VPN Access 250, VPN Access 1000, X8500,

Release Notes
Systemsoftware 7.8.7

Version 1.0

Ziel und Zweck

Dieses Dokument beschreibt neue Funktionen, Änderungen und behobene Fehler in **Systemsoftware 7.8.7**.

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

1.1 Gültigkeit

Systemsoftware 7.8.7 steht ausschließlich für folgende Geräte zur Verfügung und kann auf anderen Geräten nicht eingesetzt werden:

- **VPN Access 250**
- **VPN Access 1000**
- **X8500**.

1.2 Inkompatibilität

Konfigurationen, die unter **Systemsoftware 7.8.7** erstellt oder gesichert werden, sind unter Umständen zu einigen Versionen unserer Systemsoftware inkompatibel.

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

1.2.1 Vorbereitung und Update

Gehen Sie ggf. folgendemaßen vor, um ein Update auf **Systemsoftware 7.8.7** 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 Gateways 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 7.8.7** wie gewohnt durch und starten Sie das Gateway neu.
   Das Gateway startet mit der neuen Software, die bestehende Boot-Konfiguration wird verwendet.

1.2.2 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 das Gateway. Es startet nun mit der zuvor gesicherten Boot-Konfiguration und der älteren Version der Systemsoftware.

2 Neue Funktionen

Systemsoftware 7.8.7 enthält eine Reihe neuer Funktionen, die den Leistungsumfang gegenüber Systemsoftware 7.4.1 erheblich erweitern:

2.1 Neues Discovery Protokoll

Ab Systemsoftware 7.8.7 steht das neue Discovery Protokoll SNMP-Multicast zur Verfügung.

Der Dime Manager nutzt dieses Protokoll, um Funkwerk-Geräte im Netz zu finden.

2.2 Software-Update und Dateitransfer erweitert

Ab **Systemsoftware 7.8.7** können Sie HTTP(S) und Web-Server-Authentifizierung für ein Software-Update oder für den Transfer von Konfigurationsdateien verwenden.

Für die URL-Kodierung wird das Standardformat benutzt:

http[s]://[<Benutzername>:<Passwort>@] <Host> [:<Port>]/<Pfad>/<Datei>

tftp://<Server>/<Datei>

Sie können diese Angaben beim Update und beim Transfer einer Konfigurationsdatei auf der Kommandozeile verwenden sowie im entsprechenden Feld auf der Seite Systemwartung unter *http://<IP-Adresse Ihres Gateways>/maint*.

Hinweis

Bitte beachten Sie, dass die URL auf der Kommandozeile in zwei Teile (*hosturl* und *file*) aufgeteilt werden muss, um das Dateiformat festzulegen (siehe Beispiele weiter unten).

Bei der Systemwartung können Sie ausschließlich die komplette URL im neuen Dateiformat verwenden.

Software-Update

Im Folgenden sehen Sie Beispiele für Eingaben, wenn mit dem Kommando *update* ein Software-Update durchgeführt werden soll:

update http://server:8080/download/R232bw_bl7802.sx6

update https://server/download/R232bw_bl7802.sx6

update http://user:secret@server/download/R232bw_bl7802.sx6.

Konfiguration

Konfigurationsdateien können in zwei unterschiedlichen Formaten vorliegen: dem alten unverschlüsselten Format und dem neuen CSV-Format (siehe **Release Notes Systemsoftware 7.5.1**).

Hinweis

Beachten Sie, dass Sie ausschließlich das neue CSV-Format verwenden sollten, da die verwendete Datei in diesem Format kleiner ist, bei Bedarfi verschlüsselt werden kann und die Kompatibilität zwischen den verschiedenen Systemsoftware-Versionen besser gewährleistet ist.

Wenn Sie Konfigurationsdateien an einen Web-Server übertragen wollen, der über die HTTP-Erweiterung WEBDAV (PUT Methode) verfügt, müssen Sie Folgendes eingeben:

cmd=put_all hosturl="http://<Server>/<Pfad>" file="<config>.cf" (für das veraltete Format).

cmd=put_all hosturl="http://<Server>/<Pfad>" file:"<config>.cf" (für das neue CSV-Format, wenn es unverschlüsselt verwendet werden soll)

cmd=put_all hosturl="http://<Server>/<Pfad>" file="<pwd>:<config>.cf" (für das neue CSV-Format, wenn die Daten mit Passwort verschlüsselt werden sollen)

(<config> bedeutet, dass Sie hier den Namen der gewünschten Konfigurationsdatei ohne Klammern eingeben müssen.)

Wenn Sie Konfigurationsdateien von einem Web-Server herunterladen wollen, müssen Sie Folgendes eingeben:

cmd=get_all hosturl="http://<Server>/<Pfad>" file="<config>.cf" (erkennt veraltetes und neues Format automatisch)

cmd=get_all hosturl="http://<Server>/<Pfad>" file="<pwd>:<config>.cf" (lädt eine verschlüsselte Datei herunter).

2.3 Abfrage der BOSS Mindestversion

Ab **Systemsoftware 7.8.7** 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.

2.4 Simple Network Time Protocol Server

Mit Systemsoftware 7.8.7 wird die SNTP Server Funktion unterstützt.

Bisher blieben Zeitanfragen unbeantwortet, die von einem Client an das Gateway geschickt wurden. Mit der SNTP Server Funktion verfügt das Gateway über einen internen Zeitserver und kann eine Antwort auf solche Client-Anfragen schicken (Zeiteinstellungen und andere Optionen).

Die SNTP Server Funktion können Sie im Setup Tool im Menü ***System*** ➜ ***Time and Date*** im neuen Feld ***Internal Time Server*** konfigurieren:

Parameter	Wert
Internal Time Server	Bestimmt, ob der interne Zeitserver aktiviert werden soll und wenn ja, in welchem Modus er benutzt werden soll. Folgende Optionen sind möglich: ■ *disabled* (Standardwert): Zeitanfragen eines Clients werden nicht beantwortet. Dies entspricht dem Verhalten in früheren Software-Versionen. ■ *enabled*: Zeitanfragen eines Clients werden mit der aktuellen Systemzeit beantwortet. Diese wird als GMT ohne Offset angegeben. ■ *depends on client mode*: Client-Anfragen werden beantwortet, wenn die Systemzeit von einem NTP Server stammt oder über das ISDN bezogen wurde.

Tabelle 2-1: Zusätzliches Feld im Menü ***System*** ➜ ***Time and Date***

Hinweis

Beachten Sie, dass für die SNTP Server Funktion die MIB-Variable *biboAdmNTPServer* benutzt wird, (und nicht die MIB-Variable *biboAdmTimeServer*).

2.5 ISDN-Diebstahlsicherung

Ab Systemsoftware 7.8.7 können Sie mit der Funktion ISDN-Diebstahlsicherung verhindern, dass sich ein Dieb, der ein Gateway gestohlen hat, Zutritt zum LAN des Gateway-Besitzers verschafft. (Ohne Diebstahlsicherung könnte er sich über ISDN in das LAN einwählen, wenn das Feld *SHORTHOLD* = *-1* gesetzt ist.)

