Release Notes
Systemsoftware 7.9.1

Version 1.2

Ziel und Zweck

Dieses Dokument beschreibt neue Funktionen, Änderungen und behobene Fehler in **Systemsoftware 7.9.1**.

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 7.9.1 aufmerksam, um Probleme beim Update oder bei der Verwendung der Software zu vermeiden.

1.1 Gültigkeit

Systemsoftware 7.9.1 steht ausschließlich für folgende Geräte zur Verfügung und kann auf anderen Geräten nicht eingesetzt werden:

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

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.

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 und dem Setup Tool.

1.2.1 Vorbereitung und Update mit dem FCI

Das Update der Systemsoftware mit dem Funkwerk Configuration Interface erfogt mit einem BLUP (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 von unterbrochenen Update-Vorgängen könnte sein, dass Ihr Gateway nicht mehr bootet. Schalten Sie Ihr Gateway nicht aus, während das Update durchgeführt wird.

Gehen Sie ggf. folgendermaßen vor, um mit dem **Funkwerk Configuration Interface** ein Update auf **Systemsoftware 7.9.1** vorzubereiten und durchzuführen:

1. Für das Update benötigen Sie die Datei *XXXXX_bl7901.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.
   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 *Auf Diskette/Festplatte 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 7.9.1** über das Menü ***WARTUNG*** ➜ ***SOFTWARE & KONFIGURATION*** durch.
   Wählen Sie dazu:
   AKTION = *Systemsoftware aktualisieren*
   QUELLE = *Lokale Datei*
   DATEINAME = *XXXXX_bl7901.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. The system must be restarted."
   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.

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. The system must be restarted."
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_bl7807.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. The system must be restarted."
   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 7.9.1 enthält eine Reihe neuer Funktionen, die den Leistungsumfang gegenüber der letzten Version der Systemsoftware erheblich erweitern:

2.1 Assistenten im FCI

Ab Systemsoftware 7.9.1 stehen Assistenten für einige häufig benötigte Konfigurationsaufgaben zur Verfügung.

Sie finden diese Assistenten in der Navigationsleiste des FCI.

Für folgende Aufgaben können Sie Assistenten verwenden:

- Erste Schritte
- Internetzugang
- VPN
- SWYX (nur verfügbar, wenn in Ihrem Gerät ein DSP-Modul gesteckt und aktiv ist)
- Wireless LAN (nur verfügbar bei Geräten mit WLAN-Funktionalität).

Jeder Assistent führt Sie Schritt für Schritt durch die jeweilige Konfigurationsaufgabe. Sie können einen Assistenten gegebenenfalls mehr als einmal verwenden, um mehrere Verbindungen anzulegen.

Detaillierte Informationen finden Sie in der Hilfe zum jeweiligen Assistenten im entsprechenden Konfigurationsschritt.

2.2 Zeitzonenwahl für automatische Zeitumstellung

Ab Systemsoftware 7.9.1 erfolgt auf Ihrem Gerät die Umstellung von Sommer- auf Normalzeit im Herbst und von Normal- auf Sommerzeit im Frühling am jeweiligen Umschalttag automatisch.

Im FCI Menü ***Systemverwaltung*** ➜ ***Globale Einstellungen*** ➜ ***Datum und Uhrzeit*** können Sie im neuen Feld ***Systemzeitzone*** die gewünschte Zeitzone für Ihr System wählen (z. B. *Europe*/*Berlin*). Wenn für die gewählte Zeitzone Sommer- und Normalzeit festgelegt sind, erfolgt die Zeitumstellung am Umschalttag automatisch. Das Feld ***Zeitverschiebung von GMT*** wird nicht mehr benötigt und wurde entfernt.

Hinweis

Beachten Sie, dass die automatische Zeitumstellung unerwünschte Auswirkungen auf Ereignisse haben kann, die im Menü ***Lokale Dienste*** ➜ ***Scheduling*** konfiguriert sind.

Hinweis

Beachten Sie, dass die automatische Zeitumstellung bei der Umschaltung von Sommer- auf Normalzeit dazu führen kann, dass bei aufgezeichneten Ereignissen Zeitstempel doppelt auftreten.

2.3 Q-SIG

Ab Systemsoftware 7.9.1 steht das D-Kanal-Protokoll Q-SIG zur Verfügung.

Aktuell ist eine Teilmenge der verfügbaren Q-SIG-Funktionen implementiert, um Unified-Messaging-Lösungen zusammen mit unserem Partner Servonic zu realisieren.

Ein Servonic Unified Messaging System kann mit Hilfe eines bintec Gateways an eine Siemens Hicom TK-Anlage angebunden werden, z. B. an eine Hicom 300. Für die Anbindung wird der ISDN-Anlagenanschluss der Hicom verwendet; die Kommunikation zwischen Unified Messaging System und TK-Anlage

erfolgt über die bintec Remote CAPI. Um einem Nutzer des Unified Messaging Systems Vermittlungstechnische Leistungsmerkmale (Supplementary Services) zur Verfügung zu stellen, wird Q-SIG verwendet.

Folgende Q-SIG-Funktionen sind aktuell implementiert:

- Ein ausgehender Ruf wird an die gewünschte Gegenstelle weitergeleitet.
- Ein eingehender Ruf wird an die gewünschte interne Nebenstelle weitergeleitet und die Nummer des Anrufers wird signalisiert (gemäß ECMA 175/176/177/178).
- Ein eingehender Ruf wird von der gewünschten internen Nebenstelle, die z. B besetzt ist, an eine zweite Nebenstelle weitergeleitet und an der ersten Nebenstelle wird der Ruf signalisiert (MWI; gemäß EMCA 241/242).
- Ein eingehender Ruf wird von der gewünschten Nebenstelle an eine Mailbox weitergeleitet, der Ruf wird an der Nebenstelle signalisiert (MWI) und die Mailbox kann abgefragt werden (gemäß EMCA 241/242).

Um das Protokoll Q-SIG zu verwenden, wählen Sie das FCI Menü ***Physikalische Schnittstellen*** ➜ ***ISDN-Ports*** ➜ ***ISDN-Konfiguration*** ➜ ***Symbol zur Änderung eines Eintrags***. Schalten Sie ***Automatische Konfiguration beim Start*** aus und setzen Sie ***Port-Verwendung*** = *Q-SIG*.

