Release Notes
System Software 10.2.2

Content

Release Notes describe news and changes in a release for each of the devices for which the release is available. Therefore, they may contain information that is not relevant to your device. If necessary, refer to the data sheet of your device to find out which functions it supports.

1 Release 10.2.2.110 (Patch 10)

1.1 Note

This release is only available for devices of the hybrid series.

1.2 Error corrections

- **SIP - Call Aborts (#3374, 3377):** VoIP calls could be aborted on several occasions. This mainly affected connections with a very short re-registration timeout.

- **Telephony - Connection aborted in case of multiple forwarding (#3152):** In case of multiple forwarding at a Corporate Voice Solutions connection of Deutsche Telekom, the call was aborted after the second forwarding.

2 Release 10.2.2.108 (Patch 8)

2.1 Note

This release is only available for devices of the hybrid series.

2.2 Changes

- **Encryption methods adapted:** The available encryption methods were adapted according to the currently valid RFCs.

2.3 Error corrections

- **System – Update from remote server not possible (# 1398):** It was not possible to update the system software of an **IP620** or **IP630** via the bintec elmeg update server (*Update from external server*).

- **DTMF - Asymmetric settings (#2981):** If a call via the media gateway to an internal IP-PBX signaled the payload type (e.g.) 105 for "telephone-event", the media gateway responded with the payload type 101. The asymmetric negotiation could cause a termination of the call by the platform.

3 Release 10.2.2.107 (Patch 7)

3.1 Note

This release is only available for devices of the hybrid series.

3.2 Error corrections

- **SIP – Connection aborted (#3036):** If there was no final response to a SIP Invite sent via TCP, it could happen that the corresponding TCP session was considered invalid and a new one was set up. The new session was accepted by the other side, but the SIP call was not successfully "moved" to the new session, so that the call was aborted.

4 Release 10.2.2.106 (Patch 6)

4.1 Note

- **This release is only available for devices of the hybrid series.**

4.2 Error corrections

- **Telephony route selection not possible (#2173):** Under **Call Control > Dialing Rules > Interfaces / Providers > New** it was not possible to select a route for external dialing with the setting **Routing Mode** = *Route*.
- **VPN - Tooltips were missing (#1858):** In the **VPN** menu, the tooltips were missing from the status icons.
- **VPN wizard - No LAN connection (#1853):** If a client peer was created in the VPN wizard, no communication to the LAN was possible because of an inactive proxy ARP at the br0 interface.
- **WLC profiles used incorrectly (#2663):** Using two different access points (BOSS-based and OSDx-based) in a WLAN, the WLC Wizard applied a 5GHz profile to the 2.4GHz radio on one access point, and a 2.4GHz profile on the 5 GHz radio module on the other.
- **Internet Assistant - IPv6 Address issue (#2531):** The WAN interface did not receive a public IPv6 address, even though IPv6 was enabled.
- **Internet Assistant - VDSL Vodafone connection not configurable (#1512):** The Internet wizard did not allow you to configure a connection using the **Connection type** = *Internal VDSL modem* for the Internet service provider Vodafone.
- **Obtaining the IP address incorrect (#2265):** If the IP address was changed from static to DHCP, no new DNS server entry could be created.
- **IPSec Display Error (#2129):** Not all profiles were displayed in the **VPN > IPSec > Phase 1 Profiles** menu. The filters and the search did not work correctly.
- **SIP Certificate Issue (#1920, 2200, 2205):** TLS registration of a SIP Trunk did not work if **Check TLS Certificate** was enabled.
  It was not possible to use an imported certificate.
  The option to select your own HTTPS server certificate was missing from the GUI.
- **Problems with ports (#2523):** It could happen that a/b ports did not work after some time.

- **Extended Default Route Issue (#2552):** When using a default extended route, issues occurred that caused the devices to panic and reboot after about 23 days.
- **Corporate Voice Solutions (CVS) Issues (#2510):** When using call groups and call chains, codec issues were encountered under certain circumstances and no communication was possible.
- **Telephony - DTMF not possible (#2389):** Under certain circumstances it was not possible to dial a number using DTMF dialing.
- **VoIP connection broke off (#2034):** In a team call with automatic call acceptance with MoH, it could happen that VoIP connections broke off.
- **VoLTE - No data transmission (#2332):** When an IP telephone on a device called a mobile phone via VoLTE, no voice transmission occurred.
- **VoIP disconnects (#2297):** Connections were aborted because PRACK requests were sent that could not be assigned.
- **VoLTE - No voice transmission (#2295):** Due to a problem in negotiating the connection modalities, it could happen that no voice transmission occurred.
- **Configuration - Export / Import Issue (#2081):** The use of quotes in the admin password caused problems after export and subsequent import of the configuration.
- **WLAN error messages were displayed (#1493):** The irrelevant error messages "WLAN: xxxxxxx: Unknown mime request“ and „VOIP:IWU: data_read(): socket=xx, error=?? errno 108" were displayed again and again.
- **VoIP - SIP registration failed (#1885):** SIP registration of a HiPath 3000 v9 failed because of a problem with the REGISTER request header.
- **System error messages were displayed (#1144):** Error messages of the type "WARNING: MIB: ipNatPrOper (224) has 1 (more) uncommitted rows (total now 1)" and "WARNING: MIB: !!!!! ancient uncommitted MIB entries exist - investigate !!!!!! "were displayed.

