funkwerk
enterprise communications

Wx002-, WIx040-, WIx065-Serie

Release Notes
Systemsoftware 7.8.2

Version 1.0

Ziel und Zweck

Dieses Dokument beschreibt neue Funktionen, Änderungen und behobene Fehler in **Systemsoftware 7.8.2**.

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

1.1 Gültigkeit

Systemsoftware 7.8.2 steht ausschließlich für folgende Geräte zur Verfügung und kann auf anderen Geräten nicht eingesetzt werden:

- **W1002**
- **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

Bei den Geräten **W1002** und **W2002** wird, sofern Sie sie unter ACE betreiben, mit **Systemsoftware 7.8.2** das Betriebssystem auf BOSS umgestellt. Die Geräte der **WI**-Serie werden bereits mit dem Betriebssystem BOSS ausgeliefert.

Konfigurationen, die unter **Systemsoftware 7.8.2** erstellt oder gesichert werden, sind daher zu früheren Versionen unserer Systemsoftware, die unter dem Betriebsystem ACE erstellt wurden, inkompatibel.

Hinweis

Beachten Sie, dass die Konfiguration Ihres Geräts während eines Updates verlorengeht.

Die folgende Tabelle gibt einen Überblick über die verfügbaren Updates und Update-Mechanismen:

Gerät	aktuell laufende Software	neue Software	Mechanismus
Wx002	ACE	7.8.2 Downgrade nach ACE möglich	**ComPoint Manager** bzw. Konsole
	7.6.2	7.8.2 Downgrade nach ACE möglich	Konsole oder FCI

1.2.1 Vorbereitung und Update (W1002 und W2002)

Bei einem Update auf Systemsoftware 7.8.2 wird das Betriebssystem ggf. automatisch von ACE auf BOSS umgestellt.

Hinweis

Wenn Sie Ihr Gerät bereits unter **Systemsoftware 7.5.1** oder höher betreiben, verfahren Sie mit dem Update wie für die Geräte der **WI**-Serie beschrieben (siehe “Vorbereitung und Update (WI-Serie)” auf Seite 16).

Gehen Sie für das Update folgendermaßen vor:

Update vorbereiten

1. Für das Update benötigen Sie für das Gerät **W1002** die Datei *W1002_boss_s7802.afw* bzw. für das Gerät **W2002** die Datei *W2002_boss_s7802.afw*.
   Zusätzlich benötigen Sie die Datei W1002_Blup_LED_SCHEME.w1p bzw. W2002_Blup_LED_SCHEME.w2p, um nach dem Update die LEDs des jeweiligen Geräts zu aktivieren.

Stellen Sie sicher, dass das Programm **ComPoint Manager** von Artem und die Dateien, welche Sie für den Update benötigen, auf Ihrem PC verfügbar sind.
Wenn das Programm und/oder die beiden Dateien nicht auf Ihrem PC verfügbar sind, geben Sie www.funkwerk-ec.com in Ihren Browser ein.
Die Funkwerk-Homepage öffnet sich. Im Download-Bereich Ihres Geräts finden Sie das Programm und die benötigten Dateien.

2. Installieren Sie das Programm auf Ihrem Rechner.
   Alternativ können Sie das Programm von der CD-ROM laden, die Sie zusammen mit Ihrem Access Point erhalten haben.
3. Speichern Sie die beiden Dateien auf Ihrem PC.
4. Stellen Sie sicher, dass sich der Access Point, für den Sie das Update durchführen wollen, im selben Netz befindet wie der PC, auf dem das Programm **ComPoint Manager** installiert ist.
5. Starten Sie den **ComPoint Manager**.
   Der **ComPoint Manager** erkennt die im Netzwerk installierten Access Points und zeigt sie in seinem Hauptfenster in einer Liste.
6. Falls das Gerät, für welches Sie das Update durchführen wollen, noch keine IP-Adresse besitzt, weisen Sie ihm im **ComPoint Manager** unter ***Konfiguration*** ➜ ***IP-Einstellungen*** eine IP-Adresse aus Ihrem Netz zu.
7. Geben Sie im folgenden Fenster das Kennwort des Benutzers Admin ein, falls es im **ComPoint Manager** unter ***Extras*** ➜ ***Kennwort*** noch nicht eingegeben wurde.

Boot-Konfiguration sichern

Sichern Sie die aktuelle Boot-Konfiguration für einen etwaigen späteren Downgrade. Gehen Sie dazu folgendermaßen vor:

1. Wählen Sie im **ComPoint Manager** in der Geräteliste das Gerät, dessen Boot-Konfiguration Sie sichern wollen.
2. Wählen Sie im **ComPoint Manager** ***Konfiguration*** ➜ ***Konfiguration speichern***.
3. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort ein.
   Das Fenster ***Speichern unter*** öffnet sich.
4. Wählen Sie den gewünschten Ordner, den Dateinamen können Sie übernehmen. Klicken Sie auf **Speichern**.
   Sie sehen die Meldung "Gerätekonfiguration erfolgreich gespeichert."

5. Bestätigen Sie mit **OK**.
   Die Konfiguration ist im gewählten Ordner gespeichert.

Update durchführen

Führen Sie das Update als Firmware Upgrade mit dem **ComPoint Manager** durch.

Achtung!

Die Folge von unterbrochenen Update-Vorgängen könnte sein, dass Ihr Access Point nicht mehr bootet. Schalten Sie Ihren Access Point nicht aus, während das Update durchgeführt wird.

1. Klicken Sie im Hauptfenster des **ComPoint Managers** in der Geräteliste auf das Gerät, für welches Sie das Update durchführen wollen.
2. Wählen Sie ***KONFIGURATION*** ➜ ***FIRMWARE LADEN***.
3. Klicken Sie auf **Software auswählen**.
4. Klicken Sie auf **Durchsuchen**, wählen Sie den Ordner, in welchem sich die Dateien befinden und bestätigen Sie mit **OK**.
   Sie sehen die gewünschte(n) Datei(en).
5. Wählen Sie abhängig vom Gerät die gewünschte Firmware, d.h. *W1002_boss_s7802.afw* für **W1002** bzw. *W2002_boss_s7802.afw* für **W2002**, bestätigen Sie Ihre Einstellungen mit **OK** und klicken Sie auf **Firmware aufspielen**.
   Der **ComPoint Manager** prüft, ob die gewählte Firmware für das Gerät geeignet ist und überträgt sie gegebenenfalls an das Gerät.
   Die serielle Schnittstelle wird dabei gemäß des BOSS-Standards automatisch auf 9600 Baudrate, 8 Datenbits, keine Parität, 1 Stoppbit, No Handshake umgeschaltet.
   Sie sehen die Meldung "Die geladene Firmware wird nach einem Neustart aktiv."

6. Wählen Sie die Option "Jetzt neu starten (empfohlen)" und bestätigen Sie mit **OK**.
   Das Gerät startet neu.

Hinweis

Das Gerät startet mit der neuen Software und der Standard-IP-Adresse *192.168.0.252*, aber ohne Konfiguration. Die LEDs sind nicht aktiv.

Nach dem Update von ACE auf BOSS können Sie nur folgende Funktionen des **ComPoint Managers** nutzen:

- *Discovery Server*
- *IP-Konfiguration.*

Alle weiteren Konfigurationsoptionen werden unter BOSS mit dem **Funkwerk Configuration Interface** vorgenommen.

LEDs aktivieren

Um die Funktion der LEDs zu aktivieren, müssen Sie je nach Gerät die Datei W1002_Blup_LED_SCHEME.w1p bzw. W2002_Blup_LED_SCHEME.w2p laden.

1. Stellen Sie sicher, dass sich Ihr PC im selben Netz befindet wie der Access Point, dessen LEDs Sie aktivieren wollen. Weisen Sie dazu Ihrem PC in den Netzwerkeinstellungen gegebenenfalls eine geeignete (zweite) IP-Adresse zu.
2. Geben Sie die Standard-IP-Adresse Ihres Geräts *192.168.0.252* in einen Browser ein.
   Das Browser-Fenster öffnet sich.
3. Melden Sie sich mit dem Benutzernamen *admin* und dem Passwort *funkwerk* an Ihrem Gerät an und klicken Sie auf **Login**.
   Die Status-Seite des **Funkwerk Configuration Interface** öffnet sich.
4. Stellen Sie sicher, dass als Sprache *Deutsch* eingestellt ist.
5. Klicken Sie auf ***Wartung*** ➜ ***Software & Konfiguration***.
6. Wählen Sie im Feld ***Aktion*** den Wert *Systemsoftware aktualisieren*.
7. Wählen Sie im Feld ***Quelle*** den Wert *Lokale Datei* und klicken Sie auf die Schaltfläche **Durchsuchen**.
8. Klicken Sie auf den gewünschten Dateinamen, z. B. *W1002_Blup_LED_SCHEME.w1p* und dann auf **Öffnen**.
9. Bestätigen Sie mit **Los**.
   Die Meldung "Router Maintenance. Please stand by. Operation in pro-

gress." zeigt, dass die gewählte Datei in das Gerät geladen wird. Wenn der Ladevorgang beendet ist, sehen Sie die Meldung "Router Maintenance. Success. Operation completed successfully. The router must be restarted."

10. Klicken Sie auf **Reboot**.
    Das Gerät startet, die LEDs leuchten. Das Browser-Fenster öffnet sich.

Sie können sich an Ihrem Gerät anmelden und es konfigurieren.

Downgrade

Bei einem Downgrade wird automatisch das Betriebssystem von BOSS auf ACE umgestellt.

Für diesen Vorgang benötigen Sie je nach Gerät die Datei *W1002_ace_6_18.w1p* bzw. *W2002_ace_6_18.w2p,* die Sie unter www.funkwerk-ec.com finden (siehe “Update vorbereiten” auf Seite 10).

Hinweis

Beachten Sie, dass die Konfiguration Ihres Geräts während eines Downgrades verlorengeht. Lediglich die Konfiguration, die Sie vor dem Update gesichert haben, können Sie nach einem Downgrade weiterverwenden.

Achtung!

Die Folge von unterbrochenen Update- bzw. Downgrade-Vorgängen könnte sein, dass Ihr Access Point nicht mehr bootet. Schalten Sie Ihren Access Point nicht aus, während ein Downgrade durchgeführt wird.

Downgrade durchführen

Wenn Sie einen Downgrade von **Systemsoftware 7.8.2** durchführen wollen, gehen Sie folgendermaßen vor:

1. Geben Sie die IP-Adresse Ihres Geräts in einen Browser ein.
   Das Browser-Fenster öffnet sich.
2. Melden Sie sich mit Ihrem Benutzernamen und Passwort an Ihrem Gerät an und klicken Sie auf **Login**.
3. Stellen Sie sicher, dass als Sprache *Deutsch* eingestellt ist.
4. Klicken Sie auf ***Wartung*** ➜ ***Software & Konfiguration***.
5. Wählen Sie im Feld ***Aktion*** den Wert *Systemsoftware aktualisieren*.
6. Wählen Sie im Feld ***Quelle*** den Wert *Lokale Datei* und klicken Sie auf die Schaltfläche **Durchsuchen**.

7. Klicken Sie auf den gewünschten Dateinamen, z. B. auf *W1002_ace_6_18.w1p* und dann auf **Öffnen**.
8. Bestätigen Sie mit **Los**.
   Der Vorgang nimmt einige Minuten in Anspruch. Währenddessen erscheint die Meldung "Router-Maintenance. Please stand by. Operation in progress." Die Meldung "Router-Maintenance. Success. Operation completed successfully. The router must be restarted" zeigt, dass der Ladevorgang beendet ist.
9. Klicken Sie auf **Reboot**.
   Der Vorgang kann einige Minuten dauern. Das Gerät startet, die Status LED leuchtet grün.

Hinweis

Mit dem **ComPoint Manager** können Sie den Access Point finden. Über den Browser ist das Gerät nicht mehr erreichbar.

Konfiguration laden

Nach dem Downgrade auf ACE können Sie die Konfiguration wieder in Ihr Gerät laden, die Sie eventuell vor dem Update auf BOSS gesichert haben.

1. Starten Sie den **ComPoint Manager**.
   Der **ComPoint Manager** öffnet sich. Er erkennt die im Netzwerk installierten Access Points und zeigt sie in seinem Hauptfenster in einer Liste.
2. Weisen Sie Ihrem Gerät mit dem **ComPoint Manager** unter ***Konfiguration*** ➜ ***IP-Einstellungen*** eine IP-Adresse aus Ihrem Netz zu.
3. Wählen Sie in der Liste das Gerät, in welches Sie die gespeichert Konfiguration laden wollen.
4. Wählen Sie im **ComPoint Manager** ***Konfiguration*** ➜ ***Konfiguration aufspielen***.
5. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort des Benutzers Admin ein.
   Das Fenster ***Öffnen*** öffnet sich.
6. Wählen Sie die gewünschte Datei. Klicken Sie auf **Öffnen**.
   Sie sehen die Meldung "Konfiguration (Version *x.xx*) auf das Gerät (Version *x.xx*) aufspielen und einen Neustart durchführen?"
7. Wenn die beiden Versionsangaben übereinstimmen, bestätigen Sie die Einstellungen mit **Ja**.

Die Konfiguration wird in das Gerät übertragen.
Sie sehen die Meldung "Konfiguration erfolgreich aufgespielt."

8. Klicken Sie auf **OK**.
   Sie können die Konfiguration in Ihrem Gerät verwenden.

1.2.2 Vorbereitung und Update (WI-Serie)

Die Geräte der WI-Serie werden bereits mit Systemsoftware 7.6.2 ausgeliefert, verfügen also zur Konfiguration und Wartung über das Funkwerk Configuration Interface, das ein einfaches Update der Software ermöglicht. Daher ist ein Update auf zweierlei Arten möglich.

