Release Notes

System Software 7.9.5

Version 1.0

Purpose

This document describes new features, changes, and solved problems of **System Software 7.9.5.**

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 5
1.1 Expire Time 5
1.2 Update and Downgrade 6
1.2.1 Preparation and update with the FCI 6
1.2.2 Downgrade with the FCI 7
2 New Functions 9
2.1 FCI - Displaying the system name 10
2.2 FCI - New Assistant VoIP PBX in the LAN 10
2.3 FCI - New standard licence button available 10
2.4 FCI - New ADSL Line Profile field available (R200 series, TR200xw) . . 11
2.5 FCI - GPRS/UMTS (R1200wu, RS120wu) 11
2.6 FCI - Second UMTS interface available (RS120wu) 11
2.7 FCI - Wireless LAN - Access Client added (RS series) 12
2.8 FCI - WLAN Channel Plan (RS series) 12
2.9 FCI - NAT Configuration - New menu 12
2.10 FCI - Quality of Service (QoS) - New menu 18
2.11 FCI - Monitoring QoS - New menu 30
2.12 FCI - Surveillance - New Options 31
2.13 FCI - bintec Router Redundancy Protocol (BRRP) - New menu 31
2.13.1 Terms and Definitions 31
2.13.2 Configuration 33
2.14 FCI - Media Gateway - New SRTP Field 41
2.15 FCI - PBX - New SRTP Field (TR200) 41
2.16 FCI - Certificates 42

3 Changes 43

3.1 Save configuration changed 43

3.2 FCI - Administrative access changed 44

3.3 FCI - Interface Mode changed 44

3.4 FCI - Services adapted 44

3.5 FCI - Buttons removed 44

3.6 FCI - VPN Assistant - Settings adapted 45

3.7 FCI - ***DISPLAY ADMINISTRATIVE ACCESS RULES*** removed 45

3.8 FCI - Media Gateway - Protocol TLS added 45

4 Problems Solved 47

4.1 File transfer failed (RS series) 47

4.2 IPSec - NAT-T faulty 47

4.3 ISDN connection failed 47

4.4 TACACS+ missing (RS series) 48

4.5 Cobion Orange Filter cannot be used 48

4.6 FCI - Log entries displayed incorrectly 48

4.7 FCI - incorrect bridge link quality displayed 49

4.8 FCI - AUX and UMTS menu missing (R1xxx/R3xxx/R4xxx) 49

4.9 FCI - Alert messages displayed 49

4.10 Setup Tool - ***SERIAL CONSOLE*** not visible 50

4.11 Setup Tool - UMTS - Incorrect menu displayed 50

1 Important Information

Please read the following information about System software 7.9.5 carefully to avoid problems when updating or using the software.

1.1 Expire Time

System software 7.9.5 is available only for the following devices and cannot be used on other devices:

- **R230a**, **R230aw**, **R232b**, **R232aw**, **R232bw**,
- **TR200aw**, **TR200bw**,
- **RS120**, **RS120wu**, **RS230a**, **R230aw**, **RS232b**, **RS232bw**,
- **R1200**, **R1200w**, **R1200wu**, **R1200-VoIP**,
- **R1202**, **R3002**, **R3802**, **R4402**,
- **RT1202**, **RT2302**, **RT4202**, **RT4402**,
- **R3000**, **R3000w**, **R3400**, **R3800**,
- **R4100**, **R4300**, **R4100-VoIP**,
- **VPN Access 250**, **VPN Access 1000**,
- **X8500**.

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.

Note

Please note that descriptions concerning the FCI are not valid for the **VPN Access 250**, **VPN Access 1000**, **X8500** devices.

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.

1.2.1 Preparation and update with the FCI

The update of the system software with the Funkwerk Configuration Interface uses a BLUP file (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 an interrupted update operation could be that your gateway does no longer boot. Do not turn your gateway off during the update.

To prepare and carry out an update to **System software 7.9.5** with the **Funkwerk Configuration Interface**, proceed as follows:

1. For the update you will need the file *XXXXX_bl7905.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 before updating.
   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 file* 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 7.9.5** via the ***MAINTENANCE*** ➜ ***SOFTWARE & CONFIGURATION*** menu.
   To do this, select:
   ACTION = *Update system software*
   SOURCE = *Local File*
   FILENAME = *XXXXX_bl7905.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.

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.”
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_bl7901.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.”
   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 7.9.5 includes a number of new functions that significantly extend the performance compared with the previous version of the system software:

- “FCI - Displaying the system name” on page 10
- “FCI - New Assistant VoIP PBX in the LAN” on page 10
- “FCI - New standard licence button available” on page 10
- “FCI - New ADSL Line Profile field available (R200 series, TR200xw)” on page 11
- “FCI - GPRS/UMTS (R1200wu, RS120wu)” on page 11
- “FCI - Second UMTS interface available (RS120wu)” on page 11
- “FCI - Wireless LAN - Access Client added (RS series)” on page 12
- “FCI - WLAN Channel Plan (RS series)” on page 12
- “FCI - NAT Configuration - New menu” on page 12
- “FCI - Quality of Service (QoS) - New menu” on page 18
- “FCI - Monitoring QoS - New menu” on page 30
- “FCI - Surveillance - New Options” on page 31
- “FCI - bintec Router Redundancy Protocol (BRRP) - New menu” on page 31
- “FCI - Media Gateway - New SRTP Field” on page 41
- “FCI - PBX - New SRTP Field (TR200)” on page 41
- “FCI - Certificates” on page 42.

2.1 FCI - Displaying the system name

From System software 7.9.5 the system name is displayed in the FCI top left corner.

The content of the field ***System Name*** that you have configured in the ***System Management*** ➜ ***Global Settings*** ➜ ***System*** menu is displayed on the left-hand side of the FCI underneath the device label, if the setting differs from the device label.

2.2 FCI - New Assistant VoIP PBX in the LAN

The new Assistant *VoIP PBX in LAN* is available from System software 7.9.5.

The Assistant is required to connect a VoIP PBX (telephone system with voice over IP, e.g. **elmeg hybird 300** or **elmeg hybird 600**) to the LAN .

The Assistent helps you with setting up voice prioritisation via QoS (Quality of Service) on your device and to make the required settings in the NAT firewall. External communication is carried out over a single IP address behind which the internal addresses are hidden, and NAT is used as a full-cone NAT version.

Detailed information on this Assistant as well as step-by-step instructions on how to configure it can be found in the Assistant online help section of the corresponding configuration step.

