funkwerk
enterprise communications

Release Notes

System Software 7.9.1

Version 1.2

Purpose

This document describes new features, changes, and solved problems of **System Software 7.9.1.**

Liability

While every effort has been made to ensure the accuracy of all information in this manual, Funkwerk Enterprise Communications GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information and changes can be found at www.funkwerk-ec.com.

As multiprotocol gateways, Bintec gateways set up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. Funkwerk Enterprise Communications GmbH accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks

Bintec and the Bintec logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

Other product names and trademarks mentioned are usually the property of the respective companies and manufacturers.

Copyright

Guidelines and standards

Bintec gateways comply with the following guidelines and standards:

R&TTE Directive 1999/5/EG

CE marking for all EU countries and Switzerland

You will find detailed information in the Declarations of Conformity at www.funkwerk-ec.com.

How to reach Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +49 180 300 9191 0 Fax: +49 180 300 9193 0 Internet: www.funkwerk-ec.com	Funkwerk Enterprise Communications 6 Avenue de la Grande Lande - CS 20102 33173 Gradignan cedex France Telephone: +33 (0)1 61 37 32 76 Fax: +33 (0)1 61 38 15 51 Internet: www.funkwerk-ec.com

1 Important Information

Please read the following information about System software 7.9.1 carefully to avoid problems when updating or using the software.

1.1 Expire Time

System software 7.9.1 is available only for the following devices and cannot be used on other devices:

- **R230a, R230aw, R232b, R232aw, R232bw,**
- **TR200aw, TR200bw,**
- **R1200, R1200w, R1200wu, R1200-VoIP,**
- **R3000, R3000w, R3400, R3800,**
- **R4100, R4300, R4100-VoIP,**
- **W1002, W1002n, W2002,**
- **WI1040, WI2040, WI3040,**
- **WI1065, WI2065, WI3065**.

Note

Please note that new features, changes or the solution of a problem are only available on your device if the menu described is shown.

1.2 Update and Downgrade

Take note of the following indications regarding the update and the possibilities of a downgrade.

You can carry out an update or downgrade using the **Funkwerk Configuration Interface** (FCI) or - if desired - using the SNMP shell and the Setup tool.

1.2.1 Preparation and update with the FCI

The update of the system software with the Funkwerk Configuration Interface uses a BLUP (bintec Large Update) so as to update all necessary modules intelligently. All those elements are updated that are newer in the BLUP than on your gateway.

Attention!

The result of interrupted updating operations could be that your gateway no longer boots. Do not turn your gateway off during the update.

To prepare and carry out an update to **System software 7.9.1** with the **Funkwerk Configuration Interface**, proceed as follows:

1. For the update you will need the file *XXXXX_bl7901.xxx*, where *XXXXX* stands for your device.
   Ensure that the file that you need for the update is available on your PC.
   If the file is not available on your PC, enter www.funkwerk-ec.com in your browser.
   The Funkwerk 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.
   Export the current boot configuration using the ***Maintenance*** ➜ ***Software & Configuration*** menu on the **Funkwerk Configuration 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 window *Opening <name of gateway>.cf* will open. Leave the selection *Save to diskette/hard disk* and click **OK** to save the configuration to your PC.
   The file *<Name of gateway.cf>* is saved, the *Downloads* window shows the saved file.
3. Carry out the update to **System software 7.9.1** via the ***Maintenance*** ➜ ***Software & Configuration*** menu.

To do this, select:
ACTION = *Update system software*
SOURCE = *Local File*
FILENAME = *XXXXX_bl7901.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. The system must be restarted.”
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.

You can log into your device and configure it.

1.2.2 Downgrade with the FCI

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

1. Replace the current boot configuration with the previous backup version.
   Import the backup boot configuration via 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.” shows that the selected system software is being uploaded to the device. When the upload procedure is finished, you will see the message “System - Maintenance. Success. Operation completed successfully. The system must be restarted.”
   Click **Reboot**.
   You will see the message “System - Reboot. Rebooting. Please wait. This

takes approximately 40 seconds." The device will start and the browser window will open. Log into your device.

2. Carry out the downgrade to the required software version via the ***MAINTENANCE*** ➜ ***SOFTWARE & CONFIGURATION*** menu.
   To do this, select:
   ACTION = *Update system software*
   SOURCE = *Local File*
   FILENAME = *R3000_bl7807.r3d* (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 system software is being uploaded to the device. When the upload procedure is finished, you will see the message "System - Maintenance. Success. Operation completed successfully. The system must be restarted."
   Click **Reboot**.
   You will see the message "System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds." The device will start with the previously backed up boot configuration and the old version of the system software. The browser window will open.

You can log into your device and configure it.

2 New Functions

System software 7.9.1 includes a number of new functions that significantly extend the performance compared with the previous version of the system software:

2.1 Wizards in the FCI

In System software 7.9.1 wizards are offered for several frequently used configuration tasks.