Update vorbereiten

1. Für das Update benötigen Sie für die Geräte der **WI**-Serie die Datei *bl7802.iny*.
   Stellen Sie sicher, dass das Programm **ComPoint Manager** von Artem und die Datei, welche Sie für den Update benötigen, auf Ihrem PC verfügbar sind.
   Wenn das Programm und/oder die Datei nicht auf Ihrem PC verfügbar sind, geben Sie www.funkwerk-ec.com in Ihren Browser ein.
   Die Funkwerk-Homepage öffnet sich. Im Download-Bereich Ihres Geräts finden Sie das Programm und die benötigten Dateien.
2. Installieren Sie das Programm auf Ihrem Rechner.
   Alternativ können Sie das Programm von der CD-ROM laden, die Sie zusammen mit Ihrem Access Point erhalten haben.
3. Speichern Sie die beiden Dateien auf Ihrem PC.
4. Stellen Sie sicher, dass sich der Access Point, für den Sie das Update durchführen wollen, im selben Netz befindet wie der PC, auf dem das Programm **ComPoint Manager** installiert ist.
5. Starten Sie den **ComPoint Manager**.
   Der **ComPoint Manager** erkennt die im Netzwerk installierten Access Points und zeigt sie in seinem Hauptfenster in einer Liste.
6. Falls das Gerät, für welches Sie das Update durchführen wollen, noch keine IP-Adresse besitzt, weisen Sie ihm im **ComPoint Manager** unter ***KONFIGURATION*** ➜ ***IP-EINSTELLUNGEN*** eine IP-Adresse aus Ihrem Netz zu.

7. Geben Sie im folgenden Fenster das Kennwort des Benutzers Admin ein, falls es im **ComPoint Manager** unter ***Extras*** ➜ ***Kennwort*** noch nicht eingegeben wurde.

Hinweis

Sie können nur folgende Funktionen des **ComPoint Managers** nutzen:

- *Discovery Server*
- *IP-Konfiguration.*

Alle weiteren Konfigurationsoptionen werden unter BOSS mit dem **Funkwerk Configuration Interface** vorgenommen.

Update über das Funkwerk Configuration Interface

Am komfortabelsten können Sie ein Update über das **Funkwerk Configuration Interface** im Menü ***Wartung*** ➜ ***Software & Konfiguration*** vornehmen.

Wenn Sie das Update durchführen wollen, gehen Sie folgendermaßen vor:

1. Sichern Sie die aktuelle Boot-Konfiguration über das Menü ***Wartung*** ➜ ***Software & Konfiguration***:
   a) Wählen Sie bei ***Aktion*** *Konfiguration exportieren*.
   b) Belassen Sie alle anderen Einstellungen und klicken Sie auf **Los**.
   c) Folgen Sie zum Sichern der Datei auf Ihrem PC den Anweisungen Ihres Browsers.
2. Bleiben Sie im Menü ***Wartung*** ➜ ***Software & Konfiguration***.
3. Wählen Sie im Feld ***Aktion*** *Systemsoftware aktualisieren* aus.
4. Wählen Sie als ***Quelle*** für die Aktualisierung *Aktuelle Software vom Funkwerk-Server* aus. Die Systemdatei liegt auf dem offiziellen Funkwerk-Update-Server.
5. Klicken Sie auf **Los**. Ihre Anfrage wird bearbeitet.
   Der Vorgang nimmt einige Minuten in Anspruch. Die Meldung " System Maintenance. Success. Operation completed successfully. The system must be restarted." zeigt, dass der Vorgang beendet ist.
6. Klicken Sie auf **Reboot**.
   Das Gerät startet, Sie können sich an Ihrem Gerät anmelden.

Weitere Möglichkeit um das Update durchzuführen:

1. Wählen Sie als ***QUELLE*** für die Aktualisierung *Lokale Datei* (Standardwert) aus. Die Systemdatei ist lokal auf Ihrem PC gespeichert. Für das Update benötigen Sie für die Geräte der **WI**-Serie die Datei *INY\Blup\bl7802.iny*, die Sie unter www.funkwerk-ec.com finden.
2. Geben Sie den Dateipfad und -namen der Datei an, oder wählen Sie die Datei mit **Durchsuchen...** über den Dateibrowser aus.
3. Klicken Sie auf **Los**. Ihre Anfrage wird bearbeitet.
   Der Vorgang nimmt einige Minuten in Anspruch. Die Meldung "System Maintenance. Success. Operation completed successfully. The system must be restarted." zeigt, dass der Vorgang beendet ist.
4. Wenn der Vorgang beendet ist, klicken Sie auf **Reboot**.
   Das Gerät startet, Sie können sich an Ihrem Gerät anmelden.

Alternativ können Sie unter ***QUELLE*** *HTTP-Server* auswählen. Hier geben Sie die ***URL*** des Update-Servers ein, von dem die Software-Datei geladen werden soll.

Update über Kommandozeile

Gehen Sie ggf. folgendermaßen vor, um ein Update auf **Systemsoftware 7.8.2** vorzubereiten und durchzuführen:

1. Sichern Sie die aktuelle Boot-Konfiguration. Verwenden Sie eine der folgenden Möglichkeiten:
   a) Geben Sie auf der SNMP Shell `cmd=save path=boot.alt` ein. Dies sichert die aktuelle Boot-Konfiguration im Flash ROM Ihres Access Points unter dem Namen "boot.alt".
   b) Starten Sie auf einem Rechner in Ihrem LAN einen TFTP-Server und exportieren Sie die aktuelle Boot-Konfiguration über das Menü ***CONFIGURATION MANAGEMENT*** des Setup Tools. Wählen Sie dazu:
   – ***OPERATION*** = *put (FLASH -> TFTP)*
   – ***TFTP SERVER IP ADDRESS*** = *<IP-Adresse des TFTP Servers im LAN>*
   – ***TFTP FILE NAME*** = *boot.alt*
   – ***NAME IN FLASH*** = *boot.*
2. Führen Sie das Update auf **Systemsoftware 7.8.2** mit dem o. g. BLUP (Bintec Large Update) durch, um alle notwendigen Module zu aktualisieren. Das Update mittels BLUP verläuft wie folgt:

```
wi3040:> update <IP-Adresse des TFTP-Servers> /INY/Blup/bl7802.iny
Starting TFTP File Transfer .....................................
..................... (139320+4887788 bytes)
List of files in this update (len 4887788):
  Version    Length  Name
7.8.2.000   4048577  Boss
7.8.2.000    774792  webpages.ez
7.8.2.000    182462  text_ger.ez

*** Don't power-off while the update takes place ***

Perform update (y or n) ?
```

Hier werden diejenigen Softwaremodule aufgelistet, die das BLUP enthält:

- BOSS - das eigentliche Betriebssystem
- webpages.ez - die HTML-Konfigurationsoberfläche
- text_ger.ez - die deutsche Lokalisierung der HTML-Oberfläche.

Wenn Sie mit *y* bestätigen, werden alle diejenigen Elemente aktualisiert, die im BLUP neuer sind als auf Ihrem Access Point. Bei einem Update auf **Systemsoftware 7.8.2** dürften das in der Regel alle drei Module sein.

Die Aktualisierung erfolgt dann für alle relevanten Module:

```
Updating Boss
Erasing Flash-ROM
.............................................................OK
Writing Flash-ROM
.............................................................OK
Verify  Flash-ROM
.............................................................OK

Software update successfully finished

Updating webpages.ez

Perform Flash-ROM update
Update  Flash-ROM ............ OK
Verify  Flash-ROM ............ OK

File update successfully finished

Updating text_ger.ez

Perform Flash-ROM update
Update  Flash-ROM . OK
Verify  Flash-ROM . OK

File update successfully finished

Rebooting... (y or n) [n] ?
```

Nach dem Neustart steht Ihnen die neue Softwareversion zur Verfügung. Sie können den Access Point in einem der unterstützten Webbrowser unter der IP-Adresse des Access Points aufrufen. Sollten Sie die Boot-Konfiguration gelöscht haben, hat der Access Point wieder die Standardadresse *192.168.0.252*.

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

1. Ersetzen Sie die aktuelle Boot-Konfiguration mit der zuvor gesicherten. Verwenden Sie eine der folgenden Möglichkeiten:
   a) Geben Sie auf der SNMP Shell `cmd=move path=boot.alt pathnew=boot` ein. Dies überschreibt die aktuelle Boot-Konfiguration mit der zuvor gesicherten. Die "boot.alt" genannte Konfiguration wird dabei aus dem Flash ROM gelöscht (wenn Sie diese im Flash erhalten wollen, verwenden Sie `cmd=copy` anstelle von `cmd=move`).
   b) Starten Sie auf einem Rechner in Ihrem LAN einen TFTP-Server und importieren Sie die zuvor gesicherte Konfiguration über das Menü ***CONFIGURATION MANAGEMENT*** des Setup Tools. Wählen Sie dazu:
   - ***OPERATION*** = get (TFTP -> FLASH)
   - ***TFTP SERVER IP ADDRESS*** = *<IP-Adresse des TFTP Servers im LAN>*
   - ***TFTP FILE NAME*** = *boot.alt*
   - ***NAME IN FLASH*** = *boot*.
2. Führen Sie das Downgrade auf die gewünschte Softwareversion durch.
3. Rebooten Sie den Access Point. Es startet nun mit der zuvor gesicherten Boot-Konfiguration und der älteren Version der Systemsoftware.

2 Neue Funktionen

Systemsoftware 7.8.2 enthält eine Reihe neuer Funktionen, die den Leistungsumfang gegenüber Systemsoftware 7.6.2 erheblich erweitern:

2.1 Funkwerk Configuration Interface - Überblick

Für die Garäte der Wx002-, WIx040- und WIx065-Serie steht eine Reihe neuer Funktionen zur Verfügung. In der unten stehenden Tabelle finden Sie die Bezeichnung der jeweiligen Funktion, den Pfad im Funkwerk Configuration Interface, unter dem Sie die Funktion finden, sowie eine kurze

Beschreibung. Ausführliche Informationen können Sie, wenn nicht in diesen Release Notes enthalten, der Hilfe des jeweiligen Geräts entnehmen.

Funktion	Pfad / Bemerkung
NAT	Im Menü ***ROUTING*** ➜ ***NAT*** können Sie Network Address Translation (NAT) nutzen, um die Quell- und Zieladressen von IP-Paketen definiert umzusetzen.
RIP	Im Menü ***ROUTING*** ➜ ***RIP*** können Sie den dynamischen Austausch der Routing-Informationen zwischen mehreren Geräten regeln.
Lastverteilung	Im Menü ***ROUTING*** ➜ ***LASTVERTEILUNG*** können Sie den Datenverkehr auf unterschiedliche Schnittstellen verteilen und mittels IP-Lastenausgleich innerhalb einer Gruppe von Schnittstelen nach verschiedenen Kriterien organisieren.
Multicast	Im Menü ***ROUTING*** ➜ ***MULTICAST*** können Sie die Kommunikation von einem Sender zu mehreren Empfängern festlegen.
Internet + Einwählen	Im Menü ***WAN*** ➜ ***INTERNET + EINWÄHLEN*** können Sie Internetzugänge und Einwahl-Verbindungen einrichten.
Real Time Jitter Control	Im Menü ***WAN*** ➜ ***REAL TIME JITTER CONTROL*** können Sie die Qualität von Telefongesprächen über das Internet optimieren.
IPSec	Im Menü ***VPN*** ➜ ***IPSEC*** können Sie gesicherte Verbindungen zwischen zwei Standorten aufbauen (VPN), um sensible Unternehmensdaten über ein unsicheres Medium wie z. B. das Internet zu übertragen.

Funktion	Pfad / Bemerkung
L2TP	Im Menü ***VPN*** ➜ ***L2TP*** können Sie das Layer-2-Tunnelprotokoll (L2TP) verwenden, um Tunneling von PPP-Verbindungen über eine UDP-Verbindung zu nutzen.
GRE	Im Menü ***VPN*** ➜ ***GRE*** können Sie das Generic Routing Encapsulation (GRE) Protokoll verwenden, um andere Protokolle einzukapseln und mittels Tunnel über das Internet Protokoll zu transportieren (siehe Seite 40).
Zertifikate	Im Menü ***VPN*** ➜ ***ZERTIFIKATE*** können Sie die vorhanden Zertifikate einsehen und gegebenenfalls weitere Zertifikate anfordern sowie importieren.
Richtlinien	Im Menü ***FIREWALL*** ➜ ***RICHTLINIEN*** können Sie Filterregeln anzeigen lassen, ändern und neue hinzufügen. Im Menü ***FIREWALL*** ➜ ***RICHTLINIEN*** ➜ ***QOS*** können Sie mit der Funktion Quality of Service (QoS) Bandbreite nach Wunsch verteilen und für bestimmte Anwendungen reservieren.
Adressen	Im Menü ***FIREWALL*** ➜ ***ADRESSEN*** können Sie die bereits konfigurierten Adressen anzeigen lassen, weitere Adressen einrichten und Adressen zu Gruppen zusammenfassen.
Dienste	Im Menü ***FIREWALL*** ➜ ***DIENSTE*** können Sie alle zur Verfügung stehenden Dienste anzeigen lassen, neue Dienste einrichten und Dienste zu Gruppen zusammenfassen.
DynDNS-Client	Im Menü ***LOKALE DIENSTE*** ➜ ***DYNDNS-CLIENT*** können Sie dafür sorgen, dass Ihr Gerät auch mit dynamischer IP-Adresse immer auffindbar ist.

Funktion	Pfad / Bemerkung
Email Alert	Im Menü ***EXTERNE BERICHTERSTATTUNG*** ➜ ***E-MAIL BENACHRICHTIGUNG*** kann sich der Administrator des Gateways über bestimmte Ereignisse per E-Mail informieren lassen (siehe Seite 42).
Monitoring IPSec	Im Menü ***MONITORING*** ➜ ***IPSEC*** werden alle konfigurierten IPSec-Tunnel und statistischen Werte zu allen IPSec-Verbindungen angezeigt.
Monitoring Bridges	Im Menü ***MONITORING*** ➜ ***BRIDGES*** werden die aktuellen Werte der konfigurierten Bridges angezeigt.

2.2 Serial over IP (SoIP; nur WIx040 und WIx065-Serie)

Die Geräte funkwerk WI1040, WI2040, WI3040, WI1065, WI2065 und WI3065 verfügen ab Systemsoftware 7.8.2 über die Funktion Serial over IP (SoIP). Die serielle Schnittstelle kann jetzt wahlweise als Konsole oder als Datenschnittstelle betrieben werden. Im Modus Datenschnittstelle können die Daten der seriellen Schnittstelle über eine IP Infrastruktur transportiert werden (Serial over IP).