2.4 ISAKMP Configuration Method (IKE Config Mode) im Client Modus

Mit Hilfe der ISAKMP Configuration Method (kurz IKE Config Mode) können Sie einen mobilen PC-Arbeitsplatz (bintec Secure IPSec Client) über IPSec an die Firmenzentrale anbinden.

Die IP-Adresse und auf Wunsch weitere Daten wie Domänen- und Serverparameter für DNS und WINS werden dem Client vom IPSec Gateway auf Anfrage zur Verfügung gestellt. Diese Methode ermöglicht die Zuteilung einer dynamischen IP-Adresse z. B. aus dem internen Adressbereich der Firmenzentrale (siehe Release Notes 7.8.2).

Ab **Systemsoftware 7.9.1** können Sie Ihr Gerät nicht nur wie bisher als Server sondern auch als Client für den IKE Config Mode konfigurieren; bisher konnten Sie als Client z. B. ein NCP Secure Client verwenden.

Im Menü ***VPN*** ➜ ***IPSec*** ➜ ***IPSec-Peers*** ➜ **Neu** wurde im Feld ***IP-Adressenvergabe*** anstelle von zwei Radiobuttons ein Dropdown-Menü implementiert, das die Werte *Statisch*, *Client für den IKE-Konfigurationsmodus* und *Server für den IKE-Konfigurationsmodus* enthält. Mit der neuen Einstellung *Client für den IKE-Konfigurationsmodus* können Sie Ihr Gateway als Client für den IKE Config Mode konfigurieren.

2.5 DHCP - Gateways im Auslieferungszustand in ein Netz integrieren

Ab Systemsoftware 7.9.1 können Geräte bei der ersten Inbetriebnahme nach der Auslieferung einfacher in ein Netz integriert werden als bisher. Abhängig vom Gerätetyp unterscheidet sich das Verhalten der Geräte, wenn noch keine Konfiguration vorhanden ist.

2.5.1 Wx002(n), WIx040, WIx065

Ein Gerät der Serien Wx002(n), WIx040 oder WIx065 startet als DHCP-Client im lokalen Netz. Es sendet DHCP-Anfragen und wartet auf die Antwort eines DHCP-Servers.

Wenn ein DHCP-Server antwortet, agiert das Gerät als DHCP-Client und nutzt die IP-Adresse, welche ihm der DHCP-Server zuweist.

Wenn kein DHCP-Server antwortet, behält das Gerät seine voreingestellte IP-Adresse *192.168.0.252*. Eine abweichende IP-Adresse können Sie ihm über das FCI oder das Setup Tool zuweisen.

Der oben beschriebene Startmodus des Geräts als DHCP-Client im Netz wird abgebrochen, wenn

- sich ein Benutzer über die serielle Schnittstelle einloggt.

- eine TCP Session zum Gerät gestartet wird (über Telnet oder mit dem FCI).
- eine feste IP-Adresse zugewiesen wird.

Der Startmodus wird ebenfalls abgebrochen, wenn ein DHCP- Server eine IP-Adresse zuweist. In diesem Fall agiert das Gerät weiterhin als DHCP-Client.

2.5.2 R2xx

Ein Gerät der R2xx-Serie startet als DHCP-Client und als BOOTP Client im Netz; es sendet nacheinander bis zu drei DHCP-Anfragen und bis zu fünf BOOTP-Anfragen.

Wenn ein DHCP-Server antwortet, benutzt das Gerät als eigene IP-Adresse den voreingestellten Wert *192.168.0.254* und sendet weiterhin BOOTP-Anfragen.

Wenn das Gerät eine BOOTP-Antwort z. B. von den Dime Tools empfängt, übernimmt es die zugewiesene IP-Adresse.

Wenn das Gerät keine Antwort erhält, agiert es als DHCP-Server und stellt einen IP-Adress-Pool mit 40 IP-Adressen zur Verfügung, beginnend mit der IP-Adresse *192.168.0.10*. Als eigene IP-Adresse wird der voreingestellte Wert *192.168.0.254* benutzt.

Hinweis

Wenn Sie das Gerät anschließend über das FCI oder das Setup Tool konfigurieren, achten Sie darauf, dass die eigene IP-Adresse und die IP-Adressen aus dem Adress-Pool konsistent bleiben.

Der oben beschriebene Startmodus als DHCP-Client und als BOOTP Client im Netz wird abgebrochen, wenn

- sich ein Benutzer über die serielle Schnittstelle einloggt.
- eine TCP Session gestartet wird (über Telnet oder mit dem FCI).
- eine feste IP-Adresse zugewiesen wird.

2.5.3 TR200aw/bw, R1xxx, R3xxx, R4xxx

Ein Gerät der Serien TR200aw/bw, R1xxx, R3xxx oder R4xxx startet als BOOTP-Client und sendet BOOTP-Anfragen. (Dieses Verhalten ist identisch mit dem Verhalten aller bintec-Geräte vor Systemsoftware 7.9.1.)

In jedem neu ausgelieferten Gerät ist die IP-Adresse *192.168.0.254* voreingestellt.

Wenn das Gerät auf seine BOOTP-Anfrage eine BOOTP-Antwort z. B. von den Dime Tools empfängt, übernimmt es die zugewiesene IP-Adresse.

Wenn Sie eine IP-Adresse über das FCI oder das Setup Tool zuweisen, benutzt das Gerät diese Adresse.

Der oben beschriebene Startmodus als BOOTP Client im Netz wird abgebrochen, wenn

- eine BOOTP-Antwort empfangen wird.
- sich ein Benutzer über die serielle Schnittstelle einloggt.
- eine TCP Session gestartet wird (über Telnet oder mit dem FCI).
- eine feste IP-Adresse zugewiesen wird.

2.6 SHDSL.bis (R3800)

Ab Systemsoftware 7.9.1 steht SHDSL.bis (ITU-T G.991.2) zur Verfügung, eine Erweiterung des SHDSL-Standards, die höhere Übertragungsraten ermöglicht. SHDSL.bis ist ausschließlich mit der Fimware RNY-SHDSL8bis-1.5.5.33.rny verwendbar. Für SHDSL.bis müssen alle Adernpaare einheitlich entweder im CPE-Modus oder im CO-Modus konfiguriert sein.

