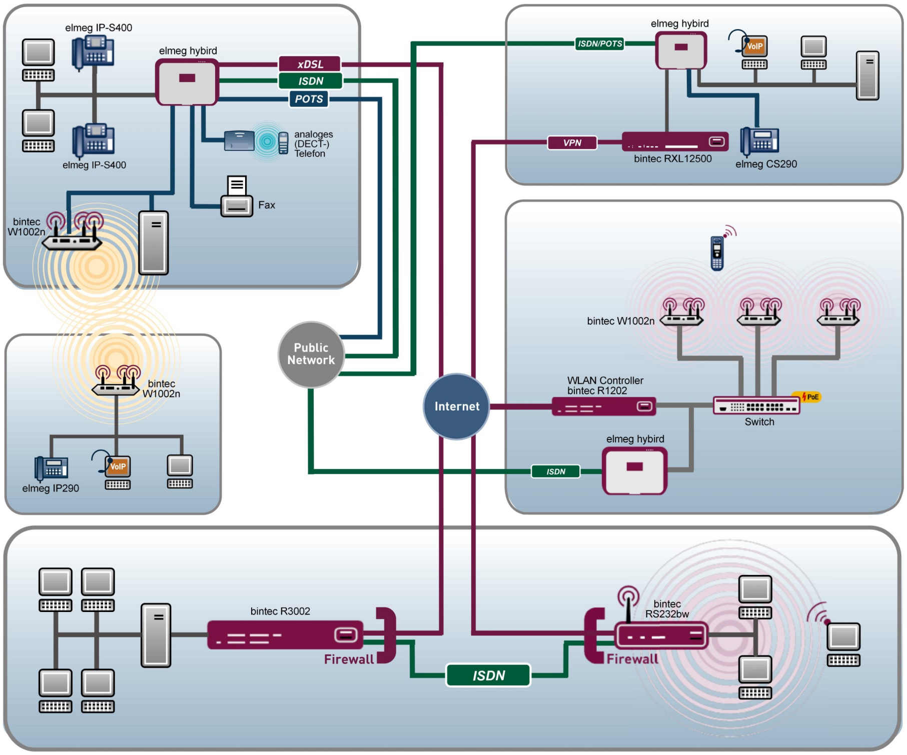

Release Notes

9.1.5

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, 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 **Systemsoftware 9.1.5** using the Graphical User Interface, proceed as follows:

(1) For the update, you'll need the `XXXXX_bl9103.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) Update the **Systemsoftware 9.1.5** using the **Maintenance**->**Software &Configuration** menu. To do this, select: **Action** = *`Update system software`*, **Source Location** = *`Local File`*, **Filename** = *`XXXXX_bl9105.xxx`*. Confirm with **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.

1.2 Downgrade with the GUI

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

(1) Replace the current boot configuration with the previous backup version. You import the saved boot configuration using the **Maintenance**->**Software &Configuration** menu. To do this, select: **Action** = *Import configuration*, **Configuration Encryption** = *disabled*, **Filename** = *<name of device>.cf*. Confirm with **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) Downgrade to the software version you want using the **Maintenance**->**Software &Configuration** menu.

To do this, select: **Action** = *Update system software*, **Source Location** = *Local File*, **Filename** = *RXL_Series_bl9105.biq* (example). Confirm with **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

Systemsoftware 9.1.5 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 Hardware: New LED mode

With **Systemsoftware 9.1.5** you can use the **Global Settings** menu and the **WLAN Controller** to switch the LED light-up behaviour through three different modes.

Note

If you have changed the LED behaviour using the **GUI** or the **WLAN Controller**, this setting will be retained after restoring the device to its as delivered status.

Status	Only the status LED flashes once per second.
Flashing	The LEDS display their default behaviour.
Off	All LEDs are disabled.

2.2 GUI: Public Source IP Address added

With **Systemsoftware 9.1.5** , the **Public Source IP Address** parameter is available in the **VPN**->**IPSec**->**IPSec Peers**->**New**->**Advanced Settings** menu.

Relevant field in the menu Advanced IP Options

Field	Description
Public Source IP Address	If you are operating more than one Internet connection in parallel, here you can specify the public IP address that is to be used as the source address for the peer's data traffic. Select whether the **Public Source IP Address** is to be enabled.

Field	Description
	The function is enabled with `Enabled`. In the input field, enter the public IP address that is to be used as the sender address. The function is disabled by default.

2.3 GUI: Parameter Restore Default Settings added

With **Systemsoftware 9.1.5** , the **Restore Default Settings** parameter is available in the **System Management**->**Administrative Access**->**Access**->**Advanced Settings** menu.

In the **System Management**->**Administrative Access**->**Access** menu you can restrict the access to individual interfaces. Every change in this menu generates entries in multiple MIB tables. To be able to lift the restrictions that have been configured using the GUI, the **Restore Default Settings** parameter has been introduced.

Relevant field in the menu Advanced Settings

Field	Description
Restore Default Settings	Only when you make changes to the configuration of the administrative access are corresponding access rules set up and enabled. You can restore the default settings using the 🗑 icon.

2.4 GUI: Updates for elmeg IP1x telephones

With **Systemsoftware 9.1.5** you can use the devices in the **elmeg hybird** series to update the connected **elmeg IP1x** telephones via the GUI.

2.4.1 elmeg IP1x Update

In the **Maintenance**->**System Phones**->**elmeg IP1x Update** menu, you'll find a list of the connected **bintec** IP telephones. You can select telephones to have their software updated immediately or permit them to download completely new software from the system.

In the case of immediate updating, there is no version control.