Funkwerk Configuration Interface

Die Serial over IP Funktion können Sie im FCI Menü ***PHYSIKALISCHE SCHNITTSTELLEN*** ➜ ***SERIELLER PORT*** ➜ ***SERIELLER PORT*** konfigurieren.

Parameter	Wert
Port-Modus	Wählen Sie aus, in welchem Modus die serielle Schnittstelle verwendet werden soll. Mögliche Werte: ■ *Konfiguration* (Standardwert): Die serielle Schnittstelle wird als Konsole verwendet. Dies entspricht dem Verhalten in früheren Software-Versionen. ■ *Datenport*: Die serielle Schnittstelle wird als Datenschnittstelle betrieben, Serial over IP wird verwendet.
Baudrate	Nur für ***PORT-MODUS*** = *Datenport*. Wählen Sie, welche Baudrate verwendet werden soll. Achten Sie darauf, dass die Gegenstelle die gewählte Baudrate beherrscht. Mögliche Werte: ■ *300* ■ *600* ■ *1200* ■ *2400* ■ *4800* ■ *9600*: (Standardwert) ■ *19200* ■ *57600* ■ *115200.*

Parameter	Wert
Datenbits	Nur für ***PORT-MODUS*** = *Datenport*. Wählen Sie, wieviel Datenbits jeweils hintereinander für Nutzdaten gesendet werden sollen. Mögliche Werte: ■ *8* (Standardwert): Acht Datenbits werden hintereinander gesendet. ■ *7*: Sieben Datenbits werden hintereinander gesendet.
Parität	Nur für ***PORT-MODUS*** = *Datenport*. Wählen Sie, ob ein Parity Bit zur Erkennung von Übertragungsfehlern verwendet werden soll. Mögliche Werte: ■ *Keiner* (Standardwert): Es wird kein Parity Bit verwendet. ■ *Gerade*: Es wird eine gerade Anzahl von "1"-Bits zur Erkennung von Übertragungsfehlern verwendet. ■ *Ungerade*: Es wird eine ungerade Anzahl von "1"-Bits zur Erkennung von Übertragungsfehlern verwendet.
Stoppbits	Nur für ***PORT-MODUS*** = *Datenport*. Stoppbits schließen die Datenübertragung einer Übertragungseinheit ab. Wählen Sie, ob ein Stoppbit verwendet werden soll oder ob zwei Stoppbits verwendet werden sollen. Mögliche Werte: ■ *1* (Standardwert) ■ *2.*

Parameter	Wert
Handshake	Nur für ***PORT-MODUS*** = *Datenport*. Wählen Sie, wie der Empfänger die Datenübertragung anhalten kann, damit keine Datenverluste auftreten, wenn aktuell keine weiteren Daten verarbeitet werden können. Mögliche Werte: ■ Keiner: Der Empfänger kann die Datenübertragung nicht anhalten. ■ *RTS/CTS*: Der verwendeten Hardware-Handshake steuert den Datenfluss über die Leitungen RTS und CTS. ■ *XON/XOFF*: Beim verwendeten Software-Handshake sendet der Empfänger zur Steuerung des Datenflusses spezielle Zeichen an den Sender.
Modus	Nur für ***PORT-MODUS*** = *Datenport*. Wählen Sie den Modus, in welchem das Gateway IP-Datenpakete verarbeiten soll. Mögliche Werte: ■ *Server* (Standardwert): Das Gateway wartet auf eingehende TCP-Verbindungen. ■ *Client*: Das Gateway baut aktiv eine TCP-Verbindung auf. ■ *UDP*: Das Gateway sendet und empfängt UDP-Pakete.

Parameter	Wert
Lokale IP-Adresse	Nur für ***PORT-MODUS*** = *Datenport*. Für ***MODUS*** = *Server* Geben Sie die IP-Adresse des Clients an, der sich anmelden will. Wenn ***LOKALE IP-ADRESSE*** = *0.0.0.0*, kann sich jeder beliebige Client anmelden.
Lokaler Port	Nur für ***PORT-MODUS*** = *Datenport*. Geben Sie den Port zur ***LOKALE IP-ADRESSE*** ein.
Entfernte IP	Nur für ***PORT-MODUS*** = *Datenport*. Für ***MODUS*** = *Client* Geben Sie die IP-Adresse des Servers an, an dem sich Ihr Gateway als Client anmelden soll.
Portnumber	Nur für ***PORT-MODUS*** = *Datenport*. Geben Sie den Port zur ***ENTFERNTE IP*** ein.
Bytezahl	Nur für ***PORT-MODUS*** = *Datenport*. Bevor ein IP-Paket gesendet wird, wird solange gewartet bis die angegebene Anzahl von Bytes empfangen wurde. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Mögliche Werte: *1 .. 1460*. Standardwert: *128*.
Timeout	Nur für ***PORT-MODUS*** = *Datenport*. Bevor ein IP-Paket gesendet wird, wird solange gewartet bis die angegebene Zeit in ms seit dem Empfang des letzten Zeichens verstrichen ist. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Mögliche Werte: *0 .. 65535*. Standardwert: *0*.

Parameter	Wert
Inter-ByteGap	Nur für ***PORT-MODUS*** = *Datenport*. Bevor ein IP-Paket gesendet wird, wird solange gewartet bis die angegebene Zeit in ms seit dem Empfang des ersten Zeichens verstrichen ist. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Mögliche Werte: *0* .. *65535*. Standardwert: *100*.
Seriellen RX-Zwischenspeicher löschen	Nur für ***PORT-MODUS*** = *Datenport*. Wählen Sie die Schalrfläche **Löschen**, um den Empfangspuffer zu leeren.
Seriellen TX-Zwischenspeicher löschen	Nur für ***PORT-MODUS*** = *Datenport*. Wählen Sie die Schaltfläche **Löschen**, um den Sendepuffer zu leeren.

Tabelle 2-1: Felder im Menü ***PHYSIKALISCHE SCHNITTSTELLEN*** ➜ ***SERIELLER PORT*** ➜ ***SERIELLER PORT***

2.3 ISAKMP Configuration Method (IKE Config Mode)

Mit Systemsoftware 7.8.2 können Sie mit Hilfe der ISAKMP Configuration Method (kurz IKE Config Mode) einen mobilen PC-Arbeitsplatz (Secure IPSec Client) über VPN an die Firmenzentrale anbinden. Die IP-Adresse und auf Wunsch weitere Daten wie Domänen- und Serverparameter für DNS und WINS werden dem Client vom VPN Gateway auf Anfrage zur Verfügung gestellt. Diese Methode ermöglicht die Zuteilung einer dynamischen IP-Adresse aus dem internen Adressbereich der Firmenzentrale.

IKE Config Mode ist über eine Erweiterung der IPSec Konfiguration realisiert. Die Übertragung der Daten vom Gateway zum Client erfolgt in IPSec nach IKE (Phase 1) und ist daher durch die entsprechende Verschlüsselung geschützt.

Hinweis

Beachten Sie, dass IKE Config Mode nur für IPSec Peers mit virtuellem Interface zur Verfügung steht.

Gehen Sie folgendermaßen vor, um IKE Config Mode zu nutzen.

1. Legen Sie mindestens einen IP-Adress-Bereich an. Wählen Sie dazu das FCI Menü ***VPN*** ➜ ***IPSec*** ➜ ***IP Pools*** und klicken Sie auf die Schaltfläche **Hinzufügen**. Geben Sie ***IP-Poolname*** und ***IP Poolbereich*** für den aktuellen IP-Adress-Bereich ein. Mit **Hinzufügen** können Sie weitere IP-Adress-Bereiche anlegen. Speichern Sie die angelegten IP-Adress-Bereiche mit **OK**.
   Die angelegten IP-Adress-Bereiche stehen zur Verfügung.
2. Wählen Sie IKE Config Mode aus und ordnen Sie den gewünschten IP-Adress-Bereich zu. Wählen Sie dazu das FCI Menü ***VPN*** ➜ ***IPSec*** ➜ ***IPSec-Peers*** und klicken Sie auf **Neu**. Wählen Sie ***IP-Adressenvergabe*** = *IKE-Konfigurationsmodus*. Wählen Sie ***IP-Zuordnungspool*** = *<gewünschter Pool>*. Speichern Sie mit **OK**.

Die IKE Config Mode Konfiguration ist abgeschlossen, ein Secure IPSec Client kann sich beim Gateway einwählen.

2.4 Layer 2.5 Bridge

Ab Systemsoftware 7.8.2 können Sie mit der Funktion Layer 2.5 Bridge Bridging für Geräte hinter Access Clients realisieren. Zusätzlich kann in einem Wildcard Modus festgelegt werden, wie Unicast nicht-IP-Frames bzw. nicht-ARP Frames verarbeitet werden sollen.

Um die Funktion Layer 2.5 Bridge zu nutzen, müssen Sie Konfigurationsschritte in mehreren FCI Menüs vornehmen.

1. Wählen Sie das FCI Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Einstellungen Funkmodul*** und klicken Sie auf das Symbol zur Änderung eines Eintrags.
2. Wählen Sie im Feld ***Funkmodul*** *aktiviert* aus.

Das Menü wird angezeigt.

3. Wählen Sie ***Betriebsmodus*** = *Access Client* und speichern Sie die Einstellungen mit **OK**.
4. Wählen Sie das Menü ***Systemverwaltung*** ➜ ***Schnittstellenmodus / Bridge-Gruppen*** ➜ ***Schnittstellen***.

Die zusätzliche Schnittstelle *sta1-0* wird angezeigt.

5. Wählen Sie für die Schnittstelle sta1-0 ***Modus / Bridge-Gruppe*** = *br0 (<IP-Adresse>)* sowie ***Konfigurationsschnittstelle*** = *en1-0* und speichern Sie die Einstellungen mit **OK**.
6. Klicken Sie auf die Schaltfläche **Konfiguration speichern**, um alle Konfigurationseinstellungen zu speichern.

Sie können die Layer 2.5 Bridge verwenden.

Wildcard Modus

Um den Wildcard Modus zu konfigurieren, müssen Sie zusätzliche Konfigurationsschritte vornehmen.

7. Klicken Sie im Menü ***Systemverwaltung*** ➜ ***Schnittstellenmodus / Bridge-Gruppen*** ➜ ***Schnittstellen*** in der Zeile der Schnittstelle sta1-0 auf das Symbol zur Änderung eines Eintrags.

Das Menü Layer 2.5 Optionen öffnet sich. Als ***Schnittstelle*** wird *sta1-0* angezeigt.

8. Wählen Sie einen ***Wildcard Modus***.
   Drei Möglichkeiten stehen Ihnen zur Verfügung:
   Mit der Einstellung *statisch* müssen Sie zusätzlich die MAC-Adresse eines Geräts eingeben, das über IP angebunden ist. Jedes Paket ohne IP und ohne ARP wird an dieses Gerät weitergereicht. Dieses Vorgehen wird auch dann beibehalten, wenn das entsprechende Gerät nicht mehr angeschlossen ist. Mit ***Transparent MAC Address*** *aktiviert* wird die Wildcard MAC Adresse zusätzlich als WLAN MAC Adresse benutzt, um damit die Verbindung zum Access Point herzustellen.
   Mit der Einstellung *first* wird die MAC-Adresse des ersten Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame, der an irgendeiner der Ethernet Schnittstellen ankommt, als Wildcard MAC Adresse benutzt. Diese Wildcard MAC Adresse kann nur durch einen Reboot des Geräts oder die Auswahl eines anderen Wildcard Modus zurückgesetzt werden.
   Mit der Einstellung *last* wird die eigene WLAN MAC-Adresse benutzt, um die Verbindung zum Access Point herzustellen. Sobald ein Nicht-IP-Uni-

cast-Frame bzw Nicht-ARP-Unicast-Frame auftaucht, wird er an diejenige MAC-Adresse weitergeleitet, von welcher der letzte Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame bei einer Ethernet Schnittstelle des Geräts eingetroffen ist. Diese Wildcard MAC Adresse wird mit jedem Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame erneuert.

2.5 Fast Roaming für WLAN Client Modus

Ab Systemsoftware 7.8.2 steht Ihnen sogenanntes Fast Roaming für WLAN Client Modus, d.h. Roaming für schnell bewegliche Clients, zur Verfügung. Ein Einsatzgebiet für diese Funktion ist die Datenübertragung von einem Client installiert in einer U-Bahn an Access Points im U-Bahn Tunnel. Dabei muss das Roaming des Clients von einem Access Point zum anderen wegen der hohen Geschwindigkeiten der U-Bahn sehr schnell erfolgen.

Fast Roaming für WLAN Client Modus können Sie im FCI Menü ***Wireless LAN*** → ***WLANx*** → ***Einstellungen Funkmodul*** konfigurieren.

1. Klicken Sie auf das Symbol zur Änderung eines Eintrags, um das Menü zu öffnen.
2. Klicken Sie im Feld ***Funkmodul*** auf *aktiviert*, um das vollständige Menü anzuzeigen.
3. Wählen Sie ***Betriebsmodus*** = *Access Client*. Falls gewünscht, können Sie die Standardeinstellungen der übrigen Felder ändern.
4. Legen Sie im Menü ***Erweiterte Einstellungen*** die Parameter für Client Fast Roaming fest.

Das FCI Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Einstellungen Funkmodul*** ➜ ***Symbol zur Änderung eines Eintrags*** ➜ ***Erweiterte Einstellungen*** enthält mit der Einstellung ***Betriebsmodus*** = *Access Client* folgende Felder:

Parameter	Wert
Kanäle scannen	Mit der Einstellung *Alle* sucht das Garät auf allen Kanäle nach verfügbaren Drahtlosnetzwerken. Standardmäßig ist *Alle* aktiv. Wenn die Einstellung *Alle* nicht aktiv ist, können Sie im Feld ***Ausgewählte Kanäle*** die gewünschten Kanäle für den Suchprozess festlegen.
Ausgewählte Kanäle	Nur wenn im Feld ***Kanäle scannen*** die Einstellung *Alle* nicht aktiv ist. Wenn Sie die Einstellung ***Betriebsmodus*** = *Access Client* mit **OK** gespeichert haben, sehen Sie hier alle aktuell ausgewählten Kanäle. Sie können die Kanäle festlegen, auf denen das Gerät nach verfügbaren Drahtlosnetzwerken suchen soll. Sie können aktuell ausgewählte Kanäle löschen. Wenn nicht alle Kanäle ausgewählt sind, können Sie mit **Hinzufügen** fehlende Kanäle hinzufügen.

