funkwerk
enterprise communications

Release Notes
Systemsoftware 7.9.5

Version 1.0

Ziel und Zweck

Dieses Dokument beschreibt neue Funktionen, Änderungen und behobene Fehler in **Systemsoftware 7.9.5**.

Haftung

Der Inhalt dieses Dokuments wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Dokument gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Dokument können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Änderungen finden Sie unter www.funkwerk-ec.com.

Als Multiprotokoll-Gateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EC

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.funkwerk-ec.com.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
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 Wichtige Informationen

Bitte lesen Sie die folgenden Informationen zu Systemsoftware 7.9.5 aufmerksam, um Probleme beim Update oder bei der Verwendung der Software zu vermeiden.

1.1 Gültigkeit

Systemsoftware 7.9.5 steht ausschließlich für folgende Geräte zur Verfügung und kann auf anderen Geräten nicht eingesetzt werden:

- **R230a, R230aw, R232b, R232aw, R232bw,**
- **TR200aw, TR200bw,**
- **RS120**, **RS120wu**, **RS230a**, **RS230aw**, **RS232b**, **RS232bw**,
- **R1200, R1200w, R1200wu, R1200-VoIP,**
- **R1202**, **R3002**, **R3802**, **R4402**,
- **RT1202**, **RT3002**, **RT4202**, **RT4402**,
- **R3000, R3000w, R3400, R3800,**
- **R4100, R4300, R4100-VoIP**
- **VPN Access 250, VPN Access 1000,**
- **X8500.**

Hinweis

Beachten Sie, dass eine Neuerung, Änderung oder die Lösung eines Problems auf Ihrem Gerät nur dann zur Verfügung steht, wenn das beschriebene Menü angezeigt wird.

Hinweis

Beachten Sie, dass Beschreibungen, die das FCI betreffen, nicht für die Geräte **VPN Access 250, VPN Access 1000** und **X8500** gültig sind.

1.2 Update und Downgrade

Beachten Sie die folgenden Hinweise zum Update und zu den Möglichkeiten eines Downgrades.

Sie können ein Update oder ein Downgrade mit dem **Funkwerk Configuration Interface** (FCI) durchführen oder - falls gewünscht - auch mit der SNMP Shell.

1.2.1 Vorbereitung und Update mit dem FCI

Das Update der Systemsoftware mit dem Funkwerk Configuration Interface erfogt mit einer BLUP-Datei (Bintec Large Update), um alle notwendigen Module intelligent zu aktualisieren. Dabei werden alle diejenigen Elemente aktualisiert, die im BLUP neuer sind als auf Ihrem Gateway.

Achtung!

Die Folge eines unterbrochenen Update-Vorgangs könnte sein, dass Ihr Gateway nicht mehr bootet. Schalten Sie Ihr Gateway deshalb nicht aus, während das Update durchgeführt wird.

Gehen Sie ggf. folgendermaßen vor, um mit dem **Funkwerk Configuration Interface** ein Update auf **Systemsoftware 7.9.5** vorzubereiten und durchzuführen:

1. Für das Update benötigen Sie die Datei *XXXXX_bl7905.xxx*, wobei *XXXXX* für Ihr Geät steht.
   Stellen Sie sicher, dass die Datei, welche Sie für das Update benötigen, auf Ihrem PC verfügbar ist.
   Wenn die Datei nicht auf Ihrem PC verfügbar ist, geben Sie www.funkwerk-ec.com in Ihren Browser ein.
   Die Funkwerk-Homepage öffnet sich. Im Download-Bereich Ihres Gateways finden Sie die benötigte Datei. Speichern Sie sie auf Ihrem PC.
2. Sichern Sie die aktuelle Boot-Konfiguration vor dem Update.
   Exportieren Sie die aktuelle Boot-Konfiguration über das Menü ***Wartung*** ➜ ***Software & Konfiguration*** des **Funkwerk Configuration Interface**. Wählen Sie dazu:

AKTION = *Konfiguration exportieren*
AKTUELLER DATEINAME IM FLASH = *boot*
ZERTIFIKATE UND SCHLÜSSEL EINSCHLIEßEN = aktiviert
VERSCHLÜSSELUNG DER KONFIGURATION = deaktiviert
Bestätigen Sie mit **Los**. Das Fenster *Öffnen von <Name des Gateways>.cf* öffnet sich. Belassen Sie die Auswahl *Datei speichern* und klicken Sie auf **OK**, um die Konfiguration auf Ihrem PC zu speichern.
Die Datei *<Name des Gateways.cf>* wird gespeichert, das Fenster *Downloads* zeigt die gespeicherte Datei.

3. Führen Sie das Update auf **Systemsoftware 7.9.5** über das Menü ***WARTUNG*** ➜ ***SOFTWARE & KONFIGURATION*** durch.
   Wählen Sie dazu:
   AKTION = *Systemsoftware aktualisieren*
   QUELLE = *Lokale Datei*
   DATEINAME = *XXXXX_bl7905.xxx*
   Bestätigen Sie mit **Los**.
   Die Meldung "System Anfrage. Bitte warten. Ihre Anfrage wird bearbeitet." bzw. "System Maintenance. Please stand by. Operation in progress." zeigt, dass die gewählte Datei in das Gerät geladen wird. Wenn der Ladevorgang beendet ist, sehen Sie die Meldung "System - Maintenance. Sucess. Operation completed successfully."
   Klicken Sie auf **Reboot**.
   Sie sehen die Meldung "System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds." Das Gerät startet mit der neuen Systemsoftware, das Browser-Fenster öffnet sich.

Sie können sich an Ihrem Gerät anmelden und es konfigurieren.

1.2.2 Downgrade mit dem FCI

Wenn Sie ein Downgrade durchführen wollen, gehen Sie folgendermaßen vor:

1. Ersetzen Sie die aktuelle Boot-Konfiguration durch die zuvor gesicherte.
   Importieren Sie die gesicherte Boot-Konfiguration über das Menü ***WARTUNG*** ➜ ***SOFTWARE & KONFIGURATION***.
   Wählen Sie dazu:
   AKTION = *Konfiguration importieren*

VERSCHLÜSSELUNG DER KONFIGURATION = deaktiviert
DATEINAME = *<Name des Geräts>.cf*
Bestätigen Sie mit **Los**. Die Meldung "System Anfrage. Bitte warten. Ihre Anfrage wird bearbeitet." bzw. "System Maintenance. Please stand by. Operation in progress." zeigt, dass die gewählte Konfiguration in das Gerät geladen wird. Wenn der Ladevorgang beendet ist, sehen Sie die Meldung "System - Maintenance. Sucess. Operation completed successfully."
Klicken Sie auf **Reboot**.
Sie sehen die Meldung "System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds." Das Gerät startet, das Browser-Fenster öffnet sich. Melden Sie sich an Ihrem Gerät an.

2. Führen Sie das Downgrade auf die gewünschte Softwareversion über das Menü ***WARTUNG*** ➜ ***SOFTWARE & KONFIGURATION*** durch.
   Wählen Sie dazu:
   AKTION = *Systemsoftware aktualisieren*
   QUELLE = *Lokale Datei*
   DATEINAME = *R3000_bl7901.r3d* (Beispiel)
   Bestätigen Sie mit **Los**.
   Die Meldung "System Anfrage. Bitte warten. Ihre Anfrage wird bearbeitet." bzw. "System Maintenance. Please stand by. Operation in progress." zeigt, dass die gewählte Systemsoftware in das Gerät geladen wird. Wenn der Ladevorgang beendet ist, sehen Sie die Meldung "System - Maintenance. Sucess. Operation completed successfully."
   Klicken Sie auf **Reboot**.
   Sie sehen die Meldung "System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds." Das Gerät startet mit der zuvor gesicherten Boot-Konfiguration und der älteren Version der Systemsoftware. Das Browser-Fenster öffnet sich.

Sie können sich an Ihrem Gerät anmelden und es konfigurieren.

2 Neue Funktionen

Systemsoftware 7.9.5 enthält eine Reihe neuer Funktionen, die den Leistungsumfang gegenüber der letzten Version der Systemsoftware erheblich erweitern:

2.1 FCI - Anzeige des Systemnamens

Ab Systemsoftware 7.9.5 wird der Systemname im FCI oben links angezeigt.

Der Inhalt des Feldes ***SYSTEMNAME***, den Sie im Menü ***SYSTEMVERWALTUNG*** ➜ ***GLOBALE EINSTELLUNGEN*** ➜ ***SYSTEM*** konfiguriert haben, wird im FCI links oben unter der Gerätebezeichnung angezeigt, sofern Ihre Eingabe von der Gerätebezeichnung abweicht.

2.2 FCI - Neuer Assistent VoIP PBX im LAN

Ab Systemsoftware 7.9.5 steht der neue Assistent *VOIP PBX IM LAN* zur Verfügung.

Der Assistent wird für die Anbindung einer VoIP PBX (Telefonanlage mit Voice over IP, z. B. **elmeg hybird 300 oder elmeg hybird 600**) im LAN benötigt.