Folgende Übertragungsraten stehen maximal zur Verfügung:

Adernpaar(e) - Drähte	Modus	Maximale Übertragungsrate in Mbit/s
1 - 2	PHY Layer Bonding	5,7
2 - 4	PHY Layer Bonding	11,4
2 - 4	IMA	11,4
3 - 6	IMA	17,1
4 - 8	IMA	22,4

2.7 FCI - SNMP-Browser

Ab Systemsoftware 7.9.1 steht ein SNMP-Browser zur Verfügung.

Sie können diesen Browser in der Kopfleiste des FCI im Feld ***ANSICHT*** unter der Bezeichnung *SNMP-Browser* wählen.

Sie haben Zugriff auf alle MIB-Tabellen und -Variablen Ihres Systems und können diese anzeigen lassen und bearbeiten. Wenn Verbindung zum Internet besteht, ist eine Online-Hilfe für den SNMP-Browser verfügbar, die dynamisch vom FEC Web Server geladen wird.

2.8 Hot Spot

Ab Systemsoftware 7.9.1 können Sie Ihren Kunden über die neu implementierte Hot Spot Funktionalität einen Internetzugang zur Verfügung stellen.

Die sogenannte bintec Hotspot Solution ermöglicht die Bereitstellung von öffentlichen Internetzugängen mittels WLAN oder kabelgebundenem Ethernet. Die Lösung ist geeignet zum Aufbau kleinerer und größerer Hotspot-Lösungen für Cafes, Hotels, Unternehmen, Wohnheime, Campingplätze usw.

Die bintec Hotspot Solution besteht aus einem vor Ort installierten bintec Gateway (mit eigenem WLAN Access Point oder zusätzlich angeschlossenem WLAN-Gerät oder kabelgebundenem LAN) und aus dem Hotspot Server, der zentral in einem Rechenzentrum steht. Über ein Administrations-Terminal (z. B. dem Rezeptions-PC im Hotel) wird ein Betreiber-Konto auf dem Server verwaltet, z. B. zum Erfassen von Registrierungen, zum Erzeugen von Tickets, für statistische Auswertungen usw.

Im Menü ***Lokale Dienste*** ➜ ***Hotspot-Gateway*** ➜ ***Hotspot-Gateway*** ➜ **Neu** konfigurieren Sie das vor Ort installierte bintec Gateway für die bintec Hotspot Solution.

Hinweis

Benutzen Sie zum Einloggen ssh an Stelle von telnet, wenn Sie Login Authentication via RADIUS konfigurieren (d.h. wenn Sie im Menü ***Syytemverwaltung*** ➜ ***Remote Authentifizierung*** ➜ ***RADIUS*** ➜ **Neu** das Feld ***Authentifizierungstyp*** = *Login-Authentifizierung* setzen).

Im Menü ***Monitoring*** ➜ ***Hotspot-Gateway*** ➜ ***Hotspot-Gateway*** können Sie Ihr Hotspot-Gateway überwachen und eine Liste aller verbundenen Hosts einsehen.

Detaillierte Informationen zur bintec Hotspot Solution finden Sie im FCI in der Online Hilfe zu Ihrem bintec Gerät.

2.9 VoIP - Lizenz für interne Teilnehmernummern (TR200)

Zehn interne Teilnehmernummern stehen für VoIP kostenlos zur Verfügung, für weitere Nummern benötigen Sie eine Lizenz.

Ihr System verfügt standardmäßig über zehn interne Teilnehmernummern. Die Lizenzierung weiterer Nummern erfolgt in Blöcken zu zehn Nummern, die zu den vorhandenen Nummern hinzugefügt werden bis maximal 40 Nummern erreicht sind.

Sie sehen die aktuell verfügbaren internen Teilnehmernummern im FCI Menü ***PBX*** ➜ ***Interne Rufnummern*** ➜ ***VoIP***.

Der Lizenzierungsmechanismus ist derselbe wie bei IPSec, die Bezeichnung einer VoIP-Lizenz für jeweils zehn Teilnehmernummern lautet *SNxSIP10*. Sie können die neuen Lizenzdaten nach der Online Lizenzierung im Menü ***Systemverwaltung*** ➜ ***Globale Einstellungen*** ➜ ***Systemlizenzen*** ➜ **Neu** eintragen. Wenn das Maximum von 40 Nummern erreicht ist, wird die Schaltfläche **Neu** ausgeblendet.

Wenn eine Konfiguration geladen wird, die mehr Teilnehmernummern enthält als lizensiert sind, so erscheint eine Warnung. Sie werden aufgefordert, Einträge zu löschen.

2.10 Fax-Lizenz (R4100)

Systemsoftware 7.9.1 bietet Ihnen für das Gerät R4100 mit 30-Kanal-DSP-Modul eine FAX-Unterstützung an. Sie benötigen dazu eine Lizenz.

Mit Lizenz ist eine FAX-Unterstützung über die Protokolle T.30 und T.38 verfügbar.

Der Lizenzierungsmechanismus ist derselbe wie bei IPSec, die Bezeichnung für eine FAX-Lizenz lautet *R4xFAX30*. Sie können die neuen Lizenzdaten nach der Online Lizensierung im Menü ***Systemverwaltung*** ➜ ***Globale Einstellungen*** ➜ ***Systemlizenzen*** ➜ **Neu** eintragen.

Wenn eine FAX-Lizenz aktiv ist, wird sie im Menü ***Systemverwaltung*** ➜ ***Status*** im Feld ***DSP-Modul*** angezeigt.

2.11 Befehl cert get mit HTTPS

Ab Systemsoftware 7.9.1 ist der Befehl *cert get* zum Import von Zertifikaten über HTTPS verfügbar.

2.12 Scheduler - Platzhalter für Seriennummer verfügbar

Mit Systemsoftware 7.9.1 können Sie im Scheduler in Befehlen die Zeichenfolge SN als Platzhalter für die Seriennummer benutzen.

Sie können z. B. im Setup Tool Menü ***System*** ➜ ***Schedule & Monitor*** ➜ ***Event Scheduler (Time & SNMP)*** ➜ ***Schedule Commands*** ➜ **ADD** das Feld ***Set value active*** = *get_all;http://10.9.1.2/tftp:file SN.cf* setzen, um die Konfigurationsdateien mehrerer Gateways zu holen.

2.13 WLAN - 5.8 GHz Band für UK verfügbar

Ab Systemsoftware 7.9.1 kann mit der Ländereinstellung UK das Frequenzband 5.8 GHz verwendet werden.

