

Benutzerhandbuch Release Notes

7.10.1

Copyright© Version 1.1, 2011 Funkwerk Enterprise Communications GmbH

Rechtlicher Hinweis

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von Funkwerk-Geräten. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind zu finden unter www.funkwerk-ec.com.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch 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 Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Release Notes für funkwerk-Gateways finden Sie unter www.funkwerk-ec.com.

Funkwerk-Produkte bauen 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

funkwerk und das funkwerk-Logo, bintec und das bintec-Logo, artem und das artem-Logo, elmeg und das elmeg-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

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

Copyright

Alle Rechte sind vorbehalten. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung der Firma Funkwerk Enterprise Communications GmbH in irgendeiner Form reproduziert oder weiterverwertet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Funkwerk Enterprise Communications GmbH nicht gestattet.

Richtlinien und Normen

Informationen zu Richtlinien und Normen 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, Deutschland, Telefon: +49 911 9673 0, Fax: +49 911 688 07 25

Funkwerk Enterprise Communications France S.A.S., 6/8 Avenue de la Grande Lande, F-33174 Gradi-gnan, Frankreich, Telefon: +33 5 57 35 63 00, Fax: +33 5 56 89 14 05

Internet: www.funkwerk-ec.com

Inhaltsverzeichnis

Kapitel 1	Wichtige Informationen	1
1.1	Vorbereitung und Update mit dem FCI	1
1.2	Downgrade mit dem FCI	2
1.3	Sierra Wireless MC8700 Firmware-Update für RS232bu+	2
Kapitel 2	Neue Funktionen	4
2.1	FCI - Provider-Auswahl im Internetzugangsassistenten	4
2.2	FCI - Anzeige der WAN-Schnittstellen auf der Statusseite	4
2.3	FCI - Anzeige der UMTS-Schnittstelle	4
2.4	FCI - Modus neuer Schnittstellen verändern	5
2.5	FCI - Flusskontrolle für Ethernet-Schnittstellen	5
2.6	FCI- IPSec-Callback über UMTS	5
2.7	FCI - GSM Fallback	6
2.8	FCI - UMTS-PUK-Eingabefeld	6
2.9	UMTS - Unterstützung für Sierra Wireless AirCard 319U	6
2.10	FCI - Erweiterte Übersicht für Netzwerk-Routen.	6
2.11	FCI - Geänderte QoS-Filter-Konfiguration	6
2.12	FCI - Geänderte QoS-Schnittstellen-Konfiguration	7
2.13	FCI - Konfiguration von Zugriffsregeln	7
2.14	FCI - MTU für PPPoE-Verbindungen angeben	8
2.15	FCI - Timeout bei Inaktivität von PPP-Verbindungen geändert	8
2.16	FCI - Statusänderung von IPSec-Verbindungen.	8
2.17	FCI - Lebensdauer eines IPSec IKE-Phase-1-Schlüssel in Prozent	8

2.18	FCI - IKE Version 2	9
2.19	IPSec - NAT-T	9
2.20	IPSec - Exakte Berechnung des IPSec-Protokoll-Headers	9
2.21	FCI - Eigener PPTP-IP-Pool	10
2.22	FCI - Vollständige Filterung für Firewall	10
2.23	FCI - Media Gateway - Option TLS fehlte	10
2.24	Media Gateway - RFC 4040 - ISDN via IP	10
2.25	Media Gateway - Anzeige der umgeleiteten Rufnummer	10
2.26	FCI - DHCP-IP-Poolname	10
2.27	FCI - Erweitertes Scheduling	11
2.28	FCI - E-Mail-Betreff in E-Mail-Benachrichtigung	11
2.29	FCI - Geänderte Schnittstellen-Monitoring-Details	12
Kapitel 3	Änderungen	13
3.1	FCI - Geänderte Wireless LAN Controller Konfiguration	13
3.2	FCI - Geänderte Routing-Konfiguration	14
3.2.1	Netzwerk	14
3.2.2	Routing-Protokolle einsetzen	14
3.3	FCI - Geänderte und erweiterte Multicast-Konfiguration	15
3.3.1	Allgemein	15
3.3.2	PIM	15
3.4	FCI - QoS-Queue DEFAULT nicht löschar	15
Kapitel 4	Behobene Fehler	16
4.1	IPSec - Keine dynamischen Peers mit Proxy ARP	16
4.2	FCI - Import eines Konfigurationsdatei dauert sehr lange oder schlug fehl	16

4.3	xDSL - Keine DSL-Datenübertragung	16
4.4	IPSec - Falsche IPSec Phase-2-Policy führt zu Verbindungsabbruch . . .	17
4.5	FCI - Fehlerhafte Keepalive-Konfiguration für IPSec Phase-2.	17
4.6	Zertifikate - Löschen temporärer Zertifikate führte zu Stacktrace/Neustart	17
4.7	FCI - Kein VLAN-Option für PPPoE-Verbindungen verfügbar	18
4.8	FCI - Unklare DSL-Modus-Beschreibung.	18
4.9	FCI - Firewall-Filterregel-Konfiguration führte zu Stacktrace und Panic. . .	18
4.10	RTSP - RTSP-Datenstrom für Video on Demand nicht möglich	18
4.11	FCI - Falsche Zeitberechnung für Web-Filter	19
4.12	FCI - Fehlerhafte ISDN-Login-Einstellungen in Administrativer Zugriff . . .	19
4.13	FCI - Löschen von RIP-Filtern fehlerhaft	19
4.14	FCI - Falsche Angabe bei Statistik zum Lastverteilung-Datenverkehr . . .	20
4.15	FCI - Falsche Schnittstellenauswahl für BRRP	20
4.16	FCI - Fehlerhafter Schnittstellenmoduswechsel	20
4.17	Zertifikate - Fehlerhafte Zertifikatschlüssellänge und DSA-Auswahl	20
4.18	Hotspot - Fehlende Tabellenbeschriftung	21
4.19	ATM - Falsche voreingestellte MAC-Adresse	21
4.20	Media Gateway - Zu wenig mögliche Anrufkontroll-Einträge	21
4.21	Media Gateway - Fehlerhafte SRTP-Option für SIP-Konten.	22
4.22	IPSec - Phase-2-Profil nicht als Standardprofil markiert	22
4.23	IPSec - Phase-1-Profile-Schlüssellänge mit AES fehlerhaft.	22
4.24	SNMP-Browser - Stacktrace bei Eintrag in biboAdmUsrTrapTable.	22
4.25	Webfilter - Kein Internetzugang nach Deaktivierung des Webfilters	23
4.26	Media Gateway - Faxerkennung bei ausgehendem Fax fehlerhaft.	23