Der Assistent hilft Ihnen dabei, auf Ihrem Gerät Sprachpriorisierung über QoS (Quality of Service) einzurichten und in der NAT Firewall entsprechende Einstellungen vorzunehmen. Die Kommunikation nach außen erfolgt über eine einzige IP-Adresse, hinter der die internen Adressen verborgen sind; NAT wird in der Variante full-cone NAT verwendet.

Detaillierte Informationen zu diesem Assistenten sowie Schritt-für-Schritt-Anleitungen zur Konfiguration finden Sie in der Online-Hilfe zum Assistenten im entsprechenden Konfigurationsschritt.

2.3 FCI - Neue Schaltfläche Standardlizenzen verfügbar

Um Standardlizenzen wiederherstellen zu können, wurde im FCI Menü *SYSTEMVERWALTUNG* ➜ *GLOBALE EINSTELLUNGEN* ➜ *SYSTEMLIZENZEN* die Schaltfläche Stdrd. Lizenzen (Standardlizenzen) hinzugefügt.

2.4 FCI - Neues Feld ADSL-Leitungsprofil verfügbar (R200-Serie, TR200xw)

Im FCI Menü *PHYSIKALISCHE SCHNITTSTELLEN* ➜ *ADSL-MODEM* ➜ *ADSL-KONFIGURATION* ➜ *ERWEITERTE EINSTELLUNGEN* ist das neue Feld *ADSL-LEITUNGSPROFIL* verfügbar.

Das Feld ***ADSL-LEITUNGSPROFIL*** benötigen Sie für bestimmte Internet-Service-Provider, die hier ausgewählt werden können.

2.5 FCI - GPRS/UMTS (R1200wu, RS120wu)

Im FCI Menü *PHYSIKALISCHE SCHNITTSTELLEN* ➜ *UMTS/HSDPA* ➜ Symbol zur Änderung eines Eintrags können Sie im Feld *BEVORZUGTER NETZWERKTYP* die Optionen *Automatisch*, *Nur GPRS*, *Nur UMTS*, *Bevorzugt GPRS* **oder** *Bevorzugt UMTS* **wählen.**

Diese Optionen sind bei ungünstigen Standorten nützlich.

2.6 FCI - Zweite UMTS-Schnittstelle verfügbar (RS120wu)

Ab Systemsoftware 7.9.5 ist neben dem integrierten UMTS/HSDPA-Modem eine zweite UMTS-Schnittstelle verfügbar, wenn ein UMTS/HSDPA-USB-Stick gesteckt ist.

Im Menü ***PHYSIKALISCHE SCHNITTSTELLEN*** ➜ ***UMTS/HSDPA*** werden die verfügbaren Schnittstellen angezeigt: das integrierte Modem *Slot6 Unit 0 UMTS* und der Stick *Slot6 Unit 1 UMTS* (wenn gesteckt). Sie können die angezeigten Schnittstellen hier konfigurieren.

Im Assistenten ***INTERNETZUGANG*** können Sie bei der Konfiguration ebenfalls zwischen dem integrierten Modem und dem Stick wählen, wenn der Stick gesteckt ist.

2.7 FCI - Wireless LAN - Access Client hinzugefügt (RS-Serie)

Im FCI Menü *WIRELESS LAN* ➜ *WLAN* ➜ *EINSTELLUNGEN FUNKMODUL* ➜ Symbol zur Änderung eines Eintrags wurde im Feld *BETRIEBSMODUS* die Auswahlmöglichkeit *Access Client* **hinzugefügt.**

2.8 FCI - WLAN Kanalplan (RS-Serie)

Ab Systemsoftware 7.9.5 ist ein sogenannter Kanalplan implementiert, der bei der Kanalwahl eine Vorauswahl trifft. Dadurch wird sichergestellt, dass sich keine Kanäle überlappen, d.h. dass zwischen den verwendeten Kanälen ein Abstand von z. B. vier Kanälen eingehalten wird. Dies ist nützlich, wenn mehrere Access Points eingesetzt werden, deren Funkzellen sich überlappen.

Wenn Sie im Menü ***WIRELESS LAN*** ➜ ***WLAN*** ➜ ***EINSTELLUNGEN FUNKMODUL*** ➜ ***SYMBOL ZUR ÄNDERUNG EINES EINTRAGS*** die Felder ***BETRIEBSMODUS*** = *Access-Point* und ***KANAL*** = *Auto* gesetzt haben, können Sie unter ***ERWEITERTE EINSTELLUNGEN*** das Feld ***KANALPLAN*** nutzen.

Mit der Einstellung ***KANALPLAN*** = *Auto* werden abhängig von der Region, vom Frequenzband, vom drahtlosen Modus und von der Bandbreite diejenigen Kanäle zur Verfügung gestellt, die vier Kanäle Abstand haben.

Mit der Einstellung ***KANALPLAN*** = *Benutzerdefiniert* können Sie die gewünschten Kanäle selbst auswählen.

Mit der Einstellung ***KANALPLAN*** = *Alle* können bei der Kanalwahl alle Kanäle gewählt werden.

2.9 FCI - NAT-Konfiguration - Neues Menü

Ab Systemsoftware 7.9.5 ist das neue Menü *ROUTING* ➜ *NAT* ➜ *NAT-KONFIGURATION* ➜ Neu verfügbar. Es ersetzt das Menü *ROUTING* ➜ *NAT* ➜ *PORTWEITERLEITUNG* ➜ Neu.

Das neue NAT-Menü vereinfacht die Konfiguration und erweitert die Funktionalität. Neben dem Umsetzen von Adressen und Ports können Sie jetzt einfach und komfortabel Daten von NAT ausnehmen. Sie können verschiedene NAT-Methoden konfigurieren. Sie können unter anderem festlegen, wie ein externer Host eine Verbindung zu einem internen Host herstellen darf (siehe RFC 3489).

Das Menü ***NAT-KONFIGURATION*** ➜ ***BASISPARAMETER*** besteht aus folgenden Feldern:

Feld	Wert
Beschreibung	Geben Sie eine Bezeichnung für die NAT-Konfiguration ein.
Schnittstelle	Wählen Sie die Schnittstelle, für die NAT konfiguriert werden soll.
Art des Datenverkehrs	Wählen Sie, für welche Art von Datenverkehr NAT konfiguriert werden soll. Mögliche Werte: ■ *eingehend (Ziel-NAT)* (Standardwert): Der Datenverkehr, der von außen kommt. ■ *ausgehend (Quell-NAT)*: Der Datenverkehr, der nach außen geht. ■ *exklusiv (ohne NAT)*: Der Datenverkehr, der von NAT ausgenommen ist.

Feld	Wert
NAT-Methode	Nur für ***ART DES DATENVERKEHRS*** = *ausgehend (Quell-NAT)*. Wählen Sie die NAT-Methode für ausgehenden Datenverkehr. Ausgangspunkt für die Wahl der NAT-Methode ist ein NAT-Szenario, bei dem ein "interner" Quell-Host über die NAT-Schnittstelle eine IP-Verbindung zu einem "externen" Ziel-Host initiiert hat und bei der eine intern gültige Quelladresse und ein intern gültiger Quellport auf eine extern gültige Quelladresse und einen extern gültigen Quellport umgesetzt werden. Mögliche Werte: ■ *full-cone* (nur UDP): Jeder beliebige externe Host darf IP-Pakete über die externe Adresse und den externen Port an die initiierende Quelladresse und den initialen Quellport senden. ■ *restricted-cone* (nur UDP): Wie full-cone NAT; als externer Host ist jedoch ausschließlich der initiale "externe" Ziel-Host zugelassen. ■ *port-restricted-cone* (nur UDP): Wie restricted-cone NAT; es sind jedoch ausschließlich Daten vom initialen Ziel-Port zugelassen.

Feld	Wert
NAT-Methode (Fortsetzung	■ *symmetrisch* (Standardwert) (beliebiges Protokoll): In ausgehender Richtung werden eine extern gültige Quelladresse und ein extern gültiger Quell-Port administrativ festgelegt. In eingehender Richtung sind nur Antwortpakete innerhalb der bestehenden Verbindung zugelassen.

Tabelle 2-1: Felder im Menü ***NAT-KONFIGURATION*** ➜ ***BASISPARAMETER***

Im Menü ***NAT-KONFIGURATION*** ➜ ***URSPRÜNGLICHEN DATENVERKEHR ANGEBEN*** können Sie konfigurieren, für welchen Datenverkehr NAT verwendet werden soll.