Parameter	Wert
Roaming-Profil	Hier wählen Sie, unter welchen Bedingungen Roaming vorgenommen werden soll. Sie können dazu entweder ein vordefinierte Profil verwenden, das für alle Parameter feste Werte enthält, oder Sie können alle Parameter selbst festlegen. Jeder AP, der dem Client bekannt ist, wird mit Hilfe dieser Parameter bewertet und mit einer Zahl versehen, Der Client verbindet sich mit dem AP mit der höchsten Zahl. Mögliche Werte: ■ *Schnelles Roaming*: Bei Datenraten von 26 Mbit/s oder weniger wird Roaming durchgeführt sobald ein Access Point mit besserer Datenrate verfügbar ist. ■ *Normales Roaming* (Standardwert): Bei Datenraten von ca. 18 Mbit/s oder weniger wird Roaming durchgeführt sobald ein Access Point mit besserer Datenrate verfügbar ist. ■ *Langsames Roaming*: Bei Datenraten von ca. 6 Mbit/s oder weniger wird Roaming durchgeführt sobald ein Access Point mit besserer Datenrate verfügbar ist. ■ *Kein Roaming*: Roaming wird nur durchgeführt, wenn die Verbindung zum Access Point unterbrochen ist. ■ *Benutzerdefiniertes Roaming*: Sie können die Roaming Parameter nach ihren Wünschen festlegen.

Parameter	Wert
Scan-Schwelle	Nur für ***ROAMING-PROFIL*** = *Benutzerdefiniertes Roaming* kann der Wert verändert werden, bei allen anderen Einstellungen für ***ROAMING-PROFIL*** ist jeweils ein bestimmter Wert fest zugeordnet. Geben Sie den Schwellwert in dBm ein, ab dem nach verfügbaren Drahtlosnetzwerken gesucht werden soll. Der Standardwert ist *-70* dBm.
Scan-Intervall	Nur für ***ROAMING-PROFIL*** = *Benutzerdefiniertes Roaming* kann der Wert verändert werden, bei allen anderen Einstellungen für ***ROAMING-PROFIL*** ist jeweils ein bestimmter Wert fest zugeordnet. Geben Sie ein, in welchen zeitlichen Abständen in Millisekunden nach verfügbaren Drahtlos-netzwerken gesucht werden soll. Der Standardwert ist *5000* ms.
Channel Sweep	Nur für ***ROAMING-PROFIL*** = *Benutzerdefiniertes Roaming* kann der Wert verändert werden, bei allen anderen Einstellungen für ***ROAMING-PROFIL*** ist jeweils ein bestimmter Wert fest zugeordnet. Geben Sie die Zahl der Frequenzen an, die für einen Suchvorgang benutzt werden soll. Der Standardwert ist *2*. Der Wert *0* schaltet den Suchvorgang ab. Der Wert -1 benutzt alle verfügbaren Frequen-zen für einen Suchvorgang.

Parameter	Wert
Min. Zeitraum aktiver Scan	Nur für ***ROAMING-PROFIL*** = *Benutzerdefiniertes Roaming* kann der Wert verändert werden, bei allen anderen Einstellungen für ***ROAMING-PROFIL*** ist jeweils ein bestimmter Wert fest zugeordnet. Geben Sie das kleinste Zeitintervall ein, das beim Active Scanning für eine Frequenz verwendet werden soll. (Active Scanning bedeutet, dass der Client aktiv nach Access Points in seiner Reichweite sucht.) Der Standardwert ist *10* ms.
Max. Zeitraum aktiver Scan	Nur für ***ROAMING-PROFIL*** = *Benutzerdefiniertes Roaming* kann der Wert verändert werden, bei allen anderen Einstellungen für ***ROAMING-PROFIL*** ist jeweils ein bestimmter Wert fest zugeordnet. Geben Sie das größte Zeitintervall ein, das beim Active Scanning für eine Frequenz verwendet werden soll. (Active Scanning bedeutet, dass der Client aktiv nach Access Points in seiner Reichweite sucht.) Der Standardwert ist *40* ms.
Min. Zeitraum passiver Scan	Nur für ***ROAMING-PROFIL*** = *Benutzerdefiniertes Roaming* kann der Wert verändert werden, bei allen anderen Einstellungen für ***ROAMING-PROFIL*** ist jeweils ein bestimmter Wert fest zugeordnet. Geben Sie das kleinste Zeitintervall ein, das beim Passive Scanning für eine Frequenz verwendet werden soll. (Beim Passive Scanning empfängt und bewertet der Client die Signale, die alle Access Points senden.) Der Standardwert ist *20* ms.

Parameter	Wert
Max. Zeitraum passiver Scan	Nur für ***ROAMING-PROFIL*** = *Benutzerdefiniertes Roaming* kann der Wert verändert werden, bei allen anderen Einstellungen für ***ROAMING-PROFIL*** ist jeweils ein bestimmter Wert fest zugeordnet. Geben Sie das größte Zeitintervall ein, das beim Passive Scanning für eine Frequenz verwendet werden soll. (Beim Passive Scanning empfängt und bewertet der Client die Signale, die alle Access Points senden.) Der Standardwert ist *120* ms.
Association Advantage	Nur für ***ROAMING-PROFIL*** = *Benutzerdefiniertes Roaming* kann der Wert verändert werden, bei allen anderen Einstellungen für ***ROAMING-PROFIL*** ist jeweils ein bestimmter Wert fest zugeordnet. Dieser Parameter ist ein Maß dafür, wie wichtig es ist, dass bei einem Client Roaming stattfindet. Je größer der Wert ist, desto größer ist die Wahrscheinlichkeit, dass kein Roaming stattfindet sondern der Client beim aktuellen Access Point bleibt. Der Standardwert ist *10*.
RSSI Advantage	Nur für ***ROAMING-PROFIL*** = *Benutzerdefiniertes Roaming* kann der Wert verändert werden, bei allen anderen Einstellungen für ***ROAMING-PROFIL*** ist jeweils ein bestimmter Wert fest zugeordnet. Dieser Parameter ist ein Maß dafür, wie stark die Signalstärke bei der Roaming-Entscheidung berücksichtigt wird. Je höher der Wert ist, desto eher findet Roaming statt. Der Standardwert ist *10*.

Parameter	Wert
Weight of Age	Nur für ***ROAMING-PROFIL*** = *Benutzerdefiniertes Roaming* kann der Wert verändert werden, bei allen anderen Einstellungen für ***ROAMING-PROFIL*** ist jeweils ein bestimmter Wert fest zugeordnet. Dieser Parameter ist ein Maß dafür, wie stark der Zeitraum in die Roaming-Entscheidung eingeht, den der Client den AP bereits "kennt". Je höher der Wert ist, desto wahrscheinlicher ist es, dass der Client beim Roaming auf einen bereits bekannten AP zurückgreift. Der Standardwert ist *5*.
Weight of Penalty	Nur für ***ROAMING-PROFIL*** = *Benutzerdefiniertes Roaming* kann der Wert verändert werden, bei allen anderen Einstellungen für ***ROAMING-PROFIL*** ist jeweils ein bestimmter Wert fest zugeordnet. Mit diesem Parameter können Sie die Roaming- Entscheidung zusätzlich beeinflussen. Der Wert gibt an, wie stark der Wert von ***PENALTY-WERT*** die Roaming Entscheidung beeinflusst. Der Standardwert ist *10.*

Parameter	Wert
Penalty-Wert	Nur für ***ROAMING-PROFIL*** = *Benutzerdefiniertes Roaming* kann der Wert verändert werden, bei allen anderen Einstellungen für ***ROAMING-PROFIL*** ist jeweils ein bestimmter Wert fest zugeordnet. Mit diesem Parameter können Sie die Roaming Entscheidung zusätzlich beeinflussen. Je größer der Wert ist desto größer ist der Einfluss auf die Roaming Entscheidung. Der Standardwert ist *50*.

Tabelle 2-2: Felder im Menü ***WIRELESS LAN*** ➜ ***WLANx*** ➜ ***EINSTELLUNGEN FUNKMODUL*** ➜ ***SYMBOL ZUR ÄNDERUNG EINES EINTRAGS*** ➜ ***ERWEITERTE EINSTELLUNGEN***

2.6 GRE

Ab Systemsoftware 7.8.2 ist die Funktion GRE im FCI verfügbar. Im Menü *VPN* ➜ *GRE* können Sie das Generic Routing Encapsulation (GRE) Protokoll verwenden, um andere Protokolle einzukapseln und mittels Tunnel über das Internet Protokoll zu transportieren.

Das Menü ***VPN*** ➜ ***GRE*** ➜ ***GRE-TUNNEL*** ➜ ***NEU*** enthält folgende Felder:

Parameter	Wert
Beschreibung	Geben Sie eine Bezeichnung für den GRE-Tunnel ein.
Lokale GRE-IP-Adresse	Geben Sie die Quell-IP-Adresse der GRE-Pakete zum GRE-Partner ein. Wird keine IP-Adresse angegeben (dies entspricht der IP-Adresse 0.0.0.0), wird die Quell-IP-Adresse der GRE-Pakete automatisch aus einer der Adressen der Schnittstellen ausgewählt, über die der GRE-Partner erreicht wird.

Parameter	Wert
Remote-GRE-IP-Adresse	Geben Sie die Ziel-IP-Adresse des Hosts bzw. des Netzwerks ein, zu dem die Pakete durch den GRE-Tunnel geschickt werden sollen.
Standardroute	Wenn Sie die ***STANDARDROUTE*** aktivieren, werden automatisch alle Daten auf eine einzige Verbindung geleitet. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Geben Sie die IP-Adresse ein, die als Quelladresse für diese GRE-Verbindung genutzt wird.
Routeneinträge	Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. Fügen Sie mit **Hinzufügen** neue Einträge hinzu. ***ENTFERNTE IP-ADRESSE***: IP-Adresse des Ziel-Hosts oder -Netzwerkes. ***NETZMASKE***: Netzmaske zu ***ENTFERNTE IP-ADRESSE***. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. ***METRIK***: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0* ... *15*). Standardwert ist *1*.
MTU	Geben Sie die maximale Paketgröße (Maximum Transfer Unit, MTU) in Bytes an, die für die GRE-Verbindung zwischen den Partnern verwendet werden darf. Mögliche Werte sind *1* bis *8192*. Der Standardwert ist *1500*.

Parameter	Wert
Schlüssel verwenden	Aktivieren Sie die Eingabe einer Kennung für die GRE-Verbindung, welche die Unterscheidung mehrerer parallel laufender GRE-Verbindungen zwischen zwei GRE-Partnern ermöglicht (siehe RFC 1701). Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Schlüsselwert	Nur für ***SCHLÜSSEL VERWENDEN*** = *aktiviert*. Geben Sie die GRE-Verbindungskennung ein. Mögliche Werte sind *0* bis *2147483647*. Der Standardwert ist *0*.

Tabelle 2-3: Felder im Menü ***VPN*** ➜ ***GRE*** ➜ ***GRE-TUNNEL*** ➜ ***NEU***

2.7 E-Mail-Benachrichtigung

Ab Systemsoftware 7.8.2 ist die Funktion E-Mail-Benachrichtigung im FCI verfügbar. Der Administrator des Gateways kann sich über bestimmte Ereignisse, die durch Syslog Meldungen angezeigt werden, per E-Mail informieren lassen.

Die Funktion E-Mail-Benachrichtigung können Sie im FCI Menü ***EXTERNE BERICHTERSTATTUNG*** ➜ ***E-MAIL-BENACHRICHTIGUNG*** konfigurieren.

Das Menü ***EXTERNE BERICHTERSTATTUNG*** ➜ ***E-MAIL-BENACHRICHTIGUNG*** ➜ ***E-MAIL-BENACHRICHTIGUNGS-SERVER*** ➜ ***BASISPARAMETER*** enthält folgende Felder:

Parameter	Wert
Benachrichtigungsdienst	Hier aktivieren bzw. deaktivieren Sie die Funktion. Standardmäßig ist die Funktion aktiv.
E-Mail-Adresse des Absenders	Tragen Sie hier die E-Mail-Adresse ein, die im Absenderfeld der E-Mail angezeigt werden soll.

Parameter	Wert
Maximale Nachrichten-zahl pro Minute	Hier können Sie die Anzahl der ausgehenden E-Mails pro Minute begrenzen. Zur Verfügung stehen Werte von *1* bis *15*. Der Standardwert ist *6*.

Tabelle 2-4: Felder im Menü ***Externe Berichterstattung*** ➜ ***E-Mail-Benachrichtigung*** ➜ ***E-Mail-Benachrichtigungs-Server*** ➜ ***Basisparameter***

Das Menü ***Externe Berichterstattung*** ➜ ***E-Mail-Benachrichtigung*** ➜ ***E-Mail-Benachrichtigung-Server*** ➜ ***SMTP-Einstellungen*** enthält folgende Felder:

Parameter	Wert
SMTP-Server	Geben Sie die Adresse (IP-Adresse oder gültiger DNS-Name) des Mailservers ein, der zum Versenden der E-Mails verwendet werden soll. Die Eingabe ist auf 40 Zeichen begrenzt.
SMTP-Authentifizierung	Wählen Sie, ob eine Authentifizierung zwischen Client und Server benutzt werden soll und wenn ja, welches Protokoll verwendet werden soll. Mögliche Werte: ■ *Keine* (Standardwert): Es soll keine Authentifizierung verwendet werden. ■ *ESMTP*: Extended SMTP mit Authentifizierung soll verwendet werden. ■ *SMTP after POP*: Zuerst soll POP (Post Office Protocol) mit Authentifizierung verwendet werden und danach SMTP mit derselben Authentifizierung.