These wizards can be found in the FCI navigation bar.

You can use wizards for the following tasks:

- First steps
- Internet Access
- VPN
- SWYX (only available if a DSP module is plugged into your device and is enabled)
- Wireless LAN (only available for WLAN-enable devices).

Each wizard leads you step by step through the respective configuration task. You can use a wizard more than once, if required, to create several connections.

Detailed information on each wizard can be found in the corresponding configuration step.

2.2 Time zone selection for automatic daylight saving

In System software 7.9.1 your device automatically switches from summer time to standard time in autumn and from standard time to summer time in spring on the respective changeover date.

In the FCI menu ***System Management*** ➜ ***Global Settings*** ➜ ***Date and Time*** you can select the required time zone for your system (e.g. *Europe/Berlin*) in the new ***System Time Zone*** field. If summer time and standard time are defined for the chosen time zone, the changeover is carried out automatically on the changeover date. The ***Time Offset from GMT*** field is no longer required and has been removed.

Note

Note that automatic daylight saving can have an undesirable effect on events that are configured in the ***Local Services*** ➜ ***Scheduling*** menu.

Note

Note that automatic daylight saving can result timestamps being duplicated for recorded events when switching from summer time to standard time.

2.3 Q-SIG

In System software 7.9.1 the D-channel protocol Q-SIG is available.

Some of the available Q-SIG functions have so far been implemented to realize unified messaging solutions together with our partner Servonic.

A Servonic unified messaging system can be connected to a Siemens Hicom 300 PABX using a bintec gateway, e.g. to a Hicom 300. Hicom's ISDN point-to-point connection is used; communication between the unified messaging system and the PABX occur via the bintec Remote CAPI. Q-SIG is used to offer the user of the unified messaging system supplementary services.

The following Q-SIG functions have so far been implemented:

- An outgoing call is passed to the desired remote terminal.
- An incoming call is passed to the desired internal extension and the number of the caller is indicated (in accordance with ECMA 175/176/177/178).
- An incoming call is passed by the desired internal extension, e.g. if busy, to a second extension and is signalled to the first extension (MWI; in accordance with ECMA 241/242).
- An incoming call is passed by the desired extension to a mailbox, the call is signalled to the extension (MWI) and the mailbox can be queried (in accordance with ECMA 241/242).

To use the Q-SIG protocol, select the FCI menu ***Physical Interfaces*** ➜ ***ISDN Ports*** ➜ ***ISDN Configuration*** ➜ ***Icon to change an entry***. Disable ***Autoconfiguration on Bootup*** and set ***Port Usage*** to *Q-SIG*.

2.4 ISAKMP Configuration Method (IKE Config Mode) in client mode

The ISAKMP Configuration Method (IKE Config Mode for short) allows you to connect a mobile PC workstation (Secure IPSec Client) to the head office over IPSec.

The IP address and, if required, other data such as the domain and server parameters for DNS and WINS are sent to the client by the IPSec gateway on request. This method allows a dynamic IP address to be assigned, e.g. from the internal address range for the head office (see Release Notes 7.8.2).

In **System software 7.9.1** you can now not only configure your device as a server as before, but also as a client for IKE Config Mode; previously you could use an NCP Secure Client, for example as a client.

The two radio buttons in the ***IP Address Assignment*** field in the ***VPN*** ➜ ***IPSec*** ➜ ***IPSec Peers*** ➜ **New** menu have been replaced with a dropdown menu containing the values *Static*, *IKE Config Mode Client* and *IKE Config Mode Server*.

The new setting *IKE Config Mode Client* allows you to configure your gateway as a client for IKE Config Mode.

2.5 DHCP - Integrating gateways into a network in the ex works state

In System software 7.9.1 devices can be more easily integrated into a network on initial start-up after delivery. Depending on the device type, the device behaves differently if there is no configuration available.

2.5.1 Wx002(n), WIx040, WIx065

A device in series Wx002(n), WIx040 or WIx065 starts as DHCP client in the local network. It sends DHCP requests and waits for the response from a DHCP server.

If a DHCP server responds, the device acts as DHCP client and uses the IP address, which assigns it to the DHCP server.

If no DHCP server responds, the device receives its predefined IP address *192.168.0.252*. You can assign a different IP address using the FCI or the setup tool.

The start mode for the device described above as DHCP client in the network is cancelled, if

- a user logs in over the series interface.
- a TCP session for the device starts (over Telnet or with the FCI).
- a fixed IP address is assigned.

Start mode is also terminated, if a DHCP server assigns an IP address. In this case, the device continues to act as DHCP client.

2.5.2 R2xx

A device in series R2xx starts as DHCP client and as BOOTP client in the network; it sends up to three DHCP requests and up to five BOOTP requests in sequence.

If a DHCP server responds, the device uses the predefined value *192.168.0.252* as its own IP address and continues to send BOOTP requests.

If the device receives a BOOTP response, e.g. from the Dime tools, it applies the assigned IP address.