Alle Schnittstellen, für welche die Diebstahlsicherung aktiv ist, werden beim Booten des Gateways administrativ auf "down" gesetzt (d.h. MIB-Variable *AdminStatus = down)*.

Anschließend ruft sich das Gateway über ISDN selbst an und überprüft seinen Standort. Wenn die konfigurierten ISDN Rufnummern von den gewählten Rufnummern abweichen, bleiben die Schnittstellen deaktiviert.

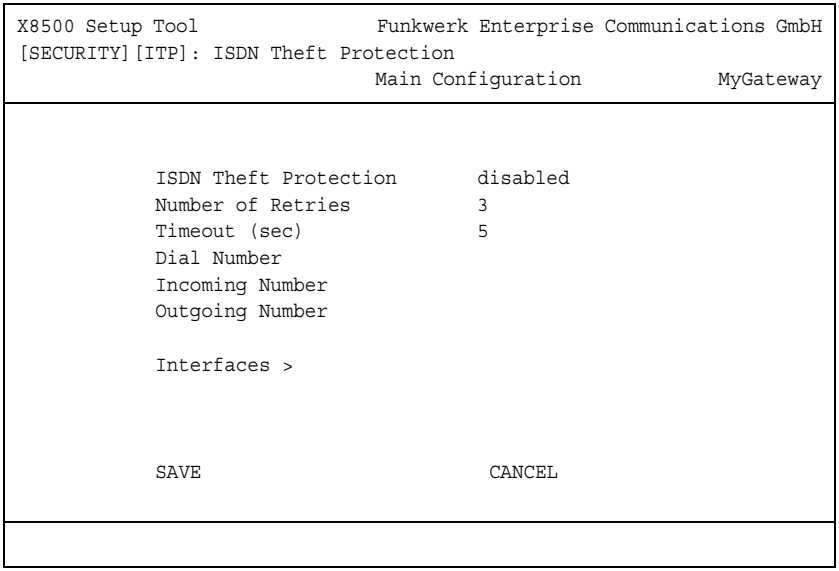
Stimmen die Nummern überein, geht das Gerät davon aus, dass es sich am ursprünglichen Standort befindet und die Schnittstellen werden auf "up" gesetzt (*AdminStatus = up)*.

Um Kosten zu sparen, nutzt die Funktion den ISDN D-Kanal.

Hinweis

Beachten Sie, dass die Funktion ISDN-Diebstahlsicherung für Ethernet-Schnittstellen nicht zur Verfügung steht.

Die Funktion ISDN-Diebstahlsicherung können Sie im Setup Tool im Menü ***SECURITY ➜ ISDN THEFT PROTECTION*** konfigurieren.



Das Menü enthält folgende Felder:

Parameter	Wert
ISDN Theft Protection	Bestimmt den Status der Diebstahlsicherung. ■ *disabled* (Standardwert): Die Diebstahlsicherung ist nicht aktiv. ■ *enabled* : Der Diebstahlsicherung ist aktiv.
Number of Retries	Anzahl der Wählversuche, die das Gateway unternimmt, um sich über ISDN selbst anzurufen. Mögliche Werte: *1* .. *255*.

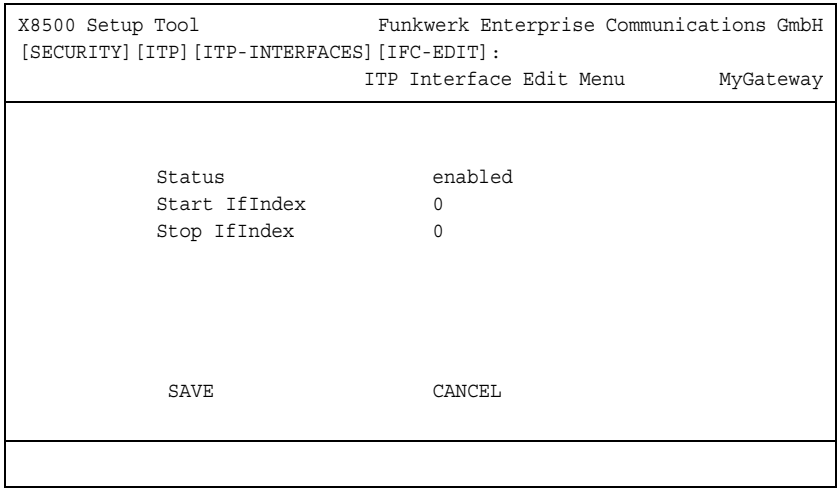
Parameter	Wert
Timeout (sec)	Zeitspanne in Sekunden, die das Gateway nach einem Wählversuch bis zu einem erneuten Wählversuch wartet, wenn der der erste der beiden Wählversuche erfolglos war. Mögliche Werte: *2* .. *20*.
Dial Number	Rufnummer, die gewählt wird.
Incoming Number	Nummer, die mit der aktuellen Calling Party Number verglichen wird.
Outgoing Number	Eigene Rufnummer, d.h. die Nummer, die als Calling Party Number gesetzt wird.

Tabelle 2-2: Felder im Menü ***SECURITY*** ➜ ***ISDN THEFT PROTECTION***

Unter ***SECURITY*** ➜ ***ISDN THEFT PROTECTION*** ➜ ***INTERFACES*** sehen Sie die Schnittstellen, für welche die Diebstahlsicherung vorgesehen ist. Das Menü enthält Beispielwerte, vor der Konfiguration ist die Liste leer.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[SECURITY][ITP][ITP-INTERFACES]: ITP Interface List           MyGateway


            Status          StartIndex          StopIndex

            enabled         10001               10015
            enabled         10018               10018
            disabled        10016               10017