Parameter	Wert
Benutzername	Nur für ***SMTP-Authentifizierung*** = *ESMTP* oder ***SMTP-Authentifizierung*** = *SMTP after POP*. Geben Sie den Benutzernamen des Clients für die Authentifizierung an.
Password	Nur für ***SMTP-Authentifizierung*** = *ESMTP* oder ***SMTP-Authentifizierung*** = *SMTP after POP*. Geben Sie das Passwort des Clients für die Authentifizierung an.
POP3-Server	Nur für ***SMTP-Authentifizierung*** = *SMTP after POP*. Geben Sie die Adresse (IP-Adresse oder gültiger DNS-Name) des POP3-Servers ein, von dem die Mails abgerufen werden sollen. Damit der Mailserver Anfragen per POP3 beantworten kann, muss eine entsprechende POP3-Server-Software installiert sein.
POP3-Timeout	Nur für ***SMTP-Authentifizierung*** = *SMTP after POP*. Geben Sie die Zeitspanne ein, nach deren Ablauf die Authentifizierung als ungültig betrachtet wird. Danach können keine E-Mails mehr versandt werden. Mögliche Werte sind *60* bis *3600* Sekunden, der Standardwert ist *600*.

Tabelle 2-5: Felder im Menü ***Externe Berichterstattung*** ➜ ***E-Mail-Benachrichtigung*** ➜ ***E-Mail-Benachrichtigungs-Server*** ➜ ***SMTP-Einstellungen***

Das Menü ***Externe Berichterstattung*** ➜ ***E-Mail-Benachrichtigung*** ➜ ***E-Mail-Benachrichtigungsempfänger*** ➜ ***Neu*** ➜ ***E-Mail-***

BENACHRICHTIGUNGSEMPFÄNGER HINZUFÜGEN/BEARBEITEN enthält folgende Felder:.

Parameter	Wert
Empfänger	Tragen Sie hier die E-Mail-Adresse des Empfängers ein.
Enthaltene Zeichenfolge	Geben Sie die Zeichenfolge ein, bei deren Auftreten in einer Syslog Meldung eine E-Mail geschickt werden soll. Bedenken Sie, dass ohne die Verwendung von Wildcards (z. B. "*") nur diejenigen Zeichenfolgen die Bedingung erfüllen, die exakt der Eingabe entsprechen. Daher wird in der Regel die eingegebene Zeichenfolge Wildcards enthalten. Um über alle Syslog-Meldungen des gewählten Levels informiert zu werden, geben Sie lediglich "*" ein.
Schweregrad	Wählen Sie den Syslog-Level, auf dem die im Feld ***ENTHALTENE ZEICHENFOLGE*** eingegebene Zeichenfolge vorkommen muss, damit eine E-Mail-Benachrichtigung ausgelöst wird. Mögliche Werte: ■ *Notfall* (Standardwert) ■ *Alarm* ■ *Kritisch* ■ *Fehler* ■ *Warnung* ■ *Benachrichtigung* ■ *Informationen* ■ *Debug.*

Parameter	Wert
Timeout für Nachrichten	Geben Sie ein, wieviel Sekunden das Gateway nach einem entsprechenden Ereignis höchstens warten darf, bevor eine E-Mail versandt wird. Zur Verfügung stehen Werte von *0* bis *86400*, der Standardwert ist *60*. Der Wert *0* deaktiviert den Timeout.
Anzahl Nachrichten	Hier geben Sie die Anzahl an Syslog Meldungen ein, die erreicht sein muss, ehe eine E-Mail für diesen Fall gesendet werden kann. Wenn ***TIMEOUT FÜR NACHRICHTEN*** konfiguriert ist, wird die E-Mail bei dessen Ablauf gesendet, auch wenn die ***ANZAHL NACHRICHTEN*** noch nicht erreicht ist. Der Standardwert ist *1*.
Nachrichtenkomprimierung	Hier können Sie auswählen, ob der Text der E-Mail-Nachricht verkürzt werden soll. Die E-Mail enthält dann die Syslog-Meldung nur einmal und zusätzlich die Anzahl der entsprechenden Ereignisse. Aktivieren oder deaktivieren Sie die Funktion. Standardmäßig ist die Funktion aktiv.

Tabelle 2-6: Felder im Menü ***EXTERNE BERICHTERSTATTUNG*** ➜ ***E-MAIL-BENACHRICHTIGUNG*** ➜ ***E-MAIL-BENACHRICHTIGUNGSEMPFÄNGER*** ➜ ***NEU*** ➜ ***E-MAIL-BENACHRICHTIGUNGSEMPFÄNGER HINZUFÜGEN/ BEARBEITEN***

Das Menü ***Externe Berichterstattung ➜ E-Mail-Benachrichtigung ➜ E-Mail-Benachrichtigungsempfänger ➜ Neu ➜ Überwachte Subsysteme*** enthält folgendes Feld:

Parameter	Wert
Subsystem	Hier wählen Sie die Subsysteme aus, die überwacht werden sollen. Fügen Sie mit **Hinzufügen** neue Subsysteme hinzu.

Tabelle 2-7: Felder im Menü ***Externe Berichterstattung ➜ E-Mail-Benachrichtigung ➜ E-Mail-Benachrichtigungsempfänger ➜ Neu ➜ Überwachte Subsysteme***

2.8 SSH Client

Ab **Systemsoftware 7.8.2** ist die Funktion SSH (Secure Shell) Client verfügbar. Sie können von Ihrem Gateway zu einem entfernten Rechner oder zu einem zweiten Gateway eine gesicherte Verbindung herstellen und z. B. die Kommandozeile des entfernten Rechners auf Ihrem Gateway ausgeben lassen oder die Konfiguration des zweiten Gateways prüfen.

Um sich auf einem entfernten Rechner bzw. auf einem zweiten Gateway einzuwählen, geben Sie auf der Kommandozeile *ssh <Benutzername Gateway>@<IP-Adresse des entfernten Rechners bzw. IP-Adresse des zweiten Gateways>* ein.

2.9 IGMP Host für lokale Applikationen

Systemsoftware 7.8.2 unterstützt IGMP für lokale Multicast Applikationen; d.h. lokale Applikationen (z. B. Access Point Discovery Daemon) melden sich mit IGMP Reports an bestimmte Multicast-Gruppen an und können so Multicast-Pakete empfangen. Dies ist beispielsweise notwendig im Umfeld von Switches, die IGMP Snooping einsetzen.

Für diesen Modus brauchen Sie IGMP nicht mehr für jede Anwendung manuell auf der entsprechenden Schnittstelle zu aktivieren, sondern es genügt, den implementierten Automatismus zu benutzen: Sobald ein Host eine lokale Anwendung öffnet, die Multicast verwendet, wird IGMP automatisch auf der entsprechenden Schnittstelle aktiviert und die IGMP-Schnittstelle wird im Host-Modus betrieben.

Diesen Automatismus konfigurieren Sie im FCI Menü ***Routing*** ➜ ***Multicast*** ➜ ***Optionen*** mit der Einstellung ***IGMP-Status*** = *Auto*.

Falls der IGMP-Status auf aktiv steht (***IGMP-Status*** = *Aktiv)*, müssen Sie die jeweiligen Schnittstellen manuell für IGMP Host konfigurieren. Wird eine Schnittstelle im "Nur-Host-Modus" betrieben (***Routing*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ ***Symbol zur Änderung eines Eintrags*** mit ***Modus*** = *Nur Host*), so ist nur garantiert, dass Anwendungen auf dieser Schnittstelle Pakete erhalten. Um IGMP Stati von anderen Systemen auf dieser Schnittstelle zu verwalten und eingehende Pakete dorthin zu routen, muss Routing erlaubt sein (***Routing*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ ***Symbol zur Änderung eines Eintrags*** mit ***Modus*** = *Host und Routing*).

Im Menü ***Routing*** ➜ ***Multicast*** ➜ ***IGMP*** sehen Sie die Schnittstellen, auf denen IGMP entweder durch den erwähnten Automatismus oder von Hand im Menü ***Routing*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ ***Neu*** aktiviert wurde.

2.10 HTML-Seite für Update

Ab **Systemsoftware 7.8.2** steht nach dem Einloggen unter der Adresse *http://<IP-Adresse Ihres Gateways>/maint* eine HTML-Seite als Teil der Systemsoftware zur Verfügung, um ein Update des Gateways durchzuführen.

2.11 SSL Tunnel

Ab Systemsoftware 7.8.2 können Sie ungesicherte TCP Daten sicher über einen SSL Tunnel transportieren, ohne ein VPN zu benötigen. Jeder SSL

Tunnel kann dabei bis zu fünf TCP Verbindungen enthalten, z. B. für HTTP, wo meist mehrere TCP Verbindungen aufgebaut werden.

SSL Tunnel können Sie im Setup Tool Menü ***SECURITY*** ➜ ***SSL TUNNEL*** konfigurieren.

Das Menü ***SECURITY*** ➜ ***SSL TUNNEL*** enthält folgende Felder:

Parameter	Wert
SSL Tunnel	Hier aktivieren bzw. deaktivieren Sie die Funktion. Mögliche Werte: ■ *down* (Standardwert): Die Funktion ist nicht aktiv. ■ *up*: Die Funktion ist aktiv.
TCP Keepalive Retries	Wenn auf der TCP-Verbindung aktuell keine Daten ausgetauscht werden, können Sie hier festlegen, wie oft maximal ein TCP-Paket zu Testzwecken versendet wird, um festzustellen, ob der Partner die aktuelle TCP-Sitzung aufrecht erhält. Die Felder ***TCP KEEPALIVE RETRIES*** und ***TCP KEEPALIVE TIMEOUT (SEC)*** legen fest, wie oft und in welchem zeitlichen Abstand ein TCP-Paket zu Testzwecken geschickt wird. Zur Verfügung stehen Werte von *0* bis *255*. Der Standardwert ist *3*.

Parameter	Wert
TCP Keepalive Timeout (sec)	Wenn auf der TCP-Verbindung aktuell keine Daten ausgetauscht werden, können Sie hier festlegen, nach wievielen Sekunden erneut ein TCP-Paket versendet wird, um festzustellen, ob der Partner die aktuelle TCP-Sitzung aufrecht erhält. Die Felder ***TCP KEEPALIVE RETRIES*** und ***TCP KEEPALIVE TIMEOUT (SEC)*** legen fest, wie oft und in welchem zeitlichen Abstand ein TCP-Paket zu Testzwecken geschickt wird. Zur Verfügung stehen Werte von *0* bis *65535*. Der Standardwert ist *5*.

Tabelle 2-8: Felder im Menü ***SECURITY*** ➜ ***SSL TUNNEL***

Im Menü ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** sehen Sie die bereits angelegten Tunnel. Im Menü ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** können Sie neue Tunnel anlegen.

Das Menü ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** enthält folgende Felder:

Parameter	Wert
Adminstatus	Hier aktivieren bzw. deaktivieren Sie den Tunnel. Mögliche Werte: ■ *down* (Standardwert): Der Tunnel ist nicht aktiv. ■ *up*: Der Tunnel ist aktiv.
Description	Geben Sie eine Beschreibung ein, welche den Tunnel eindeutig identifiziert.

Parameter	Wert
External IP	IP-Adresse der Gegenstelle ■ *client*: IP-Adresse, zu der sich der Client verbindet. ■ *server*: Ist eine IP-Adresse angegeben, so ist nur zu einem Client mit dieser IP-Adresse eine Verbindung möglich. Ist keine IP-Adresse angegeben, so kann eine Verbindung zu einem beliebigen Client aufgebaut werden.
External port	Externer Port, der entsprechend der Einstellung im Feld ***EXTERNAL MODE*** verwendet wird.
External mode	Gibt an, ob der Tunnel zum angegebenen ***EXTERNAL PORT*** aufgebaut wird oder ob am ***EXTERNAL PORT*** gelauscht wird, weil der Tunnel von der Gegenseite aufgebaut wird. Mögliche Werte: ■ *client*: Der Tunnel wird zum ***EXTERNAL PORT*** aufgebaut. ■ *server*: Am ***EXTERNAL PORT*** wird gelauscht.
Internal IP	lokale IP-Adresse des Gateways Der Standardwert ist *127.0.0.1*.
Internal port	Interner Port, der entsprechend der Einstellung im Feld ***INTERNAL MODE*** verwendet wird.

Parameter	Wert
Internal mode	Gibt an, ob der Tunnel vom angegebenen ***INTERNAL PORT*** aus aufgebaut wird oder ob am ***INTERNAL PORT*** gelauscht wird, weil der Tunnel von der Gegenseite aufgebaut wird. Mögliche Werte: ■ *client*: Der Tunnel wird vom ***INTERNAL PORT*** aus aufgebaut. ■ *server*: Am ***INTERNAL PORT*** wird gelauscht.
Certificate	Geben Sie das Zertifikat an, dass zur Authentisierung verwendet werden soll.
CA Certificate	Geben Sie das CA (Certificate Authority) Zertifikat an, dass zur Authentisierung verwendet werden soll.

Tabelle 2-9: Felder im Menü ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD**

Das Menü ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** ➜ ***(ADVANCED) TIMER SETTINGS*** enthält folgende Felder:

Parameter	Wert
Retry timeout (s)	Bestimmt bei fehlgeschlagenem Verbindungsaufbau die Zeit in Sekunden, nach der erneut versucht wird, den Tunnel aufzubauen. Zur Verfügung stehen Werte von *0* bis *3600*. Der Standardwert ist *60*.

Parameter	Wert
Maximum retries	Bestimmt bei fehlgeschlagenem Verbindungsaufbau die maximale Anzahl der Versuche den Tunnel aufzubauen. Zur Verfügung stehen Werte von *-1* bis *50*. Ein Wert von *-1* bedeutet, dass immer wieder versucht wird, einen Tunnel aufzubauen ohne die Anzahl der Versuche zu beschränken. Der Standardwert ist *3*.
Reopen delay (s)	Bestimmt bei erfolgreichem Verbindungsaufbau die Verzögerung, mit der ein unterbrochener Tunnel erneut geöffnet wird. Zur Verfügung stehen Werte von *-1* bis *315360000*. Ein Wert von *-1* bedeutet, dass der Tunnel sofort wieder geöffnet wird. Der Standardwert ist *0*.
Shorthold	Bestimmt das Inaktivitätsintervall in Sekunden. Zur Verfügung stehen Werte von *-1* bis *3600*. Ein Wert von *-1* bedeutet, dass die Verbindung immer bestehen bleibt, d.h. nie abgebaut wird.