If the device receives no response, it acts as DHCP server and supplies an IP address pool with 40 IP addresses starting with the IP address *192.168.0.10*. The predefined value *192.168.0.254* is used as its own IP address.

Note

If you then configure the device over the FCI or the setup tool, make sure that the own IP address remains consistent with the IP addresses from the address pool.

The start mode described above as DHCP client and as BOOTP client in the network is cancelled, if

- a user logs in over the series interface.
- a TCP session is started (over Telnet or with the FCI).
- a fixed IP address is assigned.

2.5.3 TR200aw/bw, R1xxx, R3xxx, R4xxx

A device in series TR200aw/bw, R1xxx, R3xxx or R4xxx starts as BOOTP client and sends BOOTP requests. (This behaviour is identical to the behaviour of all bintec devices before System software 7.9.1.)

The IP address *192.168.0.254* is predefined in each new device.

If the device receives a BOOTP response to its BOOTP request, e.g. from the Dime tools, it applies the assigned IP address.

If you assign an IP address using the FCI or the setup tool, the device uses this address.

The start mode for the device described above as BOOTP client in the network is cancelled, if

- a BOOTP response is received.
- a user logs in over the series interface.
- a TCP session is started (over Telnet or with the FCI).
- a fixed IP address is assigned.

2.6 SHDSL.bis (R3800)

In System software 7.9.1 SHDSL.bis (ITU-T G.991.2) is available, an extension of the SHDSL standard, which permits higher clock rates. SHDSL.bis can only be used with firmware RNY-SHDSL8bis-1.5.5.33.rny. For SHDSL.bis all wire pairs must be configured uniformly either in CPE mode or in CO mode.

The following maximum clock rates are available:

Wire pair(s) - wires	Mode	Maximum rate in Mbps
1 - 2	PHY Layer Bonding	5,7
2 - 4	PHY Layer Bonding	11,4
2 - 4	IMA	11,4
3 - 6	IMA	17,1
4 - 8	IMA	22,4

2.7 FCI - SNMP Browser

In System software 7.9.1 a SNMP browser is available.

You can choose this browser in the FCI header in the ***VIEW*** field under the name *SNMP Browser*.

You can access all MIB tables and variables for your system and can view and edit these. If an Internet connection is available, online help can be accessed for the SNMP browser, which is loaded dynamically from the FEC web server.

2.8 Hot Spot

In System software 7.9.1 you can provide your customers with Internet access using the new hot spot function.

The so-called HotSpot Solution allows provision of public Internet accesses (using WLAN or wired Ethernet). The solution is adapted to setup of smaller and larger Hotspot solutions for cafes, hotels, companies, communal residences, campgrounds, etc.

The bintec HotSpot Solution consists of a bintec gateway installed onsite (with its own WLAN access point or additional connected WLAN device or wired LAN) and of the Hotspot server, centrally located at a computing centre. The operator account is administered on the server via an administration terminal (e.g., a hotel reception PC); this includes functions such as registration entry, generating tickets, statistical analysis, etc.

In the ***LOCAL SERVICES*** ➜ ***HOTSPOT GATEWAY*** ➜ ***HOTSPOT GATEWAY*** ➜ **New** menu you can configure the bintec gateway installed onsite for the bintec Hotspot Solution.

Note

Use ssh instead of telnet to login when configuring login authentication via RADIUS (i.e. when you set the ***AUTHENTICATION TYPE*** = *Login Authentication* in the ***SYSTEM MANAGEMENT*** ➜ ***REMOTE AUTHENTICATION*** ➜ ***RADIUS*** ➜ **New** menu).

In the ***MONITORING*** ➜ ***HOTSPOT GATEWAY*** ➜ ***HOTSPOT GATEWAY*** menu you can monitor your HotSpot gateway and view a list of all connected hosts is shown.

Detailed information on the bintec HotSpot Solution can be found in the FCI in the online help for your bintec device.

2.9 VoIP - License for internal extension numbers (TR200)

Ten internal extensions are available free of charge for VoIP, other numbers require a license.

Your system comes with ten internal extensions by default. Licenses for other numbers are available in blocks of ten, which are added to the existing numbers up to a maximum of 40 numbers.

You can view the internal extension numbers currently available in the FCI menu ***PBX*** ➜ ***INTERNAL NUMBERS*** ➜ ***VOIP***.

The licensing mechanism is the same as in IPSec, the name of a VoIP license for ten extension numbers is *SNxSIP10*. You can enter the new license data after online licensing in the ***SYSTEM MANAGEMENT*** ➜ ***GLOBAL SETTINGS*** ➜ ***SYSTEM LICENSES*** ➜ **New** menu. Once the maximum 40 numbers has been reached, the **New** will be grayed out.

If a configuration containing more extension numbers than licenses is loaded, a warning appears. You will be asked to delete some of the entries.

2.10 Fax license (R4100)

System software 7.9.1 offers FAX support for the R4100 device with 30 channel DSP module. You need a license for this.