2.14 USB 2.0 hinzugefügt

Mit Systemsoftware 7.9.1 wurde der Standard USB 2.0 hinzugefügt, um den Kartentyp OPTION GE0421 (z. B. die Karte Mobile Connect Card Vodafone E3730) und den USB Stick Sierra Wireless Compass 885 zu unterstützen.

2.15 DynDNS Provider www.dnsexit.com verfügbar

Mit Systemsoftware 7.9.1 ist der DynDNS Provider www.dnsexit.com verfügbar.

2.16 FCI - RADIUS - Konfigurationsmöglichkeiten erweitert

Im FCI Menü *Systemverwaltung* ➜ *Remote Authentifizierung* ➜ *RADIUS* ist im Feld *Gruppenbeschreibung* die neue Auswahlmöglichkeit *Default Group 0* **verfügbar.**

Diese Einstellung wird z. B. für die Konfiguration eines Hotspot benötigt.

2.17 FCI - UMTS - Neues Feld verfügbar

Im FCI Menü *Physikalische Schnittstellen* ➜ *UMTS/HSDPA* ist das neue Feld *Modem-Status* verfügbar.

2.18 FCI - SHDSL - Neues Feld verfügbar

Im FCI Menü *Physikalische Schnittstellen* ➜ *SHDSL* ➜ *SHDSL-Konfiguration* ist für die IMA-Konfiguration (*Leitungsmodus* = *4-Draht-IMA*, *6-Draht-IMA* **oder** *8-Draht-IMA*) **das neue Feld *Minimale Anzahl aktiver Links* verfügbar.**

2.19 FCI - WLAN - Neues Feld EAP-Vorabauthentifizierung verfügbar

Ab Systemsoftware 7.9.1 ist im FCI Menü *Wireless LAN* ➜ *WLANx* ➜ *Drahtlosnetzwerke (VSS)* ➜ Neu/Symbol zur Änderung eines Eintrags mit der Einstellung *Sicherheitsmodus* = *WPA-Enterprise* **das neue Feld *EAP-Vorabauthentifizierung* verfügbar.**

2.20 FCI - WDS-Links - Konfigurationsmöglichkeiten erweitert

Im FCI Menü *Wireless LAN* ➜ *WLANx* ➜ *WDS-Links* ➜ Neu sind im Feld *Schutz* die neuen Werte *WPA* und *WPA2* verfügbar.

2.21 FCI - WLAN - WDS mit AES und TKIP möglich

Mit Systemsoftware 7.9.1 können bei der Konfiguration von WDS-Links im Access-Point-Modus auch AES und TKIP zur Verschlüsselung ausgewählt werden.

2.22 FCI - IPSec - Mehrere Benutzer über denselben Peer

Ab Systemsoftware 7.9.1 kann im FCI ein IPSec-Peer so konfiguriert werden, dass sich mehrere Benutzer über diesen IPSec-Peer einwählen können.

Wählen Sie dazu das FCI Menü ***VPN*** ➜ ***IPSec*** ➜ ***IPSec-Peers*** ➜ **Neu** ➜ **Erweiterte Einstellungen** und setzen Sie ***Anzahl erlaubter Verbindungen*** = *Mehrere Benutzer*. Wir empfehlen Ihnen zusätzlich im Feld ***IP-Adressvergabe*** = *Server für den IP-Konfigurationsmodus* zu setzen.

2.23 FCI - Neues Feld Faxkopfzeile verfügbar

Im FCI Menü *Lokale Dienste* ➜ *CAPI-Server* ➜ *Optionen* ist bei installiertem DSP-Modul das Feld *Faxkopfzeile* verfügbar.

Mit dem Feld ***FAXKOPFZEILE*** können Sie festlegen, ob am oberen Rand eines ausgehenden Fax eine Kopfzeile gedruckt werden soll.

2.24 FCI - Scheduler abschaltbar

Im FCI Menü *LOKALE DIENSTE* ➜ *SCHEDULING* ➜ *OPTIONEN* ist das neue Feld *SCHEDULE-INTERVALL* verfügbar.

Sie können das Feld ***SCHEDULE-INTERVALL*** aktivieren oder deaktivieren, um den Scheduler ein- oder ausschalten.

2.25 Setup Tool - PUK-Eingabe verfügbar

Im Setup Tool Menü UMTS6-0 wurde das Feld *SIM CARD USES PUK* hinzugefügt.

Der Personal Unblocking Key (PUK) dient zum Entsperren der UMTS-Modemkarte, wenn die PIN mehrmals (d.h. bei den meisten Karten dreimal) falsch eingegeben wurde.

2.26 Setup Tool - ISDN Statistik

Ab Systemsoftware 7.9.1 ist im Setup Tool Menü *MONITORING & DEBUGGING* ➜ *ISDN MONITOR* über den Befehl *s* die Statistik auch für beendete Anrufe verfügbar und nicht wie bisher nur für aktuelle Anrufe.

2.27 Neue MIB-Variable HttpRedirect

Mit Systemsoftware 7.9.1 ist in der MIB-Tabelle ipExtIfTable die neue MIB-Variable HttpRedirect verfügbar.

Mit der Variablen ***HTTPREDIRECT*** können Sie HTTP-Anfragen auf einer Schnittstelle entweder mit dem Wert *local* auf den lokalen HTTP Dämon oder mit dem Wert *proxy* auf den lokalen Content Filter umleiten.

3 Änderungen

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

3.1 Java SNMP Browser entfernt

Ab **Systemsoftware 7.9.1** ist der Java SNMP Browser entfernt.

3.2 HTML Setup Tool entfernt

Ab **Systemsoftware 7.9.1** ist das HTML Setup Tool entfernt.

3.3 Funktionalität Credits entfernt

Ab **Systemsoftware 7.9.1** ist die Funktionalität Credits entfernt.

3.4 Befehl dmesg erweitert

Mit **Systemsoftware 7.9.1** wird der Befehl dmesg um die Option -t erweitert, um den Inhalt des Kernelpuffers ab dem Zeitpunkt des Befehlsaufrufs auszugeben.

3.5 Preshared Keys - Warnung hinzugefügt

Folgende Warnung wurde in **Systemsoftware 7.9.1** hinzugefügt, um den Benutzer aufzufordern, die Standardeinstellung des Preshared Key zu ändern,: "Ändern Sie unbedingt den Standard Preshared Key! Solange der Key nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!"