Values in the list elmeg IP1x Update

Field	Description
Description	Displays the description entered for the system telephone.
Phone Type	Displays the system telephone type.
MAC Address	Displays the system telephone's MAC address.
SD Card Vers.	Displays the inserted SD card version.
Status/Update Status	Displays the system telephone status, or a progress bar during the update progress. ⬆ Identifies a system telephone that is connected and whose system software is supported by your **hybird**. ⬇ Identifies a system telephone that is either not connected, or whose system software is not supported by your **hybird**. For IP telephone, there is no restriction on simultaneous updating of system software. In case the system telephone's system software is not supported by your **hybird**, there is still a way to update the system software. During system software updating, you see a progress bar.
Update enabled	Displays whether connected telephones can autonomously download new software from the system. You can select individual entries using the checkbox in the corresponding line, or select them all using the **Select all** or **Deselect all** buttons.
Update immediately	Displays whether the system telephone software should be updated immediately. This function is enabled on an individual device by setting a checkmark. The function is disabled by default. For all the devices displayed, you can use the **Select all** or **Disable all** buttons.

2.5 IPSec: MobIKE

With **Systemsoftware 9.1.5** the **MobIKE** function is available.

You will find this function in the **VPN**->**IPSec**->**IPSec Peers**->**New** menu under **Advanced IP Options**.

Relevant field in the menu Advanced IP Options

Field	Description
MobIKE	Only for peers with IKEv2. **MobIKE** With changing public IP addresses, enables only these addresses to be updated in the SAs, without having to renegotiate the SAs themselves. The function is enabled by default. Note that MobIKE requires a current IPSec client, e.g. an up-to-date Windows 7 or Windows 8 client, or the most recent version of the Teldat IPSec client.

2.6 IPSec: RADIUS Accounting

If RADIUS Accounting is configured a selected set of attributes is used, drawing on the RFCs 2139, 2866 and 2868, to map IPSec Phase 2 parameters.

2.7 WLAN: Airtime fairness

With **Systemsoftware 9.1.5** the **Airtime fairness** function is available.

You will find this new function in the **Wireless LAN**->**WLAN**->**Radio Settings**->🔧 menu and in the **Wireless LAN Controller**->**Slave AP configuration**->**Radio Profiles**->🔧 menu.

Relevant field in the menu Performance Settings

Field	Description
Airtime fairness	This function is not available for all devices. The **Airtime fairness** function ensures that the access point's send resources are distributed intelligently to the connected clients. This means that a powerful client (e. g. a 802.11n client)

Field	Description
	cannot achieve only a poor flow level, because a less powerful client (e. g. a 802.11a client) is treated in the same way when apportioning. The function is enabled with *Enabled*. The function is disabled by default. This fuction is only applied to unprioritized frames of the WMM Classe "Background".

2.8 WLAN: Client load balancing

With **Systemsoftware 9.1.5** the **Client load balancing** function is available to the **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** and **bintec W2004n** devices.

The function regulates the distribution of a radio module's clients to the configured wireless networks and the load of the radio modules and the frequency bands.

You will find this function in the menu **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)**->🔧 and in the menu **Wireless LAN Controller**->**Slave AP configuration**->**Wireless Networks (VSS)**->🔧.

Relevant fields in the Client load balancing menu for bintec W1003n, bintec W2003n, bintec W2003n-ext and bintec W2004n

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

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

For the **Client load balancing** you can view statistics at two places in the GUI.

2.8.1 Load Balancing for Wireless LAN Controller

The **Wireless LAN Controller**->**Monitoring**+**Load Balancing** menu displays an overview of the **Load Balancing**. For each VSS you see, e. g., the number of connected clients, the number of clients that are affected by the **2,4/5 GHz changeover**, and the number of rejected clients.

2.8.2 Load Balancing for WLAN

The **Monitoring**->**WLAN**+**Load Balancing** menu displays an overview of the **Load Balancing**. For each VSS you see, e. g., the number of connected clients, the number of clients that are affected by the **2,4/5 GHz changeover**, and the number of rejected clients.

Values in the list Load Balancing

Field	Description
VSS Description	Displays the unique description of the wireless network (VSS).
Network Name (SSID)	Displays the name of the wireless network (SSID).
MAC Address	Displays the MAC address being used for this VSS.
Active Clients	Displays the number of active clients.
2,4/5 GHz changeover	Displays the number of clients who have been moved to a different frequency band by the **2,4/5 GHz changeover** function.
Denied Clients soft/ hard	Displays the number of rejected clients after the absolute number of permitted clients has been reached.

2.9 WLAN: Energy saving mode available

With the **W1003n**, **W2003n**, **W2003n-ext** and **W2004n** devices **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)**->**New** an energy saving mode is available in the menu with the **U-APSD** parameter.

Relevant field in the menu Service Set Parameters

Field	Description
U-APSD	Only for **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** and **bintec W2004n** Select whether the Unscheduled Automatic Power Save Delivery (U-APSD) energy saving mode is to be enabled. The function is activated by selecting `Enabled`.

Field	Description
	The function is enabled by default.

2.10 Wireless LAN Controller: Dynamic blacklisting

With **Systemsoftware 9.1.5** the **Dynamic blacklisting** function is available.

You will find this function in the menu **Wireless LAN Controller**->**Slave AP configuration**->**Wireless Networks (VSS)**->**New**.

Relevant field in the menu MAC-Filter

Field	Description
Dynamic blacklisting	You can use the **Dynamic blacklisting** function to identify clients that want to gain possibly unauthorised access to the network and block them for a certain length of time. A client is blocked if the number of unsuccessful login attempts with a specified time exceeds a certain number. This threshold value and the duration of the block can be configured. A blocked client is blocked at all the APs that are managed by the wireless LAN controller for the VSS concerned, so neither are they able to log into a different radio cell in that VSS. If a client needs to be blocked permanently, this can be done in the **Wireless LAN Controller**->**Monitoring**+**Rogue Clients** menu. The function is activated by selecting *Enabled*. The function is activated by default.

The **Wireless LAN Controller**->**Monitoring**+**Rogue Clients** menu displays the clients that have attempted to gain unauthorised access to the network and which are, therefore, on the blacklist.