With a license, you can obtain FAX support via protocols T.30 and T.38.

The licensing mechanism is the same as in IPSec, the name of a FAX license is *R4xFAX30*. You can enter the new license data after online licensing in the ***SYSTEM MANAGEMENT*** ➜ ***GLOBAL SETTINGS*** ➜ ***SYSTEM LICENSES*** ➜ **New** menu.

If a fax license is active, it will be displayed in the ***DSP MODULE*** field in the ***SYSTEM MANAGEMENT*** ➜ ***STATUS*** menu.

2.11 cert get command with HTTPS

In System software 7.9.1 the *cert get* command is available to import certificates over HTTPS.

2.12 Scheduler - Placeholder available for serial number

In System software 7.9.1 you can use the character string SN as a placeholder for the serial number in commands in the Scheduler.

For example, you can set the field ***SET VALUE ACTIVE*** to *get_all;http://10.9.1.2/tftp:file SN.cf* in the setup tool menu ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***EVENT SCHEDULER (TIME & SNMP)*** ➜ ***SCHEDULE COMMANDS*** ➜ **ADD** to obtain the configuration files for several gateways.

2.13 WLAN - 5.8 GHz band available for UK

In System software 7.9.1 the operation band 5.8 GHz can now be used with the country setting UK.

2.14 USB 2.0 added

In System software 7.9.1 the default USB 2.0 has been added to support the card type OPTION GE0421 (e.g. Mobile Connect Card Vodafone E3730) and USB stick Stick Sierra Wireless Compass 885.

2.15 DynDNS Provider www.dnsexit.com

In System software 7.9.1 the DynDNS Provider www.dnsexit.com is now available.

2.16 FCI - RADIUS - Configuration options expanded

The new *Default Group 0* **option is available in the** ***Group Description*** **field in the FCI menu** ***System Management*** **➜** ***Remote Authentication*** **➜** ***RADIUS*** **➜ New.**

This setting is required, for example when configuring a hotspot.

2.17 FCI - UMTS - New field available

The new field ***Modem Status*** **is available in the FCI menu** ***Physical Interfaces*** **➜** ***UMTS/HSDPA*****.**

2.18 FCI - SHDSL - New field available

In the FCI menu ***Physical Interfaces*** **➜** ***SHDSL*** **➜** ***SHDS Configuration*** **the new field** ***Minimum Number of Active Links*** **is available for the IMA configuration (*Wire Mode* =** *4 wire IMA*, *6 wire IMA* **or** *8 wire IMA*).

2.19 FCI - WLAN - New field EAP preauthentification available

In System software 7.9.1 the new *EAP PREAUTHENTIFICATION* field is available in the FCI menu *WIRELESS LAN* ➜ *WLANX* ➜ *VIRTUAL SERVICE SETS* ➜ New/Icon to change an entry when *SECURITY MODE* is set to *WPA Enterprise*.

2.20 FCI - WDS Links - Configuration options expanded

The new values *WPA* and *WPA2* are now available in the *PRIVACY* field in the FCI menu *WIRELESS LAN* ➜ *WLANX* ➜ *WDS LINKS* ➜ New.

2.21 FCI - WLAN - WDS possible with AES and TKIP

In System software 7.9.1 AES and TKIP can now also be chosen for encryption when configuring WDS connections in access point mode.

2.22 FCI - IPSec - Multiple users over the same peer

In System software 7.9.1 you can configure an IPSec peer in the FCI so that multiple users can dialin over this IPSec peer.

To do this, select ***VPN*** ➜ ***IPSEC*** ➜ ***IPSEC PEERS*** ➜ **New** ➜ **Advanced Settings** from the FCI menu and set ***NUMBER OF ADMITTED CONNECTIONS*** to *Multiple Users*. We also recommend setting the ***IP ADDRESS ASSIGNMENT*** field to *IKE Config Mode Server*.

2.23 FCI - Fax header field added

The *Fax Header* field is available in the FCI menu *Local Services* ➜ *CAPI Server* ➜ *Options* for the installed DSP module.

In the ***Fax Header*** field, you can set whether or not a header is printed at the top of an outgoing fax.

2.24 FCI - Scheduler can be disabled

The new *Schedule Interval* field is now available in the FCI menu *Local Services* ➜ *Scheduling* ➜ *Options*.

You can enable or disable the ***Schedule Interval*** field by switching the Scheduler on or off.

2.25 Setup Tool - PUK input added

The *SIM card uses PUK* field has been added in the setup tool menu UMTS6-0.

The personal unblocking key (PUK) is used to unblock the UMTS modem card, if the PIN has been entered incorrectly several times (i.e. three times for most cards).

2.26 Setup Tool - ISDN statistics

In System software 7.9.1 the statistics for terminated calls, and not just current calls as in previous versions, are available using the command *s* in the setup tool menu *Monitoring & Debugging* ➜ *ISDN Monitor*.