Das Menü ***NAT-KONFIGURATION*** ➜ ***URSPRÜNGLICHEN DATENVERKEHR ANGEBEN*** besteht aus folgenden Feldern:

Feld	Wert
Dienst	Nicht einstellbar für ***ART DES DATENVERKEHRS*** = *ausgehend (Quell-NAT)* und ***NAT-METHODE*** = *full-cone*, *restricted-cone* oder *port-restricted-cone*. Wählen Sie einen der vorkonfigurierten Dienste aus. Mögliche Werte: *Benutzerdefiniert*, *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.*

Feld	Wert
Protokoll	Nur für bestimmte Dienste. Nicht einstellbar für ***ART DES DATENVERKEHRS*** = *ausgehend (Quell-NAT)* und ***NAT-METHODE*** = *full-cone*, *restricted-cone* oder *port-restricted-cone*; in diesem Fall wird UDP automatisch festgelegt) Wählen Sie ein Protokoll aus. Mögliche Werte für die Einstellung *Benutzerdefiniert*: *AH*, *Beliebig*, *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*
Quell-IP-Adresse/Netzmaske	Geben Sie die Quell-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.
Quellport	Nur für ***ART DES DATENVERKEHRS*** = *ausgehend (Quell-NAT)*, ***NAT-METHODE*** = *symmetrisch* und ***DIENST*** = *Benutzerdefiniert*. Geben Sie den Quellport der ursprünglichen Datenpakete ein. Die Standardeinstellung *Alle* bedeutet, dass der Port nicht näher spezifiziert ist.
Quell-Port/Bereich	Nicht für ***ART DES DATENVERKEHRS*** = *ausgehend (Quell-NAT)*. Geben Sie den Quellport bzw. den Quellportbereich der ursprünglichen Datenpakete ein. Die Standardeinstellung *Alle* bedeutet, dass der Port nicht näher spezifiziert ist.
Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.

Feld	Wert
Ziel-Port/Bereich	Nur für ***DIENST*** = *Benutzerdefiniert*. Geben Sie den Ziel-Port bzw. den Ziel-Port-Bereich der ursprünglichen Datenpakete ein. Die Standardeinstellung *Alle* bedeutet, dass der Port nicht näher spezifiziert ist.

Tabelle 2-2: Felder im Menü ***NAT-KONFIGURATION*** ➜ ***URSPRÜNGLICHEN DATENVERKEHR ANGEBEN***

Im Menü ***NAT-KONFIGURATION*** ➜ ***SUBSTITUTIONSWERTE*** können Sie, abhängig davon, ob es sich um eingehenden oder ausgehenden Datenverkehr handelt, neue Adressen und Ports definieren, auf welche bestimmte Adressen und Ports aus dem Menü ***NAT-KONFIGURATION*** ➜ ***URSPRÜNGLICHEN DATENVERKEHR ANGEBEN*** umgesetzt werden.

Das Menü ***NAT-KONFIGURATION*** ➜ ***SUBSTITUTIONSWERTE*** besteht aus folgenden Feldern:

Feld	Wert
Neue Ziel-IP-Adresse/Netzmaske	Nur für ***ART DES DATENVERKEHRS*** = *eingehend (Ziel-NAT)*. Geben Sie diejenige Ziel-IP-Adresse ein, auf welche die ursprüngliche Ziel-IP-Adresse umgesetzt werden soll, gegebenenfalls mit zugehöriger Netzmaske.
Neuer Ziel-Port	Nur für ***ART DES DATENVERKEHRS*** = *eingehend (Ziel-NAT)*. Belassen Sie den Ziel-Port oder geben Sie denjenigen Ziel-Port ein, auf den der ursprüngliche Ziel-Port umgesetzt werden soll. Mit Auswahl von *Original* belassen Sie den ursprünglichen Ziel-Port. Wenn Sie *Original* deaktivieren, erscheint ein Eingabefeld und Sie können einen neuen Ziel-Port eingeben. Standardmäßig ist *Original* aktiv.

Feld	Wert
Quell-IP-Adresse/Netz-maske	Nur für ***ART DES DATENVERKEHRS*** = *ausgehend (Quell-NAT)* und ***NAT-METHODE*** = *symmetrisch*. Geben Sie diejenige Quell-IP-Adresse ein, auf welche die ursprüngliche Quell-IP-Adresse umgesetzt werden soll, gegebenenfalls mit zugehöriger Netzmaske.
Neuer Quell-Port	Nur für ***ART DES DATENVERKEHRS*** = *ausgehend (Quell-NAT)* und ***NAT-METHODE*** = *symmetrisch*. Belassen Sie den Quell-Port oder geben Sie einen neuen Quell-Port ein, auf den der ursprüngliche Quell-Port umgesetzt werden soll. Mit Auswahl von *Original* belassen Sie den ursprünglichen Quell-Port. Wenn Sie *Original* deaktivieren, erscheint ein Eingabefeld und Sie können einen neuen Quell-Port eingeben. Standardmäßig ist *Original* aktiv.

Tabelle 2-3: Felder im Menü ***NAT-KONFIGURATION*** → ***SUBSTITUTIONSWERTE***

2.10 FCI - Quality of Service (QoS) - Neues Menü

Ab Systemsoftware 7.9.5 können Sie Quality of Service mit dem FCI unabhängig von der SIF (Stateful Inspection Firewall) konfigurieren.

QoS ermöglicht es, verfügbare Bandbreiten effektiv und intelligent zu verteilen. Bestimmte Anwendungen können bevorzugt behandelt und Bandbreite für diese reserviert werden. Vor allem für zeitkritische Anwendungen wie z. B. Voice over IP ist das von Vorteil.

Die QoS-Konfiguration besteht aus drei Teilen:

- IP-Filter anlegen

- Daten klassifizieren
- Daten priorisieren.

Gehen Sie zur Konfiguration von QoS in das Menü ***Routing*** ➜ ***QoS.***

Im Menü ***Routing*** ➜ ***QoS*** ➜ ***QoS-Filter*** ➜ **Neu** können Sie IP-Filter definieren.

Felder im Menü ***QoS-Filter*** ➜ ***Basisparameter***:

Feld	Wert
Beschreibung	Geben Sie die Bezeichnung des Filters an.
Protokoll	Wählen Sie ein Protokoll aus. Mögliche Werte: *12tp, ah, Chaos, egp, esp, ggp, gre, hmp, icmp, igmp, IGP, igrp, IP, ipip, ipv6, IPX in IP, ISO-IP, Kryptolan, nicht überprüfen, ospf, pim, pup, rdp, rsvp, SKIP, tcp, TLSP, udp, VRRP, xns-idp*. Die Option *nicht überprüfen* (Standardwert) passt auf jedes Protokoll.
Typ	Nur für ***Protokoll*** = *icmp*. Wählen Sie einen Typ aus. Mögliche Werte: *Any, Echo reply, Destination unreachable, Source quench, Redirect, Echo, Time exceeded, Timestamp, Timestamp reply*. Siehe RFC 792. Standardwert ist *Any*.

Feld	Wert
Verbindungsstatus	Bei ***PROTOKOLL*** = *tcp* können Sie ein Filter definieren, das den Status von TCP-Verbindungen berücksichtigt. Mögliche Werte: ■ *Hergestellt*: Das Filter erfasst diejenigen TCP-Pakete, die keine neue TCP Session etablieren würden. ■ *Beliebig* (Standardwert): Das Filter ist unabhängig vom Verbindungsstatus.
Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	Nur für ***PROTOKOLL*** = *tcp* oder *udp* Geben Sie eine Zielport-Nummer bzw. einen Bereich von Zielport-Nummern ein. Mögliche Werte: ■ *Alle* (Standardwert): Der Zielport ist nicht näher spezifiziert. ■ *Port* angeben: Geben Sie einen Zielport ein. ■ *Portbereich angeben*: Geben Sie einen Zielport-Bereich ein.
Quell-IP-Adresse/Netzmaske	Geben Sie die Quell-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.

Feld	Wert
Quell-Port/Bereich	Nur für ***PROTOKOLL*** = *tcp* oder *udp* Geben Sie eine Quellport-Nummer bzw. einen Bereich von Quellport-Nummern ein. Mögliche Werte: ■ *Alle* (Standardwert): Der Zielport ist nicht näher spezifiziert. ■ *Port* angeben: Geben Sie einen Zielport ein. ■ *Portbereich angeben*: Geben Sie einen Zielport-Bereich ein.

Feld	Wert
DSCP/TOS-Filter (Layer 3)	Wählen Sie, wie die Priorität der IP-Pakete signalisiert ist. Mögliche Werte: ■ *Nicht beachten* (Standardwert): Es wird keine Signalisierung der Priorität verwendet. ■ *DSCP-Binärwert*: Differentiated Services Code Point wird zur Signalierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format; aktuell noch nicht implementiert). ■ *DSCP-Dezimalwert*: Differentiated Services Code Point wird zur Signalierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format; Wertebereich *0 .. 63*; aktuell noch nicht implementiert). ■ *TOS-Binärwert*: Type of Service wird zur Signalierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format). ■ *TOS-Dezimalwert*: Type of Service wird zur Signalierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format, Wertebereich *0 .. 255*)
COS-Filter (802.1p/Layer 2)	Tragen Sie die Serviceklasse der IP-Pakete ein (Class of Service, COS). Wertebereich: *0 .. 7*. Der Standardwert ist *0*.

Tabelle 2-4: Felder im Menü ***QoS-Filter*** ➜ ***Basisparameter***

Im Menü ***Routing*** ➜ ***QoS*** ➜ ***QoS-Klassifizierung*** ➜ **Neu** wird der Datenverkehr klassifiziert, d.h. der Datenverkehr wird mittels Klassen-IDs verschiedenen

Klassen zugeordnet. Sie erstellen dazu Klassenpläne zur Klassifizierung von IP-Paketen anhand zuvor definierter IP-Filter. Jeder Klassenplan wird über sein erstes Filter mindestens einer Schnittstelle zugeordnet.