Possible values for Rogue Clients

Status	Meaning
Rogue Client MAC Address	Displays the MAC address of the client which is on the blacklist.
SSID	Displays the SSID involved.
Attacked Access Point	Displays the AP concerned.
Signal dBm	Displays the client's signal strength during the attempted access.

Status	Meaning
Type of attack	This displays the type of the potential attack, e. g. an incorrect authentication.
First seen	Displays the time of the first registered attempted access.
Last seen	Displays the time of the last registered attempted access.
Static Blacklist	You can categorise a rogue client as untrustworthy by selecting the checkbox in the **Static Blacklist** column. The block on the client will then not end automatically, rather you will need to lift it manually.
Delete	You can delete entries with the 🗑 icon.

2.11 Wireless LAN Controller: Cyclic Background Scanning

With **Systemsoftware 9.1.5** the **Cyclic Background Scanning** function is available.

You will find this function in the **Wireless LAN Controller**->**Slave AP configuration**->**Radio Profiles**->🔧 **/ New**->**Advanced Settings** menu.

Relevant field in the menu Advanced Settings

Field	Description
Cyclic Background Scanning	This function is not supported by all devices. To automatically search for neighbouring or rogue access points in the network at regular intervals, you can enable the **Cyclic Background Scanning** function. This search runs without impacting the function as an access point. Enable or disable the **Cyclic Background Scanning** function. The function is enabled with `Enabled`. The function is disabled by default.

2.12 Wireless LAN Controller: Region

With **Systemsoftware 9.1.5** the following countries are also available in the **Wireless LAN Controller** under **Region**: *Argentina*, *Brazil*, *Chile*, *Colombia*, *Costa Rica*, *Ecuador*, *Guatemala*, *Honduras*, *Mexico*, *Peru*, *Venezuela*.

2.13 VoIP: Announcements

With the devices in the **elmeg hybird** series, in the **Terminals**->**elmeg system phones**->**System Phone**->->🔧 menu under **Key Type**, the new *System Call (Announcement Team)* function is available for the keys on your system telephone.

You can also use announcements from and to VoIP telephones. The function may still need to be configured in the device concerned.

2.14 Hotspot: Status display and timeout added

With **Systemsoftware 9.1.5** the **Local Services**->**HotSpot Gateway**->**HotSpot Gateway**->**New**->**Advanced Settings** menu provides the **Pop-Up window for status indication** and **Default Idle Timeout** parameters.

Relevant fields in the menu Advanced Settings

Field	Description
Pop-Up window for status indication	Specify whether the device uses pop-up windows to display the status. The function is enabled by default.
Default Idle Timeout	Enable or disable the **Default Idle Timeout**. If hotspot user fails to cause any data traffic for a configurable time period, they are logged out of the hotspot. The function is enabled by default. The default value is *600* seconds.

2.15 hybird: T.38 FAX support

With **Systemsoftware 9.1.5** the **elmeg hybird 120 / 130** devices enable the transmission of a fax via T.38.

2.16 hybird: Alarm Input

The FXS interfaces can be configured as an alert input with the devices in the **elmeg hybird** series. So an alert button, e. g., can be connected to one of these interfaces: When the button is pressed, an alert call is triggered to up to eight internal or one of two external phone numbers. During an alert call, one of the **elmeg hybird** switching contacts can be enabled if required. As an option, the **Alarm Input** function can be switched on or you can switch between the two possible signalling variants using a calendar.

Before starting to configure the **Alarm Input** function you should make these preparations:

- Create a user for the alert call in the **Numbering**->**User Settings**->**Users**->**New** menu and assign this person internal and external phone numbers.
- Create a permission class for the alert call in the **Numbering**->**User Settings**->**Class of Services**->**New** menu.
- Assign this permission class to the user under **Numbering**->**User Settings**->**Users**->🔧.
- In the **Physical Interfaces**->**Relay**->**Relay Configuration** menu you can configure the switching contact that you wish to use for the **Alarm Input** function, for example to release emergency exits.

You will find the **Alarm Input** function in the menu **Applications**+**Alarm Input**+**Alarm Input**

2.16.1 Alarm Input

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

2.16.1.1 General

In the **General** area you set up the basic features of alert inputs.

The **Applications Alarm Input Alarm Input General** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Status	Enable or disable the function. The function is enabled with `Enabled`. The function is enabled by default.

Field	Description
Description	Enter a unique name for the alert call.
Interface	If necessary, select the interface to be used for this alert call.
Internal Number	Select an internal number to be used for the alert call.
Switch signalling	Specify how the alert call that has been configured is to be switched. Possible values: • *No calendar,only manually*: Manual switch is enabled. • *<calendar entry>*: Select one of the calendar entries that has been configured for the alert call.
Active Variant	Select the call variant that is to be enabled. You can configure the variants once you have confirmed the entry in the **General** tab with **OK**.

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

Fields in the menu Advanced Settings

Field	Description
Alarm Signalling Period	Enter the time in seconds for which an alert call is to be signalled. The default value is *30* seconds.
Repeat after	Enter the time between alert call repeats, in seconds. You can enter a value between *1* and *600* seconds. The default value is *10* seconds. Alert call repeats via an FXO interface are not possible.
Number of repeats	Enter the number of repeats if the alert call is not accepted. You can enter a value between 1 and 10 repeats. The default value is *2*. Alert call repeats via an FXO interface are not possible.
External Connection	Enter the maximum duration of an external alert call (in

Field	Description
Timer	seconds) after it has been accepted. You can enter a value between *1* and *600* seconds. The default value is *60* seconds.
Info Message (UUS1)	Optionally, a message (max. 32 characters) can be sent to ISDN terminals.
Relay Contact	If a relay is to be switched during the alert call: Select the relay to be used. The relay can be configured in the **Physical Interfaces**->**Relay** menu.
Wave-File	Select whether a saved Wave file is to be played when the alert call is accepted, and which one. Possible values: • *Off* (default value): A caller on hold shall hear no music-on-hold. • *<Wave file>*: The subscriber who is called should listen to the selected Wave file.
Number of playbacks	Select how many times the announcement shall be continuously repeated. Possible values: • *Infinite (default value)* • *1* to *10*

2.16.1.2 Variant 1 and 2

You can configure two variants of the alert call. As a rule, one variant will use the option of calling internal subscribers, while the other will call external subscribers.