          ADD           DELETE          EXIT
```

Unter ***SECURITY*** ➜ ***ISDN THEFT PROTECTION*** ➜ ***INTERFACES*** ➜ ***ADD/EDIT*** können Sie die Diebstahlsicherung für einzelne Schnittstellen oder Schnittstellengruppen konfigurieren.



Das Menü enthält folgende Felder:

Parameter	Wert
Status	Bestimmt, ob die Diebstahlsicherung eingeschaltet oder ausgeschaltet ist. Mögliche Werte: ■ *enabled* (Standardwert): Die Diebstahlsicherung ist für die Schnittstelle bzw. Schnittstellengruppe aktiv (eingeschaltet). ■ *disabled* (Standardwert): Die Diebstahlsicherung ist für die Schnittstelle bzw. Schnittstellengruppe nicht aktiv (ausgeschaltet).

Parameter	Wert
Start IfIndex	Bestimmt die erste Schnittstelle einer Schnittstellengruppe. Wenn ***START IFINDEX*** und ***STOP IFINDEX*** übereinstimmen, wird eine einzige Schnittstelle für die Diebstahlsicherung konfiguriert.
Stop IfIndex	Bestimmt die letzte Schnittstelle einer Schnittstellengruppe. Wenn ***STARTINDEX*** und ***STOPINDEX*** übereinstimmen, wird eine einzige Schnittstelle für die Diebstahlsicherung konfiguriert.

Tabelle 2-3: Felder im Menü ***SECURITY*** ➜ ***ISDN THEFT PROTECTION*** ➜ ***INTERFACES*** ➜ ***ADD/EDIT***

2.6 IP-Adressbereiche (Pools)

Mit Systemsoftware 7.8.7 unterstützt Ihr Gateway die zentrale Verwaltung dynamischer IP-Adressbereiche (Pools). Die Subsysteme DHCP und PPP können ab sofort dynamische IP-Adressbereiche gemeinsam nutzen.

Die Konfiguration der Adressbereiche erfolgt im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ ***ADD/EDIT***. Hier können Sie neue Bereiche anlegen oder bereits

bestehende ändern. Die Bereiche stehen unabhängig von der Zahl der enthaltenen Adressen allen Nutzern zur Verfügung.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][DYNAMIC][POOL][ADD]: Define Range of IP Addresses        MyGateway


    Identifier                          0
    Description
    IP Address
    Number of Consecutive Addresses     1
    Primary Domain Name Server
    Secondary Domain Name Server


            SAVE                                CANCEL
```

Das Menü enthält folgende Felder:

Parameter	Wert
Identifier	Eindeutige ganze Zahl zur Identifizierung des Adressbereichs. Mögliche Werte: 0 .. *999*.
Description	Beschreibung des Adressbereichs. Maximale Zeichenzahl: *20*.
IP Address	Erste IP-Adresse des Adressbereichs.
Number of Consecutive Addresses	Anzahl der IP-Adressen im Adressbereich einschließlich der ersten IP-Adresse (***IP Address***). Mögliche Werte: *1* .. *254*. Standardwert: *1*. In früheren Softwareversionen wurden Adresszuweisungen zu bestimmten Clients mit Hilfe von Adressbereichen mit einer einzigen IP-Adresse (***Number of Consecutive Addresses*** = *1)* realisiert. Ab **Systemsoftware 7.8.7** können Sie einzelne IP-Adressen im Menü ***IP*** ➜ ***IP Address Pools*** ➜ ***Assigned IP Addresses*** ➜ ***ADD/EDIT*** zuweisen (siehe Seite 100).
Primary Domain Name Server	Hier können Sie die IP-Adresse eines globalen Domain Name Servers eingeben. Ist kein Wert eingegeben, so wird die Einstellung von ***IP*** ➜ ***Static Settings*** benutzt, wenn im Menü ***IP*** ➜ ***DNS*** für das Feld ***DHCP Assignment*** = *global* gesetzt ist. Ist für das Feld ***DHCP Assignment*** = *self* gesetzt, so wird dem Client die IP-Adresse des Gateways übermittelt. Ist ***DHCP Assignment*** = *none* gesetzt, so ist kein ***Primary Domain Name Server*** und kein ***Secondary Domain Name Server*** verfügbar.

Parameter	Wert
Secondary Domain Name Server	Hier können Sie die IP-Adresse eines alternativen Domain Name Servers eingeben. Ist kein Wert eingegeben, so wird die Einstellung von ***IP*** ➜ ***STATIC SETTINGS*** benutzt, wenn im Menü ***IP*** ➜ ***DNS*** für das Feld ***DHCP ASSIGNMENT*** = *global* gesetzt ist. Ist für das Feld ***DHCP ASSIGNMENT*** = *self* gesetzt, so wird dem Client die IP-Adresse des Gateways übermittelt. Ist ***DHCP ASSIGNMENT*** = *none* gesetzt, so ist kein ***PRIMARY DOMAIN NAME SERVER*** und kein ***SECONDARY DOMAIN NAME SERVER*** verfügbar.

Tabelle 2-4: Felder im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ ***ADD/EDIT***

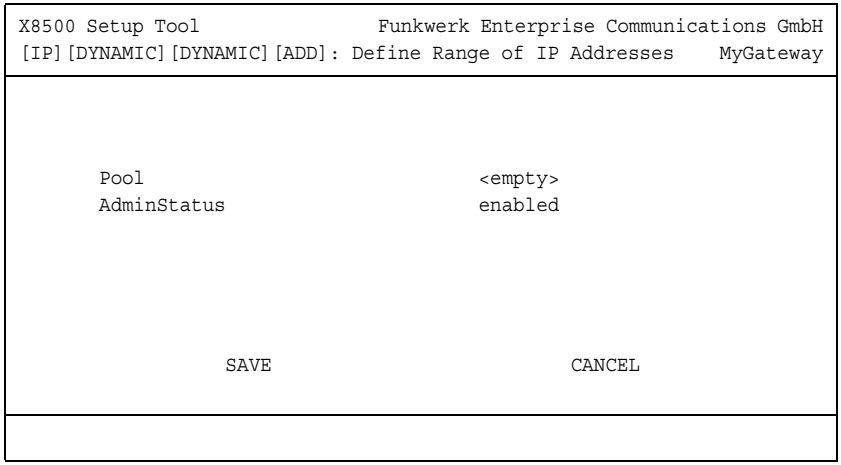
Sobald IP-Adressbereiche angelegt sind, können sie den jeweiligen Subsystemen zugewiesen werden. Wahlweise können Sie unter ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD*** einen IP-Adressbereich der gewünschten Schnittstelle zuordnen oder unter ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***IP ADDRESS POOL WAN (PPP)*** ➜ ***ADD*** einen IP-Adressbereich dem Subsystem PPP zuweisen. IP-Adressen, die dem Subsystem PPP zugewiesen sind, vergibt das Gateway als dynamischer IP-Adress-Server an WAN Partner, die sich einwählen.

Hinweis

Beachten Sie, dass dies nur für WAN Partner gilt, für die unter ***WAN PARTNER*** ➜ ***ADD*** ➜ ***IP*** ➜ ***BASIC IP-SETTINGS*** das Feld ***IP TRANSIT NETWORK*** = *dynamic server* gesetzt ist.

Im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***IP ADDRESS POOL WAN (PPP)*** sehen Sie die IP-Adressbereiche, die dem Subsystem PPP zugewiesen sind. Wenn diesem Subsystem bisher keine IP-Adressbereiche zugewiesen sind, ist die Liste leer.

Im Menü ***IP ➜ IP ADDRESS POOLS ➜ IP ADDRESS POOL WAN (PPP) ➜ ADD*** können Sie dem Subsystem PPP IP-Adressbereiche zuweisen.



Das Menü enthält folgende Felder:

Parameter	Wert
Pool	Wählen Sie hier den Namen des Pools, den Sie dem Subsystem PPP zuweisen wollen und den Sie unter ***IP ➜ IP ADDRESS POOLS ➜ POOLS ➜ ADD/EDIT*** angelegt haben. Wenn noch keine Pools angelegt sind, wird der Wert *<empty>* angezeigt.