4.27	UMTS - Probleme beim Verbindungsaufbau zu UMTS/GPRS-Netzen . . .	23
4.28	FCI - Zugriff und QoS-Filter: TCP/UDP fehlt	24
4.29	FCI - Infos über DSP-Module fehlen auf Statusseite	24
4.30	PPTP - Überflüssige Nummern bei deaktiviertem Callback	24
4.31	FCI - Keine Internet Explorer 9 Unterstützung	24
4.32	Wireless LAN Controller - WTP-Reboot bei mehreren SSIDs	25
4.33	FCI - Falsches Protokoll für manuelle Routing-Einträge	25
4.34	FCI - Fehlerhafte Anzeige für ISDN-Verwendung Extern	25
4.35	FCI - PPP-Passwörter fälschlicherweise enthalten bei Konfigurationsexport	26
4.36	IPSec - Schlechter Verbindungsaufbau	26
4.37	Wireless LAN Controller - Neue Kanalfestlegung	26
4.38	Wireless LAN Controller - Fehlerhafte IP-Adresshandling	26
4.39	IPSec - Fehlfunktion und Stacktrace mit iPhone als dynamischer IPSec-Client mit XAUTH.	27
4.40	WLAN - Häufige Stacktraces und Neustart bei Access Points.	27
4.41	Media Gateway - Häufige Stacktraces und Neustart.	27
4.42	FCI - Dynamischer DNS-Server im Assistent nicht möglich.	28
4.43	FCI - Falsch vorkonfigurierte Optionen im Assistenten	28
4.44	Wireless LAN Controller - Monitoring zeigt inaktive SSIDs	28
4.45	FCI - Routenänderung für IPSec-Peer nicht möglich.	28
4.46	FCI - Standard-Benutzerpasswort für RADIUS an falscher Stelle	29
4.47	FCI - Überflüssige Rufnummer in ISDN-Port-Konfiguration	29
4.48	PPP - CHAP-Authentifizierung schlug fehl	29
4.49	FCI - Fehlerhafte Beschreibung beim Import von Zertifikaten	29

4.50	FCI - Lokale GRE-IP-Adresse ohne Eintrag nicht möglich	30
4.51	IPSec - Falsche maximale Anzahl IPSec-Phase-1-SAs	30
4.52	UMTS - ISDN-Login mit GSM funktionierte nicht	30
4.53	FCI - Konfiguration des SHDSL 4-Draht-Modus nicht möglich.	31
Kapitel 5	Bekannte Probleme.	32
5.1	Wireless LAN Controller - WTP Softwareaktualisierung funktioniert nicht .	32
5.2	Wireless LAN Controller - Keine Unterstützung einer zweiten IP-Adresse	32
5.3	IPSec Callback über UMTS - Verbindung zu ISDN-Gegenstelle nicht konfigurierbar.	32
5.4	IPSec - Panic bei IKEv2-Tunnel	33
5.5	IPSec - Endlosschleife mit IKEv2-Tunnel.	33
5.6	IPSec - Sporadische Panic und Stacktrace	33

Kapitel 1 Wichtige Informationen

1.1 Vorbereitung und Update mit dem FCI

Das Update der Systemsoftware mit dem Funkwerk Configuration Interface erfolgt 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.



Hinweis

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 folgendermaßen vor, um mit dem Funkwerk Configuration Interface ein Update auf **Systemsoftware 7.10.1** vorzubereiten und durchzuführen:

- (1) Für das Update benötigen Sie die Datei `XXXXX_b171001.xxx`, wobei `XXXXX` für Ihr Gerät 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 bei *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 7.10.1 über das Menü **Wartung->Software & Konfiguration** durch. Wählen Sie dazu: **Aktion** = *Systemsoftware aktualisieren*, **Quelle** = *Lokale Datei*, **Dateiname** = `XXXXX_b171001.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. Success. Operation completed success-“

fully“: 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.

1.2 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. Success. 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_b17901.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 Datei in das Gerät geladen wird. Wenn der Ladevorgang beendet ist, sehen Sie die Meldung „System - Maintenance. Success. 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.

1.3 Sierra Wireless MC8700 Firmware-Update für RS232bu+

Um die UMTS-Funktionalität auf den Geräten **RS232bu+** zu gewährleisten, führen Sie bitte vor Einsetzen der UMTS-SIM-Karte ein Firmware-Update speziell für das Sierra Wireless MC8700 Modul durch.

Gehen Sie dazu folgendermaßen vor:

- (a) Laden Sie im Internet unter <http://www.funkwerk-ec.com> im Download-Bereich für die **RS-Serie** mit **Release 7.10.1** die Software-Datei `MC8700_M3_0_9_0.ced` herunter und speichern diese auf den PC, über den Sie das Firmware-Update durchführen.
- (b) Führen Sie das Update über das Menü **Wartung->Software & Konfiguration** durch.

Wählen Sie dazu: **Aktion** = *Systemsoftware aktualisieren*, **Quelle** = *Lokale Datei*, **Dateiname** = `MC8700_M3_0_9_0.ced`. 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. Success. Operation completed successfully.“

**Wichtig**

Der Update-Vorgang dauert ca. 4 Minuten!

Kapitel 2 Neue Funktionen

Systemsoftware 7.10.1 enthält eine Reihe neuer Funktionen, die den Leistungsumfang gegenüber der letzten Version der Systemsoftware erheblich erweitern.



Hinweis

Bitte beachten Sie, dass nicht alle hier aufgeführten neuen Funktionen für alle Geräte zur Verfügung stehen. Informieren Sie sich ggf. im aktuellen Datenblatt Ihres Gerätes oder im entsprechenden Handbuch.

2.1 FCI - Provider-Auswahl im Internetzugangsassistenten


Die Auswahl für die Konfiguration eines Internetzugangs im FCI Assistenten wurde vereinfacht. Hier wählt man nun zunächst den **Typ** des Providers aus und entscheidet zwischen *Benutzerdefiniert* und *Vordefiniert*. Für *Benutzerdefiniert* kann der Benutzer seine individuellen Providereinstellungen vornehmen. Für *Vordefiniert* wird ein weiteres Feld **Land** angezeigt. Wenn man das gewünschte **Land** auswählt, erscheinen in den Optionen für das Feld **Internet Service Provider** nur die entsprechenden Einträge.

2.2 FCI - Anzeige der WAN-Schnittstellen auf der Statusseite

Im Menü **Systemverwaltung** -> **Status** werden im unteren Bereich keine **Systemmeldungen** mehr angezeigt. An dieser Stelle wird nun der Status der **WAN-Schnittstellen** angezeigt. Es werden deren **Beschreibung**, die **Verbindungsinformation** und der aktuelle Status der Verbindung unter **Link** angezeigt.

2.3 FCI - Anzeige der UMTS-Schnittstelle

Auf der Statusseite **Systemverwaltung** -> **Status** wird im Bereich **Physikalische Schnittstellen** der Status einer ggf. vorhandenen UMTS-Schnittstelle angezeigt. Sie sehen eine grafische Darstellung der Empfangsqualität und der entsprechenden Sendestärke in dBm.

Diese Anzeige finden Sie ebenfalls im Menü **Physikalische Schnittstellen** -> **UMTS/HSDPA** -> **UMTS/HSDPA/HSUPA** ->  unter der Bezeichnung **Netzwerkqualität**.

2.4 FCI - Modus neuer Schnittstellen verändern

Im Menü **Systemverwaltung** ->**Schnittstellenmodus / Bridge-Gruppen**->**Schnittstellen** können Sie durch Auswahl der Schaltfläche **Hinzufügen** den Modus weiterer Schnittstellen bearbeiten. Es öffnet sich eine Seite, in der Sie im Feld **Schnittstelle** die gewünschte Schnittstelle auswählen. Nach Klicken von **OK** können Sie in der Übersichtsseite den Modus der Schnittstelle dann wie gewünscht anpassen (*Routing-Modus* oder *Neue Bridge-Gruppe* oder bestehende Bridge-Gruppe auswählen).