3.6 SIF Alias Namen für Schnittstellen geändert

Ab **Systemsoftware 7.9.1** sind die SIF Alias Namen für Schnittstellen verbessert, um Missverständnissen vorzubeugen. Es kann jetzt zwischen folgenden Kategorien unterschieden werden: LAN, WLAN, IPSec, Leased, Bundle und Bridge. Beispielsweise heißt die bisherige Schnittstelle *LAN_PEER_2_R4100_1* ab sofort *IPSEC_PEER_2_R4100_1*.

3.7 FCI - Zusätzliche Zugriffsregel

Wenn zum ersten Mal eine Regel für den administrativen Zugriff erstellt wird, wird automatisch eine zusätzliche Regel erstellt, die sicher stellt, dass kein Datenverkehr ungewollt blockiert wird.

3.8 FCI - Status - Schnittstellen umbenannt

Im FCI Menü ***Systemverwaltung*** ➜ ***Status*** wurde die Schnittstelle *com6-0* in *USB/UMTS* und die Schnittstelle *bri4-0* in *ISDN* umbenannt.

3.9 FCI - WLAN - Einstellmöglichkeiten Funkmodul geändert

Ab **Systemsoftware 7.9.1** sind im FCI Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Einstellungen Funkmodul*** ➜ **Symbol zur Änderung eines Eintrags** die Einstellmöglichkeiten geändert. Das Feld ***Funkmodul*** wurde entfernt, das Feld ***Betriebsmodus*** enthält aktuell die Auswahlmöglichkeiten ***Aus***, ***Access-Point***, ***Access Client*** und ***Bridge***.

3.10 FCI - Drahtlosnetzwerke (VSS) mit Sicherheitsmodus

Ab **Systemsoftware 7.9.1** ist für das standardmäßig angezeigte VSS im FCI Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Drahtlosnetzwerke (VSS)*** ➜ **Symbol zur Änderung eines Eintrags** der Wert ***Sicherheitsmodus*** = *WPA-PSK* voreingestellt.

3.11 FCI - DNS - Feld umbenannt

Im FCI Menü ***Lokale Dienste*** ➜ ***DNS*** ➜ ***Statische Hosts*** wurde das Feld ***Beschreibung*** in ***DNS-Hostname*** umbenannt.

3.12 Setup Tool - Cobion Orange Filter - Feld umbenannt

Im Setup Tool Menü ***Security*** ➜ ***Cobion Orange Filter*** wurde das Feld ***Filtered Interface*** in ***Filtered Source Interface*** umbenannt.

3.13 Setup Tool - QoS - Wertebereich vergrößert

Im Setup Tool Menü ***QoS*** ➜ ***Interfaces and Policies*** ➜ **Edit** ➜ ***QoS Scheduling and Shaping*** wird mit der Einstellung ***Queueing and Scheduling Algorithm*** = *priority queueing (PQ)* und ***Specify Traffic Shaping*** = ***yes*** das Feld ***Maximum Transmit Rate (Bits per Second)*** angezeigt. Der Wertebereich dieses Feldes wurde von *100000000* auf *1000000000* vergrößert.

3.14 Bei ausgehenden Rufen der eigenen Rufnummer Parameter mitgeben

Um bei ausgehenden Rufen der eigenen Rufnummer bestimmte Parameter nach Q.931 "mitgeben" zu können, kann in der MIB-Tabelle ***biboDialTable*** die MIB-Variable ***Screening*** auch für ausgehende Rufe verwendet werden. Darüber hinaus steht für diesen Zweck die neue MIB-Variable ***TypeOfLocalNumber*** zur Verfügung.

3.15 MIB-Tabelle wlanIfTable ergänzt

Die MIB-Variable ***BAND*** ist jetzt nur noch in der MIB-Tabelle ***WLANIFTABLE*** enthalten (und nicht mehr als redundante Information in der Tabelle ***WLANCLIENTTABLE***). Ebenfalls in der MIB-Tabelle ***WLANIFTABLE*** wurden in der MIB-Variablen ***MODE*** die Werte *m802-11abgn*, *m802-11abg* und *m802-11agn* hinzugefügt.

4 Gelöste Probleme

Nicht alle im Kapitel “Wichtige Informationen” auf Seite 9 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 7.9.1 gelöst worden:

4.1 Serielle Schnittstelle nicht verfügbar

(ID 12240)

Die serielle Schnittstelle war nicht verfügbar, weil in der MIB-Tabelle ***AUXCONFIGTABLE*** die Einträge nicht automatisch erstellt wurden.

Das Problem ist gelöst.

4.2 Stacktrace nach Eingabe von dmesg

(ID 12104)

Nach Eingabe des Befehls *dmesg* folgte ein Stacktrace.

Das Problem ist gelöst.

4.3 Setup Tool - Stacktrace wegen Speicherverlust

(ID n/a)

Clients mit falschem Preshared Key versuchten sich immer wieder zu verbinden und verursachten daher einen Stacktrace wegen Speicherverlust.

Das Problem ist gelöst.

4.4 Setup Tool - Stacktrace wegen falscher Lifetime Policy

(ID 12531)

Wenn im Setup Tool bei Konfiguration von IPSec bei einer Eingabe im Feld ***LIFETIME POLICY*** der vorgegebene Wertebereich von *0 .. 4294967295* überschritten wurde, folgte ein Stacktrace. Dabei machte es keinen Unterschied, ob die Eingabe in Sekunden oder in KByte erfolgte.

Das Problem ist gelöst.

4.5 PIM - Stacktrace

(ID n/a)

Beim Herunterfahren von PIM trat ein Stacktrace auf, wenn die entsprechende Schnittstelle nicht verfügbar war.

Das Problem ist gelöst.

4.6 Stacktrace bei trace über DSL

(ID 12392)

Ein trace der Tunnel-Schnittstelle über DSL bei einer Tunnelverbindung unter Last verursachte einen Stacktrace.

Das Problem ist gelöst.

4.7 Bridge Link - Keine Verbindung

(ID 11978)

Trotz eines WDS-Links (Bridge-Links) mit dem Status *up*, war kein IP-Datenverkehr möglich.

Das Problem ist gelöst.