Felder im Menü ***QoS-Klassifizierung*** ➜ ***Basisparameter***:

Feld	Wert
Klassenplan	Wählen Sie den Klassenplan, den Sie anlegen oder bearbeiten wollen. Mögliche Werte: *Neu* (Standardwert): Mit dieser Einstellung legen Sie einen neuen Klassenplan an. <*Name des Klassenplans*>: Zeigt einen bereits angelegten Klassenplan, den Sie auswählen und bearbeiten können.
Beschreibung	Nur für ***Klassenplan*** = *Neu*. Geben Sie die Bezeichnung des Klassenplans ein.
Filter	Wählen Sie ein IP-Filter aus. Bei einem neuen Klassenplan wählen Sie das Filter, das an die erste Stelle des Klassenplans gesetzt werden soll. Bei einem bestehenden Klassenplan wählen Sie das Filter, das an den Klassenplan angehängt werden soll. Um ein Filter auswählen zu können, muss mindestens ein Filter konfiguriert sein (siehe Seite 20).

Feld	Wert
Richtung	Wählen Sie die Richtung der Datenpakete, die klassifiziert werden sollen. Mögliche Werte: ■ *Eingehend*: Eingehende Datenpakete sollen klassifiziert werden. ■ *Ausgehend* (Standardwert): Ausgehende Datenpakete sollen klassifiziert werden. ■ *Beide*: Eingehende und ausgehende Datenpakete sollen klassifiziert werden.
High-Priority-Klasse	Aktivieren oder deaktivieren Sie die High-Priority-Klasse. Wenn die High-Priority-Klasse aktiv ist, werden die Datenpakete der Klasse mit der höchsten Priorität zugeordnet, die Priorität *0* wird automatisch gesetzt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Klassen-ID	Nur für ***HIGH-PRIORITY-KLASSE*** nicht aktiv. Wählen Sie eine Zahl, welche die Datenpakete einer Klasse zuweist. Hinweis: Die Klassen-ID ist eine Kennziffer, um Datenpakete bestimmten Klassen zuzuordnen. (Die Klassen-ID legt keine Priorität fest.) Mögliche Werte sind ganze Zahlen zwischen *1* und *254*.
Schnittstellen	Nur für ***KLASSENPLAN*** = *Neu*. Wählen Sie beim Anlegen eines neuen Klassenplans diejenigen Schnittstellen, an die Sie den Klassenplan binden wollen. Ein Klassenplan kann mehreren Schnittstellen zugeordnet werden.

Tabelle 2-5: Felder im Menü ***QOS-KLASSIFIZIERUNG*** ➜ ***BASISPARAMETER***

Im Menü ***Routing*** ➜ ***QoS*** ➜ ***QoS-Schnittstellen/Richtlinien*** ➜ **Neu** legen Sie die Priorisierung der Daten fest.

Hinweis

Daten können nur ausgehend priorisiert werden.

Pakete der High-Priority-Klasse haben immer Vorrang vor Daten mit Klassen-ID 1 .. 254..

Es ist möglich, jeder Queue und somit jeder Datenklasse einen bestimmten Anteil an der Gesamtbandbreite der Schnittstelle zuzuweisen bzw. zu garantieren. Darüber hinaus können Sie die Übertragung von Sprachdaten (Real-Time-Daten) optimieren.

Abhängig von der jeweiligen Schnittstelle wird für jede Klasse automatisch eine Queue (Warteschlange) angelegt, jedoch nur für ausgehend klassifizierten Datenverkehr sowie für in beide Richtungen klassifizierten Datenverkehr. Den automatisch angelegten Queues wird hierbei eine Priorität zugeordnet. Der Wert der Priorität ist dabei gleich dem Wert der Klassen-ID. Sie können diese standardmäßig gesetzte Priorität einer Queue ändern. Wenn Sie neue Queues hinzufügen, können Sie über die Klassen-ID auch Klassen anderer Klassenpläne verwenden.

Die Konfiguration erfolgt im Menü ***Routing*** ➜ ***QoS*** ➜ ***QoS-Schnittstellen/Richtlinien*** ➜ **Neu**:

Felder im Menü:***QoS-Schnittstellen/Richtlinien*** ➜ ***Basisparameter***

Feld	Wert
Schnittstelle	Wählen Sie die Schnittstelle aus, für die QoS konfiguriert werden soll.

Feld	Wert
Priorisierungsalgorithmus	Wählen Sie den Algorithmus aus, nach dem die Abarbeitung der Queues erfolgen soll. Sie aktivieren bzw. deaktivieren damit QoS auf der ausgewählten Schnittstelle. Mögliche Werte: ■ *Prioritiy Queueing* (Standardwert) QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird streng gemäß der Priorität der Queues verteilt. ■ *Weighted Round Robin* QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird gemäß der Gewichtung (weight) der Queues verteilt. Ausnahme: High-Priority-Pakete werden immer vorrangig behandelt. ■ *Weighted Fair Queueing* QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird möglichst "fair" unter den (automatisch erkannten) Datenverbindungen (Traffic-Flows) innerhalb einer Queue aufgeteilt. Ausnahme: High-Priority-Pakete werden immer vorrangig bedient. ■ *Deaktiviert* QoS wird auf der Schnittstelle deaktiviert. Die ggf. vorhandene Konfiguration wird nicht gelöscht und kann bei Bedarf wieder aktiviert werden.
Traffic Shaping	Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate in Senderichtung. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Wert
Maximale Upload-Geschwindigkeit	Nur für ***TRAFFIC SHAPING*** *aktiviert.* Geben Sie für die Schnittstelle eine maximale Datenrate in kBits pro Sekunde in Senderichtung ein. Mögliche Werte sind *1* bis *1000000*. Der Standardwert ist *0*, d.h. es erfolgt keine Begrenzung, die Queue kann die maximale Bandbreite belegen.
Größe des Protokoll-Headers unterhalb Layer 3	Wählen Sie den Schnittstellentyp, um die Größe des jeweiligen Overheads eines Datagramms in die Berechnung der Bandbreite einzubeziehen. Mögliche Werte: ■ *Benutzerdefiniert* (Wert in Byte; Mögliche Werte sind *0* bis *100*.) ■ *Ethernet (Standardwert)* ■ *Ethernet und VLAN* ■ *PPPoE* ■ *PPPoE und VLAN* ■ *IPSec über Ethernet* ■ *IPSec über Ethernet und VLAN* ■ *IPSec via PPP over Ethernet* ■ *IPSec via PPPoE and VLAN*

Feld	Wert
Real Time Jitter Control	Nur für ***TRAFFIC SHAPING*** *aktiviert*. Real Time Jitter Control führt zu einer Optimierung des Latenzverhaltens bei der Weiterleitung von Real-Time-Datagrammen. Die Funktion sorgt für eine Fragmentierung großer Datenpakete in Abhängigkeit von der verfügbaren Upload-Bandbreite. Real Time Jitter Control ist nützlich bei geringen Upload-Bandbreiten (< 800 kBit/s). Aktivieren oder deaktivieren Sie Real Time Jitter Control. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Wert
Kontrollmodus	Nur für ***REAL TIME JITTER CONTROL*** *aktiviert*. Wählen Sie den Modus für die Optimierung der Sprachübertragung. Mögliche Werte: ■ *Alle RTP-Streams*: Alle RTP-Streams werden optimiert. Die Funktion aktiviert den RTP-Stream-Detection-Mechanismus zum automatischen Erkennen von RTP-Streams. In diesem Modus wird der Real-Time-Jitter-Control-Mechanismus aktiv, sobald ein RTP-Stream erkannt wurde. ■ *Inaktiv*:Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt. ■ *Nur kontrollierte RTP-Streams* (Standardwert): Dieser Modus wird verwendet, wenn entweder das VoIP Application Layer Gateway (ALG) oder das VoIP Media Gateway (MGW) aktiv ist. Die Aktivierung des Real-Time-Jitter-Control-Mechanismus erfolgt über die Kontrollinstanzen ALG oder MGW. ■ *Immer*: Der Real-Time-Jitter-Control-Mechanismus ist immer aktiv, auch wenn keine Real-Time-Daten geroutet werden.

Feld	Wert
Queues/Richtlinien	Konfigurieren Sie die gewünschten QoS-Queues. Für jede angelegte Klasse aus dem Klassenplan, die mit der gewählten Schnittstelle verbunden ist, wird automatisch eine Queue erzeugt und hier angezeigt (nur für ausgehend klassifizierten Datenverkehr sowie für in beide Richtungen klassifizierten Datenverkehr). Fügen Sie mit **Hinzufügen** neue Einträge hinzu. Das Menü ***QUEUE/RICHTLINIE BEARBEITEN*** öffnet sich.