Parameter	Wert
AdminStatus	Bestimmt, ob der IP-Adressbereich aktuell dem Subsystem PPP zugewiesen ist. Mögliche Werte: ■ *enabled* (Standardwert): Der IP-Adressbereich ist aktuell dem Subsystem PPP zugewiesen. ■ *disabled*: Der IP-Adressbereich ist aktuell nicht dem Subsystem PPP zugewiesen.

Tabelle 2-5: Felder im Menü ***IP*** ➜ ***IP Address Pools*** ➜ ***IP Address Pool WAN (PPP)*** ➜ ***ADD***

Im Menü ***IP*** ➜ ***IP Address Pools*** ➜ ***Assigned IP Addresses*** können Sie sehen, ob und wie bestimmte IP-Adressen genutzt werden.

Die Überarbeitung der dynamischen IP-Adressbereiche schlägt sich folgendermaßen in den MIB-Tabellen nieder:

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.

Die MIB-Tabellen für IP-Adressbereiche (WAN) wurden ebenfalls überarbeitet:

Die MIB-Tabellen ***biboPPPIpAssignTable*** und ***biboPPPIpInUseTable*** sind nicht mehr in Gebrauch, die Tabelle ***biboPPPIpAssignTable*** existiert jedoch aktuell noch. Die Einträge der Tabelle ***biboPPPIpAssignTable*** werden zu Einträgen in der Tabelle ***ipDynAddrPoolTable*** und in der neuen Tabelle ***biboPPPIpPoolTable*** konvertiert.

2.7 Ein-/Ausgabeverknüpfung (pipe)

Mit einer pipe kann man die Eingabe eines zweiten Befehls mit der Ausgabe des ersten Befehls verknüpfen.

Dies wird in folgendem Beispiel verdeutlicht:

```
x8500:> echo test | cat
test
x8500:>
```

Der Befehl `echo` gibt hierbei die Zeichenfolge `test` aus, welche von dem Befehl `cat` als Standardeingabe benutzt wird und ausgegeben wird.

Hinweis

Beachten Sie, dass vor und nach dem Pipe-Zeichen | immer ein Leerzeichen stehen muss.

Alternativ existiert ein Kommando `pipe`, welches wie folgt verwendet werden kann:

```
x8500:> pipe
Usage: pipe <cmd1> <cmd2>
Function: Execute two commands in a pipe (i.e. <cmd1> | <cmd2>)
```

2.8 Verbesserte Schnittstellenüberwachung

Mit Systemsoftware 7.8.7 wurden die Möglichkeiten verbessert, Schnittstellen zu überwachen und die gesendeten und empfangenen Daten aufzuzeichnen und zu analysieren. Dazu steht Ihnen auf der Kommandozeile Ihres Gateways das Kommando trace zur Verfügung oder Sie können auf einem PC ein entsprechendes Programm nutzen (bricktrace für UNIX oder DimeTools für Windows).

Sowohl mit den Remote Programmen auf dem PC als auch mit dem Kommando `trace` können Sie Ethernet-, ISDN-, ATM- und WLAN-Schnittstellen protokol-

lieren sowie den unverschlüsselten Datenverkehr in einem IPSec-Tunnel, falls dieser als virtuelle Schnittstelle angelegt wurde.

bricktrace, DimeTools

Bei den Remote Programmen auf dem PC wurden folgende Erweiterungen vorgenommen:

- Aus Sicherheitsgründen ist die Protokollierung von Schnittstellen nur noch mit Authentisierung (Admin Passwort des Routers) möglich.
- Sie können die Daten in das Format libpcap schreiben lassen, um sie mit Standardprogrammen wie z. B. tcpdump, ethereal (neu: wireshark) oder ntop zu analysieren.
- Komfortable IP-Session-Filter wurden eingebaut (Optionen *-I* und *-B*).
- Die eigene Trace-Verbindung (PC <-> Gateway) wird jetzt gefiltert, wenn der PC diejenige Schnittstelle protokolliert, an welche er angeschlossen ist.

bricktrace

Sie können mit bricktrace Daten in eine libpcap-Datei schreiben und, falls gewünscht, gleichzeitig Ethereal zur Anzeige der Daten starten (Live Trace). Oder Sie können die Daten speichern und später analysieren.
Weitere Informationen zu den Möglichkeiten von bricktrace erhalten Sie über die Hilfe mit dem Befehl `-?` oder über die erweiterte Hilfe mit `--help`.

Beispiele:

```
bricktrace --ethereal router-ip 1000
```

startet den Trace auf der LAN Schnittstelle 1000 und startet gleichzeitig automatisch Ethereal über eine Pipe.

```
export TRACE_EXEC="wireshark -Sk -i"
```

startet bei der Option `--ethereal` das Programm wireshark statt des Programms ethereal.

```
bricktrace --pcap-file router 1000
```

speichert alle Datenpakete in einer libpcap-Datei. Sie können diese Datei später analysieren.

Ohne Angabe der Schnittstellennummer zeigt das Programm eine Liste der verfügbaren physikalischen Schnittstellen des Gateways.

```
-V 1..3
```

Setzt die Version des Trace-Schnittstellen-Protokolls;

für alte Geräte: 1 oder 2;
3 ist der Standardwert.

`--pwd=passwort`

Setzt das Passwort des Gateways (Version 3).

DimeTools Mit den DimeTools können Sie Daten in einer libpcap-Datei speichern und diese Datei anschließend mit dem Programm ethereal öffnen. Ein Live Trace über eine Pipe ist unter Windows nicht möglich.

Hinweis

Beachten Sie, dass mit ethereal ein Live Trace über eine Pipe aufgrund eines Fehlers im Programm nur bei Versionen ab 0.10.12 möglich ist.

trace Bei dem Kommando `trace` wurden folgende Erweiterungen vorgenommen:

- Komfortable IP-Session-Filter wurden eingebaut (Optionen *-I* und *-B*).
- Sie können die Schnittstellennummer direkt angeben, z.B. `trace 1000` für die erste LAN Schnittstelle oder `trace 100001` für die erste IPSec Schnittstelle.

IP-Session-Filter Mit den Optionen `-I` und `-B` (negiert `-I !` und `-B !`) können IP-Pakete nach den Feldern *ip-source*, *ip-destination*, *protocol*, *src-port* und *dst-port* gefiltert werden.