2.3 FCI - New standard licence button available

In order to restore the standard licences, then in the FCI menu *System Management* ➜ *Global Settings* ➜ *System Licences*, the button Default Licences was added.

2.4 FCI - New ADSL Line Profile field available (R200 series, TR200xw)

In the FCI menu *PHYSICAL INTERFACES* ➜ *ADSL MODEM* ➜ *ADSL CONFIGURATION* ➜ *ADVANCED SETTINGS*, the new *ADSL LINE PROFILE* field is available.

You will require the ***ADSL LINE PROFILE*** field for certain ISPs, which you can select here.

2.5 FCI - GPRS/UMTS (R1200wu, RS120wu)

In the FCI menu *PHYSICAL INTERFACES* ➜ *UMTS/HSDPA* ➜ Icon to change an entry, you can select the options *Automatic*, *GPRS only*, *UMTS only*, *GPRS preferred* **or** *UMTS preferred* **in the field *PREFERRED NETWORK TYPE*.**

These options are useful for bad radio reception.

2.6 FCI - Second UMTS interface available (RS120wu)

From System software 7.9.5 a second UMTS interface is available alongside the integrated UMTS/HSDPA modem if a UMTS/HSDPA-USB stick is inserted.

In the ***PHYSICAL INTERFACES*** ➜ ***UMTS/HSDPA*** menu, the available interfaces are displayed: the integrated modem *Slot6 Unit 0 UMTS* and the stick *Slot6 Unit 1 UMTS* (if inserted). You can configure the displayed interfaces here.

If a stick is inserted, the ***INTERNET ACCESS*** Assistant allows selecting between the integrated modem and the stick too.

2.7 FCI - Wireless LAN - Access Client added (RS series)

In the FCI menu *Wireless LAN* ➜ *WLAN* ➜ *Radio Settings* ➜ Icon to change an entry, the *Access Client* option was added in the *Operation Mode* field.

2.8 FCI - WLAN Channel Plan (RS series)

From System software 7.9.5 a so-called channel plan is implemented which makes a preselection when a channel is selected. This ensures that no channels overlap, i.e. a distance of four channels for example is maintained between the channels used. This is useful if more access points are used with overlapping radio cells.

If, in the ***Wireless LAN*** ➜ ***WLAN*** ➜ ***Radio Settings*** ➜ ***Icon to change an entry*** menu, you have set the fields ***Operation Mode*** = *Access Point* and ***Channel*** = *Auto*, you can use the ***Channel Plan*** field under ***Advanced Settings***.

If the setting ***Channel Plan*** = *Auto* is used, then depending on the region, operation band, wireless mode and bandwidth, the channels that have a distance of 4 channels are provided.

If the setting ***Channel Plan*** = *User-defined*, you can select the desired channels yourself.

If the setting ***Channel Plan*** = *All*, you can select from all available channels when choosing a channel.

2.9 FCI - NAT Configuration - New menu

From System software 7.9.5 the new *Routing* ➜ *NAT* ➜ *NAT Configuration* ➜ New menu is available. It replaces the *Routing* ➜ *NAT* ➜ *Portforwardings* ➜ New menu.

The new NAT menu makes it easier to configure and enhances the functionality as well. Alongside converting the addresses and ports, you can now remove data from the NAT in a simple and convenient manner. You can configure various NAT methods. You can determine how an external host establishes a connection to an internal host (refer to RFC 3489).

The ***NAT CONFIGURATION*** ➜ ***BASIC PARAMETERS*** menu consists of the following fields:

Field	Value
Description	Enter a label for the NAT configuration.
Interface	Select the interface for which NAT is to be configured.
Type of traffic	Select the type of data traffic for which NAT is to be configured. Possible values: ■ *incoming (destination NAT)* (default value): The data traffic that comes from outside. ■ *outgoing (source NAT)* : The data traffic that goes outside. ■ *exclusive (without NAT)* : The data traffic that is excluded from NAT.

Field	Value
NAT method	Only for ***TYPE OF TRAFFIC*** = *outgoing (Source NAT)*. Select the NAT method for outgoing data traffic. The starting point for choosing the NAT method is a NAT scenario where an "internal" source host has initialized an IP connection to an "external" destination host over a NAT interface and where an internal valid source address and an internal valid source port are mapped to an external valid source address and an external valid source port. Possible values: ■ *full-cone* (only UDP): Any external host may send IP packets to the initializing source address and the initial source port via external address and external port. ■ *restricted-cone* (only UDP): The same as full-cone NAT; for the external host, however, the initial "external" destination host must be used. ■ *port-restricted-cone* (only UDP): The same as restricted-cone NAT; but only data from the initial destination port are allowed. ■ *symmetric* (default value) (any protocol): In outgoing direction, an external valid source address and an external valid source port are administratively set. In incoming direction, only response packets within the established connection are permitted.

Table 2-1: Fields in the ***NAT CONFIGURATION*** ➜ ***BASIC PARAMETERS*** menu

In the ***NAT CONFIGURATION*** ➜ ***SPECIFY ORIGINAL TRAFFIC*** menu you can configure for which traffic NAT is to be used.

The ***NAT CONFIGURATION*** ➜ ***SPECIFY ORIGINAL TRAFFIC*** menu consists of the following fields:

Field	Value
Service	Not selectable for ***TYPE OF TRAFFIC*** = *outgoing (Source NAT)* and ***NAT METHOD*** = *full-cone*, *restricted-cone* or *port-restricted-cone*. Select one of the preconfigured services. Possible values: *User-defined*, *KaZaA*, *activity*, *any*, *apple-qt*, *auth*, *chargen*, *clients_1*, *clients_2*, *daytime*, *dhcp*, *discard*, *dns*, *echo*, *exec*, *finger*, *ftp*, *gopher*, *http*, *http (SSL)*, *imap*, *imap (SSL)*, *imap3*, *ip-sec*, *ipx*, *irc*, *l2dp*, *ldap*, *ldap (SSL)*, *msp*, *netbios*, *netware-ip*, *nntp*, *nntp (SSL)*, *npp*, *ntp*, *ospf*, *pop2*, *pop3*, *pop3 (SSL)*, *pptp*, *privileged*, *radius-1*, *radius-2*, *rap*, *real audio*, *remote capi*, *remote tapi*, *rip*, *rlogin*, *rpc*, *rsh*, *rtelnet*, *server*, *sftp*, *sip*, *smtp*, *snmp*, *sqlserv*, *ssh*, *sun-rpc*, *syslog*, *t-online (XCEPT)*, *talk*, *telnet*, *telnet, terminal server, tftp, time, timed, trace, unix print, unpriv, ups, uucp-path, who, whois, wins, x400.*
Protocol	For certain services only. Not selectable for ***TYPE OF TRAFFIC*** = *outgoing (Source NAT)* and ***NAT METHOD*** = *full-cone*, *restricted-cone* or *port-restricted-cone; in this case, UDP is selected automatically*. Select a protocol. Possible values for a *user-defined* service: *AH*, *Any*, *Chaos*, *EGP*, *ESP*, *GGP*, *GRE*, *HMP*, *ICMP*, *igmp*, *IGP*, *IGRP*, *IP*, *IPinIP*, *IPv6*, *IPX in IP*, *ISO-IP*, *Kryptolan*, *L2TP*, *OSPF*, *PUP*, *RDP*, *RSVP*, *SKIP*, *TCP*, *TLSP*, *UDP*, *VRRP*, *XNS-IDP*