Tabelle 2-10: Felder im Menü ***Security*** ➜ ***SSL Tunnel*** ➜ ***Tunnels*** ➜ **ADD** ➜ ***(Advanced) Timer Settings***

2.12 Abfrage der BOSS Mindestversion

Ab **Systemsoftware 7.8.2** können Sie die mindestens erforderliche BOSS Version abfragen, die z. B. für die korrekte Funktion einer bestimmten Hardware erforderlich ist. Wenn eine Mindestversion angegeben ist, benötigen Sie diese oder eine neuere Version.

Geben Sie dazu auf der SNMP-Shell *show rev* ein.

Sie erhalten folgende Ausgabe (Beispiel):

Logic : V.1.0
Bootmon : V.7.8.2
BOSS : V.7.8.2 IPSec from 2008/12/12 00:00:00
(minimal version: 7.8.2)

Die letzte Zeile enthält die Angabe der Mindestversion.

Alternativ können Sie die Mindestversion mit dem update-Kommando abfragen.

Geben Sie dazu auf der SNMP.Shell *update -i* ein:

Sie erhalten die Ausgabe:

Flash-ROM management shell
`Flash-Sh>`

Geben Sie *info -m* ein.

Wenn eine Mindestversion im Flash definiert ist, erhalten Sie folgende Ausgabe (Beispiel):

BOSS minimal version 7.8.2.

Wenn keine Mindestversion definiert ist, erhalten Sie die Ausgabe:

BOSS minimal version: none specified.

2.13 VLAN Priorisierung

Wenn ab **Systemsoftware 7.8.2** Daten mit VLAN Priorisierung entsprechend IEEE 802 empfangen werden, werden diese akzeptiert und weiterverarbeitet.

2.14 Prüfung der MAC-Adresse

Um die Gefahr von Spoofing-Attacken zu reduzieren, wurde eine zusätzliche Prüfung der MAC-Adresse hinzugefügt, wenn in der MIB-Tabelle ***ipExtIfTable*** die Variable ***AllowedPeers*** = *dhcpclients* gesetzt ist.

2.15 DNS - Bailiwick Checking

Mit **Systemsoftware 7.8.2** wurde Bailiwick Checking hinzugefügt, d.h. es können in DNS-Anworten keine ungefragt mitgelieferten Einträge (Additional Resource Records) eingeschleust werden.

2.16 FCI - Unterstützung von Opera 9.5

Ab **Systemsoftware 7.8.2** können Sie das **Funkwerk Configuration Interface** mit dem Browser Opera 9.5 benutzen.

2.17 FCI - Listeneinträge - neuer Filter

Im FCI wurde beim Filtern von Listeneinträgen unter ***Filtern in*** die Option *Status* hinzugefügt.

2.18 FCI - Nachrichtenlevel von Systemprotokolleinträgen festlegen

Im FCI Menü ***Systemverwaltung*** ➜ ***Globale Einstellungen*** ➜ ***System*** können Sie im Feld ***Maximaler Nachrichtenlevel von Systemprotokolleinträgen*** festlegen, bis zu welchem Level Systemprotolleinträge unter ***Monitoring*** ➜ ***Internes Protokoll*** angezeigt werden sollen.

2.19 FCI - Eingabefeld für DHCP-MAC-Adresse

Ab **Systemsoftware 7.8.2** können Sie im FCI Menü ***LAN*** ➜ ***IP-KONFIGURATION*** ➜ ***SCHNITTSTELLEN*** ➜ ***NEU*** im Feld ***MAC-ADRESSE*** die voreingestellte MAC-Adresse ändern.

2.20 FCI - Neues Feld TCP-MSS-Clamping

Mit **Systemsoftware 7.8.2** wurde im FCI Menü ***LAN*** ➜ ***IP-KONFIGURATION*** ➜ ***SCHNITTSTELLEN*** ➜ ***NEU / SYMBOL ZUR ÄNDERUNG EINES EINTRAGS*** ➜ ***ERWEITERTE EINSTELLUNGEN*** das neue Feld ***TCP-MSS-CLAMPING*** zur Verfügung gestellt, das von RDP, VNC, Lotus Notes und SQL Syn Prozesse über IPSec Tunnels benötigt wird.. Mit der Einstellung ***TCP-MSS-CLAMPING*** = *aktiviert* wird der Standardwert *1350* angezeigt; Sie können diesen Wert ändern.

2.21 FCI - WLAN - Neue Felder Nutzungsbereich und IEEE 802.11d-Konformität

Im FCI Menü ***WIRELESS LAN*** ➜ ***WLANX*** ➜ ***EINSTELLUNGEN FUNKMODUL*** steht für die Einstellung ***BETRIEBSMODUS*** = *Access Client* und ***CLIENT-MODUS*** = *Infrastruktur* das neue Feld ***NUTZUNGSBEREICH*** zur Verfügung.

Im FCI Menü ***WIRELESS LAN*** ➜ ***WLANX*** ➜ ***EINSTELLUNGEN FUNKMODUL*** steht für die Einstellung ***BETRIEBSMODUS*** = *Access Client* das neue Feld ***IEEE 802.11D-KONFORMITÄT*** zur Verfügung.

2.22 FCI - WLAN - Neue Option für Client-Modus

Im FCI Menü ***Wireless LAN ➜ WLANx ➜ Einstellungen Funkmodul*** steht für die Einstellung ***Betriebsmodus*** = *Access Client* im Feld ***Client-Modus*** die neue Option *Ad-Hoc* zur Verfügung.

2.23 FCI - WLAN - Neues Feld ARP Processing

Im FCI Menü ***Wireless LAN ➜ WLANx ➜ Drahtlosnetzwerke (VSS) ➜*** **Neu** steht das neue Feld ***ARP Processing*** zur Verfügung.

2.24 FCI - WLAN - Neue Felder WPA Cipher und WPA2 Cipher

Im FCI Menü ***Wireless LAN ➜ WLANx ➜ Drahtlosnetzwerke (VSS)*** stehen für die Einstellungen ***Sicherheitsmodus*** = *WPA-PSK* oder ***Sicherheitsmodus*** = *WPA-Enterprise* die Felder ***WPA Cipher*** und ***WPA2 Cipher*** zur Verfügung.

Im FCI Menü ***Wireless LAN ➜ WLANx ➜ Client Link*** steht für die Einstellung ***Sicherheitsmodus*** = *WPA-PSK* und ***WPA-Modus*** = *WPA* das Feld ***WPA Cipher*** bzw. für die Einstellung ***Sicherheitsmodus*** = *WPA-PSK* und ***WPA-Modus*** = *WPA2* das Feld ***WPA2 Cipher*** zur Verfügung.

2.25 FCI - Multicast - Erweiterungen

Wenn das FCI Menü ***Routing ➜ Multicast ➜ IGMP ➜ Symbol zur Änderung eines Eintrags*** mit **OK** verlassen wird, ohne dass unter ***Routing ➜ Routen ➜ IP-Routen*** eine ***Erweiterte Route*** angelegt ist, erscheint die Meldung "Wenn

Sie diese Seite durch Klicken auf die Schaltfläche "OK" verlassen, wird Multicast für alle Schnittstellen ohne erweiterte Routen deaktiviert."

Im FCI Menü ***Routing*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ ***Symbol zur Änderung eines Eintrags / Neu*** steht im Feld ***Modus*** die neue Option *Nur Host* zur Verfügung.

Im FCI Menü ***Routing*** ➜ ***Multicast*** ➜ ***Optionen*** steht im Feld ***IGMP-Status*** die neue Option *Auto* zur Verfügung.

2.26 FCI - Administrative Zugriffsregeln anzeigen lassen

Im FCI Menü ***Firewall*** ➜ ***Richtlinien*** ➜ ***Filterregeln*** können Sie mit ***Administrative Zugriffsregeln anzeigen*** = *aktiviert* die administratven Zugriffsregeln anzeigen lassen.

2.27 FCI - DHCP-Optionen erweitert

Ab **Systemsoftware 7.8.2** erhalten Sie im FCI Menü ***Lokale Dienste*** ➜ ***DHCP-Server*** ➜ ***DHCP Pool*** ➜ ***Symbol zur Änderung eines Eintrags*** ➜ ***Erweiterte Einstellungen*** im Feld ***DHCP-Optionen*** mit Klicken auf **Hinzufügen** das Dropdown-Menü ***Option*** mit den zusätzlichen DHCP Optionen *Zeitserver*, *DNS-Server*, *DNS-Domänenname*, *WINS/NBNS-Server*, *WINS/NBT Node Type* und *TFTP-Server*. Zusätzlich wird das Feld ***Wert*** angezeigt, in das Sie den Wert der gewählten Option eintragen müssen.

2.28 FCI - Scheduling - neue Option

Im FCI Menü ***Lokale Dienste*** ➜ ***Scheduling*** ➜ ***Zeitplan*** ➜ **Neu** wurde im Feld ***Aktion auswählen*** die Option *Dynamische DNS aktualisieren* hinzugefügt. Diese Option wird angezeigt, wenn im Menü ***Lokale Dienst*** ➜ ***DynDNS-Client*** ➜ ***DynDNS-Aktualisierung*** Einträge konfiguriert sind.

2.29 FCI - Wartung - Neues Feld Systemlogik

Im FCI Menü ***WARTUNG*** ➜ ***SOFTWARE & KONFIGURATION*** steht das neue Feld ***SYSTEMLOGIK*** zur Anzeige der Logikversion zur Verfügung, da sich die Versionen der Logik und der Systemsoftware unterscheiden können.

2.30 FCI - Schnittstellenstatistik Einzelheiten

Im FCI Menü ***MONITORING*** ➜ ***SCHNITTSTELLEN*** ➜ ***STATISTIK*** können Sie zu jeder Schnittstelle mit Hilfe des Lupe-Symbols Einzelheiten anzeigen lassen.

2.31 Setup Tool - WLAN - ARP Processing for Access Points

Im Setup Tool Menü ***WLAN*** ➜ ***VSS CONFIGURATION*** ➜ **Edit** steht mit der Einstellung ***OPERATION MODE*** = *Access Point* unter ***WLAN*** das neue Feld ***ARP PROCESSING*** zur Verfügung. ARP Processing dient zur Reduzierung des ARP Datenverkehrs im WLAN-Netz durch Umwandeln der Broadcast ARP Requests in Unicast ARP Requests und zur Erhöhung der Datenübertragungsrate, da Unicast Pakete mit größerer Geschwindigkeit gesendet werden können als Broadcast- bzw. Multicast-Pakete.

2.32 Setup Tool - HTTPS hinzugefügt

Im Setup Tool Menü ***SECURITY*** ➜ ***LOCAL SERVICES*** ➜ ***ACCESS CONTROL*** ➜ **Add** wurde im Feld ***SERVICE*** die Option *https (tcp)* hinzugefügt.

2.33 Setup Tool - Neue Option für Monitoring Interfaces

Im Setup Tool Menü ***MONITORING AND DEBUGGING*** ➜ ***INTERFACES*** ➜ **EXTENDED** steht im Feld ***OPERATION*** die neue Option *set interface dialup* zur Verfügung.

2.34 DHCP - Neue MIB-Variable SendRepliesToRelay

In der MIB-Tabelle ***IPDHCPPOOLTABLE*** wurde die Variable ***SENDREPLIESTORELAY*** hinzugefügt, um bei Bedarf DHCP-Anworten des internen DHCP Servers zum DHCP Relay senden zu können.

2.35 Bandwidth on Demand (BoD) erweitert

Ab **Systemsoftware 7.8.2** können Sie in der MIB-Tabelle ***PPPEXTIFTABLE*** mit der MIB-Variablen ***BODMODE*** = *bod-reduce-incoming* die Zahl der Links / B-Kanäle bei eingehenden Verbindungen automatisch reduzieren lassen, wenn diese nicht benutzt werden.

Das ist z. B. nützlich, wenn Windows Clients für Multilink PPP-Einwahl konfiguriert wurden, das Gateway jedoch ohne Multilink PPP und ohne Channel Bundling konfiguriert ist.

2.36 Neue MIB-Tabelle wlanIfFeatureTable

Mit **Systemsoftware 7.8.2** steht die neue MIB-Tabelle ***WLANIFFEATURETABLE*** zur Verfügung. Sie enthält die Parameter zur Konfiguration einer Wireless Karte.

2.37 Neue Variablen in MIB-Tabelle authEapol

Mit **Systemsoftware 7.8.2** stehen in der MIB-Tabelle ***authEapol*** die neuen MIB-Variablen ***QuietPeriod***, ***TxPeriod***, ***SuppTimeout***, ***MaxReq***, ***ReAuthPeriod***, ***ReAuthEnabled*** und ***KeyTxEnabled*** zur Verfügung.

3 Änderungen

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

3.1 Passwortlänge begrenzt

Ab **Systemsoftware 7.8.2** ist die Länge des Passworts für die Konfigurationsdatei auf 10 Zeichen begrenzt.

3.2 Ping-Funktion ergänzt

Ab **Systemsoftware 7.8.2** kann in ausgehenden IP-Paketen das sogenannte Don't-Fragment-Flag gesetzt werden. Geben Sie dazu *ping -M <IP-Adresse>* ein.

3.3 DNS mit zwei IP-Adressen

Manche SIP-Provider nutzen eine Infrastruktur mit optimierter Lastverteilung, um für ihre Nutzer hohe Verfügbarkeit zu garantieren.

Schickt ein Gateway einen DNS Request an einen dieser Provider, so werden zwei IP-Adressen zurückgegeben. Ab **Systemsoftware 7.8.2** werden beide Adressen vom Gateway weitergeleitet und nicht wie bisher nur eine einzige IP-Adresse. Die beiden Adressen können mit dem Befehl `nslookup` z. B. unter Windows XP ermittelt werden.

3.4 DNS Query IDs zufallsgeneriert

Ab **Systemsoftware 7.8.2** werden aus Sicherheitsgründen die DNS Query IDs zufallsgeneriert.

3.5 IP-Adress-Bereiche (Pools) überarbeitet

Die Verwaltung der IP-Adressen wurde überarbeitet, da IP-Adress-Bereiche inzwischen von verschiedenen Subsystemen verwendet werden.