Wenn Sie mehrere Filter ohne Option angeben, werden sie mit logischem UND verknüpft, die Option `-o` verknüpft sie mit ODER.

```
syntax:
       -I:         filter, unidirectional session
       -B:         filter, bidirectional session

usage: -I ip1:ip2:proto:port1:port2
       -B ip1:ip2:proto:port1:port2

   ip1:    source IP address
   ip2:    destination IP address
   proto:  protocol (1=ICMP, 6=TCP, 17=UDP, 50=ESP, 51=AH,
                     2=IGMP, 8=EGP, 46=RSVP)
   port1:  source port
   port 2: destination port

examples:
  -I 1.1.1.10               : all packets from 1.1.1.10
  -I !1.1.1.10              : no packets from 1.1.1.10
  -B !1.1.1.10              : no packets from and to 1.1.1.10
  -I :1.1.1.10              : all packets to 1.1.1.10
  -I 1.1.1.10:1.1.1.20      : all packets from 1.1.1.10 to 1.1.1.20
  -B 1.1.1.10:1.1.1.20     : all packets between 1.1.1.10 and 1.1.1.20
  -I ::6                    : all TCP packets
  -I ::6 -o -I ..17         : all TCP and UDP packets
  -I !::50                  : no ESP packets
  -I ::17::512              : all UDP packets to port 512
  -I 1.2.3.4::17::512       : all UDP packets from 1.2.3.4 to any
                              host/port 512
  -B ::6:1026:23           : all TCP packets between ports 1026 and 23
```

Informationen zu den IP-Session-Filtern erhalten Sie für das Kommando `trace` mit `-?` und für das Programm bricktrace mit `--help`.

2.9 Autovervollständigung mit der Tabulator-Taste (Tab Completion)

Mit Systemsoftware 7.8.7 wird eine Autovervollständigung mit der Tabulatortaste (Tab Completion) unterstützt.

Eingaben auf der SNMP Shell Ihres Geräts können nun mit der Tabulatortaste automatisch vervollständigt werden, d.h. Sie geben den Anfang eines Kommandos ein und erreichen durch Drücken der Tabulator-Taste die automatische Vervollständigung des Kommandos.

Folgende Eingaben können vervollständigt werden:

- externe Kommandos (`ping`, `ifconfig` usw.)
- lokale Kommandos (`echo`, `sleep`, `halt` usw.)
- SNMP Kommandos (Tabellen, Werte)
- MIB Gruppen.

Für die Autovervollständigung existiert zudem ein complete-Kommando (z. B. für den Fall, dass aufgrund von Terminaleinstellungen das Tabulator-Zeichen nicht korrekt übermittelt wird), das wie folgt benutzt werden kann:
`complete <gesuchte Zeichenfolge>`

Bsp. Alle Befehle, die mit *l* anfangen, sollen gelistet werden.

```
x8500:> complete l
l                       loop                    linkd
l2tpd                   l2tp                    l2tpGlobals
l2tpSessionTable        l2tpTunnelProfileTable  l2tpTunnelTable
localTcpAllowTable      localUdpAllowTable
x8500:>
```

2.10 Neues Kommando "grep"

Mit Systemsoftware 7.8.7 wird ein einfacher grep-Befehl unterstützt.

Mit dem grep-Befehl können Sie auf der SNMP Shell Ihres Geräts nach Begriffen suchen. Auf den Suchbegriff passende Zeilen werden hierbei ausgegeben, alle anderen verworfen. Die Ausgabe aller Befehle auf der Shell kann hierbei verknüpft werden.

Folgende Syntax wird verwendet:

```
x8500:> grep -h
Usage: grep [hvdie:] <pattern>
    -e <pattern>   specify multiple <pattern>
    -i             ignore case
    -v             invert match
    -d             debug
    -h             display help and exit
```

Bsp.

Sie finden die Prozess-ID zum DynDNS-Daemon mit:

```
x8500:> ps -ef | grep ddnsd
```

Bsp.

Sie suchen die Prozess-ID des ddnsd und des bootpd mit:

```
x8500:> ps -ef | grep -e ddnsd -e bootpd
```

Bsp.

Um NAT-Debugmeldungen auszuklammern verwenden Sie:

```
x8500:> debug all | grep -v NAT
```

Der grep-Befehl unterstützt einfache reguläre Ausdrücke. Hierbei können die Zeichen `*` `?` `[ ]` verwendet werden.

Bsp.

```
x8500:> echo test | grep *t[ae]s?
```

`*` liefert eine Übereinstimmung mit einer beliebig langen Zeichenkette.

`?` liefert eine Übereinstimmung mit einem beliebigen Zeichen.

`[ ]` entspricht einer ODER-Verknüpfung, d.h. eines der angegebenen Zeichen muss übereinstimmen.

2.11 Kommando Ping erweitert

Mit Systemsoftware 7.8.7 ist das SNMP-Shell-Kommando Ping um die Optionen -t und -Q erweitert worden.

Mit den neuen Optionen können Sie in ICMP Paketen die TOS- und TTL-Felder explizit setzen.

ping -Q <tos>: Setzt den angegebenen TOS-Wert.
(Wertebereich <*tos*>: *0 - 15*.)

ping -t <ttl>: Setzt den angegebenen TTL-Wert.

2.12 Kommando traceroute erweitert

Mit Systemsoftware 7.8.7 ist das Kommando traceroute um die Option -s erweitert worden.

Mit der neuen Option können Sie für einen Rechner mit mehreren IP-Adressen die als Absender verwendete IP-Adresse explizit setzen.

traceroute -s <IP address>: Setzt die angegebene IP-Adresse als Absender.

2.13 BOOTP Relay

Mit Systemsoftware 7.8.7 unterstützt Ihr Gateway die Konfiguration von BOOTP Relay Servern nicht nur für das System als Ganzes sondern auch für ausgewählte Schnittstellen.

Globale BOOTP Relay Server

Die Konfiguration globaler BOOTP Relay Server wurde vom Menü ***IP*** ➜ ***STATIC SETTINGS*** in das Menü ***IP*** ➜ ***BOOTP RELAY*** ➜ ***EDIT*** verschoben.

Spezifische BOOTP Relay Server

Schnittstellen-spezifische BOOTP Relay Server können Sie im Menü ***IP*** ➜ ***BOOTP RELAY*** ➜ ***ADD/EDIT*** konfigurieren.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][BOOTP][ADD]: BOOTP Relay Interface Settings                MyGateway


    Interface                          en1-0
    Admin State                        enabled
    Primary BOOTP Server
    Secondary BOOTP Server