4.8 PPP-Verbindungen fehlgeschlagen

(ID 11303)

In seltenen Fällen konnte es dazu kommen, dass der Aufbau einer PPP-Verbindung scheiterte und das Interface blockierte, bis es manuell zurückgesetzt oder neu gestartet wurde.

Das Problem ist gelöst.

4.9 IPSec - Probleme beim Aufbau der Phase 2

(ID 12163)

Beim Aufbau der Phase 2 einer IPSec-Verbindung konnte es zu Problemen aufgrund der Auswahl der Quelladresse kommen.

Das Problem ist gelöst.

4.10 IPSec - trace zeigte UDP Pakete nicht an

(ID 12455)

Bei einem trace eines IPSec Tunnels wurden die Datenpakete nicht angezeigt, die vom Router mit hoher Priorität gesendet wurden.

Das Problem ist gelöst.

4.11 IPSec - IKE Config Mode - Eintrag in MIB-Tabelle ipDynaAddrTable falsch

(ID 12471)

Im IKE Config Mode enthielt die MIB-Tabelle ***ipDynaAddrTable*** den Eintrag ***ifIndex*** = *10001* (an Stelle von ***ifIndex*** = *100002* für den IPSec Peer).

Das Problem ist gelöst.

4.12 IPSec - Keine Verbindung mit Zertifikat

(ID 11313)

Mit IPSec konnte über RADIUS keine Verbindung aufgebaut werden, wenn ein Zertifikat benutzt wurde, in welchem der Parameter User-Name eine Länge von 64 Zeichen überschritt.

Das Problem ist gelöst.

4.13 FCI - Falscher Annex-Typ wählbar

(ID n/a)

Im FCI konnte auch für Annex-B-Geräte bei der ADSL-Konfiguration Annex M ausgewählt werden.

Das Problem ist gelöst.

4.14 WLAN - Verbindung zum Gateway nicht möglich

(ID 12271)

Eine Verbindung über WLAN zum Gateway war nicht möglich, da die Zahl der maximal möglichen Clients fälschlicherweise auf den Wert *0* gesetzt war und daher alle Clients zurückgewiesen wurden.

Das Problem ist gelöst.

4.15 WLAN - Probleme mit automatischer Konfiguration im Bridge-Link -Modus

(ID 11424)

Beim Aufbau eines Bridge Links im 5 GHz-Band und mit 40 MHz Bandbreite konnte es zu unvorhergesehenen und unerwünschten Ergebnissen (wie nicht funktionsfähigen Verbindungen oder geringem Datendurchsatz) kommen.

Das Problem ist gelöst.

4.16 WLAN - Clients fälschlicherweise zurückgewiesen

(ID 11254)

Nachdem einige Clients, die mit dem Gateway im Access-Point-Modus verbunden waren, zurückgewiesen wurden, weil sie beim RADIUS Server nicht registriert waren, wurden fälschlicherweise danach alle Clients zurückgewiesen und das Gerät musste gebootet werden.

Das Problem ist gelöst.

4.17 WLAN - WDS Scan nicht möglich

(ID 11621)

Solange das Radiomodul nicht vollständig initialisiert war, erfolgte keine Fehlermeldung, wenn versucht wurde, einen WDS Scan durchzuführen.

Das Problem ist gelöst.

4.18 Speichern der Konfiguration fehlgeschlagen

(ID 12251)

Es konnte vorkommen, dass bei wenig freiem Speicherplatz im Flash eine Boot-Konfiguration nicht korrekt gespeichert werden konnte und keine Fehlermeldung erschien.

Das Problem ist gelöst.

4.19 Mehrfacheinwahl über Hotspot fälschlicherweise möglich

(ID 11363)

Mit ein- und demselben RADIUS Account konnte man sich mittels Hotspot über verschiedene Clients einwählen.

Das Problem ist gelöst.

4.20 Media Gateway - Sprachverbindung unidirektional

(ID 12407)

Nach einer CAPI- oder isdnlogin-Verbindung schlug ein Ruf über das Media Gateway auf demselben Port fehl, die Sprachverbindung funktionierte nur in eine Richtung.

Das Problem ist gelöst.

4.21 Sprachverbindungen unidirektional

(ID 10776)

Nach RAS-Einwahl in das Gateway funktionierten Sprachverbindungen nur in eine Richtung.

Das Problem ist gelöst.

4.22 SNR Margins falsch angezeigt

(ID 12276)

Für ADSL1-Links wurden mit den Firmware Versionen 6.2.12 / E.74.2.53 und 6.2.13 / E.74.2.55 für Annex B zu hohe SNR Margins in den Syslog Messages oder mit Hilfe des Befehls *dsl status* angezeigt. Im Setup Tool Menü ***MONITORING AND DEBUGGING*** ➜ ***ADSL*** und in der MIB-Tabelle ***ADSLATUCPHYSTABLE*** wurden ebenfalls falsche Werte angezeigt, die außerdem von den oben erwähnten Werten abwichen.

Das Problem ist gelöst.

4.23 Multicast nicht funktionsfähig

(ID n/a)

Es konnte vorkommen, dass Multicast nicht funktionierte, weil es mehrmals aktiviert wurde.

Das Problem ist gelöst.

4.24 Multicast - Weiterleiten von Paketen fehlgeschlagen

(ID n/a)

In Szenarien mit Source Specific Multicast (SSM) schlug das Weiterleiten von Paketen fehl.

Das Problem ist gelöst.

4.25 Multicast auf IPSec-Schnittstellen fehlgeschlagen

(ID n/a)

Auf IPSec-Schnittstellen konnten keine Multicast-Pakete übertragen werden.

Das Problem ist gelöst.

4.26 Multicast - Timer Problem

(ID n/a)

Es konnte vorkommen, dass auf einer Schnittstelle sehr viele Queries und Reports versendet bzw. empfangen wurden.

Das Problem ist gelöst, die Timer sind angepasst worden.

4.27 RADIUS Reload funktionierte nicht

(ID n/a)

Ein nicht funktionierender RADIUS Dialout Reload verursachte eine Endlosschleife von Get Requests.

Das Problem ist gelöst.

4.28 FCI - Texte falsch angezeigt

(ID 12268)

Im FCI wurden einige Texte HTML-kodiert angezeigt.

Das Problem ist gelöst, die Texte werden korrekt angezeigt.