4.3 Known Restrictions

- **System – Update from remote server not possible (# 1398):** It is currently not possible to update the system software of an **IP620** or **IP630** via the bintec elmeg update server (*Update from external server*). If necessary, download the current software version for your phone from our website and update via the phone's configuration interface (in the menu **System > Firmware Update**).

5 Release 10.2.2.105 (Patch 5)

5.1 Notes

- **This release is only available for devices of the hybrid series.**

5.2 Error corrections

- **Telephony - SIP Forking (#1979):** SIP forking was not supported, so it could happen that outgoing calls were missing the ringing tone.
- **Telephony – Volume setting not stored (#1809):** If the headset volume had been set to more than "3" on **S560**, this was not stored correctly on the **be.IP**. Upon provisioning (e.g. after a disconnect) the setting was not transmitted correctly to the phone.
- **Telephony - Call transfer failed (#1637):** It could happen that an internal call transfer failed after a callback and the call was released.
- **IP Routing - Presentation of Extended Routes (#666):** The display of extended IPv4 routes in the overview did not allow easy identification of individual routes.
- **IPv6 Packet Loss (#1604):** When routing fragmented IPv6 packets it could happen that associated fragments were collected, but then discarded.
- **VoIP – No Call transfer (#2258):** A call transfer initiated by a DECT 150 device sporadically failed.
- **VoIP – Connection aborted (#2034)**: It could happen that VoIP connections were aborted when calling a team with Automatic Call Pick-up with MoH.

6 Release 10.2.2.104 (Patch 4)

6.1 Notes

- **This release is only available for devices of the hybrid series.**
- **Please note that not all new functions are available in all our products. Refer to the data sheet of your device for information about its scope of functions.**
- **A new function may be provided for different devices at different times.**

6.2 New functions

6.2.1 "Partial Rerouting"

Some service providers require the function of partial rerouting for call forwarding in the exchange. Due to the diversion in the exchange, no voice channels are allocated at the originally called subscriber. Partial Rerouting must be supported and activated by the provider. The configuration then takes place in the telephone system of the customer.

A special configuration is not required for the activation of partial routing.

6.3 Changes

- **IPSec - IKEv2 Rekeying**: In order to configure the active rekeying of an IKEv2 SA, you can specify the lifetime percentage that triggers the rekeying in the **VPN> IPSec> Phase 1 Profiles> Create New IKEv2 Profile** menu.

6.4 Error corrections

- **DHCP - Multiple IP addresses not possible via MAC address (#1494):** It was not possible to statically assign multiple IP addresses to a client with a single MAC address in the GUI.
- **GUI - Missing options in self-configured access (#1445):** If a profile has been created in the **System Management> Configuration Access> Access Profiles** menu that allows access to the **Global Settings** menu, the menu options **Maximum Number of Syslog Entries** and **Maximum Message Level of Syslog Entries** were missing.
- **HotSpot - Too high values possible (#807):** When configuring a HotSpot server, it was possible to specify a very high number of clients for the field **Devices per ticket** (previously **Max. Number of sessions per user**). The maximum number has been reduced to *10*.
- **SIP - Call aborted (#1452 - Media Gateway):** It could happen that a parked call over an SRTP connection was terminated by the exchange when it was resumed.
- **Telephony – Automatic pick-up without MoH (#1675):** If a team configured automatic pick-up with Music on Hold, the music was not played reliably.
- **IPSec- Panic in Rekeying (#1651):** It could happen that a panic occurred if both sides requested a rekeying of the IKE SA at the same time.
- **SIP - No telephony (#1577):** After a SIP transmission error, no further SIP data were transferred.
- **SIP Registration issue (#1480, 1514 - PBX):** Some service providers require the private IP address of a client in order to maintain registration if the public IP address changes. This was not guaranteed until now.
  In addition, problems could occur if the IP addresses contained in the SIP REGISTER and SIP INVITE messages were not the same.
- **System - Bad quality of recorded messages (#1536):** Recorded audio files (e.g. messages on the answering machine) showed poor recording quality.
- **SIP - Panic (#1483 - Media Gateway):** There may be sporadic reboots of the device.
- **SIP - Call terminations (#1464 - PBX):** Calls were not established if SIP messages on the part of the service provider and on the part of a be.IP interfered with each other – e.g., if a SIP UPDATE from the device met a re-INVITE from the remote site.
- **UMTS/LTE - Incoming SMS interrupts Internet connection (#1613):** An incoming SMS on a UMTS/LTE interface caused the Internet connection via this interface to be disabled; reconnection required a reboot.
- **SIP - Call misinterpreted (#1598):** An incoming call to a modem connected to an FXS port resulted in a tone being interpreted as a fax tone. Then a Re-INVITE with T.38 was sent to the provider, and the modem connection was never established.
- **SIP – Incorrect number assumed (#1516):** If the FROM field of the SIP header contained no "user=phone" information, it could happen that the

phone number in the INVITE was not extracted correctly. To work around this, a user name that begins with a "+" is now interpreted as a phone number.