2.5 FCI - Flusskontrolle für Ethernet-Schnittstellen


Im Menü **Physikalische Schnittstellen**->**Ethernet-Ports**->**Portkonfiguration** können Sie auswählen, ob auf einer Ethernet-Schnittstelle eine **Flusskontrolle** vorgenommen werden soll. Folgende mögliche Werte stehen zur Verfügung:

- *Deaktivieren* (Standardwert): Es wird keine Flusskontrolle vorgenommen.
- *Aktiviert*: Es wird eine Flusskontrolle durchgeführt.
- *Auto*: Es wird eine automatische Flusskontrolle durchgeführt.



2.6 FCI- IPSec-Callback über UMTS

IPSec-Callback wird dazu verwendet, einen IPSec-Peer zu veranlassen, eine Internetverbindung aufzubauen, um so einen IPSec-Tunnel über das Internet zu ermöglichen. Mit Hilfe eines direkten Anrufs über das UMTS-Mobilfunknetz kann dem Peer signalisiert werden, dass man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den Anruf über Mobilfunk veranlasst, eine Verbindung aufzubauen.

Die Konfiguration der UMTS-Karte führen Sie im Menü **Physikalische Schnittstellen**->**UMTS/HSDPA**->**UMTS/HSDPA/HSUPA** ->**Bearbeiten** durch. Hier steht zu diesem Zweck nun die Option *IPSec* für **Eingehender Dienstyp** zur Verfügung.


Im Menü **VPN**->**IPSec**->**IPSec-Peers**->->**Erweiterte Einstellungen** können Sie unter **Eigene IP-Adresse per ISDN/GSM übertragen** zudem auswählen, ob die IP-Adresse zum IPSec-Tunnelaufbau in dem Callback-UMTS-Ruf mitgesendet werden soll. Dieses verkürzt und erleichtert unter Umständen den Tunnelaufbau.

2.7 FCI - GSM Fallback

Im Menü **Physikalische Schnittstellen** -> **UMTS/HSDPA** -> **UMTS/HSDPA/HSUPA** ->  können Sie die unter **Fallback-Nummer** die Rufnummer für die Funktion GSM Fallback eintragen. Wenn ein Sprachruf auf diese Nummer eingeht, wird eine ggf. aktive Verbindung sofort getrennt und der Betriebsmodus des Modems auf GSM zurückgesetzt, in welchem das Modem so lange bleibt, bis wieder ein Datenruf (PPP, ISDN-Login, IPSec-Callback) erfolgt. Ist für die WAN-Verbindung der Flatrate-Modus aktiviert (Option **Immer aktiv** aktiviert in **WAN**->**Internet + Einwählen**->**GPRS/UMTS**-> ) , führt dies zu sofortigem Verbindungswiederaufbau.

Beachten Sie, dass die SIM-Karte diese Funktion unterstützen muss und nicht alle Mobilfunk-Anbieter Sprachrufe auf Daten-SIM-Karten weiterleiten.

2.8 FCI - UMTS-PUK-Eingabefeld

Es wird nun ein Eingabefeld zur Eingabe der PUK im Menü **Physikalische Schnittstellen** -> **UMTS/HSDPA** -> **UMTS/HSDPA/HSUPA** ->  angezeigt.

2.9 UMTS - Unterstützung für Sierra Wireless AirCard 319U

Der USB-UMTS-Stick **Sierra Wireless AirCard 319U** wird nun ebenfalls unterstützt.

2.10 FCI - Erweiterte Übersicht für Netzwerk-Routen

Im umgestalteten Menü **Netzwerk**->**Routen**->**IP-Routen** werden nun unter **Typ** der Netzwerktyp (*Direkt* oder *Indirekt*) angezeigt, und das **Protokoll**.

2.11 FCI - Geänderte QoS-Filter-Konfiguration

Die Konfiguration von QoS-Filtern im Menü **Netzwerk**->**QoS**->**QoS-Filter**->**Neu** wurde erweitert. Sie können nun im Feld **Dienst** vordefinierte Dienste auswählen oder durch die Option *Benutzerdefiniert* individuelle Einstellungen vornehmen.

Für die Parameter **Ziel-IP-Adresse/Netzmaske** und **Quell-IP-Adresse/Netzmaske** haben Sie nun die Möglichkeit, den **Typ** der Adresse zu bestimmen. Zur Auswahl stehen *Beliebig*, *Host* und *Netzwerk*.

2.12 FCI - Geänderte QoS-Schnittstellen-Konfiguration

Die Konfiguration der QoS-Schnittstellen im Menü **Netzwerk->QoS->QoS-Schnittstellen/Richtlinien->Neu** wurde erweitert. Sie können nun im Feld **Verschlüsselungsmethode** vordefinierte Methoden der Verschlüsselung der auf dieser IPSec-Schnittstelle gesendeten Pakete auswählen.

Möglich sind die Werte *DES, 3DES, Blowfish, Cast - (Cipher-Blockgröße = 64 Bit)* und *AES128, AES192, AES256, Twofish - (Cipher-Blockgröße= 128 Bit)*.

2.13 FCI - Konfiguration von Zugriffsregeln

Das Menü **Netzwerk** wurde durch ein neues Untermenü **Zugriffsregeln** ergänzt.

Im Menü **Netzwerk->Zugriffsregeln** definieren Sie, ob und wie der Zugriff auf Daten und Funktionen eingegrenzt werden soll (welcher Benutzer welche Dienste und Dateien nutzen darf).

Im Menü **Zugriffsfilter** definieren Sie Filter für IP-Pakete, um den Zugang von bzw. zu den verschiedenen Hosts in angeschlossenen Netzwerken zu erlauben oder zu sperren. So können Sie verhindern, dass über das Gateway unzulässige Verbindungen aufgebaut werden. Hierzu definieren Sie die Art des IP-Traffics, den das Gateway annehmen oder ablehnen soll.

Im Menü **Regelketten** definieren Sie die Aktionen, die durchgeführt werden sollen, wenn die in **Zugriffsfilter** definierten Bedingungen eintreten. Sie können mehrere getrennte Regelketten anlegen. Eine gemeinsame Nutzung von Filtern in verschiedenen Regelketten ist dabei möglich.

Im Menü **Schnittstellenzuweisung** definieren Sie, auf welcher Schnittstelle welche Regelkette angewendet werden soll.



Achtung

Achten Sie darauf, dass Sie sich beim Konfigurieren der Filter nicht selbst aussperren!

2.14 FCI - MTU für PPPoE-Verbindungen angeben

Im Menü **WAN->Internet + Einwählen->PPPoE** ist es nun möglich, die maximale Paketgröße (Maximum Transfer Unit, **MTU**) in Bytes anzugeben, die für die Verbindung verwendet werden darf.

Mit dem Standardwert *Automatisch* wird der Wert beim Verbindungsaufbau durch das Link Control Protocol vorgegeben.

Wenn Sie *Automatisch* deaktivieren, können Sie einen Wert eingeben.

Möglich sind Werte bis *8192*.

Standardwert ist *0*, das bedeutet automatische Aushandlung.

2.15 FCI - Timeout bei Inaktivität von PPP-Verbindungen geändert

Bei PPP-Verbindungen kann man nun einen Wert zwischen *0* und *10* angeben für die Zeit in Sekunden, die gewartet werden soll, bis die Verbindung abgebaut werden soll, wenn keine Nutzdaten mehr gesendet werden. Die Konfiguration erfolgt im Menü **WAN->Internet + Einwählen-><Verbindungstyp>->Neu** in dem Feld **Timeout bei Inaktivität**.

2.16 FCI - Statusänderung von IPSec-Verbindungen

Im Menü **VPN->IPSec->IPSec-Peers** ist es nun möglich, eine IPSec-Verbindung zu aktivieren oder zu deaktivieren. Dieses konfigurieren Sie in der Peer-Tabellenspalte **Aktion**.