Field	Value
Source IP Address / Netmask	Enter the source IP address and, if required, the corresponding netmask of the original data packets.
Source Port	Only for ***TYPE OF TRAFFIC*** = *outgoing (source NAT)*, ***NAT METHOD*** = *symmetric* and ***SERVICE*** = *User-defined*. Enter the source port of the original data packets. The default setting *All* means that the port is not specified.
Source Port/rRange	Not selectable for ***TYPE OF TRAFFIC*** = *outgoing (Source NAT)*. Enter the source port or the source port range of the original data packets. The default setting *All* means that the port is not specified.
Destination IP Address / Netmask	Enter the destination IP address and, if required, the corresponding netmask of the original data packets.
Destination Port/Range	Only for ***SERVICE*** = *User-defined*. Enter the destination port or the destination port range of the original data packets. The default setting *All* means that the port is not specified.

Table 2-2: Fields in the ***NAT CONFIGURATION*** ➜ ***SPECIFY ORIGINAL TRAFFIC*** menu

In the ***NAT CONFIGURATION*** ➜ ***REPLACEMENT VALUES*** menu you can define new addresses and ports, depending on whether the traffic is incoming or outgoing, to which specific addresses and ports are translated from the ***NAT CONFIGURATION*** ➜ ***SPECIFY ORIGINAL TRAFFIC*** menu.

The ***NAT CONFIGURATION*** ➜ ***REPLACEMENT VALUES*** menu consists of the following fields:

Field	Value
New destination IP address/netmask	Only for ***TYPE OF TRAFFIC*** = *incoming (Destination NAT)*. Enter the destination IP address and, if required, the corresponding netmask to which the original destination IP address is to be translated.
New destination port	Only for ***TYPE OF TRAFFIC*** = *incoming (Destination NAT)*. Leave the destination port as it appears or enter the destination port to which the original destination port is to be translated. Selecting *Original* leaves the original destination port. If you disable *Original* , an input field appears in which you can enter a new destination port. *Original* is active by default.
Source IP Address / Netmask	Only for ***TYPE OF TRAFFIC*** = *outgoing (Source NAT)* and ***NAT METHOD*** = *symmetric.* Enter the source IP address and, if required, the corresponding netmask to which the original source IP address is to be translated.

Field	Value
New source port	Only for ***TYPE OF TRAFFIC*** = *outgoing (Source NAT)* and ***NAT METHOD*** = *symmetric.* Leave the source port as it appears or enter a new source port to which the original source port is to be translated. Selecting *Original* leaves the original source port. If you disable *Original* , an input field appears in which you can enter a new source q-port. *Original* is active by default.

Table 2-3: Fields in the ***NAT CONFIGURATION*** ➜ ***REPLACEMENT VALUES*** menu

2.10 FCI - Quality of Service (QoS) - New menu

From System software 7.9.5 you can configure Quality of Service within the FCI independently from a SIF (Stateful Inspection Firewall) configuration.

QoS makes it possible to distribute the available bandwidths effectively and intelligently. Certain applications can be given preference and bandwidth reserved for them. This is an advantage, especially for time-critical applications such as VoIP.

The QoS configuration consists of three parts:

- Creating IP filters
- Classifying data
- Prioritising data.

To configure QoS go to the ***ROUTING*** ➜ ***QOS*** menu.

In the ***ROUTING*** ➜ ***QOS*** ➜ ***QOS FILTER*** ➜ **New** menu you can define IP filters.

Fields in the ***QoS Filter*** ➜ ***Basic Parameters*** menu:

Field	Value
Description	Enter the name of the filter.
Protocol	Select a protocol. Possible values: *ah, Chaos, dont-verify, egp, esp, ggp, gre, hmp, icmp, igmp, IGP, igrp, IP, ipip, ipv6, IPX in IP, ISO-IP, Kryptolan, l2tp, ospf, pim, pup, rdp, rsvp, SKIP, tcp, TLSP, udp, VRRP, xns-idp*. The *dont-verify* option (default value) matches any protocol.
Type	Only for ***Protocol*** = *icmp*. Select the type. Possible values: *Any, Echo reply, Destination unreachable, Source quench, Redirect, Echo, Time exceeded, Timestamp, Timestamp reply*. See RFC 792. The default value is *Any* .
Connection State	If ***Protocol*** = *tcp*, you can define a filter that takes the status of the TCP connections into account. Possible values: ■ *Established*: All TCP packets that would not establish any new TCP session on routing over the gateway match the filter. ■ *Any* (default value): The filter is independent from the connection state.
Destination IP Address/Netmask	Enter the destination IP address of the data packets and the corresponding netmask.

Field	Value
Destination Port/Range	Only if ***PROTOCOL*** = *tcp* or *udp* Enter a destination port number or a range of destination port numbers. Possible values: ■ *All* (default value): The destination port is not specified. ■ *Specify port*: Enter a destination port. ■ *Specify port range* : Enter a destination port range.
Source IP Address/Net-mask	Enter the source IP address of the data packets and the corresponding netmask.
Source Port/Range	Only if ***PROTOCOL*** = *tcp* or *udp* Enter a source port number or a range of source port numbers. Possible values: ■ *All* (default value): The destination port is not specified. ■ *Specify port*: Enter a destination port. ■ *Specify Port Range* : Enter a destination port range.