- **Telephony - registration fails (#1976, 1981):** It could happen that registration with the SIP provider failed after the IP address of the interface to which the SIP account was bound had changed.
  Registration errors could also occur if the Internet connection was temporarily interrupted: The first registration attempts failed, but subsequent attempts were successful.
- **Telephony - Key tones not transmitted (#1719):** The key tones of analogue and ISDN telephones were not transmitted successfully to the remote side.
- **Telephony - Panic (#1909, 1930):** A panic could occur if a call was made from an IP phone. Also, using CFU with a macro key could cause a reboot.

7 Release 10.2.2.102 (Patch2)

7.1 New function

- **IPSec:** Rekeying an active IKE connection through a Child SA without reinitializing the entire connection is now supported (see RFC 7296: *Rekeying IKE SAs with the CREATE_CHILD_SA Exchange*).

7.2 Error corrections

- **IPSec - Panic (#1469):** When rekeying an IPSec connection, a panic could occur.
- **ISDN - ISDN login active (ID #1454 - only be.IP 4isdn in operation as a Media Gateway): ISDN Login** was active in the default settings. ISDN login connections to other devices could not be established because they were always terminated on the bintec elmeg device.
  *The update only changes the default configuration of the device. To fix an existing problem, the option can be disabled in the **System Management > Administrative Access** menu. Alternatively, a factory reset restores the default configuration and solves the problem as well.*

1 Release 10.2.2.101 (Patch 1)

1.1 Notices

1.1.1 Update issues

It can happen that an update to system software version 10.2.2.100 fails or remains incomplete because the amount of available flash memory was insufficient. The size of release 10.2.2.101 has been reduced so that an update is possible without problems in most cases.

The following devices were affected:

- hybird 300 / 600

- hybird 1x0

If you want to update one of the affected devices, you should delete language files using the Option **Delete Software/Firmware** in the menu **Software and Configuration**. Language files are displayed with a name of the form “text_<international language code>.ez”, e.g. ”text_ger.ez”.

After an update English and German will be available again for the configuration interface.

1.2 Error corrections

- **WLAN Controller - SSID transferred multiple times (ID #1444):** It could happen that the WLAN controller configured the SSI to be transferred to an access point multiple times.
- **Telephony - Caller number for CLIP no Screening (ID #1362):** With activated CNS, the phone number of an incoming call was forwarded as a national phone number if the option **Show phone number of remote caller** was activated. This is not supported by all providers and could lead to aborted calls. A national number is now converted to the international format.
- **SSH command line (ID #1412):** If the SSH keys were created using the command line program *ssh-keygen*, non-functional keys could be created.
- **SSH - session not terminated (ID #703):** It could happen that the TCP session of a failed SSH connection was not terminated correctly. As a result, no further SSH connections were possible.
- **IPSec - Pathfinder connection rejected (ID #1383):** An IPSec-Pathfinder connection was rejected although the option was enabled in the IPSec configuration.
- **WLAN Controller - SSID not activated (ID #469):** If the default SSID was changed (SSID name and PSK) during WLAN Controller Wizard configuration without prior configuration of the WLAN, this SSID was inactive and the PSK was lost after the wizard was completed.
- **VoIP - Endless registration attempts (ID #1446):** If the registration of a SIP account failed due to an incorrect password, unlimited registration attempts were made.
- **System Reboot (ID #1342):** The device could be rebooted sporadically without any detectable errors.
- **Telephony - Call signaling does not stop (ID #1339):** If a call was not answered and the caller hung up, the signaling of the call did not immediately end with the called party.
- **SIP - SIP trunk not functional (ID #1507 - only be.IP):** Under the following conditions it could happen that incoming calls could not be signaled at the internal ISDN connections:
    a. The device was put into operation in PBX mode.
    b. There was no VoIP configuration made.
    c. The operating mode was changed to Media Gateway.
    d. The ISDN connections were configured as point-to-point connections, and a SIP trunk was set up.

- **SIP – One-sided connection (ID #1523):** There occasionally were one sided connections between SIP accounts by Deutsche Telekom and Vodafone.

2 Release 10.2.2.100

2.1 Notices

- **To enable switching between the two operating modes (PBX and Media Gateway) of *be.IP plus* and *be.IP world edition* without losing the configuration through a "factory reset", we have created a uniform system software for both operating modes. The division into an image for each operating mode is therefore unnecessary.**
- **If you want to reset your device to an earlier software version after an update to release 10.2.2, do not only replace the system software, but also install - if available - the "USB Content" suitable for the release. If applicable, you can find it in the download area of your device.**
- **Please note that not all new functions are available in all our products. Refer to the data sheet of your device for information about its scope of functions.**
- **A detailed description of the individual new functions can be found in the online help of your device.**
- **A new function may be provided for different devices at different times.**

2.2 Security changes

2.2.1 Protection against KRACK

As of Release 10.2.2 our WiFi products are protected against Key Reinstallation Attacks (KRACK, see also https://www.krackattacks.com/), which allow an attack on devices which are operated in client mode.

2.3 New functions

2.3.1 Switching the operating mode

With system software 10.2.2, the operating mode can now be switched over from telephone system (PBX) to Media Gateway or vice versa without the device being reset to its delivery state.