2.27 New MIB variable HttpRedirect

In System software 7.9.1 the new MIB variable HttpRedirect is now available in the MIB table ipExtIfTable.

With the variable ***HTTPREDIRECT*** you can either redirect HTTP requests to the local HTTP demon (*local*) or to the local content filter (*proxy*).

3 Changes

The following changes have been made in our system software to improve its performance and usability:

3.1 Java SNMP browser removed

In **System software 7.9.1** the Java SNMP browser has been removed.

3.2 HTML Setup tool removed

In **System software 7.9.1** the HTML Setup tool has been removed.

3.3 Credits functionality removed

In **System software 7.9.1** the Credits functionality has been removed.

3.4 dmesg command extended

In **System software 7.9.1** the command dmesg has been extended with the option -t to output the content of the kernel buffer from the time of the command call.

3.5 Preshared Keys - Warning added

The following warning has been added in **System software 7.9.1** to prompt the user to change the default setting of the Preshared Key: “Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!”

3.6 SIF alias names changed for interfaces

In **System software 7.9.1** the SIF alias names for interfaces have been improved to avoid misunderstandings. A distinction can now be made between the following categories: LAN, WLAN, IPSec, Leased, Bundle and Bridge. For example, the current interface is *LAN_PEER_2_R4100_1* but will now be renamed *IPSEC_PEER_2_R4100_1*.

3.7 FCI - Additional access rule

When a rule is created for administrative access for the first time, an additional rule is automatically created to ensure that no data traffic is blocked by mistake.

3.8 FCI - Status - Interfaces renamed

The interfaces *com6-0* and *bri4-0* have been renamed *USB/UMTS* and *ISDN* respectively in the FCI menu ***System Management*** ➜ ***Status***.

3.9 FCI - WLAN radio setting options changed

In **System software 7.9.1** the setting options have been changed in FCI menu ***Wireless LAN*** ➜***WLANx*** ➜ ***Radio Settings*** ➜ **Icon to change an entry**. The ***Radio*** field has been removed, the ***Operation Mode*** field now contains the selection options ***Off***, ***Access Point***, ***Access Client*** and ***Bridge***.

3.10 FCI - Virtual Service Sets with security mode

In **System software 7.9.1** the value ***Security Mode*** = *WPA-PSK* is preset for the default VSS displayed in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Virtual Service Sets*** ➜ **Icon to change an entry**.

3.11 FCI - DNS - Field renamed

The ***Description*** field has been renamed ***DNS Hostname*** in the FCI menu ***Local Services*** ➜ ***DNS*** ➜ ***Static Hosts***.

3.12 Setup Tool - Cobion Orange Filter - Field renamed

The ***FILTERED INTERFACE*** field has been renamed ***FILTERED SOURCE INTERFACE*** in the setup tool menu ***SECURITY*** ➜ ***COBION ORANGE FILTER***.

3.13 Setup Tool - QoS - Value range expanded

In the Setup Tool menu ***QOS*** ➜ ***INTERFACES AND POLICIES*** ➜ **Edit** ➜ ***QOS SCHEDULING AND SHAPING*** the setting ***QUEUEING AND SCHEDULING ALGORITHM*** = *priority queueing (PQ)* and ***SPECIFY TRAFFIC SHAPING*** = ***YES*** displays the field ***MAXIMUM TRANSMIT RATE (BITS PER SECOND)***. The value range for this field has been expanded from *100000000* to *1000000000*.

3.14 Giving parameters when making outgoing calls from your own subscriber number

To "give" specific parameters in accordance with Q.931 when making outgoing calls from your own subscriber number, the MIB variable ***SCREENING*** in MIB table ***BIBODIALTABLE*** can also be used for outgoing calls. The new MIB variable ***TYPEOFLOCALNUMBER*** is also available for this purpose.

3.15 MIB table wlanIfTable extended

The MIB variable ***BAND*** is now still only available in MIB table ***WLANIFTABLE*** (and no longer as redundant information in table ***WLANCLIENTTABLE***). The values *m802-11abgn*, *m802-11abg* and *m802-11agn* have also been added to the MIB variables ***MODE*** in MIB table ***WLANIFTABLE***.

4 Problems Solved

Not all devices listed in chapter “Important Information” on page 9 were affected by the following problems. If your device does not have the menu or property in question, you can ignore the problem mentioned.

The following problems have been solved in System software 7.9.1

4.1 Serial interface unavailable

(ID 12240)

The serial interface was unavailable, as entries were not created automatically in the MIB tale ***AUXCONFIGTABLE***.

The problem has been solved.

4.2 Stacktrace after input of dmesg

(ID 12104)

A stacktrace occurred after entering the command *dmesg*.

The problem has been solved.

4.3 Stacktrace due to memory problems

(ID n/a)

Clients with the incorrect WPA mode, repeatedly attempted to connect and caused a stacktrace due to a memory overrun.

The problem has been solved.