Fields in the menu Basic Settings

Field	Description
Assignment	You can assign up to eight internal phone numbers or two external numbers to each alert call. Define whether, with an alert call, the calls are to be signalled to internal or external subscribers. Possible values:

Field	Description
	- *External*: The entered external number is called. With an alert call, two external numbers can be called, alternating between the two. - *Internal* (default value): The subscribers assigned to the selected number are called according to the defined signalling. With an alert call, eight internal subscribers can be called simultaneously.
First External Number	Only for **Assignment** = *External*Enter the first number of the external subscriber.
Second External Number	Only for **Assignment** = *External*Enter the second number of the external subscriber.
Internal Assignment	Only for **Assignment** = *Internal*Select the internal subscribers. Use **Add** to add more internal numbers.

2.17 hybird: Automatic number transmission available

With **Systemsoftware 9.1.5** , the number of the update server that you can configure on the devices in the `hybird 300` product lines in the **Maintenance**->**System Phones**->**Settings** menu as **Internal Number** is automatically transmitted to the system telephone whenever the telephone logs into the **elmeg hybird** concerned.

After being transmitted, the number is displayed on the telephone under **Menu**->**Service**->**Software Update**. If you press the OK key the number becomes available in the call preparation.

2.18 hybird: bintec CAPI available

With **Systemsoftware 9.1.5** the devices in the **elmeg hybird 120 / 130** series have **bintec CAPI** available.

2.18.1 CAPI

In the **Terminals**->**Other phones**+**CAPI** menu, you configure the connected CAPI terminals. For example, you perform assignment of a configured internal number.

2.18.1.1 Edit or New

Select the 🔧 icon to edit existing entries. Select the **New** button to add another CAPI terminal.

The **Terminals**->**Other phones**+**CAPI**->**New** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	Enter a description for the CAPI telephone.

Fields in the menu Basic Phone Settings

Field	Description
Internal Numbers	Use **Add** to select the internal number for this terminal. You can define several internal numbers. Possible values: • *No free Extension Available*: All configured internal numbers are already in use. First configure another user with additional numbers. • *<Internal number>*: Select one of the existing numbers of the configured users.

Chapter 3 Changes

The following changes have been made in **Systemsoftware 9.1.5** .

3.1 GUI: Display Advanced Settings

When a page is reloaded, the status of the **Advanced Settings** area of the page is maintained, i.e. if the parameters in the **Advanced Settings** area were displayed, they will continue to be displayed after a reload and do not need to be selected again.

3.2 GUI: Sortable columns

As of now, the content of the columns in the **Local Services**->**DHCP Server**->**IP/MAC Connection** menu can be sorted.

3.3 GUI: Automatic Page Updating removed

In the **Network**->**Load Distribution**->**Special Session Handling** menu, Automatic Page Updating has been removed because only static values are used on this page.

3.4 GUI: SSH upgraded

In the **System Management**->**Administrative Access**->**SSH** menu the parameters **SSH Port**, **Maximum number of concurrent connections** and **Login Grace Time** have been added. The parameters **Compression**, **TCP Keepalives** and **Logging Level** have been moved to the **Advanced Settings** menu.

Relevant fields in the menu SSH (Secure Shell) Parameters

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

Relevant fields in the menu Advanced Settings

Field	Value
Login Grace Time	Enter the time (in seconds) that is available for establishing the connection. If a client cannot be successfully authenticated within this time, the connection is terminated. The default value is `600` seconds.
Compression	Select whether data compression should be used. The function is activated by selecting *`Enabled`*. The function is disabled by default.
TCP Keepalives	Select whether the device is to send keepalive packets. The function is activated by selecting *`Enabled`*. The function is enabled by default.
Logging Level	Select the syslog level for the syslog messages generated by the SSH Daemon. Possible settings: • *`Information`* (default value): Fatal and simple errors of the SSH Daemon and information messages are recorded. • *`Fatal`*: Only fatal errors of the SSH Daemon are recorded. • *`Error`*: Fatal and simple errors of the SSH Daemon are recorded. • *`Debug`*: All messages are recorded.

3.5 Network: Routes revised

The **Network**->**Routes**->**IPv4 Routes**->**New** menu has been revised and upgraded. The **Network**->**Routes**+**IPv4 Routing Table** menu is new.

Now you can also configure routes for interfaces in DHCP Client mode.

3.5.1 IPv4 Routes

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

3.5.1.1 Edit or New

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

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

The **Network**->**Routes**->**IPv4 Routes**->**New** consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Interface	Select the interface to be used for this route.
Route Type	Select the type of route. Possible values: • *Default Route via Interface*: Route via a specific interface which is used if no other suitable route is available. • *Default Route via Gateway*: Route via a specific gateway which is used if no other suitable route is available. • *Host Route via Interface*: Route to a single host via a specific interface. • *Host Route via Gateway*: Route to a single host via a specific gateway. • *Network Route via Interface* (default value): Route to a network via a specific interface. • *Network Route via Gateway*: Route to a network via a specific gateway. Only for interfaces being run in DHCP Client mode: Even if an interface is configured for DHCP Client mode routes can be configured for data traffic via this interface. The settings received from the DHCP server are then copied to the active routing table along with those configured here. With dynamically changing gateway addresses this enables, e. g., particular routes to be maintained and routes with a different metric (i. e. different priority) to be specified. However, if the DHCP server transmits static routes (so-called Classless Static Routes), the settings configured here are not copied to the routing. • *Default Route Template per DHCP*: All the routing in-

Field	Description
	formation is taken from the DHCP server. Only extended parameters can be additionally configured. This route remains unchanged by other routes created for this interface and is copied to the routing table in parallel with them. • *Host Route Template per DHCP*: The settings received by DHCP are supplemented with routing information about a particular host. • *Network Route Template per DHCP*: The settings received by DHCP are supplemented with routing information about a particular network. ☞ **Note** If the DHCP lease expires or the device is restarted, the routes comprising a combination of DHCP settings and settings made here are initially deleted again from the active routing. When the DHCP is reconfigured they are then re-generated and re-enabled.
Route Class	Select the **Route Class** type. Possible values: • *Standard*: Defines a route with the default parameters. • *Extended*: Select whether the route is to be defined with extended parameters. If the function is active, a route is created with extended routing parameters such as source interface and source IP address, as well as protocol, source and destination port, type of service (TOS) and the status of the device interface.