4.29 FCI - Systemverwaltung - Irrtümliche Fehlermeldung

(ID 11470)

Wenn im FCI Menü ***Systemverwaltung*** ➜ ***Administrativer Zugriff*** ➜ ***Zugriff*** versucht wurde, die Einstellungen zu ändern, wurde die Fehlermeldung "Der Wert muss größer oder gleich dem folgenden sein: 0" angezeigt und es waren keine Änderungen möglich.

Das Problem ist gelöst.

4.30 FCI - WLAN - Menü *Bridge-Links* unvollständig

(ID 12463)

Wenn im FCI Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Einstellungen Funkmodul*** ➜ ***Symbol zur Änderung eines Eintrags*** die Einstellung ***Betriebsmodus*** = *Bridge* gesetzt war und auf die Schaltfläche **OK** geklickt wurde, fehlte unter ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Bridge-Links*** der standardmäßig angelegte Eintrag.

Das Problem ist gelöst.

4.31 FCI - WLAN - Menü *WDS-Links* fehlte

(ID 11616)

Wenn im FCI Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Einstellungen Funkmodul*** ➜ ***Symbol zur Änderung eines Eintrags*** die Einstellungen ***Betriebsmodus*** = *Access-Point*, ***Frequenzband*** = *5 GHz Indoor* und ***Ausgewählter Kanal*** ungleich *Auto* gesetzt waren und auf die Schaltfläche **OK** geklickt wurde, fehlte der Reiter ***WDS-Links*** und das entsprechende Menü.

Das Problem ist gelöst.

4.32 FCI - Max. Link-Entfernung fälschlicherweise angezeigt

(ID 12237)

Im Menü FCI ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Einstellungen Funkmodul*** ➜ **Symbol zur Änderung eines Eintrags** wurde das Feld ***Max. Link-Entfernung*** für alle WLAN-Schnittstellen angezeigt, obwohl es nur für Bridge Links sinnvoll ist.

Das Problem ist gelöst, das Feld ***Max. Link-Entfernung*** wird ausschließlich für die Einstellung ***Betriebsmodus*** = *Bridge* angezeigt.

4.33 FCI - IPSec - Peers nicht angezeigt

(ID 12213)

Im Menü FCI ***VPN*** ➜ ***IPSec*** ➜ ***IPSec-Peers*** wurden Peers nicht angezeigt, die über Traffic Listen konfiguriert waren, im Menü ***Monitoring*** ➜ ***IPSec*** wurden diese Peers angezeigt.

Das Problem ist gelöst.

4.34 FCI - IPSec - Falsche Einstellmöglichkeit

(ID 12200)

Wenn im FCI Menü ***VPN*** ➜ ***IPSec*** ➜ ***IPSec-Peers*** ➜ **Neu** das Feld ***IP-Adressvergabe*** = *Client im IKE-Konfigurationsmodus* gesetzt war, konnte in das Feld ***Lokale IP-Adresse*** eine IP-Adresse eingegeben werden.

Das Problem ist gelöst, das Feld ***Lokale IP-Adresse*** wird im oben beschriebenen Fall nicht mehr angezeigt.

4.35 FCI - DNS-Namen nicht akzeptiert

(ID 12227)

Im Menü FCI ***VPN*** ➜ ***PPTP*** ➜ ***PPTP-TUNNEL*** ➜ **Neu** wurden im Feld ***ENTFERNTE PPTP-IP-ADRESSE*** ausschließlich IP-Adressen und keine DNS-Namen akzeptiert.

Das Problem ist gelöst, es werden IP-Adressen und DNS-Namen, z. B. *xyz.dyndns.org* akzeptiert.

4.36 FCI - ISDN fälschlicherweise wählbar

(ID 12347)

Bei Geräten ohne ISDN war fälschlicherweise im FCI Menü ***VPN*** ➜ ***PPTP*** ➜ ***PPTP-TUNNEL*** ➜ **Neu** ➜ ***ERWEITERTE EINSTELLUNGEN*** das Feld ***CALLBACK*** verfügbar. Wenn Callback eingeschaltet war, wurden die Felder ***EINGEHENDE ISDN-NUMMER*** und ***AUSGEHENDE ISDN-NUMMER*** angezeigt.

Das Problem ist gelöst, die Felder werden nicht mehr angezeigt.

4.37 FCI - PPTP - Feld nicht angezeigt

(ID 12435)

Für Windows XP (SP2) PPTP-Clients benötigen Sie im FCI Menü ***VPN*** ➜ ***PPTP*** ➜ ***OPTIONEN*** die Einstellung ***GRE-WINDOW-ANPASSUNG*** = *deaktiviert* und ***GRE-WINDOW-GRÖßE*** = *256*. Wenn ***GRE-WINDOW-ANPASSUNG*** deaktiviert war, wurde das Feld ***GRE-WINDOW-GRÖßE*** nicht angezeigt und es konnte daher kein Wert eingegeben werden.

Das Problem ist gelöst.

4.38 FCI - Firewall - Falsche Anzeige

(ID 12269)

Wenn im FCI Menü ***Firewall*** ➜ ***Adressen*** ➜ ***Adressliste*** ➜ ***Neu*** das Feld ***Adresstyp*** = *Adressbereich* gesetzt war, so wurde im Feld ***Adressbereich*** als zweiter Wert *255.255.255.255* angezeigt. Wenn im Menü ***Firewall*** ➜ ***Adressen*** ➜ ***Adressliste*** ➜ ***Neu*** das Feld ***Adresstyp*** = *Adresse/Subnetz* gesetzt war, so wurde im Feld ***Adresse/Subnetz*** für das Subnetz kein voreingestellter Wert angezeigt.

Das Problem ist gelöst.

4.39 FCI - Media Gateway - Falsche Anzeige

(ID 12356)

Im FCI Menü ***VoIP*** ➜ ***Media Gateway*** ➜ ***SIP-Konten*** wurde mit ***Trunk-Modus*** = *Server* das Feld ***Registrar*** angezeigt.

Das Problem ist gelöst, das Feld ***Registrar*** wird im oben beschriebenen Fall nicht mehr angezeigt.

4.40 FCI - Media Gateway - Feld Status fehlte

(ID 12245)

Das Media Gateway ist standardmäßig ausgeschaltet. Wegen des fehlenden Feldes ***Status des Media Gateways*** im FCI Menü ***VoIP*** ➜ ***Media Gateway*** ➜ ***Optionen*** konnte es nicht eingeschaltet werden.