An Stelle der MIB-Tabelle ***ipDynAddrTable*** werden jetzt zwei Tabellen benutzt, die Tabelle ***ipDynaAddrTable*** für dynamisch erzeugte Einträge, die nicht in der Konfiguration gespeichert werden, und ***ipStatAddrTable*** für manuell erzeugte Einträge, die in der Konfiguration gespeichert werden. In der Tabelle

IPDYNAADDRTABLE wurde die MIB-Variable ***STATE*** um die beiden Werte *iprequest* und *ipreply* erweitert. Darüber hinaus werden in diesem Zusammenhang die MIB-Tabelle ***IPDYNADDRPOOLTABLE*** , die alle IP-Adressen enthält, die dynamisch zugewiesen werden können, und die MIB-Tabelle ***IPADDRTABLE*** verwendet.

3.6 Standardwert für Anzahl der NAT Ports vergrößert

Der Standardwert für die Anzahl von NAT Ports in globalen Pools wurde von 4000 auf 32767 erhöht.

3.7 NAT - Pass-Through hinzugefügt

Ab **Systemsoftware 7.8.2** können Sie mit Hilfe der neuen MIB-Tabelle ***IPNATEXCLUDETABLE*** einen Teil des Datenverkehrs von NAT ausnehmen, d.h. NAT Pass-Through konfigurieren.

3.8 UDP Portnummern zufallsgeneriert

Ab **Systemsoftware 7.8.2** werden die Nummern die UDP Ports für ***LOKALE DIENSTE*** zufällig im Bereich 1024 bis 60000 zugewiesen. Bisher wurden sie beginnend mit 1024 in aufsteigender Reihenfolge verwendet.

3.9 FCI - IP-Konfiguration - Update

Ab **Systemsoftware 7.8.2** wird nach Änderungen im FCI Menü ***SYSTEMVERWALTUNG*** ➜ **Schnittstellenmodus / Bridge-Gruppen** im Feld ***MODUS / BRIDGE-GRUPPE*** ein Update der IP-Konfiguration durchgeführt.

3.10 FCI - Fast Roaming - Kanäle festlegen

Im FCI Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Einstellungen Funkmodul*** ➜ ***Symbol zur Änderung eines Eintrags*** können Sie mit der Einstellung ***Betriebsmodus*** = Access *Client* und ***Kanäle scannen*** = *deaktiviert* (unter ***Erweiterte Einstellungen***) im Feld ***Ausgewählte Kanäle*** festlegen, auf welche Kanälen der WLAN-Client nach verfügbaren Drahtlosnetzwerken scannen soll.

3.11 FCI - NAT-Eintrag für ausgehende Verbindung

Bisher wurde im FCI Menü ***Routing*** ➜ ***NAT*** ➜ ***Portweiterleitung*** bei Portweiterleitung von eingehenden Verbindungen automatisch gleichzeitig ausgehendes NAT Mapping durchgeführt, d.h. ein Eintrag in der MIB-Tabelle ***ipNatOutTable*** angelegt. Jetzt können Sie im Feld ***Entsprechender NAT-Eintrag für ausgehende Verbindung*** wählen, ob dieser Eintrag angelegt werden soll oder nicht.

3.12 FCI - DHCP-Konfiguration geändert

Im FCI Menü ***Lokale Dienste*** ➜ ***DHCP-Server*** ➜ ***IP/MAC-Bindung*** wurde wegen geänderter DHCP-Konfiguration die Schaltfläche **Löschen** entfernt.

3.13 FCI - Layout, Rechtschreibung, Terminologie

Kleine Schönheitsfehler im Layout wurden beseitigt. Die Bedienbarkeit einiger Menüs wurde verbessert. Rechtschreibung und Terminologie wurden überarbeitet.

3.14 FCI / Setup Tool - DHCP Pool Konfiguration erweitert

Wenn Sie einen DHCP Pool unabhängig von einem IP- oder Routeneintrag anlegen wollen, können Sie im FCI Menü ***LOKALE DIENSTE*** ➜ ***DHCP-SERVER*** ➜ ***DHCP POOL*** ➜ ***NEU*** ➜ ***ERWEITERTE EINSTELLUNGEN*** im Feld ***GATEWAY*** die Option *Kein Gateway* wählen. Alternativ können Sie im Setup Tool Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ **ADD** im Feld ***GATEWAY*** die Option *no* wählen. Beide Einstellungen benutzen die MIB-Variable ***GATEWAYENABLED*** in der MIB-Tabelle ***IPDHCPPOOLTABLE***.

3.15 Setup Tool - Schnittstelle - Bezeichnung geändert

Im Setup Tool Menü ***WAN PARTNER*** ➜ **ADD/EDIT** ➜ ***ADVANCED SETTINGS*** wurde im Feld ***SPECIAL INTERFACE TYPES*** die Bezeichnung der Option *Call-by-Call (dialin only)* in *Multiuser (dialin only)* geändert.

3.16 Setup Tool - Configuration Management erweitert

Im Setup Tool Menü ***CONFIGURATION MANAGEMENT*** wurde das Feld ***OPERATION*** um die Optionen *get-all (TFTP -> FLASH)* und *put-all (FLASH -> TFTP)* erweitert.

3.17 Setup Tool - Verbesserter Konfigurationswechsel

Die Umsetzung der IP- und DHCP-Konfiguration beim Wechsel einer Schnittstelle von Routing zu Bridging und umgekehrt ist verbessert worden, um jeweils konsistente Konfigurationen zu erhalten.

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 7.8.2 gelöst worden:

4.1 Stacktrace bei Routing over L2TP bzw Bridging over L2TP

(ID 10619)

Bei Routing over L2TP bzw. Bridging over L2TP konnte es bei hohen Datenraten zu einer Panic gefolgt von einem Stacktrace kommen.

Das Problem ist gelöst worden.

4.2 PPPoE und Ethernet Schnittstellen - Probleme mit externen DSL-Modems

(ID 9225)

Wenn die MIB-Variable ***MAXTXRATE*** der MIB-Tabelle ***QOSIFTABLE*** geändert worden war, wurde in der Tabelle ***IFTABLE*** die Variable ***SPEED*** für PPPoE und Ethernet Schnittstellen nicht angepasst. Das führte zu Latenzprobleme in Szenarien mit externen DSL-Modems.

Das Problem ist gelöst worden.

4.3 PPPoE-Multilink - fehlende Fehlerprüfung

(ID n/a)

Bisher konnten für einen PPPoE-Multilink mehrere Schnittstellen mit derselben MAC Adresse verwendet werden, weil eine Fehlerprüfung fehlte.

Das Problem ist gelöst worden.

4.4 Zahl der Telnet Sessions unbegrenzt

(ID 1882)

Wenn viele eingehende Telnet Sessions gleichzeitig geöffnet wurden, reagierte das Gateway nicht mehr.

Das Problem ist gelöst worden, die Anzahl der Telnet Sessions ist jetzt begrenzt, der Standardwert ist *10*.

4.5 RIP - Source IP-Adresse fehlerhaft

(ID 10378)

Über WAN-Schnittstellen wurden RIP-Pakete mit Source IP-Adresse 0.0.0.0 versendet.

Das Problem ist gelöst worden.

4.6 Syslog-Meldungen - Werte nicht ausgegeben

(ID 10305)

In Syslog-Meldungen wurden Werte im 64-Bit-Format nicht ausgegeben; stattdessen wurde ’u’ angezeigt.

Das Problem ist gelöst worden, die Werte werden korrekt ausgegeben.

4.7 SNMP Shell - Ein-/Ausgabeverknüpfung (pipe) fehlerhaft

(ID n/a)

Bei Verwendung einer pipe konnte es vorkommen, dass Prozesse eingefroren wurden.

Das Problem ist gelöst worden.

4.8 SNMP Shell - Probleme mit Signal Interrupt

(ID n/a)

Beim Senden eines SIGINT (Signal Interrupt; z. B. mit der Tastenkombination **Strg** + **c** oder mit der Eingabe *kill*) an die SNMP Shell während der Anzeige des Prompt, konnte es vorkommen, dass sich der Prompt veränderte und es nicht möglich war, die vorher angezeigte Tabelle erneut anzeigen zu lassen.

Das Problem ist gelöst worden.

4.9 QoS - Zählerüberlauf

(ID n/a)

Wegen der hohen Datenraten moderner Schnittstellen kam es bei Verwendung von Qos häufig zum Überlauf der Oktet-Zähler.

Das Problem ist gelöst worden., es werden jetzt 64-Bit-Zähler verwendet.

4.10 Multicast Protokolle - Verlust von 64-Byte-Blöcken

(ID n/a)

Wenn Multicast Protokolle wie z. B. IGMP eingeschaltet waren, gingen 64-Byte-Blöcke verloren, wenn ein "Nicht-Daten" Multicast Paket gesendet wurde.

Das Problem ist gelöst worden.

4.11 Name-Server-Antworten nicht akzeptiert

(ID n/a)

Fälschlicherweise wurden "manke" DNS-Requests nicht akzeptiert und mit der Fehlermeldung "Bailiwick check failed for <xxx>.com" abgelehnt. Irrtümlicherweise wurde bei der Validierung eines Top-Level-Records die Domain-Zugehörigkeit intern falsch berechnet.

Das Problem ist gelöst worden.

4.12 FCI - Keine Extended Routen nach Reboot

(ID 9386)

Wenn Extended Routen angelegt und in der Boot Konfiguration gespeichert wurden, waren sie nach einem Reboot nicht mehr vorhanden.

Das Problem ist gelöst worden.

4.13 FCI - Online-Hilfe fehlerhaft

(ID n/a)

In der Online-Hilfe des FCI traten wegen doppelter IDs Fehler in der Navigation auf.

Das Problem ist gelöst worden.

4.14 FCI - Aktive Sitzungen fälschlicherweise angezeigt

(ID n/a)

Im FCI Menü ***Systemverwaltung*** ➜ ***Status*** wurden für Geräte der **Wx002**-Serie fälschlicherweise aktive Sitzungen angezeigt.

Das Problem ist gelöst worden.

4.15 FCI - Aktive Sitzungen nicht angezeigt

(ID 9345)

Im FCI Menü ***Systemverwaltung*** ➜ ***Status*** wurde im Feld ***Aktive Sitzungen (SIF, RTP, etc...)*** immer *0* angezeigt.

Das Problem ist gelöst worden.

4.16 FCI - Unterschiedliche Formate bei Zeitangaben

(ID n/a)

Im FCI Menü ***Systemverwaltung*** ➜ ***Status*** im Feld ***Systemdatum*** und im FCI Menü ***Systemverwaltung*** ➜ ***Globale Einstellungen*** ➜ ***Datum und Uhrzeit***

im Feld ***Neues Datum*** wurden die Zeitangaben in unterschiedlichen Formaten angezeigt.

Das Problem ist gelöst worden, in beiden Feldern wird dasselbe Format benutzt.

4.17 FCI - Layout nicht korrekt

(ID 10122)

Im FCI Menü ***Systemverwaltung*** ➜ ***Globale Einstellungen*** ➜ ***Datum und Uhrzeit*** war bei verschiedenen Gerätetypen die Beschriftung des Reiters im Browser nicht einheitlich und auf der Seite selbst war das Layout nicht korrekt.

Die Probleme sind gelöst worden.

4.18 FCI - Bridge Gruppen - Liste nicht korrekt

(ID n/a)

Im FCI Menü ***Systemverwaltung*** ➜ ***Schnittstellenmodus / Bridge-Gruppen*** zeigte die Liste virtuelle Ethernet-Schnittstellen, obwohl diese Schnittstellen nicht im Bridging-Modus betrieben werden können.

Das Problem ist gelöst worden.

4.19 FCI - Standardschnittstellen löschbar

(ID n/a)

Im FCI Menü ***Systemverwaltung*** ➜ ***Administrativer Zugriff*** konnten mit Hilfe des Symbols Mülltonne Standardschnittstellen gelöscht werden.

Das Problem ist gelöst worden, das Symbol Mülltonne ist bei den Standardschnittstellen entfernt worden.

4.20 FCI - Probleme mit SIF

(ID 8575)

Im FCI Menü ***Systemverwaltung*** ➜ ***Administrativer Zugriff*** traten Probleme mit den Schnittstellen-basierten SIF-Richtlinien auf.

Die Probleme sind durch eine Standardkonfiguration der SIF-Regeln für die physikalischen Schnittstellen und eine Standardregel für den Zugriff auf die Lokalen Dienste gelöst worden.

4.21 FCI - Umschalten vom DHCP-Modus zu statischer IP-Adresse

(ID n/a)

Wenn im FCI Menü ***LAN*** ➜ ***IP-Konfiguration*** ➜ ***Schnittstellen*** ➜ ***Symbol zur Änderung eines Eintrags*** das Feld ***Adressmodus*** von *DHCP* zu *Statisch* geändert wurde, war es möglich, die Konfiguration mit leerem Feld ***IP-Adresse*** zu speichern. Wenn die einzige IP Ethernet Schnittstelle mit dieser Konfiguration gespeichert wurde, konnte nur noch über die serielle Konsole auf das Gerät zugegriffen werden.

Das Problem ist gelöst worden, unabhängig von der gewählten Schnittstelle erscheint bei leerem Feld ***IP-Adresse*** die Meldung "Bitte geben Sie eine gültige IP-Adresse ein!"

4.22 FCI - Entfernen eines VLAN schlug fehl

(ID 10230)

Wenn im FCI Menü ***LAN*** ➜ ***VLAN*** ➜ ***VLANs*** ➜ ***Symbol zur Änderung eines Eintrags*** alle ***VLAN-Mitglieder*** eines VLANs gelöscht waren, konnte es vorkommen, dass das VLAN selbst nicht gelöscht werden konnte. Wenn ein VLAN ***VLAN-Mitglieder*** enthielt, wurde trotzdem das Papierkorb-Symbol zum Löschen angezeigt.

Die Probleme sind gelöst worden.

4.23 FCI - Menü Wireless LAN überarbeitet

(ID 9287)

Das FCI Menü ***Wireless LAN*** war nicht Style Guide konform.

Das Problem ist gelöst worden, das Menü ***Wireless LAN*** ist überarbeitet und an den FCI Style Guide angepasst worden.

4.24 FCI - Monitoring Bridges fälschlicherweise angezeigt

(ID 10638)

Obwohl im FCI Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Einstellungen Funkmodul*** mit der Einstellung ***Betriebsmodus*** = *Access Client* keine Bridge konfiguriert werden kann, wurde das Menü ***Monitoring*** ➜ ***Bridges*** angezeigt.