In previous releases, changing the operating mode between PBX and Media Gateway (MGW) and vice versa always meant a loss of configuration. This is now be prevented as of Release 10.2.2. The configuration that is active after a change of the operating mode depends on the deployment history. The following cases are to be distinguished:

2.3.1.1 Switching from PBX to MGW after initial deployment as PBX

This is the main application case, since the initial commissioning as of Release 10.2.2 always takes place in the PBX operating mode. The prompt for the desired operating mode no longer takes place in the first step of commissioning but only after configuration of the customer-specific access data (Internet access, VoIP accounts, WLAN).

In this case, the configuration is completely migrated. In other words, the complete IP configuration (Internet access, WLAN, IPSec, firewall, NAT, etc.) is retained. The Media Gateway configuration is migrated based on the VoIP accounts configured in PBX mode of operation.

Important

Before switching, the currently running PBX configuration is saved. The name of the backup file is "pbx_restore".

Note

If both, single MSN accounts and a DDI account are configured on the device, the MGW configuration is always migrated based on the DDI account. This means that the ISDN ports are configured in point-to-point mode and call routing uses only the DDI account. The single MSN accounts are active after switching but are not considered in call routing.

2.3.1.2 Switching back from MGW to PBX after initial deployment and a subsequent switch according to Case 1 ("pbx_restore" present)

In this case, the backup file "pbx_restore" stored during the previous switchover will be downloaded from the device. The backup file "pbx_restore" is renamed to "boot". After restarting the system, all previous PBX configuration settings will be active again. Exceptions are the administrator password and the BABE service ticket data. This data will be migrated. The login to the system after switching is thus possible with the currently used access data.

Important

Other changes made in the current MGW operating mode will be lost. Before switching, the currently running MGW configuration is saved. The name of the backup file is "mgw_restore".

2.3.1.3 Switching back from PBX to MGW after a switch according to Case 2 ("mgw_restore" present)

In this case, the backup file "mgw_restore" stored during the previous switchover will be downloaded from the device. The backup file "mgw_restore" will be renamed to "boot". After restarting the system, all previous MGW configuration settings will be active again. Exceptions are the administrator password and the BABE service ticket data. This data will be migrated. The login to the system after switching is thus possible with the currently used access data.

Important

Other changes made in the current PBX operating mode will be lost. Before switching, the currently running PBX configuration is saved. The name of the backup file is "pbx_restore".

2.3.1.4 Switching from MGW to PBX, no backup configuration ("pbx_restore") available

This special case occurs under the following conditions:

a) The instrument has been taken into operation in MGW mode with an earlier release, e.g. 10.1.27.
b) The backup file "pbx_restore" has been deleted by the user.

In this case, the complete IP configuration (Internet access, WLAN, IPSec, Firewall, NAT, etc.) is retained. The exception is the VoIP configuration data. These are reset to factory settings (as after a "factory reset").

The VoIP configuration data must, therefore, be configured again.

- .

Important

Before switching, the currently running MGW configuration is saved. The name of the backup file is "mgw_restore".

2.3.2 "Sticky Client"

A client in a WiFi network is called a "sticky client" if it tends to hang on to the original access point (AP) currently registered to. This is also true if the data rate is significantly decreasing and there is an AP with a stronger signal nearby which the client could join.

This behavior is caused by the fact that many clients are originally designed for home network environments where only a single AP is in use and the connection to this AP should be maintained. Roaming is not required here. In professional environments, requirements are completely different because several APs operate in a WiFi network. Here, optimal roaming increases WiFi performance considerably.

2.3.2.1 Roaming

Clients in a larger WiFi network should monitor the indicators for the quality of their connection to an AP. A change in these parameters should cause a roaming decision, i.e. the client should associate to another AP. The Receive Signal Strength Indicator (RSSI), the signal to noise ratio and the number of errors or retries during data transfer may be such indicators.

2.3.2.2 Consequences for other clients

The optimal roaming process of a client in a WiFi network does not only benefit the client itself but all other clients in this WiFi network, as well. If a client operates at a low

transmission rate, the data transfer of a certain data volume takes more time. and clients in the same AP cell must wait longer than necessary to transfer their data.

2.3.2.3 Mitigating "sticky clients"

To mitigate the consequences of "sticky client" behavior, the AP can influence the roaming decisions of the client.

Received Signal Strength Indicator (RSSI)

For this purpose, System Software 10.1.23 supports the RSSI threshold in **bintec W2003ac** devices. The function is available if the parameter **Operation Mode** = *Access-Point / Bridge Link Master* is set under **Wireless LAN -> WLAN -> Radio Setting -> Edit**.

In the menus **Wireless LAN -> WLAN -> Wireless Networks (VSS) -> New/Edit -> Advanced Settings** and **Wireless LAN Controller -> Slave AP configuration -> Wireless Networks (VSS) -> New,** you can define a threshold for the signal level using the parameter **RSSI threshold** under **Low RSSI threshold management**. If an AP recognizes that one of its clients falls below the signal level for a longer period than set under **Grace time**, it stops communicating with this client. Normally, a client tries to connect to the "old" AP for several times and then searches for a new one.