2.17 FCI - Lebensdauer eines IPSec IKE-Phase-1-Schlüssel in Prozent

Im Menü **VPN->IPSec->Phase-1-Profile->Neu** können Sie nun die **Lebensdauer** eines IKE-Phase-1-Schlüssels auch in Prozent eintragen.


2.18 FCI - IKE Version 2



Hinweis

IKE V. 2 steht derzeit nur für die Geräte der RS- und der R(T)xx02-Serien zur Verfügung.

Für die Verwaltung der Security Associations (SAs) zum Aufbau eines IPSec-Tunnels steht nun ebenfalls die Verwendung der Version 2 des Internet Key Exchange Protokolls (IKE) zur Verfügung.

Im Menü **VPN IPSec IPSec-Peers** werden daher in der Übersicht über die IPSec-Peers nun zwei getrennte Bereiche angezeigt. Die untere Tabelle zeigt alle IPSec-Peers an, bei denen die Verwendung von IKEv2 ausgewählt wurde. Die Auswahl nehmen Sie im Menü **VPN IPSec IPSec-Peers**  / **Neu** im Feld **IKE (Internet Key Exchange)** vor. Mögliche Werte sind hier *IKEv1* und *IKEv2*.

Desweiteren sind im Menü **VPN->IPSec->Phase-1-Profile** die Profile unterteilt nach IKEv1- und IKEv2-Verwendung. Wählen Sie unter **Neues IKEv2-Profil erstellen** die Schaltfläche **Neu**, um die von Ihnen benötigten Einstellungen für Phase 1 mit IKEv2 vorzunehmen.

2.19 IPSec - NAT-T

Bei IPSec-Verbindungen kann bei aktivierter NAT-Aushandlung erzwungen werden, auch wenn auf beiden Seiten kein NAT erkannt wurde, auf UDP-Port 4500 zu schalten. Beachten Sie, dass diese Funktion nur im Initiator Modus funktioniert, und dass beim IPSec-Partner ebenfalls NAT-Aushandlung aktiviert ist. Die Konfiguration wird im Menü **VPN->IPSec->Phase-1-Profile ->Neu->Erweiterte Einstellungen** vorgenommen. Hierfür steht nun im Feld **NAT-Traversal** neben *Aktiviert* und *Deaktiviert* die Option *Erzwingen* zur Verfügung.

2.20 IPSec - Exakte Berechnung des IPSec-Protokoll-Headers

Es wurde eine Funktion eingefügt, mittels derer die Größe des Headers von IPSec-Paketen automatisch exakt berechnet wird. Dieses ist in seltenen Fällen notwendig, z.B. bei der parallelen Verwendung der QoS-Funktionalität.

2.21 FCI - Eigener PPTP-IP-Pool

Im Menü **VPN->PPTP->IP Pools** konfigurieren Sie IP-Adressbereiche für die Adressvergabe bei PPTP-Verbindungen.

Ihr Gerät kann als dynamischer IP-Adress-Server für PPTP-Verbindungen agieren. Dafür stellen Sie einen oder mehrere Pools von IP-Adressen zur Verfügung. Diese IP-Adressen können für die Dauer der Verbindung an einwählende Verbindungspartner vergeben werden.

2.22 FCI - Vollständige Filterung für Firewall

Im Menü **Firewall->Richtlinien->Optionen** steht nun die Option **Vollständige Filterung** zur Verfügung.

2.23 FCI - Media Gateway - Option TLS fehlte

Im Menü **VoIP->Media Gateway->SIP-Konten->Neu** kann nun die Option *TLS* für **Protokoll** konfiguriert werden.

2.24 Media Gateway - RFC 4040 - ISDN via IP

Mit der Umsetzung des RFC 4040 ist es nun möglich, 64 kbit/s-Kanal-Daten transparent in RTP-Paketen zu transportieren, wobei eine Pseudo-Codec "Clearmode" verwendet wird.

2.25 Media Gateway - Anzeige der umgeleiteten Rufnummer

Durch die Erweiterung der SIP-P-Protokoll-Unterstützung durch das UPDATE Element kann die Rufnummer von weitergeleiteten Rufen angezeigt werden.

2.26 FCI - DHCP-IP-Poolname

Im Menü **Lokale Dienste->DHCP-Server->DHCP Pool->Neu** kann nun unter **IP-Poolname** eine frei wählbare Beschreibung für den IP-Adresspool eingetragen werden.

2.27 FCI - Erweitertes Scheduling

Die Scheduling-Funktion ist in diesem Release grundlegend überarbeitet worden.

Ihr Gerät verfügt nun über einen erweiterten Aufgabenplaner. Abgesehen von voreingestellten und einfach zu konfigurierenden Standardanwendungen wie zeit- oder volumengesteuerte Aktivierung bzw. Deaktivierung von Schnittstellen, ermöglicht es der Aufgabenplaner, beliebig auf MIB-Parameter zuzugreifen. Dadurch können beliebige Ereignisse in der MIB als Auslöser ebenfalls beliebiger Aktionen definiert werden. Die Konfiguration erfolgt im Menü **Lokale Dienste->Scheduling**.



Hinweis

Voraussetzung für den Betrieb des Aufgabenplaners ist ein auf Ihrem Gerät eingestelltes Datum ab dem 1.1.2000.



Warnung


Die Konfiguration der nicht voreingestellten Aktionen erfordert umfangreiches Wissen über die Funktionsweise des Systems. Eine Fehlkonfiguration kann zu erheblichen Störungen im Betrieb führen. Sichern Sie ggf. die ursprüngliche Konfiguration z. B. auf Ihrem PC.

Informationen zu den MIB-Variablen und deren Wertebereiche finden Sie in der Online Hilfe der SNMP-Browser-Ansicht der Konfigurationsoberfläche. Beachten Sie, dass dafür ein aktiver Internetzugang nötig ist.

2.28 FCI - E-Mail-Betreff in E-Mail-Benachrichtigung

Im Menü **Externe Berichterstellung->E-Mail-Benachrichtigung->E-Mail-Benachrichtigungsempfänger** kann nun in das Feld **E-Mail-Betreff** ein beliebiger Text eingegeben werden, der in versendeten E-Mails als Betreff der Mail erscheint.

2.29 FCI - Geänderte Schnittstellen-Monitoring-Details




Im Menü **Monitoring->Schnittstellen** können Sie über die -Schaltfläche die statistischen Daten für die einzelnen Schnittstellen im Detail anzeigen lassen. Über die Filterleiste können Sie auswählen, ob **Gesamttransfer** oder **Transferdurchsatz** angezeigt werden soll. Folgende Daten zur Schnittstelle können Sie dann einsehen: **Beschreibung**, **MAC-Adresse**, **Tx-Pakete**, **Tx-Bytes**, **Rx-Pakete**, **Rx-Bytes**. Für die über diese Schnittstelle aktiven TCP-Verbindungen werden folgende Werte angezeigt: **Status**, **Lokale Adresse**, **Lokaler Port**, **Remote-Adresse**, **Entfernter Port**.

Kapitel 3 Änderungen

Folgende Änderungen sind in **Systemsoftware 7.10.1** vorgenommen worden.

3.1 FCI - Geänderte Wireless LAN Controller Konfiguration

Der Wireless LAN Controller zum Aufbau und zur Verwaltung einer WLAN-Infrastruktur mit mehreren Access Points (APs) wurde verändert und erweitert.