4.4 Stacktrace due to wrong Lifetime Policy

(ID 12531)

During configuring IPSec with the Setup tool, exceeding the value range *0* .. *4294967295* in the ***LIFETIME POLICY*** field caused a stacktrace. There was no difference between setting the value in seconds or in kbps.

The problem has been solved.

4.5 PIM - Stacktrace

(ID n/a)

When shutting down PIM, a stacktrace occurred when the corresponding interface was unavailable.

The problem has been solved.

4.6 Stacktrace at trace over DSL

(ID 12392)

A trace of the tunnel interface over DSL with a tunnel connection under load triggered a stacktrace.

The problem has been solved.

4.7 Bridge link - No connection

(ID 11978)

Despite a WDS link (bridge link) with the status *up*, no IP data traffic was possible.

The problem has been solved.

4.8 PPP connections failed

(ID 11303)

In rare cases, the set-up of a PPP connection failed and the interface froze until it was manually reset or rebooted.

The problem has been solved.

4.9 IPSec - Problems setting up phase 2

(ID 12163)

When setting up phase 2 of an IPSec connection problems occurred when selecting the source address.

The problem has been solved.

4.10 IPSec - trace did not display UDP packets

(ID 12455)

When performing a trace of an IPSec tunnel, data packets sent with high priority by the router were not displayed.

The problem has been solved.

4.11 IPSec - IKE Config Mode - Wrong entry in MIB table ipDynaAddrTable

(ID 12471)

In IKE config mode the MIB table ***ipDynaAddrTable*** contains the entry ***ifIndex*** = *10001* (instead of ***ifIndex*** = *100002* for the IPSec Peer).

The problem has been solved.

4.12 IPSec - No tunnel with certificate

(ID 11313)

With IPSec no connection could be established over RADIUS if the certificate used had a parameter user name with a length of more than 64 characters.

The problem has been solved.

4.13 FCI - Incorrect annex type selectable

(ID n/a)

In the FCI, annex M was offered for selection for annex B devices during ADSL configuration.

The problem has been solved.

4.14 WLAN - connection to gateway unavailable

(ID 12271)

Connection over WLAN to the gateway could not be established, as the maximum number of possible clients was incorrectly set to the value *0* and so all clients were rejected.

The problem has been solved.

4.15 WLAN - Problems with automatic configuration in bridge link mode

(ID 11424)

When setting up a bridge link in the 5 GHz band and with 40 MHz bandwidth, unexpected and undesirable results sometimes occurred (such as non-functioning connections or low data throughput).

The problem has been solved.

4.16 WLAN - Clients rejected incorrectly

(ID 11254)

After some clients that were connected with the gateway in access point mode were rejected, because they were not registered with the RADIUS server, all clients were mistakenly rejected and the device had to be rebooted.

The problem has been solved.

4.17 WLAN - WDS scan unavailable

(ID 11621)

If the radio module was not fully initialised, no error message appears when a WDS scan is attempted.

The problem has been solved.

4.18 Saving the configuration failed

(ID 12251)

When there was not much free memory in the flash, a boot configuration was not saved correctly but no error message appeared.

The problem has been solved.

4.19 Multi-User via hotspot available incorrectly

(ID 11363)

A single RADIUS account could be used to dial-in using hotspots over various clients.

The problem has been solved.

4.20 Media Gateway - Unidirectional voice connection

(ID 12407)

After a CAPI or isdnlogin connection, a call over the media gateway failed and the voice connection only operated in one direction.

The problem has been solved.

4.21 Unidirectional voice connections

(ID 10776)

After selecting RAS in the gateway, voice connections only worked in a single direction.

The problem has been solved.

4.22 SNR Margins displayed incorrectly

(ID 12276)

For ADSL1-Links the firmware versions 6.2.12 / E.74.2.53 and 6.2.13 / E.74.2.55 for Annex B display too high SNR margins in the syslog messages and with the command *dsl status*. Incorrect values were also displayed in the setup tool menu ***Monitoring and Debugging*** ➜ ***ADSL*** and in the MIB table ***adslAtucPhysTable***, which also differ from the above values.

The problem has been solved.

4.23 Multicast not functioning

(ID n/a)

In some cases multicast did not function because it had been enabled several times.

The problem has been solved.

4.24 Multicast - Forwarding packets failed

(ID n/a)

In scenarios with Source Specific Multicast (SSM), the forwarding of packets failed.

The problem has been solved.

4.25 Multicast failed on IPSec interfaces

(ID n/a)

No multicast packets could be transferred on IPSec interfaces.

The problem has been solved.

4.26 Multicast - Timer problem

(ID n/a)

In some cases, many queries and reports have been sent and received on an interface.

The problem has been solved; the timers have been adjusted.

4.27 RADIUS reload did not work

(ID n/a)

The non-functioning RADIUS dialout reload caused a continuous loop of get requests.

The problem has been solved.

4.28 FCI - Texts displayed incorrectly

(ID 12268)

In the FCI some texts were displayed in HTML code.