Data rate trimming

System Software 10.1.23 supports **Data Rate Trimming** for **bintec W2003ac** devices. To access this function, set **Operation Mode** = *Access-Point / Bridge Link Master* under **Wireless LAN -> WLAN -> Radio Setting -> Edit**. Using **Data Rate Trimming** increases WiFi performance by blocking low data transfer rates and enforcing the use of higher data rates.

If the distance between a client and its current AP increases, the signal level received by the client as well as the signal quality decreases. To compensate this, the client decreases its data transmission rate because using lower data rates reduces error rates. If using lower data rates is prevented (so called data rate trimming), a client is forced to connect to another AP as soon as the distance to its current AP increases. All clients are forced to use the allowed data rates only.

You can configure the supported data rates under **Data-Rate Trimming** in the **Wireless LAN -> WLAN -> Wireless Networks (VSS) -> New/Edit -> Advanced Settings** and **Wireless LAN Controller -> Slave AP configuration -> Wireless Networks (VSS) -> New** menus. Depending on the selected frequency band several predefined data rate profiles are available.

2.3.3 SIP – Network-side services

System software 10.2.2 supports RFC 5627. Provided a corresponding contract with your provider, the services Call Holding, Toggle, 3-party conference and Call Waiting will be made available on the network side, i.e. not in the PBX, if **Call Hold inside the PBX system** is switched off in the PBX.

The number of voice connections is limited to a number adapted to the existing DSL bandwidth. If there is a bandwidth restriction, the network supports a bandwidth reservation so that each connected device in PBX mode can have one active and one held call. The max. number of calls that are possible at the same time is limited by the number of allowed simultaneous calls to the SIP provider.

The functionality of GRUU (Globally Routable User-Agent URI), Bandwidth Reservation, and Network-Based Services is described in 1TR114 Amendment 4 and implemented accordingly.

Activation of the network-side services takes place in the GUI via the button **Call Hold inside the PBX system** in the **Advanced Settings** of a SIP provider. Disabling the option supports network-side services. If a SIP provider makes more than one SIP account available at one port, the option must be disabled for all accounts, as this is the only way to support bandwidth reservations over multiple phone numbers.

If the network-side services are activated, each outgoing SIP call is set up with a GRUU in the Contact Header Field. If a second connection is established via the same SIP provider, the network checks whether bandwidth can be made available for the corresponding GRUU. If this is not the case, the connection is rejected.

General information about the function

- If an external call is on hold, the PBX will not play music on hold. This is also provided on the network side.
- Internal phones use normal procedures to control network-side services.
- The Conference service is implemented as a client-side 3-way conference, in which the PBX treats the two external connections as standard SIP calls. Building a conference is only possible if two voice channels can be assigned at the same time. In addition, due to the bandwidth limitation, the conference may be rejected by the public network.
- DDI accounts do not support network-side services.
- The function is not active in the standard configuration and must be activated for each SIP provider.
- Holding multiple external calls from a terminal that would result in three or more simultaneous external calls is not supported.

2.3.4 Error announcements

The user is informed about critical errors by means of voice announcements on his phone.

If an outgoing call cannot be established due to an error, the device plays a corresponding message describing the error that has occurred. This makes it easier to estimate if you should take troubleshooting steps yourself or contact support.

The following messages are available:

Index	Name	Description	Length (Sec.)
1	"ann_intern_1.wav"	"Error internet dsl down"	10
2	"ann_intern_2.wav"	"Error no registration"	18
3	"ann_intern_3.wav"	"Error all lines busy"	8

The following errors are intercepted with the following announcements:

Error	Announcement Nr.
The number of simultaneously allowed calls to the SIP provider is exceeded.	(3)
The network rejects a call with the SIP message "Status 606 not acceptable".	(3)
The status of the SIP provider is "not registered".	(2)
The verification of the IP connection of the VoIP subsystem before the call setup fails.	(2)
Checking the IP connection fails, the interface is not active.	(1)

In the following cases no announcement is played, but the busy tone signals:

- if a call is rejected for a reason other than the ones mentioned above,
- if a SIP provider is manually deactivated in the GUI,
- when establishing function calls, e.g. when a callback is established,
- when an emergency number is dialed,

- if the announcement is not contained in the RAM disk of the release,
- if no resources can be allocated to the announcement.

2.3.5 VLAN in WLAN operation

WLAN configuration can be carried out via the wireless LAN controller integrated into the device. To prevent conflicts with the previously used **Wireless LAN** menu, this menu disappears when the Wireless LAN Controller has been activated, e.g., by a configuration with the **WLAN Wizard (WLC)** or by the quick start.

With Release 10.2.2 the menu **Wireless LAN** is displayed again, but the usage is blocked with a corresponding hint as long as the Wireless LAN Controller is activated.

Moreover, the WLAN assistant allows the configuration of guest WLANs. In the process, the wizard makes VLAN settings to disconnect guest Wi-Fi on Layer 2 from the rest of the network. The actual VLAN configuration is handled by the Wireless LAN Controller.

To avoid conflicts with VLAN configurations created via the **LAN -> VLAN** menu, this menu has also been hidden. With release 10.2.2 the menu is now displayed again. However, usage is blocked with a corresponding note as long as the wireless LAN controller is activated.