Tabelle 2-6: Felder im Menü ***QOS SCHNITTSTELLEN/RICHTLINIEN*** ➜ ***BASISPARAMETER***

Felder im Menü ***QOS QUEUES*** ➜ ***QUEUE/RICHTLINIE BEARBEITEN***

Feld	Wert
Beschreibung	Geben Sie die Bezeichnung der Queue/Richtlinie an.
Ausgehende Schnittstelle	Zeigt die Schnittstelle an, für die QoS-Queues konfiguriert werden.
Priorisierungs-Queue	Wählen Sie den Typ für die Priorisierung der Queue aus. Mögliche Werte: ■ *Klassenbasiert* (Standardwert): Queue für "normal"-klassifizierte Daten. ■ *Hohe Priorität*: Queue für "high-priority"-klassifizierte Daten. ■ *Standard*: Queue für Daten, die nicht klassifiziert wurden bzw. für deren Klasse keine eigene Queue angelegt worden ist.

Feld	Wert
Klassen-ID	Nur für ***PRIORISIERUNGS-QUEUE*** = *Klassenbasiert*. Wählen Sie die QoS-Paketklasse, für die diese Queue gelten soll. Dazu muss vorher mindestens eine Klassen-ID vergeben worden sein (siehe “Klassen-ID” auf Seite 25).
Priorität	Nur für ***PRIORISIERUNGS-QUEUE*** = *Klassenbasiert*. Wählen Sie die Piorität der Queue. Mögliche Werte sind *1* bis *254*. Der Standardwert ist *1*.
RTT-Modus (Realtime-Traffic-Modus)	Aktivieren oder deaktivieren Sie die Echtzeitübertragung der Daten. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Der RTT- Modus sollte für QoS-Klassen aktiviert werden, in denen Realtime-Daten priorisiert werden. Dieser Modus führt zu einer Verbesserung des Latenzverhaltens bei der Weiterleitung von Realtime-Datagrammen. Es ist möglich, mehrere Queues mit aktiviertem RTT-Modus zu konfigurieren. Queues mit aktiviertem RTT-Modus müssen immer eine höhere Priorität als Queues mit inaktivem RTT-Modus haben.

Feld	Wert
Traffic Shaping	Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate (=Traffic Shaping) in Senderichtung. Die Begrenzung der Datenrate gilt für die gewählte Queue. (Es handelt sich dabei nicht um die Begrenzung, die an der Schnittstelle festgelegt werden kann.) Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Maximale Upload-Geschwindigkeit	Nur für ***TRAFIC SHAPING*** aktiviert. Geben Sie eine maximale Datenrate in kBit pro Sekunde für die Queue ein. Mögliche Werte sind *0* bis *1000000*. Der Standardwert ist *0*.
Überbuchen zugelassen	Nur für ***TRAFIC SHAPING*** aktiviert. Aktivieren oder deaktivieren Sie die Funktion. Die Funktion steuert das Bandbreitenbegrenzungsverhalten. Bei aktiviertem ***ÜBERBUCHEN ZUGELASSEN*** kann die Bandbreitenbegrenzung überschritten werden, die für die Queue eingestellt ist, sofern freie Bandbreite auf der Schnittstelle vorhanden ist. Bei deaktiviertem ***ÜBERBUCHEN ZUGELASSEN*** kann die Queue niemals Bandbreite über die eingestellte Bandbreitenbegrenzung hinaus belegen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Wert
Burst-Größe	Nur für ***TRAFIC SHAPING*** aktiviert. Geben Sie die maximale Anzahl von Bytes ein, die kurzfristig noch übertragen werden darf, wenn die für diese Queue erlaubte Datenrate bereits erreicht ist. Mögliche Werte sind *0* bis *64000*. Der Standardwert ist *0*.

Tabelle 2-7: Felder im Menü ***QUEUE/RICHTLINIE BEARBEITEN***

Felder im Menü:***QUEUE/RICHTLINIE BEARBEITEN*** ➜ ***ERWEITERTE EINSTELLUNGEN***:

Feld	Wert
Dropping-Algorithmus	Wählen Sie das Verfahren, nach dem Pakete in der QoS-Queue verworfen werden, wenn die maximale Größe der Queue überschritten wird. Mögliche Werte: ■ *Tail Drop* (Standardwert): Das neu hinzugekommene Paket wird verworfen. ■ *Head Drop*: Das älteste Paket in der Queue wird verworfen. ■ *Random Drop*: Ein zufällig ausgewähltes Paket aus der Queue wird verworfen.
Min. Queue-Größe	Geben Sie die minimale Größe der Queue in Byte ein. Mögliche Werte sind *0* bis *16384*. Der Standardwert ist *0*.

Feld	Wert
Max. Queue-Größe	Geben Sie die maximale Größe der Queue in Byte ein. Mögliche Werte sind *0* bis *16384*. Der Standardwert ist *16384*

Tabelle 2-8: Felder im Menü ***Queue/Richtlinie bearbeiten*** ➜ ***Erweiterte Einstellungen***

2.11 FCI - Monitoring QoS - Neues Menu

Ab Systemsoftware 7.9.5 ist das neue Menü *Monitoring* ➜ *QoS* verfügbar.

Das neue Menü ermöglicht Ihnen, Ihre QoS-Konfiguration zu überwachen.

2.12 FCI - Überwachung - Neue Wahlmöglichkeiten

Im FCI Menü *Lokale Dienste* ➜ *Überwachung* ➜ *Hosts* ➜ Neu können Sie im Feld *Regulierte Schnittstellen* als Schnittstellenaktion ab sofort zusätzlich zu *Aktivieren* **und** *Deaktivieren* **auch** *Zurücksetzen* **oder** *Erneut wählen* **verwenden.**

2.13 FCI - bintec Router Redundancy Protocol (BRRP) - Neues Menü

Ab Systemsoftware 7.9.5 können Sie das bintec Router Redundancy Protocol (BRRP) mit dem FCI konfigurieren.

Gehen Sie in das Menü ***Lokale Dienste*** ➜ ***BRRP.*** In diesem Menü können Sie eine Redundanz für Ihr Gateway konfigurieren. Ob Ihr Gerät im Auslieferungs-

zustand über diese Funktion verfügt oder ob für die Nutzung dieser Funktion eine Lizenz erworben werden muss, erfahren Sie auf dem Datenblatt zu Ihrem Gerät, das Sie unter www.funkwerk-ec.com abrufen können. Für Geräte der R23x-Serie und der RS-Serie benötigen Sie eine kostenpflichtige Lizenz.

BRRP (Bintec Router Redundancy Protocol) ist eine bintec-spezifische Implementierung des VRRP (Virtual Router Redundancy Protocol). Ein Router-Redundanzverfahren dient hauptsächlich dazu, die Verfügbarkeit eines physikalischen Gateways im LAN oder WAN sicherzustellen.

2.13.1 Begriffe und Definitionen

Zur Beschreibung der Funktionalität werden einige spezielle Begriffe verwendet.

Folgende Begriffe werden im entsprechenden RFC und im Internet-Entwurf definiert.

Begriff	Bedeutung
VRRP-Router	"Ein Router, der das Virtual Router Redundancy Protocol benutzt. Er kann in einen oder in mehrere "virtuelle Router" integriert sein."
Virtueller Router	"Ein abstraktes, von VRRP gesteuertes Objekt, das als Standard-Router für Hosts eines LAN verwendet wird. Es besteht aus einem Virtual Router Identifier (***ID DES VIRTUELLEN ROUTERS***) und einer IP-Adresse bzw. einer Gruppe zugehöriger IP-Adressen innerhalb eines gemeinsamen LAN. Ein VRRP-Router kann den Datenverkehr eines einzelnen virtuellen Routers oder mehrerer virtueller Router absichern."
IP Address Owner	"Der VRRP-Router, der die IP-Adresse(n) des virtuellen Routers als echte Schnittstellen-Adresse(n) besitzt. Es handelt sich um den Router, der, wenn er aktiv ist, auf Pakete für ICMP-Pings, TCP-Verbindungen etc. an eine dieser IP-Adressen antwortet."

Begriff	Bedeutung
Primary IP Address	"Eine IP-Adresse, die aus der Gruppe der echten Schnittstellenadressen gewählt wird. Eine mögliche Algorithmusoption ist die Auswahl der ersten Adresse. VRRP Advertisements werden immer mit der Primary IP-Adresse als Quelle des IP-Pakets verschickt."
VRRP Advertisement	Ein Keepalive, das der Master zu den Backup-Gateways schickt, um seine Erreichbarkeit zu signalisieren.
Virtual Router Master	"Der VRRP-Router, der das Weiterleiten der Pakete übernimmt, die an die mit dem "virtuellen Router" verbundenen IP-Adressen geschickt wurden, und der für die Beantwortung von ARP (Address Resolution Protocol) Requests an diese IP-Adressen zuständig ist.
Virtual Router Backup	"Die Gruppe der VRRP-Router, welche die Verantwortung für das Weiterleiten übernehmen, falls der Master ausfallen sollte." Im Backup-Status sind diese VRRP-Router inaktiv, d.h. beantworten keine ARP-Requests.