Fields in the menu Route Parameters

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

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

Fields in the menu Extended Route Parameters

Field	Description
Description	Enter a description for the IP route.
Source Interface	Select the interface over which the data packets are to reach the device. The default value is *None*.
New Source IP Address/Netmask	Enter the IP address and netmask of the source host or source network.
Layer 4 Protocol	Select a protocol. Possible values: *ICMP*, *IGMP*, *TCP*, *UDP*, *GRE*, *ESP*, *AH*, *OSPF*, *PIM*, *L2TP*, *Any*. The default value is *Any*.
Source Port	Only for **Layer 4 Protocol** = *TCP* or *UDP* Enter the source port.

Field	Description
	First select the port number range. Possible values: • *Any* (default value): The route is valid for all port numbers. • *Single*: Enables the entry of a port number. • *Range*: Enables the entry of a range of port numbers. • *Privileged*: Entry of privileged port numbers: 0 ... 1023. • *Server*: Entry of server port numbers: 5000 ... 32767. • *Clients 1*: Entry of client port numbers: 1024 ... 4999. • *Clients 2*: Entry of client port numbers: 32768 ... 65535. • *Not priviliged*: Entry of unprivileged port numbers: 1024 ... 65535. Enter the appropriate values for the individual port or start port of a range in **Port** and, if appropriate, the end port in **to Port**.
Destination Port	Only for **Layer 4 Protocol** = *TCP* or *UDP* Enter the destination port. First select the port number range. Possible values: • *Any* (default value): The route is valid for all port numbers. • *Single*: Enables the entry of a port number. • *Range*: Enables the entry of a range of port numbers. • *Privileged*: Entry of privileged port numbers: 0 ... 1023. • *Server*: Entry of server port numbers: 5000 ... 32767. • *Clients 1*: Entry of client port numbers: 1024 ... 4999. • *Clients 2*: Entry of client port numbers: 32768 ... 65535. • *Not priviliged*: Entry of unprivileged port numbers: 1024 ... 65535. Enter the appropriate values for the individual port or start port of a range in **Port** and, if appropriate, the end port in **to Port**.
DSCP / TOS Value	Select the Type of Service (TOS).

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

Field	Description
	interface is "up". In this case, an alternative interface with a poorer metric is used for routing until the interface is "up".

3.5.2 IPv4 Routing Table

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

Fields in the menu IPv4 Routing Table

Field	Description
Destination IP Address	Displays the IP address of the destination host or destination network.
Netmask	Displays the netmask of the destination host or destination network.
Gateway	Displays the gateway IP address. Nothing is displayed here when routes are received via DHCP.
Interface	Displays the interface being used for this route.
Metric	Displays the route's priority. The lower the value, the higher the priority of the route
Route Type	Displays the route type.
Extended Route	Displays whether a route has been configured with extended parameters.
Delete	You can delete entries with the 🗑 icon.

3.6 DHCP: Pool configuration changed

The configuring of DHCP pools in the menu **Local Services**->**DHCP Server**->**DHCP Pool** has been split up into the two menus **Local Services**->**DHCP Server**->**IP Pool Configuration** and **Local Services**->**DHCP Server**->**DHCP Configuration**.

Local Services->**DHCP Server**->**DHCP Pool** displays all the IP pools in all systems, including those that have been configured in other menus.

The two menus are described fully below.

3.6.1 IP Pool Configuration

A list of all configured IP pools is displayed in the menu **Local Services**->**DHCP Server**+**IP Pool Configuration**. This list is global and also displays the pools configured in other menus.

3.6.1.1 Edit or New

Choose the **New** button to set up new IP address pools. Select the 🔧 icon to edit existing entries.

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	**Primary**: Enter the IP address of the DNS server that is to be used, preferably, by clients that get an address from this pool. **Secondary**: Enter the IP address of an alternative DNS server.

3.6.2 DHCP Configuration

To activate your device as a DHCP server, you must first define IP address pools from which the IP addresses are distributed to the requesting clients.

A list of all configured IP address pools is displayed in the menu **Local Services**->**DHCP Server**+**DHCP Configuration**.

In the list, for each entry, you can, under **Status**, enable or disable the configured DHCP pools.

Note

In the ex works state the DHCP pool is preconfigured with the IP addresses 192.168.0.10 to 192.168.0.49 and is used if there is no other DHCP server available in the network.

3.6.2.1 Edit or New

Choose the **New** button to set up new IP address pools. Select the 🔧 icon to edit existing entries.

The **Local Services**->**DHCP Server**+**DHCP Configuration**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Select the interface over which the addresses defined in **IP Address Range** are to be assigned to querying DHCP clients. When a DHCP request is received over this **Interface**, one of the addresses from the address pool is assigned.
IP Pool Name	Enter any description to uniquely identify the IP pool.
Pool Usage	Specify whether the IP pool is used for DHCP requests in the same subnet or for DHCP requests that have been forwarded to your device from another subnet. In this case it is possible to define IP addresses from another network. Possible values: • *Local* (default value): The DHCP pool is only used for DHCP requests in the same subnet. • *Relay*: The DHCP pool is only used for DHCP requests forwarded from other subnets. • *Local/Relay*: The DHCP pool is used for DHCP requests in the same subnet and from other subnets.