Field	Value
DSCP/TOS filter (Layer 3)	Specify how the priority of the IP packets is signalled. Possible values: ■ *Ignore* (default value): No priority signalling is used. ■ *DSCP Binary Value*: Differentiated Services Code Point is used to signal the priority of IP packets (indicated in binary format; currently not implemented). ■ *DSCP Decimal Value*: Differentiated Services Code Point is used to signal the priority of IP packets (indicated in decimal format; possible values: *0 .. 63* currently not implemented). ■ *TOS Binary Value*: Type of Service is used to signal the priority of IP packets (indicated in binary format). ■ *TOS Decimal Value*: Type of Service is used to signal the priority of IP packets (indicated in decimal format; possible values: *0 .. 255*)
COS filter (802.1p/Layer 2)	Enter the service class of the IP packets (Class of service, COS). Possible values: *0 .. 7*. The default value is *0*.

Table 2-4: Fields in the ***QoS Filter*** ➜ ***Basic Parameters*** menu

The data traffic is classified in the ***Routing*** ➜ ***QoS*** ➜ ***QoS Classification*** ➜ **New** menu, i.e. the data traffic is associated using class IDs of various classes. To do this, create class maps for classifying IP packets based on pre-defined IP filters. Each class map is associated to at least one interface via its first filter.

Fields in the ***QoS Classification*** ➜ ***Basic Parameters*** menu:

Field	Value
Class map	Choose the class map you want to create or edit. Possible values: *New* (default value): You can create a new class map with this setting. <*Name of class map*>: Shows a class map that has already been created, which you can select and edit.
Description	Only if ***class map*** = *New*. Enter the name of the class map.
Filter	Select an IP filter. If the class map is new, select the filter to be set at the first point of the class map. If the class map already exists, select the filter to be attached to the class map. To select a filter, at least one filter must be configured (see page 19).
Direction	Select the direction of the data packets to be classified. Possible values: ■ *Incoming* : Incoming data packets are to be classified. ■ *Outgoing* (default value): Outgoing data packets are to be classified. ■ *Both* : Incoming and outgoing data packets are to be classified.

Field	Value
High Priority Class	Enable or disable the high priority class. If the high priority class is active, the data packets are associated with the class with the highest priority and priority *0* is set automatically. The function is activated with *Enabled*. The function is disabled by default.
Class ID	Only if ***HIGH PRIORITY CLASS*** is inactive. Choose a number which assigns the data packets to a class. Note: The class ID is a label to assign data packets to specific classes. (The class ID defines the priority.) Possible values are whole numbers between *1* and *254*.
Interfaces	Only if ***CLASS MAP*** = *New*. When creating a new class map, select the interfaces to which you want to link the class map. A class map can be assigned to multiple interfaces.

Table 2-5: Fields in the ***QOS CLASSIFICATION*** ➜ ***BASIC PARAMETERS*** menu

You can define the priority in the ***ROUTING*** ➜ ***QOS*** ➜ ***QOS INTERFACES/POLICIES*** ➜ **New** menu.

Hinweis

Data can only be prioritized in the outgoing direction.

Packets in the high-priority class always take priority over data with class IDs 1... 254..

It is possible to assign or guarantee each queue and thus each data class a certain part of the total bandwidth of the interface. In addition, you can optimise the transmission of voice data (real time data).

Depending on the respective interface, a queue is created automatically for each class, but only for data traffic classified as outgoing and for data traffic classified in both directions. A priority is assigned to these automatic queues. The value of the priority is equal to the value of the class ID. You can change the default priority of a queue. If you add new queues, you can also use classes in other class maps via the class IDs.

Configuration is carried out in the ***Routing*** ➜ ***QoS*** ➜ ***QoS Interfaces/Policies*** ➜ **New** menu:

Fields in the menu:***QoS Interfaces/Policies*** ➜ ***Basic Parameters***

Field	Value
Interface	Select the interface for which QoS is to be configured.
Prioritisation algorithm	Select the algorithm according to which the queues are to be processed. This activates and deactivates QoS on the selected interface. Possible values: ■ *Prioritiy Queueing* (default value) QoS is enabled on the interface. The available bandwidth is distributed strictly according to the queue priority. ■ *Weighted Round Robin* QoS is enabled on the interface. The available bandwidth is distributed according to the weighting (weight) of the queue. Exception: High-priority packets are always handled with priority. ■ *Weighted Fair Queueing* QoS is enabled on the interface. The available bandwidth is distributed as “fairly” as possible among the (automatically detected) traffic flows in a queue. Exception: High-priority packets are always handled with priority.

Field	Value
Prioritisation algorithm (Continuation)	■ *Disabled* QoS is disabled on the interface. The existing configuration is not deleted, but can be activated again if required.
Traffic shaping	Activate or deactivate data rate limiting in the send direction. The function is activated with *Enabled*. The function is disabled by default.
Maximum Upload Speed	Only enabled for ***TRAFFIC SHAPING*** . Enter a maximum data rate for the interface in the send direction in kbits. Possible values are *1* to *1000000*. The default value is *0*, i.e. no limits are set, the queue can occupy the maximum bandwidth.
Protocol Header Size below Layer 3	Choose the interface type to include the size of the respective overheads of a datagram when calculating the bandwidth. Possible values: ■ *User-defined* (value in bytes; Possible values *0* to *100*.) ■ *Ethernet (default value)* ■ *Ethernet and VLAN* ■ *PPPoE* ■ *PPPoE and VLAN* ■ *IPSec over Ethernet* ■ *IPSec over Ethernet and VLAN* ■ *IPSec via PPP over Ethernet* ■ *IPSec via PPPoE and VLAN*

Field	Value
Real Time Jitter Control	Only for ***TRAFFIC SHAPING*** *enabled*. Real Time Jitter Control optimises latency when forwarding real time datagrams. The function ensures that large data packets are fragmented according to the available upload bandwidth. Real Time Jitter Control is useful for small upload bandwidths (< 800 kBit/s). Activate or deactivate Real Time Jitter Control. The function is activated with *Enabled*. The function is disabled by default.
Control Mode	Only enabled for ***REAL TIME JITTER CONTROL*** . Select the mode for optimising voice transmission. Possible values: ■ *All RTP Streams*: All RTP are optimised. The function activates the RTP stream detection mechanism for the automatic detection of RTP streams. In this mode, the Real Time Jitter Control is activated as soon as an RTP stream has been detected. ■ *Inactive*:Voice data transmission is not optimised. ■ *Controlled RTP Streams only* (default value): This mode is used if either the VoIP Application Layer Gateway (ALG) or the VoIP Media Gateway (MGW) is active. Real Time Jitter Control is activated by the control instances ALG or MGW. ■ *Always*: Real Time Jitter Control is always active, even if no real time data is routed.