The problem has been solved; the texts are displayed correctly.

4.29 FCI - System Management - Incorrect error message

(ID 11470)

When attempting to modify the settings in the FCI menu ***System Management ➜ Administrative Access ➜ Access***, the error message “Value must be greater than or equal the following: 0” appeared and no changes could be made.

The problem has been solved.

4.30 FCI - WLAN *Bridge Links* menu incomplete

(ID 12463)

If in the FCI menu ***Wireless LAN ➜ WLANx ➜ Radio Settings ➜ Icon to change an entry***, when ***Operation Mode*** was set to *Bridge* and you clicked **OK**, the default entry was missing under ***Wireless LAN ➜ WLANx ➜Bridge Links***.

The problem has been solved.

4.31 FCI - WLAN - *WDS LINKS* menu missing

(ID 11616)

If in the FCI menu ***WIRELESS LAN*** ➜ ***WLANX*** ➜ ***RADIO SETTINGS*** ➜ ***ICON TO CHANGE AN ENTRY***, the settings ***OPERATION MODE*** = *Access Point* and ***OPERATION BAND*** = *5 GHz Indoor* were made and ***SELECTED CHANNELS*** was not set to *Auto* and you clicked **OK**, the ***WDS LINKS*** tab and corresponding menu were missing.

The problem has been solved.

4.32 FCI - Max. Link Distance displayed incorrectly

(ID 12237)

The ***MAX. LINK DISTANCE*** field in the FCI menu ***WIRELESS LAN*** ➜ ***WLANX*** ➜ ***RADIO SETTINGS*** ➜ **Icon to change an entry** was displayed for all WLAN interfaces, although it only applies to bridge links.

The problem has been solved; the ***MAX. LINK DISTANCE*** field is only displayed if ***OPERATION MODE*** = *Bridge*.

4.33 FCI - IPSec - Peers not displayed

(ID 12213)

Peers that were configured via traffic lists were not displayed in the FCI menu ***VPN*** ➜ ***IPSEC*** ➜ ***IPSEC PEERS***. These peers were displayed in the menu ***MONITORING*** ➜ ***IPSEC***.

The problem has been solved.

4.34 FCI - IPSec - Incorrect setting option

(ID 12200)

If the ***IP Address Assignment*** field was set to *IKE Config Mode Client* in the FCI menu ***VPN*** ➜ ***IPSec*** ➜ ***IPSec Peers*** ➜ **New**, it was possible to enter an IP address in the ***Local IP Address*** in the field.

The problem has been solved; the ***Local IP Address*** field is no longer displayed in the situation described above.

4.35 FCI - DNS names not accepted

(ID 12227)

Only IP addresses and no DNS names were accepted in the ***Remote PPTP-IP Address*** field in the FCI menu ***VPN*** ➜ ***PPTP*** ➜ ***PPTP Tunnels*** ➜ **New**.

The problem has been solved; IP addresses and DNS names, e.g. *xyz.dyndns.org* are accepted.

4.36 FCI - ISDN selectable in error

(ID 12347)

In devices without ISDN, the ***Callback*** was displayed in error in the FCI menu ***VPN*** ➜ ***PPTP*** ➜ ***PPTP Tunnels*** ➜ **New** ➜ ***Advanced Settings***. If callback was activated, the fields ***Incoming ISDN Number*** and ***Outgoing ISDN Number*** were displayed.

The problem has been solved; the ***Callback*** field is no longer displayed.

4.37 FCI - PPTP - Setting option missing

(ID 12435)

For Windows XP (SP2) PPTP clients, you must set ***GRE Window Adaption*** to *disabled* and set ***GRE Window Size*** to *256* in the FCI menu ***VPN ➜ PPTP ➜ Options***. If ***GRE Window Adaption*** had been disabled, the ***GRE Window Size*** field was not displayed and so no value could be entered.

The problem has been solved.

4.38 FCI - Firewall - Incorrect display

(ID 12269)

If the ***Address Type*** field was set to *Address Range* in the FCI menu ***Firewall ➜ Addresses ➜ Address List ➜ New***, the second value *255.255.255.255* was displayed in the ***Address Range*** field. If the ***Address Type*** field was set to *Address / Subnet* in the menu ***Firewall ➜ Addresses ➜ Address List ➜ New***, no preset value was displayed in the ***Address / Subnet*** field.

The problem has been solved.

4.39 FCI - Media Gateway - Incorrect display

(ID 12356)

The ***Registrar*** field was displayed when ***Trunk Mode*** was set to *Server* in the FCI menu ***VoIP ➜ Media Gateway ➜ SIP Accounts***.

The problem has been solved; the ***Registrar*** field is no longer displayed in the situation described above.

4.40 FCI - Media Gateway - Field status missing

(ID 12245)

The media gateway is switched off by default. Due to the missing ***Media Gateway Status*** field in the FCI menu ***VoIP*** ➜ ***Media Gateway*** ➜ ***Options***, it could not be switched on.