Das Problem ist gelöst worden.

4.25 FCI - WDS-Link Menü nicht angezeigt

(ID 10642)

Wenn im FCI Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Einstellungen Funkmodul*** ➜ ***Symbol zur Änderung eines Eintrags*** das Feld ***Betriebsmodus*** = *Access Point* gesetzt war und ein ***Kanal*** ungleich *Auto* gewählt war, wurde das Menü

Wireless LAN ➜ WLANx ➜ WDS-Links nicht angezeigt und es konnte daher kein WDS-Link konfiguriert werden. Im Setup Tool konnte der WDS-Link konfiguriert werden.

Das Problem ist gelöst worden.

4.26 FCI - Fehlende Übertragungsraten

(ID 10608)

Im FCI Menü ***Wireless LAN ➜ WLANx ➜ Einstellungen Funkmodul ➜ Symbol zur Änderung eines Eintrags*** fehlten im Feld ***Max. Übertragungsrate*** im Dropdown-Menü die Werte *6 Mbit/s* und *9 Mbit/s*.

Das Problem ist gelöst worden.

4.27 FCI - WLAN - fehlende Standardeinträge

(ID n/a)

Im FCI Menü ***Wireless LAN ➜ WLANx ➜ Einstellungen Funkmodul ➜ Symbol zur Änderung eines Eintrags ➜ Erweiterte Einstellungen*** wurden die Standardeinträge nicht korrekt benutzt und es erschien eine Systemmeldung, solange das Funkmodul nicht zum ersten Mal aktiviert war.

Das Problem ist gelöst worden, die entsprechenden Felder werden erst angezeigt, wenn das Funkmodul aktiviert ist.

4.28 FCI - keine Eingabe von Hexadezimalzahlen

(ID 9679)

Im FCI Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Drahtlosnetzwerke (VSS)*** ➜ ***Symbol zur Änderung eines Eintrags / Neu*** ➜ ***Sicherheitseinstellungen*** konnten mit ***Sicherheitsmodus*** = *WEP 40* oder mit ***Sicherheitsmodus*** = WEP 104 in den Feldern ***WEP-Schlüssel 1-4*** keine Hexadezimalzahlen eingegeben werden. Mit dem Setup Tool war die Eingabe möglich.

Das Problem ist gelöst worden.

4.29 FCI - Online-Hilfe - Grafiken nicht angezeigt

(ID 9514)

Im FCI wurde in der Online-Hilfe im Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Client Link*** und im Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Client Link*** ➜ ***Client Link Scan*** je eine Grafik nicht angezeigt.

Das Problem ist gelöst worden.

4.30 FCI - WLAN - Irreführende Fehlermeldung

(ID 10320)

Wurde in der WLAN-Konfiguration im FCI Menü ***Wireless LAN*** ➜ ***Verwaltung*** das Feld ***Region*** auf "United States" geändert, während im Menü ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Einstellungen Funkmodul*** ➜ ***Symbol zur Änderung eines Eintrags*** das Feld ***Kanal*** auf *12* oder *13* gesetzt war, wurde die Fehlermeldung "Nicht unterstützte Änderungen durch das Setup Tool!" angezeigt, da die Verwendung dieser Kanäle in den USA nicht gestattet ist.

Das Problem ist gelöst worden.

4.31 FCI - Port Forwarding - Protokollliste nicht korrekt

(ID 9609)

Im FCI Menü ***Routing*** ➜ ***NAT*** ➜ ***Portweiterleitung*** ➜ **Neu** wurde mit ***Dienst*** = *Benutzerdefiniert* im Feld ***Protokoll*** im Dropdown-Menü statt *Skip* der Begriff *Überspringen* angezeigt.

Das Problem ist gelöst worden.

4.32 FCI - Lastverteilung 100% überschritten

(ID 9790)

Im FCI Menü ***Routing*** ➜ ***Lastverteilung*** ➜ ***Lastverteilungsgruppen*** ➜ **Neu** konnte mit **Hinzufügen** das ***Verteilungsverhältnis*** über alle Schnittstellen größer als 100% konfiguriert werden.

Das Problem ist gelöst worden, die Summe ist jetzt insgesamt auf 100% begrenzt. Bei Überschreiten der 100%-Grenze erscheint eine Fehlermeldung.

4.33 FCI - PPPoE - Absturz des Geräts

(ID 10612)

Im FCI Menü ***WAN*** ➜ ***Internet + Einwählen*** ➜ ***PPPoE*** ➜ **Neu** ➜ ***Erweiterte Einstellungen*** wurde bei bestehender Internet-Verbindung durch Deaktivieren der Option ***TCP-ACK-Pakete priorisieren*** ein Absturz des Geräts herbeigeführt.

Das Problem ist gelöst worden.

4.34 FCI - PPTP-Callback

(ID 9786)

Wenn im FCI Menü ***VPN*** ➜ ***PPTP*** ➜ ***PPTP-Tunnel*** ➜ **Neu** ➜ **Erweiterte Einstellungen** das Feld ***Callback*** nicht aktiviert war, wurden trotzdemdie Felder ***Eingehende ISDN-Nummer*** und ***Ausgehende ISDN-Nummer*** angezeigt.

Das Problem ist gelöst worden, die Felder werden nur angezeigt, wenn ***Callback*** aktiv ist.

4.35 FCI - DynDNS-Aktualisierung - Eingabekontrolle fehlte

(ID n/a)

Im FCI Menü ***Lokale Dienste*** ➜ ***DynDNS-Client*** ➜ ***DynDNS-Aktualisierung*** ➜ **Neu** konnten die Felder ***Hostname*** und ***Benutzername*** leer gelassen werden, im Feld ***Schnittstelle*** konnte eine ungültige Auswahl getroffen werden.

Das Problem ist gelöst worden.

4.36 FCI - DHCP-Pool-Einstellungen nicht gespeichert

(ID 10823)

Im FCI Menü ***Lokale Dienste*** ➜ ***DHCP-Server*** ➜ ***DHCP Pool*** wurde die Einstellung im Feld ***Pool für weitergeleitete DHCP-Anforderungen*** mit **OK** nicht gespeichert.

Das Problem ist gelöst worden.

4.37 FCI - WLAN - "Unbekannte Schnittstelle"

(ID n/a)

Wenn im FCI Menü ***Lokale Dienste*** ➜ ***Scheduling*** ➜ ***Zeitplan*** ➜ **Neu** das Feld ***Aktion auswählen*** = *WLAN aktivieren* gesetzt war, enthielt die Dropdown-Liste im Feld ***Schnittstelle auswählen*** den Wert *Unbekannte Schnittstelle*.

Das Problem ist gelöst worden.

4.38 FCI - Problem bei fehlender Konfigurationsdatei

(ID 10755)

Wenn Sie im FCI Menü ***Wartung*** ➜ ***Software & Konfiguration*** eine Konfiguration umbennennen, kopieren oder löschen wollten und keine Konfigurationsdatei verfügbar war, erschien ein leeres Dropdown-Menü und eine wenig hilfreiche Fehlermeldung.

Das Problem ist gelöst worden, es erscheint die Fehlermeldung "Keine Konfigurationsdatei gefunden".

4.39 FCI - Unbeabsichtigte Leerzeichen

(ID n/a)

Im FCI Menü ***Wartung*** ➜ ***Software & Konfiguration*** traten in der Tabelle unbeabsichtigte Leerzeichen auf.

Das Problem ist gelöst worden.

4.40 FCI - IP-Accounting - Seitenfilter funktionierte nicht korrekt

(ID n/a)

Im FCI Menü ***Externe Berichterstattung*** ➜ ***IP-Accounting*** ➜ ***Schnittstellen*** funktionierte beim Wechsel von *Alle auswählen* zu *Alle deaktivieren* und umgekehrt im Feld ***IP-Accounting*** der Seitenfilter nicht korrekt.

Das Problem ist gelöst worden.

4.41 FCI - Anzeige der Systemmeldungen fehlerhaft

(ID 10253)

Im FCI Menü ***Monitoring*** ➜ ***Internes Protokoll*** funktionierte mit der Einstellung ***Ansicht*** größer als 20 (z. B. 500) das Blättern nicht bzw. beim Blättern wurden die Seiten nicht korrekt angezeigt.

Das Problem ist gelöst worden.

4.42 FCI - Filter nicht korrekt

(ID 10174 / n/a)

Im FCI Menü ***Monitoring*** ➜ ***Schnittstellen*** ➜ ***Statistik*** konnte es vorkommen, dass die Filterfunktion "Beschreibung" bei WLAN-Schnittstellen nicht korrekt funktionierte. Es wurde "Nicht unterstützt" in der Spalte Typ angezeigt und es erschien zusätzlich die Meldung "Nicht unterstützte Änderungen durch das Setup Tool!".

Das Problem ist gelöst worden.

4.43 FCI - Falsches Icon für Detailansicht angezeigt

(ID n/a)

Im FCI Menü ***MONITORING*** ➜ ***SCHNITTSTELLEN*** ➜ ***STATISTIK*** wurde für die Anzeige der Detailansicht das Icon "Schraubenschlüssel" statt des Icons "Lupe" angezeigt.

Das Problem ist gelöst worden.

4.44 Setup Tool - Stacktrace bei ISDN-LAN-LAN-Verbindung

(ID 9751)

Eine ISDN-LAN-LAN-Verbindung mit statischer Kanalbündelung verursachte einen Stacktrace gefolgt von einem Reboot.

Das Problem ist gelöst worden.

4.45 Setup Tool - WAN Bridge nicht konfigurierbar

(ID n/a)

Nach der Einführung des neuen Bridge-Konzepts war eine Konfiguration des WAN Bridging im Setup Tool nicht möglich.

PPP-Schnittstellen konnten nicht mehr gleichzeitig für Routing und Bridging genutzt werden.

Das Problem ist gelöst worden.

4.46 Setup Tool - Probleme bei der Anzeige einer IP-Adresse

(ID 10833)

Wenn im Setup Tool im Bridging Modus im Menü ***ETHERNET*** ➜ **Edit** im Feld ***LOCAL IP-NUMBER*** die IP-Adresse geändert und nicht gespeichert wurde, so konnte man durch Scrollen im ersten Feld ***LOCAL IP-NUMBER*** die aktuelle IP-Adresse und im zweiten Feld ***LOCAL IP-NUMBER*** die neu eingegebene IP-Adresse sehen.

Das Problem ist gelöst worden.

4.47 Setup Tool - Schnittstelle im Bridging-Modus - Konfiguration fehlerhaft

(ID 9595)

Die Einstellungen im Setup Tool Menü ***ETHERNET*** ➜ **Edit** ➜ ***ADVANCED SETTINGS*** wurden ausschließlich auf Schnittstellen im Routing-Modus und nicht auf Schnittstellen im Bridging-Modus angewendet. Mit den entsprechenden MIB-Variablen konnten die Einstellungen korrekt gesetzt werden.

Das Problem ist gelöst worden.

4.48 Setup Tool - WLAN - falsche Felder angezeigt

(ID n/a)

Im Setup Tool wurden mit der Einstellung ***OPERATION MODE*** = *Client* unter ***WLAN*** im Menü ***WLAN*** ➜ ***CLIENT CONFIGURATION*** mit ***SECURITY MODE*** = *NONE*, ***SECURITY MODE*** = *WEP 40/64* oder ***SECURITY MODE*** = *WEP 104/128* die Felder ***WPA CIPHER*** bzw. ***WPA2 CIPHER*** angezeigt.

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

4.49 Setup Tool - PPPoE - MAC-Adressen nicht eindeutig

(ID n/a)

Wenn ein Ethernet Switch im Split-Ports-Modus betrieben wurde, konnte es bei PPPoE- oder bei Multilink-PPPoE-Verbindungen zu Problemen kommen, weil die zugeordneten MAC-Adressen mehrfach auftraten.

Das Problem ist gelöst worden. Bei Bedarf wird im Setup Tool Menü ***WAN PARTNER*** ➜ ***ADD*** ➜ ***ADVANCED SETTINGS*** ➜ ***EXTENDED INTERFACE SETTINGS*** im Feld ***CREATE NEW (UNIQUE) MAC ADDRESS <NEUE MAC-ADRESSE> FOR PORT <ENTSPRECHENDER PORT>*** eine neue MAC-Adresse zugeordnet.

4.50 Setup Tool - SIF - Port-Bereich fehlerhaft

(ID n/a)

Im Setup Tool Menü ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES*** ➜ **ADD/EDIT** konnten fälschlicherweise im Feld ***RANGE*** Werte von *0* bis *65535* eingegeben werden.

Das Problem ist gelöst worden, der Wertebereich wurde auf *1 - 65536* geändert.

4.51 Setup Tool - Fehlendes Feld Mode

(ID 9296)

Im Setup Tool Menü ***IP*** ➜ ***ROUTING*** ➜ ***ADDEXT*** wurde für die Einstellung ***ROUTE TYPE*** = *Default route* und ***NETWORK*** = *LAN* das Feld ***MODE*** nicht angezeigt.

Das Problem ist gelöst worden.

4.52 Setup Tool - Löschen zweier TDRC Einträge verursachte Stacktrace

(ID 6464)

Wenn im Setup Tool Menü ***IP*** ➜ ***Bandwidth Management (TDRC / Load Balancing / BOD)*** ➜ ***TCP Download Rate Control (TDRC)*** ➜ **ADD** zwei Einträge für eine T-DSL Schnittstelle angelegt waren, einer mit ***Optimize Download Rate via TCP ACK priorisation*** = *yes* und der andere mit ***Optimize Download Rate via TCP ACK priorisation*** = *no* und ***TDRC Mode*** = *static (fixed maximum rate for TCP download)*, beide Einträge markiert und gelöscht wurden, erschien die Meldung "Exception: 0x1c00 Data breakpoint Debug" gefolgt von einem Stacktrace ohne Reboot.

Das Problem ist gelöst worden.

4.53 Setup Tool - PPPoE Passthrough - fehlerhafte Anzeige der Schnittstellen

(ID 10106)

Im Setup Tool Menü ***PPP*** ➜ ***PPPoE Passthrough*** wurden im Bereich ***Physical or virtual Ethernet Port attached to PPPoE Client(s)*** die Bridge-Gruppen-Schnittstellen nicht angezeigt.

Das Problem ist gelöst worden.