- Im Menü **Systemverwaltung** -> **Globale Einstellungen** -> **System** können Sie bei Access Points, die durch einen Wireless-LAN-Controller gemanaged werden sollen und sich in einem IP-Netz, das ausschließlich mit statischen IP-Adressen arbeitet, befinden, die statische IP-Adresse des Wireless-LAN-Controllers eingeben.
- Im Menü **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points** werden nun die Tabellenspalten **Kanal** und **Kanalsuche** angezeigt.
- Im Menü **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points** wird nun eine Option zur erneuten Kanalauswahl angeboten. Klicken Sie unter **Neue Kanalfestlegung** auf die Schaltfläche **START**, um die zugewiesenen Kanäle erneut zuzuweisen, z. B. wenn ein neuer Access Point hinzugekommen ist.
- Im Menü **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points** ->  werden nun die Daten für Funkmodul 1 und Funkmodul 2 angezeigt, wenn das entsprechende Gerät zwei Funkmodule enthält. Bei Geräten, die mit einem einzigen Funkmodul bestückt sind, werden die Daten für Funkmodul 1 angezeigt. Das alte Menü **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodule** entfällt somit.
- Im Menü **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** ->  entfällt die Option *AES und TKIP* im Feld **WPA Cipher** und **WPA2 Cipher**.
- Im neuen Menü **Wireless LAN Controller** -> **Monitoring** + **Drahtlosnetzwerke** wird eine Übersicht über verfügbare Drahtlosnetzwerke für die aktuell verwendeten Access Points angezeigt. Sie sehen, welches Funkmodul welchem Drahtlosnetzwerk zugeordnet ist. Für jedes Funkmodul wird ein Parametersatz angezeigt (**Standort**, **VSS**, **MAC-Adresse (VSS)**, **Kanal**, **Clients**). Neue Drahtlosnetzwerke können mittels **Hinzufügen**-Schaltfläche hinzugefügt werden. Bearbeitet werden sie mit .
- Im Menü **Wireless LAN Controller** -> **Monitoring** -> **Benachbarte APs** erscheint nun ein Hinweis während eines aktiven Scans, dass der Scan-Vorgang je nach Anzahl der installierten Access Points sehr lange dauern kann.
- Das Menü **Wireless LAN** und der Assistent **Wireless LAN** sind auf Access Points, die von einem Wireless LAN Controller gemanaged werden, deaktiviert.

3.2 FCI - Geänderte Routing-Konfiguration

Das **Routing**-Menü wurde geändert und erweitert und in diesem Zuge in mehrere Bereiche aufgeteilt.

3.2.1 Netzwerk

Sie können nun die Netzwerk-Routen im Menü **Netzwerk** konfigurieren. Hier stehen die alten Untermenüs **Routen**, **NAT**, **Lastverteilung**, **QoS** zur Verfügung.

Außerdem wurde das Menü **Netzwerk** durch ein neues Untermenü **Zugriffsregeln** ergänzt.

3.2.2 Routing-Protokolle einsetzen

Im neuen Menü **Routing-Protokolle** können Sie RIP und OSPF konfigurieren.

3.2.2.1 RIP

Das Menü **RIP** ist unverändert aus der vorherigen Softwareversion übernommen worden.

3.2.2.2 OSPF

Open Shortest Path First (OSPF) ist ein dynamisches Routing-Protokoll, das häufig in größeren Netzwerken als Alternative zu RIP angewendet wird. Es wurde ursprünglich dazu entwickelt, einige Einschränkungen des RIP zu umgehen (wenn es in größeren Netzwerken verwendet wird).

Im Untermenü **Bereiche** geben Sie die Adressen der OSPF-Bereiche an. In **Schnittstellen** legen Sie für jede vorhandene Schnittstelle fest, ob und in welchem Modus OSPF aktiviert werden soll. Unter **Globale Einstellungen** haben Sie die Möglichkeit, die Funktion OSPF zu aktivieren bzw. zu deaktivieren und grundlegende Einstellungen dazu zu verändern.

Monitoring

Im Menü **Monitoring->OSPF** werden Informationen zu OSPF überwacht. Der OSPF-Monitor ist horizontal in drei Bereiche gegliedert und zeigt Informationen zu OSPF-Schnittstellen, den erkannten Nachbarn sowie die Link State Database Einträge.

3.3 FCI - Geänderte und erweiterte Multicast-Konfiguration

Das Menü **Multicast** ist um ein Untermenü **Allgemein** und **PIM** erweitert worden.

3.3.1 Allgemein

Im Menü **Allgemein** haben Sie nun die Möglichkeit, die Multicast-Funktion zu aktivieren bzw. zu deaktivieren.

3.3.2 PIM

Protocol Independent Multicast (**PIM**) ist ein Multicast-Routingverfahren, das dynamisches Routing von Multicast-Paketen ermöglicht. Bei PIM wird die Informationsverteilung über einen zentralen Punkt geregelt, der als Rendezvous Point bezeichnet wird. Dorthin werden die Datenpakete initial geleitet und auf Anfrage anderer Router den Empfängern zur Verfügung gestellt.

Bei Multicast-Routing-Protokollen unterscheidet man grundsätzlich zwischen Sparse Mode und Dense Mode. Beim Dense Mode werden alle Pakete weitergeleitet und nur die Pakete an Gruppen verworfen, die explizit abbestellt wurden. Beim Sparse Mode werden nur Pakete an Gruppen weitergeleitet, die von diesen bestellt wurden. Ihr Gerät verwendet PIM im Sparse Mode.

Monitoring

Im Menü **Monitoring->PIM->Allgemeine Statusangaben** wird der Status aller konfigurierten PIM Komponenten angezeigt.

3.4 FCI - QoS-Queue DEFAULT nicht löschar

Im Menü **Netzwerk->QoS->QoS-Schnittstellen/Richtlinien->Neu** kann unter **Queues/Richtlinien** manuell keine QoS-Queue mit **Priorisierungs-Queue** *Standard* mehr angelegt werden. Die nötige DEFAULT-Queue wird bei der Konfiguration automatisch vom System erzeugt und kann vom Benutzer nicht gelöscht werden. Diese DEFAULT-Queue kann bearbeitet werden (außer die Werte für **Beschreibung**, **Ausgehende Schnittstelle**, **Priorisierungs-Queue** und **Priorität**).

Kapitel 4 Behobene Fehler

Folgende Fehler sind in **Systemsoftware 7.10.1** behoben worden:

4.1 IPSec - Keine dynamischen Peers mit Proxy ARP

(ID 11744)

Bei einem IPSec-Peer mit dynamischer IP-Adresskonfiguration und konfiguriertem Proxy ARP wurde beim Tunnelaufbau Proxy ARP deaktiviert.

Das Problem wurde gelöst.

4.2 FCI - Import eines Konfigurationsdatei dauert sehr lange oder schlug fehl

(ID 13055)

Der Import einer Konfigurationsdatei durch die Option *Konfiguration importieren* für **Aktion** im Menü **Wartung->Software & Konfiguration ->Optionen** dauerte sehr lange und schlug dann fehl.

Das Problem wurde gelöst.

4.3 xDSL - Keine DSL-Datenübertragung

(ID 13301)

Bei DSL-Leitungen mit einer hohen Anzahl an CRC- und HEC-Fehlern konnte es vorkommen, dass über die Verbindung keine Nutzdaten übertragen werden konnten.

Das Problem wurde gelöst.