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

Fields in the menu Advanced Settings

Field	Description
Gateway	Select which IP address is to be transferred to the DHCP client as gateway. Possible values: • *Use router as gateway* (default value): Here, the IP address defined for the **Interface** is transferred.

Field	Description
	• *No gateway*: No IP address is sent. • *Specify*: Enter the corresponding IP address.
Lease Time	Enter the length of time (in minutes) for which an address from the pool is to be assigned to a host. After the **Lease Time** expires, the address can be reassigned by the server. The default value is *120*.
DHCP Options	Specify which additional data is forwarded to the DHCP client. Possible values for **Option**: • *Time Server* (default value): Enter the IP address of the time server to be sent to the client. • *DNS Server*: Enter the IP address of the DNS server to be sent to the client. • *DNS Domain Name*: Enter the DNS domain to be sent to the client. • *WINS/NBNS Server*: Enter the IP address of the WINS/ NBNS server to be sent to the client. • *WINS/NBT Node Type*: Select the type of the WINS/NBT node to be sent to the client. • *TFTP Server*: Enter the IP address of the TFTP server to be sent to the client. • *CAPWAP Controller*: Enter the IP address of the CAPWAP controller to be sent to the client. • *URL (provisioning server)*: You can use this option to send a client any URL you wish. Use this option to send querying **IP1x0** telephones the URL of the provisioning server if the telephones are to be provisioned automatically. The URL then needs to take the form *http://<IP address of the provisioning server>/eg_prov*. • *Vendor Group* (Vendor Specific Information): This option enables you to send the client vendor-specific information in the text string of your choice, should you wish to do so.

Field	Description
	Several entries are possible. Add additional entries with the **Add** button.

Edit

In the **Local Services** ->**DHCP Server** +**DHCP Configuration**->**Advanced Settings** menu you can edit an entry in the **DHCP Options** field if **Option** = *Vendor Group* is selected.

Select the ✎ icon to edit an existing entry. In the pop-up menu, you configure manufacture-specific settings in the DHCP server for specific telephones.

Fields in the Basic Parameters menu

Field	Description
Select vendor	Your device does not currently use this parameter. Here, you can select for which manufacturer specific values shall be transmitted for the DHCP server. Possible values: • *Siemens* (default value) • *Other*
Provisioning Server (code 3)	Your device does not currently use this parameter. Enter which manufacturer value shall be transmitted. For the setting **Select vendor** = *Siemens*, the default value *sdlp* is displayed. You can complete the IP address of the desired server.

3.7 NAT/SIF: Maximum number of sessions changed

The default number of available NAT and SIF sessions has been changed, depending on the device concerned.

The default number available is as follows:

Product	**Maximum number of NAT sessions**	**Maximum number of SIF sessions**
bintec RXL series	16000	16000

Product	Maximum number of NAT sessions	Maximum number of SIF sessions
bintec R(T) series	8000	8000
Other bintec devices	4000	4000

3.8 X.25 over ISDN: Entries modified in the biboDialTable MIB table

To establish the ISDN connection with X.25 over ISDN, you need to specify a phone number that can be used to reach the X.25 server. You can either generate the number using a rule with the MIB variable **x25RTDstLinkAddrRule** or you can use the relevant entries in the **biboDialTable** MIB table to do so.

Prior to this, the entries in the **biboDialTable** could only be used for outgoing calls to X25 over ISDN interfaces if the phone number was not generated using the rule above.

From **Systemsoftware 9.1.5** onwards, the entries in the **biboDialTable** are also used if the ISDN number was generated using the **x25RTDstLinkAddrRule**, providing the MIB variable **biboDialNumber** is empty or "*".

As before, a number that has already been changed by the entry in the **biboDialTable** will not be overwritten.

This change means that, e. g. entries in the **biboDialTable** can be used with different stack masks.

3.9 UMTS: Stick TP-Link MA-180

With the UMTS Stick TP-Link MA-180, the AT command `AT+CRSM` is supported as of now.

3.10 UMTS: ISDN login support

An ISDN login is now also possible with LTE connections. System software version 3.5.19.4 is required with the Sierra Wireless MC7710.

3.11 UMTS: System messages per SMS

With **Systemsoftware 9.1.5** system messages per SMS are available for QMI/LTE modems.

3.12 UMTS: Closed user groups

You can now dial into closed user groups and authenticate yourself using LTE connections.

3.13 System telephones: Shift key setup changed

Previously, for the system telephones **elmeg S530** and **elmeg S560**, you could set up a shift key on every function key on both levels using the GUI of an **elmeg hybird**.

If a shift key was set up on the first level, "no function" was displayed in the GUI on the second level. If another function key was set up on this key on the second level, it would only work incorrectly if it was a function key with an LED display.

From now on, the shift key function on the first level is deleted when a different function is set up on the same key on the second level.

You can also set up a shift key on the second level. This setup variant has been deleted from the software.

3.14 MIB: SNMP Discovery changed

You can now switch the SNMP Discovery function on and off in the **snmpAdmin** MIB table using the *`McDiscovery`* MIB variable. It is switched on by default.

Chapter 4 Bugfixes

Note

Please note that the changes described below are not the only bugs that have been fixed. 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 errors have been corrected in **Systemsoftware 9.1.5** :

4.1 Problems with new browser versions

(ID 17542, 17578, 17698, 17759)

There were problems with the file type when using the latest versions of the Chrome, Internet Explorer and Safari browsers. For example, problems were occurring when an entry had to be selected in a list. Sometimes the selection required was shown in grey and could not be selected, or the expected entry was not displayed.

The problem has been solved.

4.2 Memory problem and crashing

(ID 17573)

Very occasionally, when **bintec RXL12500** was being used with a device from a different manufacturer, there was a huge surge in memory usage followed by a crash.