Das Problem ist gelöst.

4.41 FCI - ISDN-Diebstahlsicherung - Falsche Auswahl

(ID 12295)

Im FCI Menü ***Lokale Dienste*** ➜ ***ISDN-Diebstahlsicherung*** ➜ ***Optionen*** konnten mit aktiviertem ***ISDN-Diebstahlsicherungsdienst*** unter ***Überwachte Schnittstellen*** u.a. die Ethernet-Schnittstellen ausgewählt werden.

Das Problem ist gelöst, die Ethernet-Schnittstellen sind unter ***Überwachte Schnittstellen*** nicht mehr wählbar.

4.42 FCI - Wartung - Irritierende Meldung

(ID 11849)

Im FCI Menü ***Wartung*** ➜ ***Software & Konfiguration*** folgte auf jede durchgeführte ***Aktion*** die Meldung "The system must be restarted."

Das Problem ist gelöst. Es werden ab sofort abhängig von der durchgeführten Aktion unterschiedliche Meldungen angezeigt.

Bei ***Aktion*** = *Kopieren*, *Umbenennen*, *Konfiguration löschen* oder *Konfiguration importieren* wird die Meldung "Would you like to reboot now? Changes to boot config will be activated after reboot." angezeigt.

Bei ***Aktion*** = *Sprache importieren* oder *Datei löschen* wird die Meldung "You must log in again to activate changes" angezeigt.

Bei den übrigen Auswahlmöglichkeiten im Feld ***Aktion*** wird die Meldung "Would you like to reboot now? Changes will be activated after reboot." angezeigt.

4.43 FCI - Wartung - Keine Datei verfügbar

(ID 12137)

Im FCI Menü ***Wartung*** ➜ ***Software & Konfiguration*** ➜ ***Optionen*** konnte mit ***Aktion*** = *Konfiguration löschen* im Feld ***Datei auswählen*** keine Datei gewählt werden.

Das Problem ist gelöst.

4.44 FCI - WDS-Statusanzeige falsch

(ID 12176)

Im FCI Menü ***Monitoring*** ➜ ***WLAN*** ➜ ***WDS*** wurde *Kein Link* angezeigt, obwohl ein normaler WDS-Link (kein WDS Bridge Link) aktiv und funktionsfähig war.

Das Problem ist gelöst.

4.45 FCI/Setup Tool - E-Mail-Benachrichtigung für WLAN fehlte

(ID 11554)

Sowohl im FCI als auch im Setup Tool konnte für eine E-Mail-Benachrichtigung kein WLAN ausgewählt werden. Im FCI war im Menü ***Externe Berichterstattung*** ➜ ***E-Mail-Benachrichtigung*** ➜ ***E-Mail-Benachrichtigungsempfänger*** kein ***Subsystem*** *WLAN* verfügbar. Im Setup Tool Menü ***Monitoring and Debugging*** ➜ ***Email Alert*** ➜ ***ADD*** war unter ***Select subsystems*** kein *WLAN* verfügbar.

Das Problem ist gelöst.

4.46 Setup Tool - Scheduler - Falsches Intervall nach Änderung

(ID 12096)

Wenn im Setup Tool Menü ***System*** ➜ ***Schedule & Monitor*** ➜ ***Event Scheduler (Time & SNMP)*** ➜ ***Schedule Commands*** ➜ **ADD** beispielsweise für das Feld ***Set value active*** = *1800* gesetzt wurde, während vorher *10* gesetzt war, so wurde nach Speicherung der Änderung noch einmal der Wert *10* verwendet und erst beim nächsten Mal *1800*.

Das Problem ist gelöst.

4.47 Setup Tool - Port 1 fälschlicherweise auf disabled gesetzt

(ID 12567)

Wenn bei einem Gerät im Auslieferungszustand das Setup Tool Menü ***Fast Ethernet*** ➜ ***Switch Configuration*** gewählt und mit **Save** verlassen wurde, wurde Port 1 auf disabled gesetzt und es gab keine Möglichkeit, dies zu ändern.

Das Problem ist gelöst.

4.48 Setup Tool - Standleitung - Fehler bei Auswahl der Timeslots

(ID 11323)

Wenn im Setup Tool Menü ***PRI2-4*** das Feld ***ISDN Switch Type*** = *leased line, chan. B1..B31* gesetzt ist und unter ***PRI2-4*** ➜ ***Bundle Confguration*** ➜ ***ADD*** das Feld ***Bundle Type*** = *PPP Multilink* gewählt ist, so sind in diesem Menü alle Timeslots standardmäßig gewählt, auch wenn sie mit **Save** gespeichert werden. Wenn ein Timeslot, z. B. Timeslot 11, aus der Auswahl entfernt wurde und

der Cursor zum folgenden Timeslot bewegt wurde, waren alle Timeslots aus der Auswahl entfernt.

Das Problem ist gelöst.

4.49 Setup Tool - IPSec - Blockierte Verbindung

(ID 12115)

Wenn im Setup Tool Menü ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND** ➜ ***IPSEC CALLBACK*** die Felder ***ISDN CALLBACK*** = *both*, ***TRANSFER OWN IP ADDRESS OVER ISDN*** = *yes* und ***MODE*** = *use B channel* gesetzt waren, traten Probleme mit Callback auf und es konnte unter Umständen keine Verbindung aufgebaut werden.

Das Problem ist gelöst.

4.50 Setup Tool - Problem mit SHDSL IMA Konfiguration

(ID 12538)

Im Setup Tool Menü ***SHDSL8*** ➜ **Edit** ➜ ***IPSEC CALLBACK*** konnte mit der Einstellung ***WIRE MODE*** = *4 wire IMA*, *6 wire IMA* oder *8 wire IMA* im Menü ***IMA CONFIGURATION*** der Wert des Feldes ***MINIMUM NUMBER OF LINKS*** nicht gespeichert werden.

Das Problem ist gelöst.

4.51 Falsche Einträge in der MIB-Tabelle ipHostAccessClientTable

(ID n/a)

In der MIB-Tabelle ***IPHOSTACCESSCLIENTTABLE*** blieben nach einem Reboot versehentlich einige Einträge bestehen.

Das Problem ist gelöst, die Einträge werden bei einem Reboot gelöscht.