Field	Value
Queues/Policies	Configure the desired QoS queues. For each class created from the class map, which is associated with the selected interface, a queue is generated automatically and displayed here (only for outgoing classified data traffic and for data traffic classified in both directions). Add a new entry with **Add**. The ***EDIT QUEUE/POLICY*** menu opens.

Table 2-6: Fields in the ***QOS INTERFACES/POLICIES*** ➜ ***BASIC PARAMETERS*** menu

Fields in the ***QOS QUEUE*** ➜ ***EDIT QUEUE/POLICY*** menu

Field	Value
Description	Enter the name of the queue/policy.
Outbound interface	Shows the interface for which the QoS queues are being configured.
Priorisation queue	Select the queue priority type. Possible values: ■ *Class-based* (default value): Queue for data classified as “normal”. ■ *High priority*: Queue for data classified as “high priority”. ■ *Default*: Queue for data that has not been classified or data of a class for which no specific queue has been configured.
Class ID	Only if ***PRIORISATION QUEUE*** = *Class-based*. Select the QoS packet class to which this queue is to apply. To do this, at least one class ID must be given (see “Class ID” on page 23).

Field	Value
Priority	Only if ***PRIORITY QUEUE*** = *Class-based*. Choose the priority of the queue. Possible values are *1* to *254*. The default value is *1*.
RTT Mode (Realtime Traffic Mode)	Active or deactivate the real time transmission of the data. The function is activated with *Enabled*. The function is disabled by default. RTT mode should be activated for QoS classes in which real time data has priority. This mode improves latency when forwarding real time datagrams. It is possible to configure multiple queues when RTT mode is enabled. Queues with enabled RTT mode must always have a higher priority than queues with disabled RTT mode.
Traffic Shaping	Activate or deactivate data rate (=Traffic Shaping) limiting in the send direction. The data rate limit applies to the selected queue. (This is not the limit that can be defined on the interface.) The function is activated with *Enabled*. The function is disabled by default.
Maximum Upload Speed	Only enabled for ***TRAFFIC SHAPING***. Enter a maximum data rate for the queue in kbits. Possible values are *0* to *1000000*. The default value is *0*.

Field	Value
Overbooking allowed	Only enabled for ***TRAFFIC SHAPING***. Enable or disable the function. The function controls the bandwidth limit. If ***OVERBOOKING ALLOWS*** is activated, the bandwidth limit set for this queue can be exceeded, as long as free bandwidth exists on the interface. If ***OVERBOOKING ALLOWED*** is deactivated, the queue can never occupy bandwidth beyond the bandwidth limit that has been set. The function is activated with *Enabled*. The function is disabled by default.
Burst size	Only enabled for ***TRAFFIC SHAPING***. Enter the maximum number of bytes that may still be transmitted temporarily when the data rate permitted for this queue has been reached. Possible values are *0* to *64000*. The default value is *0*.

Table 2-7: Fields in the ***EDIT QUEUE/POLICY*** menu

Fields in the menu:***EDIT QUEUE/POLICY*** ➜ ***ADVANCED SETTINGS***:

Field	Value
Dropping Algorithm	Choose the procedure for rejecting packets in the QoS queue, if the maximum size of the queue is exceeded. Possible values: ■ *Tail Drop* (default value): The newest packet received is dropped. ■ *Head Drop*: The oldest packet in the queue is dropped. ■ *Random Drop*: A randomly selected packet is dropped from the queue.
Min. queue size	Enter the minimum size of the queue in bytes. Possible values are *0* to *16384*. The default value is *0*.
Max. queue size	Enter the maximum size of the queue in bytes. Possible values are *0* to *16384*. The default value is *16384*

Table 2-8: Fields in the ***EDIT QUEUE/POLICY*** ➜ ***ADVANCED SETTINGS*** menu

2.11 FCI - Monitoring QoS - New menu

From System software 7.9.5 the new *MONITORING* ➜ *QOS* menu is available.

The new menu enables you to monitor your QoS configuration.

2.12 FCI - Surveillance - New Options

In the FCI menu *Local Services* ➜ *Surveillance* ➜ *Hosts* ➜ New in addition to using *Enable* and *Disable* as interface actions in the Controlled Interfaces field, you can also use *Reset* or *Redial* .

2.13 FCI - bintec Router Redundancy Protocol (BRRP) - New menu

From System software 7.9.5 you can configure the bintec Router Redundancy Protocol (BRRP) with the FCI.

Go to the ***Local Services*** ➜ ***BRRP*** menu. In this menu you can configure the redundancy of your gateway. Whether your device is enabled for BRRP per default or whether you will need a licence to use this feature is apparent from the data sheet for your device which you can access at www.funkwerk-ec.com. For R23x series and RS series devices you will require a licence at additional cost.

BRRP (bintec Router Redundancy Protocol) is a bintec-specific implementation of VRRP (Virtual Router Redundancy Protocol). A router redundancy procedure is used mainly to safeguard the availability of a physical gateway in a LAN or WAN.

2.13.1 Terms and Definitions

A number of special terms are used to describe the functionality.

The following terms are defined in the relevant RFC and in the Internet draft.

Term	Meaning
VRRP Router	“A router that uses the Virtual Router Redundancy Protocol. It can be integrated into one or more “virtual routers”.”

Term	Meaning
Virtual Router	“An abstract object controlled by the VRRP, which is used as default router for the hosts of a LAN. It comprises a Virtual Router Identifier (***ID OF THE VIRTUAL ROUTER***) and an IP address or a group of associated IP addresses in a common LAN. A VRRP router can protect the data traffic of one or more virtual routers.”
IP Address Owner	“The VRRP router that possesses the IP address(es) of the virtual router as real interface address(es). This is the router that – if active - answers packets for ICMP pings, TCP connections, etc. to one of these IP addresses.”
Primary IP Address	“An IP address that is selected from the group of real interface addresses. A possible algorithm option is the selection of the first address. VRRP advertisements are always sent with the primary IP address as source of the IP packet.”
VRRP Advertisement	A keepalive that sends the master to the backup gateway to indicate its reachability.
Virtual Router Master	“The VRRP router that takes over forwarding the packets that have been sent to the IP addresses associated with the “virtual router”. It is also responsible for answering ARP (Address Resolution Protocol) requests for these IP addresses.
Virtual Router Backup	“The group of VRRP routers that take over responsibility for forwarding the packets if the master fails.” In backup status these VRRP routers are inactive, i.e. they do not respond to any ARP requests.