Tabelle 2-9: Begriffe

2.13.2 Konfiguration

Bei der Verwendung eines Router-Redundanzprotokolls werden mehrere Router zu einer logischen Einheit zusammengefasst. Das Router-Redundanzprotokoll BRRP verwaltet die beteiligten Router und organisiert im einzelnen Folgendes:

- Es stellt sicher, dass jeweils nur ein Router innerhalb des logischen Verbunds aktiv ist.

- Es gewährleistet, dass bei Ausfall des aktiven Routers ein anderer Router die Funktion des ausgefallenen Geräts übernimmt. Wann welcher Router aktiv ist, wird über eine dem Router zugeordnete Priorität bestimmt.

Nehmen wir als Beispiel ein einfaches Szenario, in dem Gateway A den Internetzugang der Hosts in einem LAN ermöglicht. Wenn dieses Gateway ausfällt, haben alle Hosts keinen Zugang zum Internet, deren Routen statisch konfiguriert sind. Um den Hosts weiterhin Zugang zum Internet zu ermöglichen, bietet Gateway B allen Hosts im LAN den Dienst an, den vorher Gateway A durchgeführt hat. Alle Aufgaben eines virtuellen Routers und das Umschalten von Diensten von einem Gateway auf das andere werden von dem BRRP-Redundanzprotokoll gesteuert.

Das BRRP folgt den Spezifikationen in RFC 2338 und dem entsprechenden Internet-Entwurf. (Die Internet-Entwürfe finden Sie unter http://www.ietf.org/1id-abstracts.html.)

Die Konfiguration des Router-Redundanzverfahrens wird in folgenden Schritten durchgeführt:

- Konfiguration der Schnittstelle, über welche die BRRP-Advertisement-Datenpakete geschickt werden.

Hinweis

Diese Schnittstelle wird zur Übertragung der BRRP-Advertisement-Datenpakete sowie eventuell zur Übertragung von Keepalive-Monitoing-Datenpaketen verwendet. Zur Übertragung der Nutzdaten muss eine andere Schnittstelle im nächsten Schritt konfiguriert werden.

Die Konfiguration der Advertisement-Schnittstelle wird im Menü ***Lokale Dienste*** ➜ ***BRRP*** ➜ ***Virtuelle Router*** ➜ **Neu** ➜ ***Advertisement-Schnittstelle*** vorgenommen.
Nur der aktive Router des Routerverbunds sendet Advertisement-Datenpakete. Die IPv4-Multicast-Adresse 224.0.0.18 dient als Zieladresse für alle Router, die Bestandteil des Routerverbundes sind. Alle passiven Router des Verbundes müssen diese Adresse überwachen, damit sie bei Ausbleiben der Advertisement-Datenpakete entsprechend ihrer Priorität und der sonstigen BRRP-Konfiguration reagieren können.

- Konfiguration der Schnittstelle zur Übertragung von Nutzdaten (Konfiguration der virtuellen Schnittstelle)
  Eine virtuelle Schnittstelle wird über die Zuweisung zu einem virtuellen

Router über das BRRP-Router-Redundanzprotokoll aktiviert bzw. deaktiviert.

Die Konfiguration wird im Menü ***LOKALE DIENSTE*** ➜ ***BRRP*** ➜ ***VIRTUELLE ROUTER*** ➜ **Neu** ➜ ***BRRP-SCHNITTSTELLE*** vorgenommen.

In diesem Schritt konfigurieren Sie die IP-Adresseinstellungen und ordnen die Schnittstelle einem virtuellen Router zu. Darüber hinaus werden die Eigenschaften des virtuellen Routers (z. B. die Priorität) festgelegt

Hinweis

Das System vergibt die MAC-Adresse der virtuellen Schnittstelle nach folgendem Schema automatisch: *00:00:5E:00:01:<ID des virtuellen Routers>*. Die ID des virtuellen Routers bestimmt somit die MAC-Adresse der Schnittstelle, die zur Übertragung der Nutzdaten verwendet wird.

Hinweis

Die Konfiguration der virtuellen Schnittstelle (MAC-Adresse, IP-Adresse) sowie die Konfiguration des virtuellen Routers (Priorität, Sendeintervall für Advertisements, Master down trials) muss innerhalb des logischen Verbundes auf allen Routern mit derselbenVirtual Router ID identisch sein,

Hinweis

Sie müssen unterschiedliche IP-Adressen für die Advertisement-Schnittstelle und für die virtuelle Schnittstelle verwenden.

Hinweis

Alle virtuellen Schnittstellen auf einem physikalischen Router sollten normalerweise dieselbe Priorität haben.

- Konfiguration der Synchronisation zwischen den virtuellen Routern, sowie Konfiguration der Ereignisse, die zu einem Umschalten des Betriebszustandes der virtuellen Router führen.

  Über die Steuerung des Betriebszustandes eines virtuellen Routers wird implizit auch der Betriebszustand der Schnittstelle gesteuert, die mit dem virtuellen Router verknüpft ist. Da im Fehlerfall alle Schnittstellen eines Geräts deaktiviert werden müssen, muss der Betriebszustand aller Schnittstellen eines Geräts synchronisiert werden. Die Synchronisation ist notwendig, wenn mehrere Schnittstellen auf einem Gerät überwacht werden.

  Diese Konfiguration wird im Menü ***LOKALE DIENSTE*** ➜ ***BRRP*** ➜ ***VR-SYNCHRONISATION*** ➜ **Neu** vorgenommen.

- Einschalten des Redundanzverfahrens. Diese Konfiguration wird im Menü ***LOKALE DIENSTE ➜ BRRP ➜ OPTIONEN*** vorgenommen.

Im Menü ***LOKALE DIENSTE ➜ BRRP ➜ VIRTUELLE ROUTER ➜ Neu*** konfigurieren Sie die Advertisement-Schnittstelle und die virtuelle(n) Schnittstelle(n). Sie müssen auf allen physikalischen Routern, die am Redundanzverfahren teilnehmen, dieselben virtuellen Router mit denselben Schnittstellen konfigurieren. (Die virtuellen Router haben jedoch auf den verschiedenen physikalischen Routern unterschiedliche Priorität.)

Felder im Menü ***VIRTUELLE ROUTER ➜ BRRP-ADVERTISEMENT-SCHNITTSTELLE***:

Feld	Wert
Ethernet-Schnittstelle	Wählen Sie die Schnittstelle aus, über die BRRP-Advertisement-Pakete versendet und erwartet werden. Wenn Sie einen ***VIRTUELLEN ROUTER*** bearbeiten, wird die Ethernet-Schnittstelle angezeigt und kann nicht verändert werden. Hinweis: Die Ethernet-Schnittstelle zur Versendung der Advertisements ist immer *up* and *running* und kann daher nicht als ***SCHNITTSTELLE DES VIRTUELLEN ROUTERS*** verwendet werden.
IP-Adresse	Zeigt die IP-Adresse(n) der Schnittstelle an, über die BRRP-Advertisement-Pakete versendet und erwartet werden.

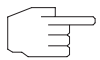
Tabelle 2-10: Felder im Menü ***VIRTUELLE ROUTER ➜ BRRP-ADVERTISEMENT-SCHNITTSTELLE***

Felder im Menü ***VIRTUELLE ROUTER ➜ BRRP ÜBERWACHTE SCHNITTSTELLE***:

Feld	Wert
Schnittstelle des virtuellen Routers	Zeigt an, auf welcher physikalischen Schnittstelle die virtuelle Schnittstelle basiert, wenn eine neue virtuelle Schnittstelle angelegt wird. Die Bezeichnung der virtuellen Schnittstelle wird beim Anlegen automatisch vergeben. Zeigt die Bezeichnung der virtuellen Schnittstelle an, wenn eine bereits angelegte virtuelle Schnittstelle bearbeitet wird.
IP-Adresse des virtuellen Routers	Geben Sie die IP-Adresse und die Netzmaske des virtuellen Routers ein. Hier geben Sie die IP-Adresse ein, die Sie im lokalen Netz als eigentliche Gateway-IP-Adresse verwenden wollen. Hinweis: Die ***IP-ADRESSE*** für Advertisements und die ***IP-ADRESSE DES VIRTUELLEN ROUTERS*** müssen unterschiedlich sein. Diese IP-Adressen dürfen aus demselben Netz stammen, sie müssen aber nicht.
ID des virtuellen Routers	Wählen Sie die ID des virtuellen Routers. Diese ID identifiziert den "virtuellen Router" innerhalb des LAN und ist Bestandteil jedes BRRP-Advertisement-Pakets, das vom aktuellen Master gesendet wird. Mögliche Werte sind ganze Zahlen zwischen *1* und *255*.

Feld	Wert
Priorität des virtuellen Routers	Legen Sie die logische Priorität des virtuellen Routers fest. Die möglichen Werte liegen zwischen *1* und *255*. Je höher der Wert, desto höher die Priorität. Der Wert *255* bestimmt, dass dieser virtuelle Router immer als Master fungiert, sobald er aktiv ist. Standardwert ist *100*. Normalerweise übernimmt der virtuelle Router mit der höchsten Priorität die Masterrolle. Nach Eintreten eines Backup-Falles wird die weitere Rollenverteilung Master-Slave von den Parametern ***Priorität des virtuellen Routers*** und ***Pre-empt-modus (zurück in master-status)*** bestimmt.