The problem has been solved.

4.41 FCI - ISDN Theft Protection - Wrong selection

(ID 12295)

In the FCI menu ***Local Services*** ➜ ***ISDN Theft Protection*** ➜ ***Options*** menu, the Ethernet interfaces are selected under ***Controlled Interfaces*** when the ***ISDN Theft Protection Service*** is enabled.

The problem has been solved; the Ethernet interfaces cannot be selected under ***Controlled Interfaces***.

4.42 FCI - Maintenance - Irritating message

(ID 11849)

The message “The system must be restarted.” appeared after each completed ***action*** in the FCI menu ***Maintenance*** ➜ ***Software & Configuration***.

The problem has been solved. Different messages are displayed to match the action.

If ***Action*** = *Copy*, *Rename*, *Delete configuration* or *Import configuration* the message “Would you like to reboot now? Changes to boot config will be activated after reboot.” appears.

If ***ACTION*** = *Import Language* or *Delete File* the message “You must log in again to activate changes” appears.

For all other selection options in the ***ACTION*** field, the message “Would you like to reboot now? Changes will be activated after reboot.” appears.

4.43 FCI - Maintenance - No file available

(ID 12137)

In the FCI menu ***MAINTENANCE*** ➜ ***SOFTWARE & CONFIGURATION*** ➜ ***OPTIONS***, no file could be selected in the ***SELECT FILE*** field when ***ACTION*** was set to *Delete configuration*.

The problem has been solved.

4.44 FCI - Incorrect WDS status display

(ID 12176)

No Link was displayed in the FCI menu ***MONITORING*** ➜ ***WLAN*** ➜ ***WDS***, although a normal WDS link (no WDS bridge link) was active and operating.

The problem has been solved.

4.45 FCI/Setup Tool - E-mail Alert for WLAN missing

(ID 11554)

No WLAN could be selected for an e-mail alert both in the FCI as well as in the setup tool. In the FCI, no ***SUBSYSTEM*** *WLAN* was available in the ***EXTERNAL REPORTING*** ➜ ***E-MAIL ALERT*** ➜ ***E-MAIL ALERT RECIPIENT*** menu. In the setup tool menu ***MONITORING AND DEBUGGING*** ➜ ***EMAIL ALERT*** ➜ ***ADD***, no *WLAN* was available under ***SELECT SUBSYSTEMS***.

The problem has been solved.

4.46 Setup Tool - Scheduler - Incorrect interval after change

(ID 12096)

If the field ***SET VALUE ACTIVE*** was set to *1800* rather than *10* in the setup tool menu ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***EVENT SCHEDULER (TIME & SNMP)*** ➜ ***SCHEDULE COMMANDS*** ➜ **ADD**, *10* was used once after saving the change and then *1800*.

The problem has been solved.

4.47 Setup Tool - Port 1 incorrectly set to disabled

(ID 12567)

If the Setup tool menu ***FAST ETHERNET*** ➜ ***SWITCH CONFIGURATION*** was selected and closed with **Save**, port 1 was set to disabled and you could not change this setting.

The problem has been solved.

4.48 Setup Tool - Leased Line - Error when selecting the timeslot

(ID 11323)

If the ***ISDN SWITCH TYPE*** field is set to *leased line, chan. B1..B31* in the setup tool menu ***PRI2-4*** and the field ***BUNDLE TYPE*** is set to *PPP Multilink* under ***PRI2-4*** ➜ ***BUNDLE CONFIGURATION*** ➜ ***ADD***, all timeslots are selected by default even if they are saved with **Save**. When a timeslot, e.g. timeslot 11, was removed from the selection and the cursor was moved to the next timeslot, all timeslots were removed from the selection.

The problem has been solved.

4.49 Setup Tool - IPSec - Tunnel blocked

(ID 12115)

If the fields ***ISDN CALLBACK*** = *both*, ***TRANSFER OWN IP ADDRESS OVER ISDN*** = *yes* and ***MODE*** = *use B channel* were set in the setup tool menu ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND** ➜ ***IPSEC CALLBACK***, problems occurred with callback and in some cases no connection could be established.

The problem has been solved.

4.50 Setup Tool - Problem with SHDSL IMA configuration

(ID 12538)

In the setup tool menu ***SHDSL8*** ➜ **Edit** ➜ ***IPSEC CALLBACK*** the value of the ***MINIMUM NUMBER OF LINKS*** field could not be saved with the setting ***WIRE MODE*** = *4 wire IMA*, *6 wire IMA* or *8 wire IMA* in the ***IMA CONFIGURATION*** menu.

The problem has been solved.

4.51 Incorrect entries in MIB table ipHostAccessClientTable

(ID n/a)

After a reboot, some entries accidentally stay in the MIB table ***IPHOSTACCESSCLIENTTABLE***.

The problem has been solved; the entries are deleted on reboot.