            SAVE                                    CANCEL
```

Das Menü enthält folgende Felder:

Parameter	Wert
Interface	Zeigt die Schnittstellen Ihres Geräts. Wählen Sie eine Schnittstelle. Wenn über die gewählte Schnittstelle eine BOOTP-Anfrage empfangen wird, wird diese Anfrage an den angegebenen BOOTP Relay Server weitergeleitet.
Admin State	Schaltet die Zuordnung zwischen Schnittstelle und BOOTP Relay Server(n) aus oder ein. Mögliche Werte: ■ *enabled* (Standardwert): Die Zuordnung zwischen Schnittstelle und BOOTP Relay Server(n) ist aktiv. ■ *disabled*: Die Zuordnung zwischen Schnittstelle und BOOTP Relay Server(n) ist nicht aktiv.
Primary BOOTP Server	Hier können Sie die IP-Adresse eines Servers angeben, an den BOOTP- oder DHCP-Anfragen weitergeleitet werden.
Secondary BOOTP Server	Hier können Sie die IP-Adresse eines alternativen BOOTP- oder DHCP-Servers angeben.

Tabelle 2-6: Felder im Menü ***IP ➜ BOOTP RELAY ➜ ADD/EDIT***

2.14 PPPoE Passthrough

Mit Systemsoftware 7.8.7 können Sie gegebenenfalls zusätzlich zu einer bereits existierenden Internetverbindung mit der Funktion PPPoE Passthrough über eine DSL-Verbindung mehrere PPPoE-Verbindungen aus dem LAN direkt ins Internet anlegen. Aktuell ist PPPoE Passthrough ausschließlich zwischen zwei Geräten mit Ethernet Interface konfigurier-

bar. Für die Funktion PPPoE Passthrough können Sie aktuell keine Filter, SIF o.ä. nutzen.

Die Konfiguration erfolgt im Menü ***PPP*** und im Menü ***PPP*** ➜ ***PPPoE PASSTHROUGH***.

Im Menü ***PPP*** wählen Sie im Feld ***PPPoE ETHERNET INTERFACE*** die Schnittstelle, die für PPPoE-Verbindungen vorgegeben wird. (Das Menü enthält Beispielwerte.)

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[PPP]: PPP Profile Configuration                                MyGateway



     Authentication Protocoll       CHAP + PAP + MS-CHAP
     Radius Server Authentication   inband

     PPP Link Quality Monitoring    no

     PPPoE Ethernet Interface       en1-1

     PPPoE Passthrough >




               SAVE                          CANCEL
```

Im Menü ***PPP*** ➜ ***PPPoE PASSTHROUGH*** konfigurieren Sie die gewünschten Paare von Ethernet Ports.

Sie können für den PPPoE Client und den PPPoE Server jeweils einen Ethernet Port wählen (bzw. den DSL-"Port" repräsentiert durch *ethoa50-0*, für Geräte, die einen DSL-Anschluss besitzen). (Das Menü enthält Beispielwerte.)

```
X8500  Setup Tool              Funkwerk Enterprise Communications GmbH
[PPP]: PPPoE Passthrough Configuration                        MyGateway

    Physical or virtual Ethernet Port attached to PPPoE Client(s)
    <x> en1-0             < > en1-4             < > en1-1
    < > en1-2

    Physical or virtual Ethernet Port attached to PPPoE Server
    < > en1-0             < > en1-4             <x> en1-1
    < > en1-2

                SAVE                          CANCEL
```

2.15 PPPoE Multilink

Mit Systemsoftware 7.8.7 können Sie mehrere DSL-Verbindungen eines Providers über PPP als statisches Bündel koppeln, um mehr Bandbreite zu erhalten. Jede dieser DSL-Verbindungen sollte dafür eine separate Ethernet-Verbindung nutzen. Aktuell ist bei vielen Providern die Funktion PPPoE Multilink erst in Vorbereitung.

Für die Konfiguration von PPPoE Multilink müssen Sie einen entsprechenden WAN-Partner anlegen. Im Menü ***WAN Partner*** ➜ ***ADD*** ➜ ***Advanced Settings*** setzen Sie für diesen WAN-Partner ***Layer 1 Protocol*** = *PPP over Ethernet (PPPoE)*. Die eigentliche Konfiguration von PPPoE Multilink erfolgt im Menü

WAN PARTNER ➜ ADD ➜ ADVANCED SETTINGS ➜ EXTENDED INTERFACE SETTINGS.
(Das Menü enthält Beispielwerte.)

```
X8500  Setup Tool                Funkwerk Enterprise Communications GmbH
[WAN][ADD][ADVANCED][EXTIF]:
             Extended Interface Settings (WAN Partner Name)   MyGateway


      PPPoE Multilink          yes


      Ethernet Ports to use

      < > en1-0          < > en1-4          <x> en1-1
      <x> en1-2




                 SAVE                          CANCEL
```

Das Menü enthält folgende Felder:

Parameter	Wert
PPPoE Multilink	Bestimmt, ob PPPoE Multilink benutzt werden soll. Mögliche Werte: ■ *no* (Standardwert): PPPoE Multilink wird nicht benutzt. ■ *yes*: PPPoE Multilink wird benutzt.
Ethernet Ports to use	Zeigt die Ethernet Interfaces Ihres Geräts. Abhängig von Ihrem Gerät und abhängig davon, ob und wie der Ethernet Switch im Split-Ports-Modus betrieben wird, stehen unterschiedliche Interfaces zur Verfügung. Wählen Sie die Interfaces, die Sie für PPPoE Multilink nutzen wollen.

Tabelle 2-7: Felder im Menü ***WAN PARTNER*** ➜ ***ADD*** ➜ ***ADVANCED SETTINGS*** ➜ ***EXTENDED INNERFACE SETTINGS***

Hinweis

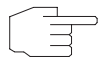
Wir empfehlen Ihnen, für PPPoE Multilink den Ethernet Switch Ihres Geräts im Split-Ports-Modus betreiben und für jede PPPoE-Verbindung ein eigenes Ethernet Interface zu benutzen, z. B. *en1-1*, *en1-2*.

Hinweis

Wenn Sie für PPoE Multilink zusätzlich ein externes Modem benutzen wollen, müssen Sie den Ethernet Switch Ihres Geräts im Split-Ports-Modus betreiben.

Hinweis

Wenn Sie ein externes Modem benutzen wollen, müssen Sie im Menü ***QoS*** ➜ ***INTERFACES AND POLICIES*** ➜ ***EDIT*** ➜ ***QoS SCHEDULING AND SHAPING*** für das Feld ***QUEUEING AND SCHEDULING ALGORITHM*** = *priority queueing (PQ)* setzen und für das Feld ***SPECIFY TRAFFIC SHAPING*** = *yes*.



Hinweis

Wenn Sie ein externes Modem nutzen wollen, müssen Sie die aktuelle Bandbreite der Upload Verbindung angeben.

2.16 VLAN und Bridging

Mit VLANs können Sie einzelne Netzwerksegmente voneinander trennen, z. B. einzelne Abteilungen einer Firma. Im neuen Menü *VLAN* unterstützt Systemsoftware 7.8.7 die Konfiguration von VLANs auf Schnittstellen, für welche der Bridging-Modus konfiguriert ist.