4.4 IPSec - Falsche IPSec Phase-2-Policy führt zu Verbindungsabbruch

(ID 13354)

Bei einer bestehenden IPSec-Verbindung konnte es zu Verbindungsabbrüchen bei der Neuaushandlung führen, da dafür die falsche Quell-IP-Adresse verwendet wurde und somit die ISAKMP-Meldung 18 (INVALID-ID-INFORMATION) vom Verbindungspartner ausgelöst wurde.

Das Problem wurde gelöst.

4.5 FCI - Fehlerhafte Keepalive-Konfiguration für IP-Sec Phase-2

(ID 13443)

Die Deaktivierung von Keepalive-Meldungen durch die Wahl der Option *Inaktiv* für **Erreichbarkeitsprüfung** im Menü **VPN->IPSec->Phase-1-Profile->Neu** war fehlerhaft und führte zu einer Vielzahl an Fehlermeldungen auf einem Fremdprodukt auf der Gegenseite.

Das Problem wurde gelöst.

4.6 Zertifikate - Löschen temporärer Zertifikate führte zu Stacktrace/Neustart

(ID 14051)

Sollte ein temporäres Zertifikat gelöscht werden, kam es zu einem Stacktrace oder Neustart des Systems.

Das Problem wurde gelöst.

4.7 FCI - Kein VLAN-Option für PPPoE-Verbindungen verfügbar

(ID 14065)

Im Menü **WAN->Internet + Einwählen->PPPoE->Neu** gab es keine und das Öffnen des Menüs führte zu Fehlermeldungen.

Das Problem wurde gelöst.

4.8 FCI - Unklare DSL-Modus-Beschreibung

(ID 14155)

Auf Geräten mit unterschiedlichen DSL-Varianten (z.B. **R3502** mit ADSL1 + ADSL2 + ADSL2+ + VDSL) war der Name für den automatischen Modus für ADSL im Menü **Physikalische Schnittstellen->ADSL-Modem->ADSL-Konfiguration** missverständlich. *Automatischer Modus* wurde umbenannt zu *Automatische Modus (ADSL)*.

4.9 FCI - Firewall-Filterregel-Konfiguration führte zu Stacktrace und Panic

(ID 14209)

Wurde im Menü **Firewall->Richtlinien->Filterregeln->Neu** ein Eintrag geöffnet und mit **OK** oder **Abbrechen** geschlossen, kam es zu Stacktrace und Panic.

Das Problem wurde gelöst.

4.10 RTSP - RTSP-Datenstrom für Video on Demand nicht möglich

(ID 14261)

Aufgrund fehlerhafter NAT-Einstellungen konnten keine RTSP-Daten für Video on Demand

übertragen werden.

Das Problem wurde gelöst.

4.11 FCI - Falsche Zeitberechnung für Web-Filter

(ID 14324)

Da die Zeit für Web-Filter-Einträge sich ungünstigerweise an der UTC orientierte, entsprach die reale Zeit für die Webfilterung nicht den in **Zeitplan (Start-/Stopzeit)** im Menü **Lokale Dienste->Web-Filter->Filterliste->Neu** konfigurierten Werten.

Das Problem wurde gelöst.

4.12 FCI - Fehlerhafte ISDN-Login-Einstellungen in Administrativer Zugriff

(ID 14357)

Wurde im Menü **Systemverwaltung+Administrativer Zugriff->Zugriff** die Option *ISDN-Login* für eine spezifische Schnittstelle deaktiviert, war für keine der vorhandenen Schnittstellen auf dem Gerät ISDN-Login mehr möglich.

Das Problem wurde gelöst.

4.13 FCI - Löschen von RIP-Filtern fehlerhaft

(ID 14366)

Wurde im Menü **Routing-Protokolle->RIP->RIP-Filter** ein einzelner Eintrag gelöscht, wurden alle anderen Tabelleneinträge ebenfalls gelöscht.

Das Problem wurde gelöst.

4.14 FCI - Falsche Angabe bei Statistik zum Lastverteilung-Datenverkehr

(ID 14394)

Im Menü **Netzwerk->Lastverteilung->Lastverteilungsgruppen->** wurden fehlerhafte Werte für **Download-Datenverkehr** und **Upload-Datenverkehr** angezeigt.

Das Problem wurde gelöst.

4.15 FCI - Falsche Schnittstellenauswahl für BRRP

(ID 14446)

Im Menü **Lokale Dienste->BRRP->Virtuelle Router->Neu** wurden fehlerhafterweise auch ethoa-Schnittstellen zur Auswahl für **Ethernet-Schnittstelle** angeboten.

Das Problem wurde gelöst.

4.16 FCI - Fehlerhafter Schnittstellenmoduswechsel

(ID 14449)

Wurde im Menü **Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen** der Modus einer Schnittstelle erst auf Bridging und danach wieder zurück auf Routing gestellt, ging entweder die IP-Konfiguration dieser Schnittstelle verloren oder es kam zu einem Stacktrace.

Das Problem wurde gelöst.

4.17 Zertifikate - Fehlerhafte Zertifikatschlüssellänge und DSA-Auswahl

(ID 14479)

Wurden im Menü **Systemverwaltung->Zertifikate->Zertifikatsliste->Zertifikatsanforde-**

ung andere Einstellungen für **Privaten Schlüssel generieren** als der Standardwert *RSA 1024* Bits eingestellt, wurde trotzdem immer der Standardwert verwendet.

Das Problem wurde gelöst.

4.18 Hotspot - Fehlende Tabellenbeschriftung

(ID 14492)

Im Menü **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway** fehlte die Beschriftung der Tabellenspalte, in der Hotspot-Einträge aktiviert bzw. deaktiviert werden können. Diese heisst nun **Status**.

Das Problem wurde gelöst.

4.19 ATM - Falsche voreingestellte MAC-Adresse

(ID 14519)

Bei Auswahl der Option **Voreingestellte verwenden** für den Parameter **MAC-Adresse** im Menü **WAN->ATM->Profile->Neu**, wurde im System die falsche MAC-Adresse eingetragen.

Das Problem wurde gelöst.

4.20 Media Gateway - Zu wenig mögliche Anrufkontroll-Einträge

(ID 14521)

Im Menü **VoIP->Media Gateway->Anrufkontrolle** konnten maximal nur 100 Einträge gemacht werden.

Das Problem wurde gelöst.

4.21 Media Gateway - Fehlerhafte SRTP-Option für SIP-Konten

(ID 14580)

Im **VoIP->Media Gateway->SIP-Konten->Neu->Erweiterte Einstellungen** wurde die Option *SRTP* für **Sortierreihenfolge** nicht richtig gesetzt und funktionierte nicht.

Das Problem wurde gelöst.

4.22 IPsec - Phase-2-Profil nicht als Standardprofil markiert

(ID 14581)

Im Menü **VPN->IPsec->IPsec-Peers->Neu->Erweiterte Einstellungen** fehlte beim Standard-**Phase-2-Profil** das Sternchen (*).

Das Problem wurde gelöst.

4.23 IPsec - Phase-1-Profile-Schlüssellänge mit AES fehlerhaft

(ID 14584)

Im Menü **VPN->IPsec->Phase-1-Profile->Neu** wurde die Schlüssellänge für die **Verschlüsselung** der **Proposals** mit AES falsch berechnet. Nun stehen die festen Werte *AES-128*, *AES-192* und *AES-256* zur Auswahl.