With release 10.2.2 the deactivating the Wireless LAN Controller as well as completely deleting the controller configuration is supported. The option **Status** in the **WLAN Controller -> Controller configuration** menu is used for this purpose. If the controller is deactivated, but there is still a configuration created by the controller on the device, this configuration can be deleted. This makes it possible (if necessary) to configure WLAN and VLAN via the menu's **Wireless LAN** or **LAN -> VLAN** (and without the **Wireless LAN Controller**).

2.3.6 1TR114 Amendment 2 (NAPTR)

As of Release 10.2.02, NAPTR protocol negotiation is supported based on the requirements of 1TR114 Amendment 2.

The priorities of the transport protocols to be used in NAPTR messages are considered. For devices that are taken into operation for the first time, the corresponding option is automatically set (**Transport Protocol** = *automatic* in the configuration of the SIP provider). Already configured devices must be set up accordingly.

Both, PBX and MGW mode support setting the protocol to *automatic* within the SIP account. If *automatic* is selected, the use of TLS can also be negotiated. If TLS is used, the device must validate the certificate of the P-CSCF. For this reason, the **TLS certificate check** option must always be active if the protocol is set to *automatic*. Since TLS only makes sense if the RTP stream is also encrypted, SRTP should also be active.

Note

In PBX mode, there is the transport protocol for both the registrar and the proxy. The transport protocol of the registrar is the decisive option. The transport protocol of the proxy is ignored because the proxy address is used only if the address is different from the registrar. Since these addresses do not deviate or the address of the proxy in the DDI case is empty, only the transport protocol of the registrar is used.

2.3.7 Alarm input

The PABX systems' FXS interface can be configured as an alarm input. E. g. an alarm button can be connected to one of these interfaces. When the button is pressed, an alarm call is triggered to either up to eight internal numbers or one of two external numbers. Provided your device is equipped with switch contacts, one of them can be activated during an alarm call. The function can, optionally, be switched on using a calendar or you can switch between the two possible signaling variants.

Note

If you intend to add Alarm input, you may first have to free an interface in the menu **Terminals->Other phones->Analogue***, i.e. delete one of the preconfigured entries*.

2.3.8 Standard IEEE 802.3ah

System software 10.2.2 supports the IEEE 802.3ah standard, the so-called "Ethernet in the First Mile". This protocol is used to monitor access lines (first and last mile) and equipment at the customer, as well as to check the lines during commissioning.

2.3.9 UTF-8 WLAN SSID

The WLAN SSID supports special characters and umlauts.

2.3.10 SIP - Send RTP Dummy (MGW only)

In the menu **VoIP -> Settings -> SIP Accounts -> New** the field **Send RTP Dummy** was added, which is needed if the Media Gateway is connected to a device with NAT, which allows the Internet connection to the SIP provider.

2.3.11 Telephony – Ring tones

System software 10.2.2 supports country-specific ringtones (for example, ringtones that are common in Italy). They are automatically selected according to the default locales. For unsupported countries, the settings for Germany are used.

2.3.12 RIPv2 available

From system software 10.2.2 the routing protocol RIPv2 is available for the media gateway be.IP plus (world edition).

2.3.13 IGMP Snooping

IGMP Snooping ensures that multicast streams are only sent to the clients who have subscribed to them. The function is active after the update and can be deactivated in the menu **Multicast> IGMP> Options -> Advanced Settings**.

2.4 Changes

2.4.1 MGW – "Type of number" not used

The "Type of number" field in a called address was not used up to now but will be considered in the future.

2.4.2 WLAN – Number of available wireless networks changed

System software 10.2.2 supports up to 16 Wireless Networks (VSS) for configuration.

2.4.3 IPSec – Peer-ID

System software 10.2.2 allows to leave the **Peer ID** field for the Peer ID types *E-mail address* and *IPv4 address* empty in the **VPN -> IPSec -> IPSec Peers -> New** menu.

2.4.4 Web filter

System software 10.2.2 supports the FlashStart web filter. Information on licensing and application can be found here: http://www.bintec-elmeg.com/en/products/software/software/bintec-elmeg-webfilter/ .

2.5 Error corrections

2.5.1 SIP – Incorrect message

(ID #542)

A team call rerouted to a full waiting queue without a drop target rejected a caller with the message "no user responding" instead of "user busy".

2.5.2 Telephony – Missing music on hold

(ID #958)

If an FXS phone initiated a team call using "Automatic Call Pick-up with MoH", the music on hold was missing.

2.5.3 SIP – Call aborted

(ID #888)

Encrypted calls were aborted after a call pickup using Styx DLAN2. (Media gateway only).

2.5.4 LDAP – Phone book not available

(ID #875)

If a PBX was combined with IP630, phones it could happen that the PBX phone book was not available via the function key on a phone.

2.5.5 MGW - RTP stream problem

(ID #881)

No RTP stream could be established for a DDI Account if the media gateway was located behind a NAT gateway. (Media gateway only)

2.5.6 SIP – Swyx problem

(ID #775)

Using Swyx, a call that reached a timeout caused a caller to get stuck in the status “ringing”. The call was not terminated.