Table 2-9: Terms

2.13.2 Configuration

When using a route redundancy protocol, multiple routers are combined into a logical unit. The router redundancy protocol BRRP manages the routes involved and organises these as follows:

- It ensures that only one routers within the logical connection is active.
- It guarantees that if the active route fails, another router takes over the function of the failed device. The time that each router is active is determined by the priority assigned to the router.

Let us take the example of a simple scenario, in which gateway A provides Internet access for the hosts in a LAN. If this gateway fails, all hosts cannot access the Internet and their routes are configured statically. To allow the hosts continued access to the Internet, gateway B offers all hosts in the LAN the service that gateway A previously performed. All the tasks of a “virtual router” and the switching of services from one gateway to the other are controlled by the BRRP redundancy procedure.

The BRRP conforms to the specifications in RFC 2338 and the relevant Internet draft. (You will find the Internet drafts at http://www.ietf.org/1id-abstracts.html.)

The configuration of the router redundancy procedure is carried out in the following steps:

- Configuration of the interface via which the BRRP advertisement data packets are sent.

Hinweis

This interface is used to transmit the BRRP advertisement data packets and possibly to transmit keepalive monitoring data packets. Another interface must be configured in the next step to transmit the usage data.

The configuration of the advertisement interface is performed in the ***LOCAL SERVICES*** ➜ ***BRRP*** ➜ ***VIRTUAL ROUTERS*** ➜ **New** ➜ ***BRRP ADVERTISEMENT INTERFACE*** menu.

Only the active router in the router group sends advertisement data packets. The IPv4 multicast address 224.0.0.18 is used as the destination address for all routers in the group. All passive routers in the group must mon-

itor this address so that if the advertisement data packets are not received that can react according to their priority and BRRP configuration.

- Configuration of the interface for transmitting usage data (configuration of the virtual interface)
  A virtual interface is enabled and disabled by assigning it to a virtual router over the BRRP router redundancy protocol.
  The configuration is performed in the ***LOCAL SERVICES*** ➜ ***BRRP*** ➜ ***VIRTUAL ROUTER*** ➜ **New** ➜ ***BRRP MONITORED INTERFACE*** menu.
  In this step, you configure the IP address settings and assign the interface to a virtual router. The properties of the virtual router (e.g. the priority) are also defined here

Hinweis

The system automatically assigns the MAC address of the virtual interface according to the following model: *00:00:5E:00:01:<ID of the Virtual Router>*. The ID of the virtual router therefore determines the MAC address of the interface, which is used to transmit the usage data.

Hinweis

The configuration of the virtual interface (MAC address, IP address) and the configuration of the virtual router (priority, sending interval for advertisement, master down trials) must be identical on all routers with the same virtual router ID within the logical group,

Hinweis

You must use different IP addresses for the advertisement interface and for the virtual interface.

Hinweis

All virtual interfaces on a physical router should normally have the same priority.

- Configuration of the synchronisation between the virtual router and configuration of the events, which result in a switching of the operating status of the virtual router.
  Controlling the operating status of a virtual router implicitly also controls the operating status of the interface to which the virtual router is linked. If an error occurs, all interfaces on a device have to be deactivated. Consequently, the operating status of all interfaces on a device must be synchro-

nised. This synchronisation is required if multiple interfaces are monitored on a single device.
This configuration is performed in the ***LOCAL SERVICES*** ➜ ***BRRP*** ➜ ***VR SYNCHRONISATION*** ➜ **New** menu.

- Switching on the redundancy procedure. This configuration is performed in the ***LOCAL SERVICES*** ➜ ***BRRP*** ➜ ***OPTIONS*** menu.

You configure the advertisement interface and the virtual interface(s) in the ***LOCAL SERVICES*** ➜ ***BRRP*** ➜ ***VIRTUAL ROUTERS*** ➜ **New** menu. You must configure the same virtual routers with the same interfaces on all physical routers involved in the redundancy procedure. (However, the virtual routers have different priorities on the various physical routers.)

Fields in the ***VIRTUAL ROUTERS*** ➜ ***BRRP ADVERTISEMENT INTERFACE*** menu:

Field	Value
Ethernet Interface	Choose the interface via which BRRP advertisement packets are sent and expected. If you edit a ***VIRTUAL ROUTER***, the Ethernet interface is displayed and cannot be changed. Note: The Ethernet Interface for sending the advertisements is always *up* and *running* and cannot therefore be used as the ***VIRTUAL ROUTER INTERFACE*** .
IP Address	Shows the IP address(es) of the interface via which BRRP advertisement packets are sent and expected.

Table 2-10: Fields in the ***VIRTUAL ROUTERS*** ➜ ***BRRP ADVERTISEMENT INTERFACE***

Fields in the ***VIRTUAL ROUTERS*** ➜ ***BRRP MONITORED INTERFACE*** menu:

Field	Value
Virtual Router Interface	Indicates on which physical interface the virtual interface is based, if a new virtual interface is created. The name of the virtual interface is assigned automatically when it is created. Shows the name of the virtual interface, if a virtual interface that has already been created is edited.
Virtual Router IP Address	Enter the IP address and the netmask of the virtual router. Here enter the IP address that you want to use in the local network as the actual gateway IP address. Note: The ***IP ADDRESS*** for advertisements and the ***VIRTUAL ROUTER IP ADDRESS*** must be different. These IP addresses can originate from the same network (optional).
Virtual Router ID	Select the ID of the virtual router. This ID identifies the “virtual router” in the LAN and is part of every BRRP advertisement packet that is sent by the current master. Possible values are whole numbers between *1* and *255*.

Field	Value
Virtual Router Priority	Define the logical priority of the virtual router. Possible values are between *1* and *255*. The higher the value, the higher the priority. The value *255* defines that this virtual router always functions as master as soon as it is active. The default value is *100*. The virtual router with the highest priority normally takes over the master role. After a backup scenario, the further master-slave role casting is determined by the parameters ***VIRTUAL ROUTER PRIORITY*** and ***PRE-EMPT MODE (GO BACK INTO MASTER STATE)***.

Table 2-11: Fields in the ***VIRTUAL ROUTERS*** ➜ ***BRRP MONITORED INTERFACE*** menu

Hinweis

In the ***VIRTUAL ROUTERS*** ➜ ***ADVANCED SETTINGS*** menu you must configure all of the parameters for all virtual routers identically on all devices in the group. We recommend leaving the preset values.