4.24 SNMP-Browser - Stacktrace bei Eintrag in biboAdmUsrTrapTable

(ID 14588)

Beim Anlegen eines neuen Eintrags in `biboAdmUsrTrapTable` über den SNMP-Browser

kam es zu Stacktrace.

Das Problem wurde gelöst.

4.25 Webfilter - Kein Internetzugang nach Deaktivierung des Webfilters

(ID 14600)

Wurde der Web-Filter-Status im Menü **Lokale Dienste->Web-Filter->Allgemein** mit deaktiviert, war kein Internetzugang über HTTP mehr möglich.

Das Problem wurde gelöst.

4.26 Media Gateway - Faxerkennung bei ausgehendem Fax fehlerhaft

(ID 14646)

Wenn das Media Gateway als Remote CAPI Fax Gateway verwendet wurde, konnte es vorkommen, dass der Faxton bei ausgehenden Faxen nicht erkannt wurde.

Das Problem wurde gelöst.

4.27 UMTS - Probleme beim Verbindungsaufbau zu UMTS/GPRS-Netzen

(ID 14652)

Bei schlechter Signalqualität konnte es vorkommen, dass zu manchen UMTS/GPRS-Netzen keine Verbindung aufgebaut werden konnte.

Das Problem wurde gelöst.

4.28 FCI - Zugriff und QoS-Filter: TCP/UDP fehlt

(ID 14665)

Die parallele Auswahl von TCP und UDP für **Protokoll** im Menü **Routing->QoS->QoS-Filter->Neu** war nicht möglich. Es steht nun eine Option *tcp/udp* zur Auswahl. Die Option ist durch die Umstrukturierung der Routing-Menüs nun im Menü **Netzwerk** zu finden.

4.29 FCI - Infos über DSP-Module fehlen auf Statusseite

(ID 14689)

Gesteckte DSP-Module wurden nicht in **Systemverwaltung->Status->Module** angezeigt.

Das Problem wurde gelöst.

4.30 PPTP - Überflüssige Nummern bei deaktiviertem Callback

(ID 14691)

Wurde eine vormals genutzte Callback-Funktion für PPTP-Verbindungen deaktiviert, wurde die eingetragene Callback-Nummer nicht gelöscht. Auch manuelles Löschen schlug fehl.

Das Problem wurde gelöst.

4.31 FCI - Keine Internet Explorer 9 Unterstützung

(ID 14714)

Das **Funkwerk Configuration Interface** kann nun auch fehlerfrei mit Microsoft Internet Explorer 9 verwendet werden.

4.32 Wireless LAN Controller - WTP-Reboot bei meh-

rereren SSIDs

(ID 15138)

Wurden mehrere SSIDs in einem vom Wireless-LAN-Controller verwalteten Drahtlos-Szenario mit mehreren WTPs betrieben, konnte es dazu kommen, dass WTPs im Netz sporadisch neu starteten.

Das Problem wurde gelöst.

4.33 FCI - Falsches Protokoll für manuelle Routing-Einträge

(ID 15127)

Wurde im Menü **Routing->Routen->IP-Routen->Neu** ein Routing-Eintrag erzeugt, wurde das Protokoll standardmäßig auf *netmgmt* gesetzt. Dieser Wert wurde zu *local* geändert und ist in der Routen-Übersicht im neuen geänderten Routing-Menü unter **Netzwerk->Routen->IP-Routen** unter **Protokoll** einsehbar.

Das Problem wurde gelöst.

4.34 FCI - Fehlerhafte Anzeige für ISDN-Verwendung Extern

(ID 15054)

Im Menü **Systemverwaltung->Status** wurden ggf. benutzte PRI-Kanäle nicht unter **ISDN Verwendung Extern** angezeigt.

Das Problem wurde gelöst.

4.35 FCI - PPP-Passwörter fälschlicherweise enthalten bei Konfigurationsexport

(ID 15044)

Wurde über das Menü **Wartung->Software &Konfiguration ->Optionen** eine Konfigurationsdatei mit Statusinformationen (**Aktion = Konfiguration mit Statusinformationen exportieren**) exportiert, waren alle PPP-Passwörter im Klartext enthalten. Da eine Konfigurationsdatei mit Statusinformationen jedoch für Support-Zwecke verwendet wird und daher keine Passwörter im Klartext enthalten sein dürfen, wurden diese entfernt.

4.36 IPSec - Schlechter Verbindungsaufbau

(ID 14985)

Der Verbindungsaufbau zu IPSec-Peers dauerte lange, wenn viele Peers konfiguriert waren. Teilweise wurde das Gerät auch vollständig blockiert.

Das Problem wurde gelöst.

4.37 Wireless LAN Controller - Neue Kanalfestlegung

(ID 14980)

Im Menü **Wireless LAN Controller->Controller-Konfiguration->Slave Access Points** wurde die Schaltfläche **Neue Kanalfestlegung** angezeigt, auch wenn das Funkmodul unkonfiguriert und kein Funkprofil zugewiesen war.

Das Problem wurde gelöst.

4.38 Wireless LAN Controller - Fehlerhafte IP-Adresshandling

(ID 14794)

Wurde der Wireless LAN Controller mit statischen IP-Adressen betrieben und wurde dafür

im Menü **Systemverwaltung** ->**Globale Einstellungen**->**System** unter **Manuelle IP-Adresse des WLAN-Controller** eine IP-Adresse angeben, kam trotzdem keine Kommunikation zwischen Controller und WTPs zustande.

Das Problem wurde gelöst.

4.39 IPSec - Fehlfunktion und Stacktrace mit iPhone als dynamischer IPSec-Client mit XAUTH

(ID 14194)

Sollten iPhones mittels IPSec mit XAUTH verbunden werden, schlug der Verbindungsaufbau fehl und es kam zu einem Stacktrace.

Das Problem wurde gelöst.

4.40 WLAN - Häufige Stacktraces und Neustart bei Access Points

(ID 14137)

Bei Access Points, besonders **bintec Wx002**, kam es häufig zu willkürlichen Neustarts.

Das Problem wurde gelöst.

4.41 Media Gateway - Häufige Stacktraces und Neustart

(ID 14082)

Würde das Media Gateway mit einem Exchange VoIP Server verbunden, kam es häufig zu Stacktraces und Neustarts.

Das Problem wurde gelöst.

4.42 FCI - Dynamischer DNS-Server im Assistent

nicht möglich

(ID 14728)

Im Assistenten **Erste Schritte** war es nicht möglich, das Gerät so zu konfigurieren, dass es dynamisch auf einen DNS-Server vom ISP zugreift und es wurde die Eingabe einer festen IP-Adresse eines DNS-Servers verlangt. Dieses wurde geändert. Nun ist es möglich die Option **Feste DNS-Server-Adresse** zu aktivieren und zwei alternative DNS-Server-Adressen einzugeben (**DNS-Server 1** und **DNS-Server 2**). Standardmässig ist die Option nicht aktiv, d.h. es wird dynamisch ein DNS-Server des ISP verwendet.

4.43 FCI - Falsch vorkonfigurierte Optionen im Assistenten

(ID 14844)

Im Assistenten **Internetzugang** wurden für den jeweiligen Modemtyp (ADSL, VDSL) fehlerhafte vordefinierte Werte für **Internet Service Provider** angeboten.

Das Problem wurde gelöst.

4.44 Wireless LAN Controller - Monitoring zeigt inaktive SSIDs

(ID 14897)

Fälschlicherweise wurden im Menü **Wireless LAN Controller->Monitoring->Drahtlosnetzwerke** inaktive SSIDs angezeigt.