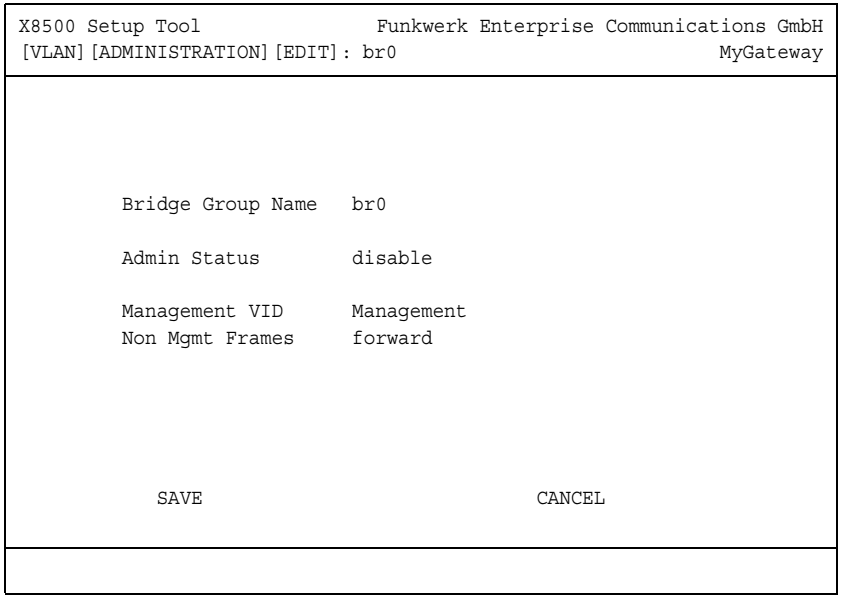
Sie können sich alle bereits konfigurierten VLANs anzeigen lassen, Ihre Einstellungen bearbeiten und neue VLANs erstellen.

Administration

Im Menü ***VLAN*** ➜ ***ADMINISTRATION*** sehen Sie eine Liste der angelegten Bridge-Gruppen. (Die Liste enthält Beispielwerte. Wenn noch keine Bridge-Gruppen angelegt sind, ist die Liste leer.)

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[VLAN][ADMINISTRATION]                                          MyGateway


  Bridge Group Name   Status   Non Mgmt Frames   Mgmt VID
  ──────────────────────────────────────────────────────

    br0               enable       forward          1
    br1               disable      drop             2
    br2               disable      forward          1




                              EXIT
```

Im Menü ***VLAN*** ➜ ***ADMINISTRATION*** ➜ ***EDIT*** nehmen Sie allgemeine Einstellungen für ein VLAN vor. Die Optionen sind für jede Bridge-Gruppe separat zu konfigurieren.



Das Menü enthält folgende Felder:

Parameter	Wert
Bridge Group Name	Zeigt die gewählte Bridge-Gruppe.
Admin Status	Aktiviert oder deaktiviert das VLAN für die gewählte Bridge-Gruppe. Mögliche Werte: ■ *disable* (Standardwert): Das VLAN ist nicht aktiv. ■ *enable*: Das VLAN ist aktiv.
Management VID	Management VLAN ID. Geben Sie die VLAN ID des VLANs ein, in dem Ihr Gerät arbeiten soll.

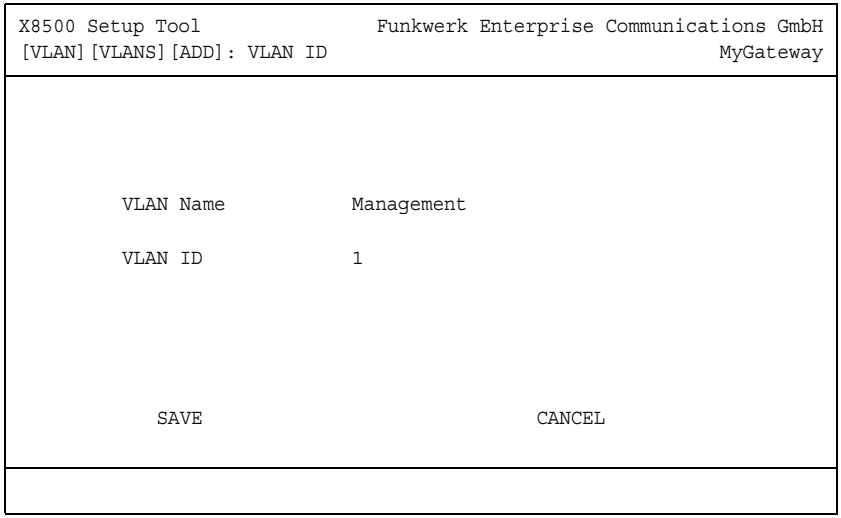
Parameter	Wert
Non Mgmt Frames	Bestimmt, ob Frames die nicht mit der Management VLAN ID Information gekennzeichnet sind, weitergeleitet oder verworfen werden sollen. Mögliche Werte: ■ *forward* (Standardwert): Die Frames werden weitergeleitet. ■ *drop*: Die Frames werden verworfen.

Tabelle 2-8: Felder im Menü ***VLAN*** ➜ ***ADMINISTRATION*** ➜ ***EDIT***

VLAN Im Menü ***VLAN*** ➜ ***VLAN*** können Sie sehen, welche VLANs angelegt sind und welcher ***VLAN NAME*** welcher ***VLAN ID*** zugeordnet ist. (Die Liste enthält Beispielwerte).

```
X8500 Setup Tool                    Funkwerk Enterprise Communications GmbH
[VLAN][VLANS]                                                      MyGateway


    VLAN Name                                   VLAN ID
    ____________________________________________________


    Management                                     1
    Support                                        2