2.5.7 SIP – Incoming call problem

(ID #918)

When rerouting a call, an incoming call could not be assigned to an existing provider account.

2.5.8 WLAN – Guest network

(ID #1044)

If a guest WLAN named “Gäste” was configured by the WLAN assistant, the name “Gäste” was displayed wrong in some menus.

2.5.9 Alert service – Threshold ignored

(ID #899)

In the **External Reporting -> Alert Service -> Alert Recipient -> New** menu, the values under **Message Timeout** and **Number of Messages** were ignored, i.e. an e-mail was sent although the configured values were not yet reached.

2.5.10 Alert service - E-mail address problem

(ID #1070)

If the sender e-mail address was not set, the device name was used as an e-mail address. If this name contains a blank character, problems occurred. Now each blank in the name is replaced by an underline character.

2.5.11 PBX – Phone LED not functioning

(ID #1060)

If a device operated as a PBX and had a registered account, the telephone LED was not on.

2.5.12 LDAP phone book – Wrong display format

(ID #1057)

The IP telephones IP620 and IP630 used the value "%givenName" in the display format of the LDAP phone book. This caused display errors in the PBX because this value does not exist in the bintec elmeg LDAP profile.

2.5.13 IGMP-Snooping – Entertain problem

(ID #1084)

Using Telekom Entertain TV, two TV sets could not receive the same station simultaneously. Both devices displayed a frozen image.

2.5.14 Telekom Entertain – Television reception problems

(ID #1058)

It could happen that an IP TV transmission was interrupted.

2.5.15 IPv6 – Faulty configuration

(ID #1077)

The “First steps” assistant configured an IPv6 ULA with a wrong on-link flag.

2.5.16 MGW – DTMF transmission faulty

(ID #1157)

For DTMF sequences sent as SIP info messages, the transformation of these sequences into RTP events was faulty if the DTMF characters were typed in very fast.

2.5.17 Telekom Entertain - Several clients problems

(ID #1087)

It could happen that an IP TV transmission of different programs to several clients caused problems.

2.5.18 Telephony – Voice mail box not reachable

(ID #1183)

Calls via MSAN POTS did not reach the voice mail box.

2.5.19 WLC – Error messages

(ID #1042)

CAPWAP messages of the type "Missing column ChannelUtil in wlcWlanIfStatTable" and "Missing column RSSIThresholdPurges in wlcVSSStatTable" were displayed because they were assigned to the „error“ level instead of the „warning“ level.

2.5.20 SIF – Rejecting SIP Sessions impossible
(ID #1153)

Firewall rules could not reject SIP sessions.

2.5.21 LTE – Ring tones distorted
(ID #1160)

If an encrypted call via VoLTE reached a mobile phone, the caller heard distorted ring tones.

2.5.22 Telephony – Voice mail box announcements in poor quality
(ID #1094)

It could happen that messages on the voice mail box were recorded in poor quality.

2.5.23 Update – Path incorrect
(ID #841)

An update of the system software failed for software images exclusively used for PBX or Media Gateway devices because the devices could not access the update server due to a wrong path.

2.5.24 Telephony – Display problem during update
(ID #744)

Only up to 20 phones could be displayed in a list when updating system phones.

2.5.25 SSH – Access impossible
(ID #634)

The SSH access with ED25519 keys did not function via PUTTY. The message „Server's Host Key is invalid" was displayed.

2.5.26 Update – No Reboot
(ID #620)

When updating via TR-069 it could happen that an update procedure did not carry out the reboot required to activate the new software version.

2.5.27 Update – No LAN
(ID #1139)

After an update it could happen that the LAN connection was interrupted.

2.5.28 DNS – Entries not functioning
(ID #964)

In **Local Services -> DNS -> Static Hosts -> New** menu, an entry with a **DNS Hostname** beginning with an asterisk * and **Answer** = *negative* did not work.

2.5.29 Telephony – Error Messages

(ID #1056)

It could happen that during a call debug messages of type „IWU: entity_insert (entity=0xXXXXXXXX, type=X) failed“appeared.

2.5.30 SIP – Registrar disappeared

(ID #1121)

It could happen that the configuration of one registrar or several registrars disappeared after an hour.

2.5.31 SIP – Registration not functioning

(ID #1039)

If an option of a SIP account was changed, the SIP registration did not function any longer.

2.5.32 SSH – Key generation faulty

(ID #1053)

Due to an error when generating an SSH key the cryptographic method was chosen automatically and not selected by the user.

2.5.33 Telephony – FXO and Team

(ID #655)

If incoming calls via FXO were forwarded to a team, problems recording a WAV file occurred.

2.5.34 Update – CAPI not functioning

(ID #912)

After an update it could happen that CAPI was not functioning, i.e. audio and FAX were not available.

2.5.35 IPSec – No payload

(ID #847)

After and uptime of four hours, no more data was transferred over an IPSec connection with IKEv2.

2.5.36 DNS – Name resolution failed

(ID 1167)

If a reply to a DNS request contained more than eight CNAME or domain name entries, the reply was ignored, and resolution therefore failed.