Das Problem wurde gelöst.

4.45 FCI - Routenänderung für IPSec-Peer nicht möglich

(ID 14900)

Die Änderung von **Routentyp** einer IPSec-Peer-Route von *Netzwerkroute* auf *Standardroute* im Menü **Netzwerk->Routen->IP-Routen** (vorher **Routing->Routen->IP-Routen**) wurde fehlerhaft ausgeführt.

Das Problem wurde gelöst.


4.46 FCI - Standard-Benutzerpasswort für RADIUS an falscher Stelle

(ID 14903)

Die Konfiguration von **Standard-Benutzerpasswort** im Menü **Systemverwaltung->Remote Authentifizierung->RADIUS->Neu** war bisher fälschlicherweise nur im RADIUS-Dialout-Kontext unter **Erweiterte Einstellungen** konfigurierbar. Da dieses jedoch auch allgemeinere Verwendung finden kann, ist der Parameter nun unter **Basisparameter** zu finden.

4.47 FCI - Überflüssige Rufnummer in ISDN-Port-Konfiguration

(ID 14915)

Das Feld **Anlagenanschluss-Rufnummer** im Menü **Physikalische Schnittstellen->ISDN-Ports->ISDN-Konfiguration->** (mit **Automatische Konfiguration beim Start** deaktiviert, **Port-Verwendung** = *Dialup (Euro-ISDN)* und **ISDN-Konfigurationstyp** *Punkt-zu-Punkt* ist nur für Geräte mit Media Gateway nötig.

Das Problem wurde gelöst.

4.48 PPP - CHAP-Authentifizierung schlug fehl

(ID 14947)

Aufgrund eine zu kleinen Wertebereichs für das Feld "Challenge Length" in einem CHAP-Authentifizierungspaket schlug die CHAP-Authentifizierung bei Gegenstellen mit höheren Werten fehl.

Das Problem wurde gelöst.

4.49 FCI - Fehlerhafte Beschreibung beim Import von Zertifikaten

(ID 14963)

Beim Import eines Zertifikats mit **Systemverwaltung ->Zertifikate->Zertifikatsliste->Importieren** wurde bei leerem Feld **Lokale Zertifikatsbeschreibung** der automatisch erstellte Zertifikatsname nicht im Zertifikatseintrag unter **Beschreibung** gespeichert. Daher wird nun eine Eingabe in **Lokale Zertifikatsbeschreibung** erzwungen.

Das Problem wurde gelöst.

4.50 FCI - Lokale GRE-IP-Adresse ohne Eintrag nicht möglich

(ID 14969)

Im Menü **VPN->GRE->GRE-Tunnel->Neu** musste unnötigerweise in **Lokale GRE-IP-Adresse** ein Eintrag gemacht werden.

Das Problem wurde gelöst.

4.51 IPSec - Falsche maximale Anzahl IPSec-Phase-1-SAs


(ID 14987)

Da die maximale Anzahl für Phase-1-SAs zu stark begrenzt war, sind ältere SAs automatisch gelöscht worden, wenn weitere ausgehandelt werden sollten.

Das Problem wurde gelöst.

4.52 UMTS - ISDN-Login mit GSM funktionierte nicht

(ID 14996)

Wenn ein Gerät mit **Bevorzugter Netzwerktyp** *Nur GPRS* und **Eingehender Dienstyp** *ISDN-Login* konfiguriert war (Menü **Physikalische Schnittstellen->UMTS/HSDPA->UMTS/HSDPA/HSUPA ->**) , wird zwar der eingehende ISDN-Datenruf in Debug-Meldungen sichtbar, es konnte jedoch keine Verbindung hergestellt werden.

Das Problem wurde gelöst.

4.53 FCI - Konfiguration des SHDSL 4-Draht-Modus nicht möglich

(ID 14790)

Die Konfiguration des SHDSL-4-Draht-Modus (**Leitungsmodus** *4-Draht*) im Menü **Physikalische Schnittstellen->SHDSL->Modem->SHDSL-Konfiguration** führte zu Fehlern.

Das Problem wurde gelöst.

Kapitel 5 Bekannte Probleme

Folgende Probleme sind in **Systemsoftware 7.10.1** bekannt:

5.1 Wireless LAN Controller - WTP Softwareaktualisierung funktioniert nicht

In einer Wireless LAN Controller Installation mit einem AC mit Software-Release 7.10.1 und einem WTP mit Software-Release 7.9.6 wird bei einer Software-Aktualisierung auf 7.10.1 auf dem WTP die Systemsoftware zwar aktualisiert, aber das System startet nicht automatisch neu, was verhindert, dass die neue Systemsoftware auf dem WTP aktiviert wird.

In diesem Fall führen Sie eine der folgenden Aktionen durch:

- (a) Starten Sie den WTP manuell neu, indem Sie das Stromkabel vom Stromanschluss trennen und wieder anschließen. Systemsoftware 7.10.1 wird auf dem WTP aktiviert.
- (b) Deaktivieren Sie den WTP über den AC, und lösen somit ebenfalls einen Neustart des WTP aus. Entfernen Sie dazu den Haken für den Wert **Administrativer Status** im Menü **Wireless LAN Controller->Slave-AP-Konfiguration->Slave Access Points** und klicken Sie **OK**.

5.2 Wireless LAN Controller - Keine Unterstützung einer zweiten IP-Adresse

Wird auf der Ethernet-Schnittstelle, über die die WTPs einer Wireless LAN Controller Installation gemanaged werden, eine zweite IP-Adresse konfiguriert, geht die Verbindung zu allen WTPs verloren. Daher ist es nicht möglich, in Wireless LAN Controller Installationen eine zweite IP-Adresse auf die entsprechende Ethernet-Schnittstelle zu binden.

5.3 IPSec Callback über UMTS - Verbindung zu ISDN-Gegenstelle nicht konfigurierbar

(ID 15038)

Für die Funktion IPSec-Callback über eine UMTS-Verbindung kann der IP-Adressaustausch nicht über den D-Kanal stattfinden. Dieser muss über den B-Kanal durch-

geführt werden. Hierfür muss die ISDN-Gegenstelle V.110 (9600) oder ISDN-Sprachdienste unterstützen (abhängig vom Provider, der SIM-Karte und dem Modem). Die Verbindung des GSM-Modems zu einer ISDN-Gegenstelle kann jedoch derzeit noch nicht konfiguriert werden.

5.4 IPSec - Panic bei IKEv2-Tunnel

(ID 15079)

Mit einem aktiven IPSec-Tunnel unter Verwendung von IKEv2 für Phase-1 kann es zu einer Panic kommen, wenn eine Delete-Meldung für eine Child-SA empfangen wird.

5.5 IPSec - Endlosschleife mit IKEv2-Tunnel

(ID 15318)

Wird das IPSec-Subsystem deaktiviert, wenn ein aktiver IPSec-Peer mit IKEv2 vorhanden ist, führt dieses zu einer Endlosschleife.

5.6 IPSec - Sporadische Panic und Stacktrace

(ID 15359 und ID 15298)

Unter folgenden Voraussetzungen kann es sporadisch zu Panic und Stacktrace kommen:

- Dynamisch konfigurierte IPSec-Peers mit RADIUS-Authentifizierung.
- Phase 2 ist mindestens einmal für einen Peer durch das Rekeying gelaufen.
- Hohe Systemlast durch häufigen Auf- und Abbau von Phase 1 und Phase 2.