Tabelle 2-11: Felder im Menü ***Virtuelle Router*** ➜ ***BRRP Überwachte Schnittstelle***



Hinweis

Im Menü ***Virtuelle Router*** ➜ ***Erweiterte Einstellungen*** müssen Sie alle Parameter für alle virtuellen Router auf allen Geräten, die am Routerverbund teilnehmen, identisch konfigurieren. Wir empfehlen Ihnen, die Voreinstellungen zu belassen.

Felder im Menü:***Virtuelle Router ➜ Erweiterte Einstellungen***:

Feld	Wert
Sendeintervall für Advertisements	Legen Sie fest, wie oft ein BRRP-Advertisement-Paket gesendet wird, wenn der virtuelle Router als Master definiert ist. Nur der aktuelle Master sendet über Multicast BRRP-Advertisements, welche auch die ID und die Priorität des Masters enthalten. Mögliche Werte sind ganze Zahlen zwischen *1* und *255*. Der Wert wird in Sekunden angegeben, Standardwert ist *1.* Basierend auf diesem Sendeintervall für Advertisements läuft routerintern ein Advertisement Timer, nach dessen Ablauf ein Advertisement-Paket gesendet wird.

Feld	Wert
Master down trials	Legen Sie die Anzahl von BRRP Advertisements fest, die fehlschlagen darf, bevor der Backup Router mit der jeweils niedrigeren Priorität annimmt, dass der Master inaktiv ist und es die Rolle des Masters übernimmt. Basierend auf dem Parameter ***MASTER DOWN TRIALS*** läuft routerintern ein Master Down Timer, nach dessen Ablauf vom Backup Router angenommen wird, dass der Master nicht erreichbar ist, falls kein Advertisment empfangen wurde. Das effektive Master Down Intervall entspricht der Zeit errechnet aus der Anzahl erwarteter, aber ausgelassener BRRP Advertisements, dem Advertisement Interval und der sogenannten Skew Time, welche einen minimalen Zeitraum abhängig von der Priorität hinzufügt. Je höher die Priorität, desto kürzer ist die hinzugefügte Zeit, so dass ein Backup-Router mit höherer Priorität früher reagiert als einer mit niedrigerer Priorität). Mögliche Werte sind ganze Zahlen zwischen *1* und *255*, Standardwert ist *10*.

Feld	Wert
Pre-Empt-Modus (zurück in Master-Status)	Legen Sie fest, ob ein Backup-Router mit höherer Priorität Vorrang hat vor einem Master-Router mit niedriger Priorität. Der Pre-Empt-Modus dient dazu, unnötige Umschaltvorgänge zu verhindern. Das bedeutet: ein aktuell aktiver Backup Router mit niedriger Priorität gibt seine Rolle auch nach Wiedererreichbarkeit des eigentlichen Master Routers nicht mehr ab. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Beachten Sie eine Ausnahme: Wird als ***Priorität des virtuellen Routers*** *255* ausgewählt, erhält das Gateway mit dieser Priorität auf jeden Fall die Masterrolle, d.h. die Einstellung in ***Pre-Empt-Modus*** wird nicht berücksichtigt. Wählen Sie daher zur Nutzung von Pre-Empt-Modus eine ***Priorität des virtuellen Routers*** kleiner *255*.
Authentisierung aktivieren	Aktivieren oder deaktivieren Sie die Authentisierung. Mit *Aktiviert* wird die Funktion aktiv. Wenn die Funktion aktiv ist, wird ein Eingabefeld angezeigt. Hier geben Sie den Authentisierungsschlüssel ein. Hinweis: Beachten Sie, dass der Authentisierungsschlüssel für alle am Routerverbund teilnehmenden virtuellen Router gleich sein muss Standardmäßig ist die Funktion nicht aktiv.

Tabelle 2-12: Felder im Menü ***Virtuelle Router*** ➜ ***Erweiterte Einstellungen***

Im Menü ***Lokale Dienste*** ➜ ***BRRP*** ➜ ***VR-Synchronisation*** ➜ **Neu** wird der Watchdog Daemon konfiguriert, d.h. Sie legen fest, wie Statusänderungen gehandhabt werden.

Nach Öffnen des Menüs ***LOKALE DIENSTE*** ➜ ***BRRP*** ➜ ***VR-SYNCHRONISATION*** wird eine Liste aller Synchronisationen angezeigt. Sie können entweder virtuelle Router untereinander synchroniseiren oder Schnittstellen. Neue Synchronisationen können im Menü **Neu** hinzugefügt werden.

Sie können z. B. die beiden virtuellen Router R1 und R2 über BRRP synchronisieren. Dazu müssen Sie zwei Einträge anlegen. Für den ersten Eintrag müssen Sie als ***MONITORING-VR/SCHNITTSTELLE*** R1 und als ***SYNCHRONISATIONS-VR/SCHNITTSTELLE*** R2 verwenden. Für den zweiten Eintrag müssen Sie als ***MONITORING-VR/SCHNITTSTELLE*** R2 und als ***SYNCHRONISATIONS-VR/SCHNITTSTELLE*** R1 konfigurieren.

Das Menü ***VR-SYNCHRONISATION*** ➜ ***BASISPARAMETER*** ➜ ***MONITORING-VR/SCHNITTSTELLE*** besteht aus folgenden Feldern:

Feld	Wert
Monitoring-Modus	Wählen Sie, welcher Mechanismus für die Überwachung eines virtuellen Routers angewendet werden soll. Mögliche Werte: ■ *BRRP* (Standardwert): Die BRRP-spezifischen Status-Advertisements werden zur Statusermittlung des Masters verwendet. (Der Master sendet Advertisements gemäß seiner Konfiguration im Menü ***VIRTUELLE ROUTER*** ➜ ***ERWEITERTE EINSTELLUNGEN***.)
ID des virtuellen Routers	Nur für ***MONITORING-MODUS*** = *BRRP*. Wählen Sie einen virtuellen Router über die ***ID DES VIRTUELLEN ROUTERS*** und legen Sie durch die Auswahl fest, welche Schnittstelle kontrolliert werden soll. Wählbar sind die vorher definierten IDs (siehe “ID des virtuellen Routers” auf Seite 41). Der Watchdog Daemon fragt die in ***VIRTUELLE ROUTER*** festgelegten Detailinformationen ab.

Tabelle 2-13: Felder im Menü ***MONITORING-VR / SCHNITTSTELLE***

Das Menü ***VR-SYNCHRONISATION*** ➜ ***BASISPARAMETER*** ➜ ***SYNCHRONISATION-VR / SCHNITTSTELLE*** besteht aus folgenden Feldern::

Feld	Wert
Synchronisationsmode	Legen Sie fest, mit welchem Mechanismus virtuelle Router bzw. Schnittstellen synchronisiert werden: ■ *BRRP* (Standardwert): BRRP wird für die Synchronisierung der virtuellen Router verwendet.
ID des virtuellen Routers	Nur für ***SYNCHRONISATIONSMODUS*** = *BRRP*. Wählen Sie die ID des virtuellen Routers, der synchronisiert werden soll. Über die Synchronisation des virtuellen Routers wird implizit die mit dem virtuellen Router verbundene virtuelle Schnittstelle synchronisiert.

Tabelle 2-14: Felder im Menü ***SYNCHRONISATIONS-VR / SCHNITTSTELLE***

Im Menü ***BRRP*** ➜ ***OPTIONS*** können Sie die Funktion BRRP ein- oder ausschalten.

Felder im Menü ***OPTIONS*** ➜ ***BASISPARAMETER***:

Feld	Wert
BRRP aktivieren	Aktivieren oder deaktivieren Sie die Funktion BRRP. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Tabelle 2-15: Felder im Menü ***OPTIONS***

2.14 FCI - Media Gateway - Neues Feld SRTP

Im FCI Menü *VoIP* ➜ *Media Gateway* ➜ *Teilnehmer* ➜ Neu ➜ Erweiterte Einstellungen können Sie im Feld *Sortierreihenfolge* die neue Option *SRTP* (Secure Real-Time Transport Protocol) nutzen.

2.15 FCI - PBX - Neues Feld SRTP (TR200)

In den FCI Menüs *PBX* ➜ *Anschlusskonfiguration* ➜ *VoIP-Konfiguration* ➜ Neu ➜ *Erweiterte Einstellungen* und *PBX* ➜ *Interne Rufnummern* ➜ *VoIP* ➜ Schaltfläche zur Änderung eines Eintrags ➜ *Erweiterte Einstellungen* wurde das Feld *SRTP* (Secure Real-Time Transport Protocol) hinzugefügt.

Mit dem neuen Feld können Sie SRTP ein- oder ausschalten. Standardmäßig ist SRTP nicht aktiv. Aktives SRTP benötigen einige Telefone für die Umsetzung von externem ISDN nach internem SIP.

2.16 FCI - Zertifikate

Das FCI Menü *VPN* ➜ *Zertifikate* wurde nach *Systemverwaltung* ➜ *Zertifikate* verschoben. Das neue Menü dient zur Verwaltung einer allgemeinen Zertifikatsliste für alle Dienste.