Fields in the menu:***VIRTUAL ROUTERS*** ➜ ***ADVANCED SETTINGS***:

Field	Value
Advertisement sen interval	Determine how often a BRRP advertisement packet is sent if the virtual router is defined as master. Only the current master sends via multicast BRRP advertisements, which also contain the ID and the priority of the master. Possible values are whole numbers between *1* and *255*. The value is indicated in seconds and the default value is *1.* An advertisement timer based on the sending interval for advertisements runs in the router and an advertisement packet is sent when the timer expires.

Field	Value
Master down trials	Define the number of BRRP advertisements that must fail before the backup router with the lowest priority assumes that the master is inactive and takes over the role of master. A master down timer based on the ***MASTER DOWN TRIALS*** runs in the router; when this timer expires, the backup assumes that the master is not reachable if no advertisement has been received. The effective master down interval is the time calculated from the number of expected but omitted BRRP advertisements, the advertisement interval and the skew time, which adds a minimum period depending on the priority. The higher the priority, the shorter the time added. Consequently, a backup router with a higher priority responds more quickly than a router with lower priority). Possible values are whole numbers between *1* and *255* and the default value is *10*.

Field	Value
Pre-empt Mode (go back into master state)	Define whether a backup router with higher priority has priority over a master router with low priority. Pre-empt mode is used to prevent unnecessary switching. This means: An active backup router with low priority does not give up its role if the master router becomes reachable again. The function is activated with *Enabled*. The function is enabled by default. Note the following exception: If ***VIRTUAL ROUTER PRIORITY*** *255* is selected, the gateway with this priority takes over the master role in all cases, i.e. the setting in ***PRE-EMPT MODE*** is not considered. You should therefore select a ***VIRTUAL ROUTER PRIORITY*** lower than *255* if you wish to use pre-empt mode.
Enable authentication	Enable or disable authentication. The function is activated with *Enabled*. If the function is active, an input field is displayed. Enter the authentication key here. Note: Note that the authentication key must be the same for all virtual routers in the group The function is disabled by default.

Table 2-12: Fields in the ***VIRTUAL ROUTERS*** ➜ ***ADVANCED SETTINGS*** menu

The watchdog daemon is configured in the ***LOCAL SERVICES*** ➜ ***BRRP*** ➜ ***VR SYNCHRONISATION*** ➜ **New** menu, i.e. you define how state changes are handled.

A list of all synchronisations is displayed when opening the ***LOCAL SERVICES*** ➜ ***BRRP*** ➜ ***VR SYNCHRONISATION*** menu. You can either synchronise virtual routers or interfaces. New synchronisations can be added in the **New** menu.

For example, you can synchronise both virtual routers R1 and R2 over BRRP. To do this, you must create two entries. For the first entry, you must use R1 as the ***MONITORING-VR/INTERFACE*** and R2 as the ***SYNCHRONISATION VR/INTERFACE***.

For the first second, you must configure R2 as the ***MONITORING-VR/INTERFACE*** and R1 as the ***SYNCHRONISATION VR/INTERFACE***.

The ***VR SYNCHRONISATION*** ➜ ***BASIC PARAMETERS*** ➜ ***MONITORING VR/INTERFACE*** menu consists of the following fields:

Field	Value
Monitoring Mode	Select which mechanism should be used for monitoring a virtual router. Possible values: ■ *BRRP* (default value): The BRRP-specific state advertisements are used for determining the state of the master. (The master sends advertisements according to its configuration in the ***VIRTUAL ROUTERS*** ➜ ***ADVANCED SETTINGS*** menu.)
Virtual Router ID	Only for ***MONITORING MODE*** = *BRRP*. Select a virtual router using the ***VIRTUAL ROUTER ID*** and define which interface is to be checked. You can choose previously defined IDs (See “Virtual Router ID” on page 36.). The watchdog daemon requests the detailed information entered in the ***VIRTUAL ROUTERS***.

Table 2-13: Fields in the ***MONITORING VR / INTERFACE*** menu

The ***VR SYNCHRONISATION*** ➜ ***BASIC PARAMETERS*** ➜ ***SYNCHRONISATION VR / INTERFACE*** menu consists of the following fields:

Field	Value
Synchronisation Mode	Determines the mechanism with which virtual routers or interfaces are synchronised: ■ *BRRP* (default value): BRRP is used to synchronise the virtual router.

Field	Value
Virtual Router ID	Only for ***SYNCHRONISATION MODE*** = *BRRP*. Select the ID of the virtual router to be synchronised. Synchronising the virtual router implicitly synchronises the virtual interface associated with the virtual router.

Table 2-14: Fields in the ***SYNCHRONISATION VR / INTERFACE*** menu

You can enable or disable the BRRP function in the ***BRRP*** ➜ ***OPTIONS*** menu.

Fields in the ***OPTIONS*** ➜ ***BASIC PARAMETERS*** menu:

Field	Value
Enable BRRP	Enable or disable the BRRP function. The function is activated with *Enabled*. The function is disabled by default.

Table 2-15: Fields in the ***OPTIONS*** menu

2.14 FCI - Media Gateway - New SRTP Field

In the FCI menu *VOIP* ➜ *MEDIA GATEWAY* ➜ *EXTENSIONS* ➜ New ➜ Advanced Settings you can enable or disable the new option *SRTP* (Secure Real-Time Transport Protocol) in the *SORT ORDER* field.

2.15 FCI - PBX - New SRTP Field (TR200)

In the FCI menus *PBX* ➜ *LINE CONFIGURATION* ➜ *VOIP CONFIGURATION* ➜ New ➜ *ADVANCED SETTINGS* and *PBX* ➜ *INTERNAL NUMBERS* ➜ *VOIP* ➜ Button to change an entry ➜ *ADVANCED SETTINGS* the field *SRTP* (Secure Real-Time Transport Protocol) was added.

You can switch SRTP on and off via the new field SRTP is not active by default. Active SRTP require separate telephones for implementing external ISDN according to internal SIP.

2.16 FCI - Certificates

The FCI menu *VPN* ➜ *CERTIFICATES* was moved to follow after *SYSTEM MANAGEMENT* ➜ *CERTIFICATES* . The new menu is used for the management of a general certificate list for all services.