2.5.37 SIP – No incoming calls

(ID #892)

It could happen that an automatic disconnection resulted in re-registering the SIP account again, but no incoming calls were received.

2.5.38 IPSec – Sporadic restart

(ID #734)

There were sporadic panics with restart when using IPSec with IKEv1.

2.5.39 NAT / Firewall assistant – entry red marked by mistake

(ID #832)

If in the **Assistants -> NAT / Firewall -> NAT / Firewall -> New** menu under **Destination** and **Service** *User-defined* and under **Protocol** *GRE* was selected and if an **IP Address** was specified, clicking on **OK** resulted in **Destination** and **Service** being marked with a red error symbol in the newly generated entry in the **List of port forwardings**.

2.5.40 NAT / Firewall assistant – entry not functioning

(ID #708)

If in the **Assistants -> NAT / Firewall -> NAT / Firewall -> New** menu **Service** *User-defined,* **Protocol** *TCP* or *UDP* and **Original Destination Port/Range** *all* was selected, clicking on **OK** generated a dysfunctional entry.

2.5.41 SNTP – Time setting changed by mistake

(ID #554)

It could happen that the system time was changed to 7.2.2036 by mistake.

2.5.42 Update – Telephony not functioning

(ID #626, #628)

It could happen that telephony was not functioning after an update via TR-069.

2.5.43 FTP – Upload Problem

(ID #487)

It could happen that the internet connection was interrupted during an FTP upload.

2.5.44 SIP – No VoIP

(ID #833)

Under certain circumstances no VoIP was available after an update of the system software.

2.5.45 Monitoring – Wrong MAC address

(ID #990)

Under certain circumstances a wrong MAC address was displayed. The help text for this address was not correct, either.

2.5.46 WLAN – Channel plan ignored

(ID #1098)

Access points ignored the configured channel plan for the secondary channel.

2.5.47 WLAN – TKIP not allowed for IEEE 802.11n

(ID #438)

On an Access point in slave mode using the 5 GHz band and 802.11n mode, TKIP could be selected in the security settings although TKIP is not allowed in the IEEE 802.11n standard.

2.5.48 SIP – Telephony via DECT not available

(ID #1265)

It could happen that several SIP registrations were suddenly interrupted and telephony via DECT was not available any more.

2.5.49 SIP – Unwanted answers

(ID #1301)

SIP requests of type message, notify or subscribe received via internet were answered. This is unwanted and will not happen in the future, because otherwise user names may be spied.

2.5.50 WLC – Wrong MAC addresses configurable

(ID #1306)

If in the **Wireless LAN Controller -> Slave AP configuration -> Wireless Networks (VSS) -> Edit** menu a wrong **MAC address** was edited with activated **Access Control**, the window could be left with **OK**. No indication of a wrong input was displayed. An error message that some parameters could not be saved was not displayed only upon trying to save the settings.

2.5.51 Automatic refresh interval – display problem

(ID #963)

The field **Automatic Refresh Interval** was displayed in the static menus **Local Services -> DNS -> Static Hosts** and **Local Services DNS -> Domain Forwarding** whereas it was absent in the dynamic menu **Local Services -> DNS -> Dynamic Hosts**.

2.5.52 SIP – NAT ping faulty

(ID #1379)

NAT ping did not function for TCP.

2.5.53 WLC – Radio profiles problem in the Wizard

(ID #1354)

When selecting a *5 GHz Radio Profile* in **Step 2** of the WLAN Controller Wizard it could happen that this setting was reset to the default value *2.4 GHz Radio Profil*e in **Step 4**.

2.5.54 WLC – Radio profile not functioning

(ID #1359)

If WTPs were discovered with the WLAN Controller and a WLAN SSID was set in the WLAN (WLC) assistant, the slave APs were administrated by the WLC, but the slave APs radio modules were not functioning.

2.5.55 ISDN – Problems

(ID #942)

Problems could occur with calls via ISDN.

2.5.56 SIP – Blocked registrars not deleted

(ID #1333)

Blocked registrars were never deleted from in the block list. Therefore, it could happen that SIP accounts could not register anymore.

2.5.57 DNS – Filtering faulty

(ID #1384)

In the **Local Services -> DNS -> Cache** menu, the filtering offered from 20 entries onwards did not function correctly.

2.5.58 WLC – Deleting a wireless network faulty

(ID #1391)

If a wireless network was deleted via the delete symbol in the **Wireless LAN Controller -> Slave AP configuration-> Wireless Networks (VSS)** menu, the corresponding entry in the MIB table **wlcRateControl** was not deleted.

2.5.59 SNMP – Error messages incorrect

(ID #1364)

It could happen that SNMP error messages contained wrong IP addresses.

2.5.60 Memory – Error message incorrect

(ID #1050)

After an update it could happen that the error messages “No card used” or “No memory card detected” were displayed by mistake.

2.5.61 DNS/SIP – DNS Interface binding

(ID #945)

If a SIP account was bound to a particular interface, the DNS queries (for example, to resolve the registrar's address) were not bound to the same interface. If specific DNS servers were configured for the interface in question, they were not used reliably, which could lead to inconsistent behavior.

To avoid potential errors in resolving DNS requests through a specific interface, it makes sense to configure a DNS server without binding to a specific interface.