Wenn Zertifikate verfügbar sind, können Sie Zertifikate in folgenden Menüs auswählen und nutzen:

- ***PBX* ➜ *Interne Rufnummern* ➜ *VoIP*** (**TR200aw** /**TR200bw**)
- ***VPN* ➜ *IPSec* ➜ *Phase-1-Profile* ➜ Neu** mit ***Authentifizierungsmethode*** = *DSA-Signatur*, *RSA-Signatur* oder *RSA-Verschlüsselung*
- ***Lokale Dienste* ➜ *HTTPS***.

Im Menü ***Systemverwaltung* ➜ *Zertifikate*** wurde in der Zertifikatsliste der Status *Läuft bald ab* hinzugefügt.

3 Änderungen

Folgende Änderungen sind an unserer Systemsoftware vorgenommen worden, um Leistung und Bedienbarkeit zu verbessern:

3.1 Konfiguration speichern geändert

Wenn Sie eine aktuelle Konfiguration speichern, können Sie diese als Boot-Konfiguration speichern wie bisher oder Sie können zusätzlich die vorhergehende Boot-Konfiguration als Backup archivieren.

Wenn Sie im FCI auf die Schaltfläche **Konfiguration speichern** klicken, erscheint die Frage "Möchten Sie die aktuelle Konfiguration wirklich als Boot-Konfiguration speichern?"

Sie haben folgende zwei Wahlmöglichkeiten:

- ***KONFIGURATION SPEICHERN***, d.h. die aktuelle Konfiguration als Boot-Konfiguration speichern
- ***KONFIGURATION SPEICHERN UND VORHERGEHENDE BOOT-KONFIGURATION SICHERN***, d.h. die aktuelle Konfiguration als Boot-Konfiguration speichern und zusätzlich die vorhergehende Boot-Konfiguration als Backup im Flash-Speicher des Routers archivieren.

Wenn Sie die archivierte Boot-Konfiguration in Ihr Gerät laden wollen, gehen Sie in das Menü ***Wartung*** ➜ ***Software & Konfiguration*** und wählen Sie ***Aktion*** = *Sicherung wiederherstellen*. Das archivierte Backup wird als aktuelle Boot-Konfiguration verwendet. Die Option *Sicherung wiederherstellen* können Sie wählen, wenn ein Backup archiviert ist.

3.2 FCI - Administrativer Zugriff geändert

Bisher basierte das FCI Menü ***Systemverwaltung*** ➜ ***Administrativer Zugriff*** ➜ ***Zugriff*** auf SIF-Regeln. Ab **Systemsoftware 7.9.5** basiert dieses Menü auf dem Subsystem Local Services Access Control und ist unabhängig von SIF. Das bedeutet, dass bei Änderungen im Menü ***Systemverwaltung*** ➜ ***Administrativer Zugriff*** ➜ ***Zugriff*** nicht mehr automatisch SIF-Regeln angelegt und im Menü ***Firewall*** ➜ ***Richtlinien*** ➜ ***Filterregeln*** angezeigt werden.

3.3 FCI - Schnittstellenmodus geändert

Im FCI Menü ***LAN*** ➜ ***IP-Konfiguration*** ➜ ***Schnittstellen*** ➜ ***Symbol zur Änderung eines Eintrags / Neu*** wurde die Beschriftung der Wahlmöglichkeiten im Feld ***Schnittstellenmodus*** in *Untagged* und *Tagged (VLAN)* geändert.

3.4 FCI - Dienste angepasst

Im FCI Menü ***Routing*** ➜ ***NAT*** ➜ ***NAT-Konfiguration*** ➜ **Neu** werden mit **Systemsoftware 7.9.5** dieselben Dienste zur Verfügung gestellt wie in der Firewall-Konfiguration.

3.5 FCI - Schaltfläche entfernt

Im FCI Menü ***Routing*** ➜ ***Lastverteilung*** ➜ ***Lastverteilungsgruppen*** ➜ **Neu** wurde die Schaltfläche **Zurück** entfernt.

3.6 FCI - VPN-Assistent - Einstellungen angepasst

Um die Funktionsfähigkeit des VPN-Assistent für PPTP-Einwahl auch unter Windows-Versionen zu gewährleisten, die jünger als Windows XP Service Pack 1 sind, wurden im FCI Menü ***VPN*** ➜ ***PPTP*** ➜ ***Optionen*** die Standardeinstellungen der Felder ***GRE-Window-Anpassung*** und ***GRE-Window-Größe*** angepasst.

3.7 FCI - *Administrative Zugriffsregeln anzeigen* entfernt

Im FCI Menü ***Firewall*** ➜ ***Richtlinien*** ➜ ***Filterregeln*** wurde die Checkbox ***Administrative Zugriffsregeln anzeigen*** entfernt.

3.8 FCI - Media Gateway - Protokoll TLS hinzugefügt

Im FCI Menü ***VoIP*** ➜ ***Media Gateway*** ➜ ***Teilnehmer*** ➜ **Neu** wurde im Feld ***Protokoll*** *TLS* als Auswahlmöglichkeit hinzugefügt.

4 Gelöste Probleme

Nicht alle im Kapitel “Wichtige Informationen” auf Seite 5 aufgezählten Geräte waren von den folgenden Problemen betroffen. Wenn Ihr Gerät nicht über das jeweilige Menü oder die jeweilige Eigenschaft verfügt, so können Sie das erwähnte Problem ignorieren.

Die folgenden Probleme sind in Systemsoftware 7.9.5 gelöst worden:

4.1 Dateitransfer misslungen (RS-Serie)

(ID 13405)

Bei umfangreichen Dateien konnte es vorkommen, dass ein Dateitransfer (z. B. FTP) durch einen IPSec-Tunnel fehlschlug.

Das Problem ist gelöst.

4.2 IPSec - NAT-T fehlerhaft

(ID 13786)

Bei einer IPSec-Verbindung konnte es trotz Verwendung von NAT-T vorkommen, dass die NAT Session vorzeitig beendet wurde.

Das Problem ist gelöst.

4.3 ISDN-Verbindung fehlgeschlagen

(ID 13487)

Mit der ADSL Logik 2.4.6.3.0.2 konnte keine ISDN-Verbindung hergestellt werden

Das Problem ist gelöst.

4.4 TACACS+ fehlte (RS-Serie)

(ID 13573)

Die Möglichkeit der Authentifizierung mit TACACS+ wurde nicht unterstützt.

Das Problem ist gelöst.

4.5 Cobion Orange Filter nicht verwendbar

(ID 13854)

Cobion Orange Filter konnten nicht aktiviert werden, weil die standardmäßig eingetragenen Server nicht mehr erreichbar waren.

Das Problem ist gelöst, die Einträge wurden angepasst.

4.6 FCI - Protokolleinträge falsch angezeigt

(ID 13477)

Wenn im FCI Menü ***Systemverwaltung*** ➜ ***Globale Einstellungen*** ➜ ***System*** im Feld ***Maximales Nachrichtenlevel von Systemprotokolleinträgen*** ein Wert gesetzt war, so wurde der Filter nicht verwendet und im Menü ***Monitoring*** ➜ ***Internes Protokoll*** wurden alle Einträge angezeigt.

Das Problem ist gelöst.

4.7 FCI - Falsche Bridge-Link-Qualität angezeigt

(ID 13335)

Für 802.11n-Verbindungen wurde die Qualität des Bridge Links falsch angezeigt, weil sie aufgrund des Signal-Rausch-Verhältnisses ermittelt wurde und nicht anhand des eigentlichen Signals.

Das Problem ist gelöst.

4.8 FCI - AUX und UMTS Menü fehlte (R1xxx/R3xxx/R4xxx)

(ID n/a)

Die FCI Menüs ***PHYSIKALISCHE SCHNITTSTELLEN*** ➜ ***AUX*** und ***PHYSIKALISCE SCHNITTSTELLEN*** ➜ ***UMTS/HSDPA*** fehlten.

Das Problem ist gelöst.

4.9 FCI - Alert-Meldungen angezeigt

(ID n/a)

Bei Aufruf des FCI Menüs ***PHYSIKALISCHE SCHNITTSTELLEN*** ➜ ***UMTS / HSDPA*** konnte es vorkommen, dass Alert-Meldungen angezeigt wurden.

Das Problem ist gelöst.

4.10 Setup Tool - *SERIAL CONSOLE* unsichtbar

(ID 13158)

Wenn im Setup Tool Menü ***SERIAL: CONSOLE*** ➜ **Edit** der Wert *Console* in *AUX* geändert wurde und danach die Änderung revidiert wurde, verschwand der Menüpunkt ***SERIAL: CONSOLE***.

Das Problem ist gelöst.

4.11 Setup Tool - UMTS - Falsches Menü angezeigt

(ID n/a)

Im Setup Tool Menü ***UMTS*** wurde der Titel des Hauptmenüs durch den Titel des Untermenüs überschrieben und somit das falsche Menü angezeigt.

Das Problem ist gelöst.