The problem has been solved.

4.3 Ethernet: Port separation ineffective

ID 17877

When the device was being started, the separation of the Ethernet interfaces was sometimes not being activated quickly enough and the switch would combine all the ports for a short period. In the worst cases, this could cause, e. g. malfunctioning WAN connections.

The problem has been solved.

4.4 USB: Problems with T-Mobile Speedstick LTE II

(ID 17685)

Deutsche Telekom's newly launched T-Mobile Speedstick LTE II was not being recognised by RS series devices.

The problem has been solved.

4.5 USB: Problems with UMTS Stick HUAWEI E352s-5

(ID 17518)

The UMTS Stick HUAWEI E352s-5 was not being recognised by RS series devices.

The problem has been solved.

4.6 System: Device in infinite loop

(ID n/a)

If an A-MPDU (Aggregated MAC Protocol Data Unit) was sent to your device and one of your frames was faulty, the device could enter an infinite loop and end up being blocked.

The problem has been solved.

4.7 LAN: Virtual interface creation failing

(ID 17598, 17622)

If more than one virtual interface had been created in the **LAN**->**IP Configuration**->**New** menu, no additional virtual interface could be created.

The problem has been solved.

4.8 LAN: Identical MAC address for different devices

(ID 17645)

If, in the **LAN**->**IP Configuration** menu under **en1-4** 🔧 was selected, **Address Mode** = *DHCP* was set and under **MAC Address** the setting **Use Preset** and under **Advanced Settings** under **DHCP MAC Address Use Preset** was also enabled and these settings had been saved with **OK**, a fixed value was being saved in the **ipDhcpClientTable** MIB table in the **PhysAddress** MIB variable. For every device, when configured identically, an identical value, i. e. the same MAC address, was being saved for **PhysAddress**.

The problem has been solved.

4.9 LAN: Panic and Stacktrace

(ID 17672)

If an IP address was assigned to *en1-0* and *en1-0* was assigned to switch port 5, this configuration was saved as the boot configuration, a LAN cable was plugged into port ETH 5, LAN data traffic was sent to the router and a reboot was done on the device, a panic with stacktrace and a reboot would be triggered.

The problem has been solved.

4.10 PPP: Name server address transmission not working

(ID 17689)

At times, the transmitting of name server addresses using IPCP was not working.

The problem has been solved.

4.11 ISDN: Incorrect format for phone number

(ID 17757)

In the **WAN**->**Internet + Dial-In**->**ISDN**->**New**->**Advanced Settings** menu, in the section **Dial Numbers** under **Entries** with **Add** in the field**Phone Number**, any characters could be entered.

The problem has been solved.

4.12 DNS/NAT: Deleted DNS entries

(ID 17355)

If an entry has been created in the **Network**->**NAT**->**NAT Configuration**->**New** menu and saved with **OK** and then deleted again, the DNS server entry for the interface concerned in the **Local Services**->**DSN**->**DNS Server** menu would also be deleted.

The problem has been solved.

4.13 Hadware encryption: Panic

ID 17593

Hardware-encrypted PPP connections could result in a panic.

The problem has been solved.

4.14 IPSec: Certificates incorrectly displayed

(ID 17565)

Where more than one CA certificate was being used, the **VPN**->**IPSec**->**Phase-1 Profiles**->**New**->**Advanced Settings** menu would only show the first certificate.

The problem has been solved.

4.15 IPSec: Proposals incorrectly displayed

(ID 17715)

In the **VPN**->**IPSec**->**Phase-1 Profiles** menu and in the **VPN**->**IPSec**->**Phase-2 Profiles** menu, an incorrect value was being displayed in the **Proposals** column,

For example, if *SHA1* was selected as **Encryption** *AES-128* and as **authentication**, *[AES/SHA1]* would be displayed, i. e. the display of the encryption would have three characters cut off. The same problem was occurring with *AES-192* and *AES-256*.

The problem has been solved.

4.16 Network: Incorrect value for Special Session Handling

(ID 17483)

If, in the **Network**->**Load Distribution**->**Special Session Handling**->**New**, e. g. **Service** = *http (SSL)* was selected and the setting was saved with **OK**, in the **ipLoadBExtHandlingTable** MIB table the **SrcIfIndex** MIB variable = *0* would be set instead of **SrcIfIndex** = *-1*.

The problem has been solved.

4.17 CAPI: Incorrect display in the remote CAPI client

(ID 17591)

In the **Remote Multi CAPI Client Configuration**, modem features were also incorrectly being displayed in the **Information About Performance Features** .

The problem has been solved.

4.18 WLAN: Sporadic panics

(ID 17262)

In the **Wireless LAN**->**Management** menu, the dropdown menu **Region** was displaying the entry *Invalid Reference*. Repeatedly opening this menu could trigger a panic.

The problem has been solved.

4.19 WLAN: Incorrect display

(ID 17353)

In devices with two radio modules, when configuring the 5GHz band, the dropdown menu **Frequency Band** was displaying the value *Invalid Reference*.

The problem has been solved.

4.20 WLAN: WDS links mistakenly displayed

(ID 17292)

In the **bintec W1003n**, **W2003n**, **W2003n-ext** and **W2004n** devices, the menus **Wireless LAN**->**WLAN**->**WDS Links** and **Monitoring**->**WLAN**->**WDS** were being displayed even though no WDS links are currently available with these devices.

The problem has been solved.

4.21 WLAN: TKIP not available

(ID 17522)

With the **bintec W1003n**, **W2003n**, **W2003n-ext** and **W2004n** devices, in the menus **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)** and **Wireless LAN Controller**->**Slave AP Configuration**->**Wireless Networks**->🔧, the *TKIP* setting was not available for the parameters **WPA Cipher** and **WPA2 Cipher**.

The problem has been solved.

4.22 WLAN: Wireless Network (VSS) accidentally deleted

(ID 17510)

If, in the menu **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)**, under **Permitted Addresses**, addresses were entered and one of them was them deleted, the entire wireless network would be deleted.