If certificates are available, you can select and use certificates in the following menus:

- ***PBX*** ➜ ***INTERNAL NUMBERS*** ➜ ***VOIP*** (**TR200aw** /**TR200bw**)
- ***VPN*** ➜ ***IPSEC*** ➜ ***PHASE-1 PROFILES*** ➜ **New** with ***AUTHENTICATION METHOD*** = *DSA Signature*, *RSA Signature* or *RSA Encryption*
- ***LOCAL SERVICES*** ➜ ***HTTPS***.

In the ***SYSTEM MANAGEMENT*** ➜ ***CERTIFICATES*** menu the status *Will soon expire* was added to the certificate list.

3 Changes

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

- "Save configuration changed" on page 43
- "FCI - Administrative access changed" on page 44
- "FCI - Interface Mode changed" on page 44
- "FCI - Services adapted" on page 44
- "FCI - Buttons removed" on page 44
- "FCI - VPN Assistant - Settings adapted" on page 45
- "FCI - Display administrative access rules removed" on page 45
- "FCI - Media Gateway - Protocol TLS added" on page 45.

3.1 Save configuration changed

If you save a current configuration, you can save this as the boot configuration or you can also archive the previous boot configuration as a backup.

If you click the **Save configuration** button in the FCI, you will be asked "Do you really want to save the current configuration as a boot configuration?"

You have the following two options:

- ***SAVE CONFIGURATION***, i.e. save the current configuration as the boot configuration
- ***SAVE CONFIGURATION WITH BOOT BACKUP***, i.e. save the current configuration as the boot configuration and also archive the previous boot configuration as a backup in the flash memory of the router.

If you want to load the archived boot configuration into your device, go to ***MAINTENANCE*** ➜ ***SOFTWARE & CONFIGURATION*** and select ***ACTION*** = *Restore*

Backup. The archived backup is used as the current boot configuration. The option *Restore Backup* is available, if a backup was saved.

3.2 FCI - Administrative access changed

Up to this point the FCI menu ***System Management*** ➜ ***Administrative Access*** ➜ ***Access*** is based on SIF rules. From **System software 7.9.5** this menu is based on the Local Services Access Control subsystem and is independent from SIF. This means that any changes in the ***System Management*** ➜ ***Administrative Access*** ➜ ***Access*** menu no longer automatically create SIF rules and are displayed in the ***Firewall*** ➜ ***Policies*** ➜ ***Filter Rules*** menu.

3.3 FCI - Interface Mode changed

In the FCI menu ***LAN*** ➜ ***IP Configuration*** ➜ ***Interfaces*** ➜ ***Icon to change an entry / New*** the labeling of options in the ***Interface Mode*** field was changed to *Untagged* and *Tagged (VLAN)* .

3.4 FCI - Services adapted

In the FCI menu ***Routing*** ➜ ***NAT*** ➜ ***NAT Configuration*** ➜ **New** then with **System software 7.9.5** the same services are made available as in the Firewall Configuration.

3.5 FCI - Buttons removed

In the FCI menu ***Routing*** ➜ ***Load Balancing*** ➜ ***Load Balancing Groups*** ➜ **New** the **Back** button was removed.

3.6 FCI - VPN Assistant - Settings adapted

In order to ensure that the VPN Assistant for PPTP dial-in can also be used with Windows versions that are newer than Windows XP Service Pack 1, then the standard field settings ***GRE Window Adaption*** and ***GRE Window Size*** in the FCI menu ***VPN*** ➜ ***PPTP*** ➜ ***Options*** were changed.

3.7 FCI - *Display administrative access rules* removed

In the FCI menu ***Firewall*** ➜ ***Policies*** ➜ ***Filter Rules*** the checkbox ***Display administrative access rules*** was removed.

3.8 FCI - Media Gateway - Protocol TLS added

In the FCI menu ***VoIP*** ➜ ***Media Gateway*** ➜ ***Extensions*** ➜ **New**, and in the ***Protocol*** field, *TLS* was added as a new option.

4 Problems Solved

Not all devices listed in chapter “Important Information” on page 5 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 7.9.5

4.1 File transfer failed (RS series)

(ID 13405)

For large files, it was possible that a file transfer (e.g. FTP) via an IPSec tunnel could have failed for large files.

The problem has been solved.

4.2 IPSec - NAT-T faulty

(ID 13786)

For IPSec connections it could happen, irrespective of the use of NAT-T, that the NAT session was ended prematurely.

The problem has been solved.

4.3 ISDN connection failed

(ID 13487)

No ISDN connection could be made with the ADSL logic 2.4.6.3.0.2

The problem has been solved.

4.4 TACACS+ missing (RS series)

(ID 13573)

An option for authentication with TACACS+ was not supported.

The problem is resolved.

4.5 Cobion Orange Filter cannot be used

(ID 13854)

Cobion Orange Filter could not be enabled because the default servers entered were no longer accessible.

The problem is resolved; the entries were adjusted.

4.6 FCI - Log entries displayed incorrectly

(ID 13477)

If a value was set in the ***Maximum Message Level of Syslog Entries*** field in the FCI menu ***System Management*** ➜ ***Global Settings*** ➜ ***System***, then the filter was not used, and in the ***Monitoring*** ➜ ***Internal Log*** all of the entries were displayed.

The problem has been solved.

4.7 FCI - incorrect bridge link quality displayed

(ID 13335)

For 802.11n connections the bridge link quality was incorrectly displayed because it was determined on the basis of the signal-to-noise ratio and was not based on the actual signal.

The problem has been solved.

4.8 FCI - AUX and UMTS menu missing (R1xxx/R3xxx/R4xxx)

(ID n/a)

The FCI menus ***Physical Interfaces*** ➜ ***AUX*** and ***Physical Interfaces*** ➜ ***UMTS/HSDPA*** were missing.

The problem has been solved.

4.9 FCI - Alert messages displayed

(ID n/a)

When selecting the FCI menu ***Physical Interfaces*** ➜ ***UMTS*** / ***HSDPA*** it may have happened that alert messages were displayed.

The problem has been solved.

4.10 Setup Tool - *SERIAL CONSOLE* not visible

(ID 13158)

If, when in the Setup Tool menu ***SERIAL: CONSOLE*** ➜ **Edit**, the value *Console* in *AUX* was changed and then the change itself was amended, then the menu item ***SERIAL: CONSOLE*** will have disappeared.

The problem has been solved.

4.11 Setup Tool - UMTS - Incorrect menu displayed

(ID n/a)

In the Setup Tool menu ***UMTS*** the title of the main menu was overwritten by the title of the submenu.

The problem has been solved.