The problem has been solved.

4.23 WLAN: Scan cancellation faulty

(ID n/a)

If the WLAN was switched off during a scan, the system remained in scanning mode.

The problem has been solved.

4.24 WLAN: Panic when automatically selecting channels

(ID n/a)

If a wireless network (VSS) was disabled during the automatic channel selection, a panic would result in the device.

The problem has been solved.

4.25 WLAN: DFS Type 4 not working

(ID n/a)

Radar detection for channels could not be used because DFS (Dynamic Frequency Selection) Type 4 was not working.

The problem has been solved.

4.26 WLAN: Not able to change country

(ID n/a)

When using certain modules, the country setting could not be changed.

The problem has been solved.

4.27 WLAN: Maximum transmission power incorrect

(ID n/a)

When specifying the maximum transmission power, the antenna gain was not being taken into account.

The problem has been solved.

4.28 WLAN: Problems with unencrypted communication

(ID 17168)

At times problems were occurring when there was unencrypted communication between 802.11n-capable bintec WLAN devices and bintec WLAN devices that were working with other standards.

The problems have been solved.

4.29 Wireless LAN controller wizard: problem when initialising the access points

(ID 17658)

When using the wireless LAN controller wizard, at times the initialising of the first found access point in a list of several found access points was failing with the debug message "WTP is offline (unexpected restart detected)" and the wizard was trying to initialise that access point in an infinite loop.

The problem has been solved.

4.30 Wireless LAN controller: Channel display incorrect

(ID 17659)

If you had configured more than one access point in the wireless LAN controller, in the menu **Wireless LAN Controller**->**Slave AP Configuration**->**Slave Access Points** the column would **Channel** column would display `0` for each one.

The problem has been solved.

4.31 Wireless LAN controller: Stacktrace:

(ID n/a)

When using the Wireless LAN Controller, at times a panic was occurring followed by a stacktrace.

The problem has been solved.

4.32 Wireless LAN controller: Problems with remote access points

(ID 17727)

If both local and remote access points were being controlled by a wireless LAN controller, there were occasionally problems with the remote APs (e. g. when using a firewall or a VPN connection), because the wireless LAN controller was using an incorrect IP address / incorrect port to send the response packets to the APs' CAPWAP requests.

The problem has been solved.

4.33 Wireless LAN Controller: CAPWAP Daemon

(ID 17657)

Sometimes, after starting the wireless LAN controller wizard, the CAPWAP Daemon was causing a CPU load of 99 % and the wireless LAN controller was being blocked.

The problem has been solved.

4.34 Wireless LAN controller: Unable to delete inactive entries

ID 17844

At times, inactive entries for slave access points in the WLAN controller could not be deleted.

The problem has been solved.

4.35 Wireless LAN controller: Spatial streams

ID 17867

When configuring radio profiles a profile with the use of three spatial streams could not be created. There are, however, supported by **W2004n**.

The problem has been solved.

4.36 VoIP: System crash

(ID n/a)

At times, the first VoIP connection was causing a system crash.

The problem has been solved.

4.37 VoIP: Malfunctioning connection

(ID 17729)

An incorrect codec selection with IP system telephones was interfering with the audio connection. You could only hear interference.

The problem has been solved.

4.38 VoIP: Syslog message displayed

(ID 17782)

If a **SIP proxy** was configured in the **VoIP**->**SIP** menu for a **bintec RS-Serie** device, at the *Debug* **Level** for the *Configuration* **Subsystem** the syslog message " NCI: outputErrorVals errorId INT_0_65535 not defined" was being displayed.

The problem has been solved.

4.39 VoIP: IP telephone IP1x0 not working

(ID n/a)

If four MSNs were issued via a device in the **hybird** series to four **IP1x0** telephones, and a fifth (or additional) MSN was issued directly to a telephone, this telephone was being tied up by the provisioning with **hybird**, i. e. the provisioning process was starting every 30 seconds so that the telephone could no longer be used.

The problem has been solved.

4.40 VoIP: Problems with audio connection

(ID n/a)

With VoIP connections, at times the audio connection was only working in one direction or not at all.

The problem has been solved.

4.41 VoIP: FAX problems

(ID 17594)

With AudioCodes DSP modules at times there were problems with incoming faxes.

The problem has been solved.

4.42 VoIP: Audio connections not working

(ID 17762)

At times the audio connections in the **elmeg hybird 120 / hybird 130** devices were not working.

The problem has been solved.

4.43 VoIP: Incorrect message with SIP connections

(ID 17707)

If the codecs being used for SIP-SIP connections did not match, the **hybird** series devices would display the irritating error message "Bandwidth limitation reached. Call rejected!".

The problem has been solved.

4.44 hybird: Music on hold not available

(ID n/a)

If the music on hold (MoH) was invoked a second time it would no longer work.

The problem has been solved.

4.45 hybird: Incorrect character interpretation

(ID 17734)

At times the **elmeg hybird** series devices were misinterpreting characters so that those characters were being incorrectly displayed on connected **elmeg S560** / **elmeg S530** system telephones.

The problem has been solved.

4.46 hybird: Status undefined

(ID 17702)

When very busy, the **elmeg hybird** series devices were sometimes going into an undefined status.

The problem has been solved.

4.47 hybird: Unable to use interfaces

ID 17899

When a large number of ISDN interfaces were added to a modular elmeg hybird, not all of the interfaces were usable.

The problem has been solved.

Chapter 5 Known Issue

5.1 WLAN Controller - Configuration of radio modules

If radio module profiles are assigned to **W2003n** or **W2004n** by the WLAN Controller, a profile for the 2.4 GHz band must be assigned to WLAN Module 1, and a profile for the 5 GHz band must be assigned to the WLAN Module 2. With any other assignment of frequency bands, the modules remain inactive after loading the configuration from the WLAN Controller.