    ADD          MEMBERS          DELETE          EXIT
```

Im Menü ***VLAN*** ➜ ***VLAN*** ➜ ***ADD*** können Sie neue Zuordnungen erstellen. Standardmäßig ist das VLAN mit dem Namen *Management* und der ID *1* bereits angelegt:



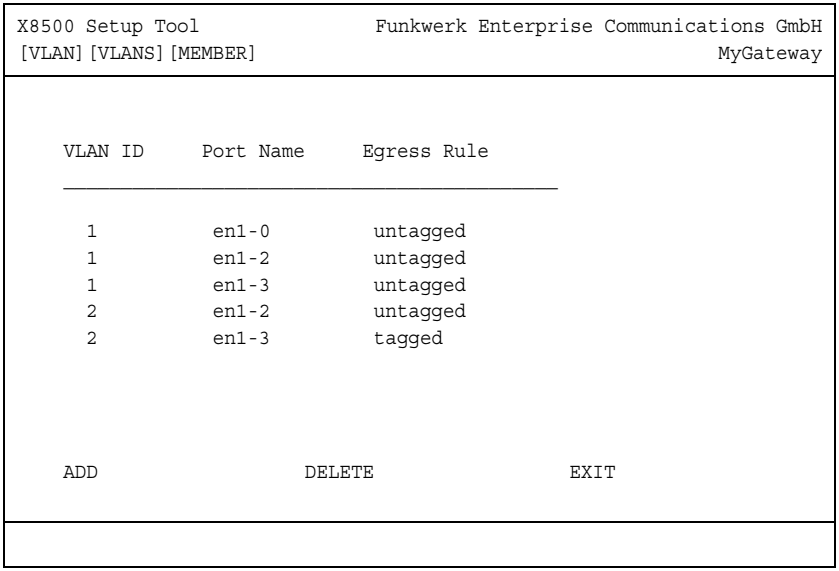
Das Untermenü ***VLAN*** ➜ ***VLAN*** ➜ ***ADD*** enthält folgende Felder:

Parameter	Wert
VLAN ID Name	Hier geben Sie einen Namen für das VLAN ein. Maximale Zeichenzahl: 32.
VLAN ID	VLAN Identifier Geben Sie eine eindeutige ganze Zahl ein, welche das VLAN identifiziert. Mögliche Werte: *1* .. *4094*. Standardwert: *1*.

Tabelle 2-9: Felder im Menü ***VLAN*** ➜ ***VLAN*** ➜ ***ADD/EDIT***

Im Menü ***VLAN*** ➜ ***VLAN*** ➜ **Members** können Sie sehen, welche VLANs welchen Schnittstellen zugeordnet sind und welche Frames über die jeweilige Schnittstelle versendet werden. (Die Liste enthält Beispielwerte.) Die Schaltflä-

che **Members** erscheint, wenn im Menü ***Ethernet Switch*** ➜ ***Fast Ethernet/en1-x*** ➜ ***EDIT*** das Feld ***Interface Mode*** = *Bridging* gesetzt ist.



Das Menü ***VLAN*** ➜ ***VLAN*** ➜ **Members** ➜ **ADD** enthält folgende Felder:

Parameter	Wert
VLAN ID	VLAN Identifier Zeigt die Namen der im Menü ***VLAN*** ➜ ***VLAN*** ➜ ***ADD*** angelegten VLANs. Sie können ein VLAN wählen.
Port Name	Hier sehen Sie alle Schnittstellen, für die Bridging konfiguriert ist (siehe Menü ***ETHERNET SWITCH*** ➜ ***FAST ETHERNET/EN1-X*** ➜ ***ADD/EDIT***). Wählen Sie die Schnittstelle, die Sie dem VLAN zuzuordnen wollen, d.h. die Mitglied des gewählten VLANs sein soll.
Egress Rule	Legt fest, ob an der gewählten Schnittstelle die Frames mit VLAN-Information oder die Frames ohne VLAN-Information übertragen werden sollen. Mögliche Werte: ■ *untagged* (Standardwert): Die Frames ohne VLAN-Information werden übertragen. ■ *tagged*: Die Frames mit VLAN-Information werden übertragen.

Tabelle 2-10: Felder im Menü ***VLAN*** ➜ ***VLAN*** ➜ ***MEMBERS*** ➜ ***ADD***

PVID Im Menü ***VLAN → PVID*** können Sie Regeln für den Empfang von Frames an den Schnittstellen des VLANs einsehen und festlegen. (Die Liste enthält Beispielwerte.)

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[VLAN] [PVIDS]                                                MyGateway


 Port Name      PVID   Untagged Frames   Non Member Frames
 ____________________________________________________________

 en1-0           1       forward           forward
 en1-2           2       drop              drop
 en1-3           1       forward           forward




              MEMBERS            EXIT
```

Das Menü ***VLAN ➜ PVID ➜ EDIT*** enthält folgende Felder:

Parameter	Wert
Port Name	Zeigt den Port, für den Sie die Regeln bearbeiten wollen.
PVID	Port VLAN Identifier Weisen Sie dem ausgewählten Port eine PVID zu.
Untagged Frames	Bestimmt, was mit Frames geschehen soll, die keine VLAN-Information enthalten. Mögliche Werte: ■ *forward* (Standardwert): Die Frames ohne VLAN-Information werden weitergeleitet. ■ *drop*: Die Frames ohne VLAN-Information werden verworfen.
Non Member Frames	Bestimmt, ob Frames, deren VLAN-Information nicht zum gewählten Port passt, weitergeleitet oder verworfen werden sollen. Mögliche Werte: ■ *forward* (Standardwert): Die Frames werden weitergeleitet ■ *drop*: Die Frames werden verworfen.

Tabelle 2-11: Felder im Menü ***VLAN ➜ PVID ➜ EDIT***

Im Menü ***VLAN ➜ PVID ➜*** **Members** können Sie sehen, welcher Schnittstelle welche VLANs zugeordnet sind und welche Frames über die jeweilige Schnittstelle versendet werden. Diese Informationen sind dieselben wie im Menü ***VLAN ➜ VLAN ➜*** **Members**.

2.17 Multicast

Im neuen Menü *IP* ➜ *MULTICAST* unterstützt Systemsoftware 7.8.7 die Nachrichtenübertragung in TCP/IP-Netzwerken an eine Gruppe von Empfängern. Während Sie mit *FORWARDING* Daten einfach weiterleiten, dienen IGMP und PIM dazu, Daten nur an bestimmte Hosts zu übermitteln und damit unnötigen Datenverkehr zu vermeiden.

Bei Multicast werden die Daten an eine Art "virtuelle Adresse" übertragen, an die sogenannte Multicast-Gruppe. Für IPv4 im Klasse D Netzwerk sind die IP-Adressen 224.0.0.0 bis 239.255.255.255 für Multicast-Gruppen reserviert.

Interessierte Empfänger können sich bei beliebig vielen Multicast-Gruppen registrieren. Hosts, in diesem Zusammenhang auch Quellen genannt, die z. B. einen Internet-Radiosender ausstrahlen, senden ihre Pakete an die jeweilige Multicast-Gruppe. Anhand der Registrierungen bei der Multicast-Gruppe werden die Pakete an ihre Empfänger weitergeleitet.

IGMP (Internet Group Management Protocol) verwaltet die Multicast-Gruppen in lokalen Netzwerken und regelt den Austausch der Mitgliedsinformationen dieser Gruppen über sogenannte Queries und Reports. Die momentan aktuelle Version von IGMP ist Version 3; sie ist zu Version 1 und Version 2 abwärtskompatibel.

Im Vergleich dazu ist PIM (Protocol Independent Multicast) ein Multicast-Routing-Protokoll. Bei PIM wird die Informationsverteilung über einen zentralen Punkt geregelt, der als Rendezvous Point bezeichnet wird. Dorthin werden die Datenpakete initial geleitet und auf Anfrage anderer Router den Empfängern zur Verfügung gestellt.

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

MSDP (Multicast Source Discovery Protocol) dient in **Systemsoftware 7.8.7** vor allem dazu, mehrere PIM Domänen zu verbinden und somit Inter-Domain-Routing zu betreiben.

Im Menü ***IP*** ➜ ***MULTICAST*** können Sie die Multicast-Funktionalität aus- bzw. einschalten.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST]: Multicast Configuration                          MyGateway


          Status                enabled

          Interfaces >

          Forwarding >
          IGMP >
          PIM >
          MSDP >




          SAVE                   CANCEL
```

Über das Menü ***IP*** ➜ ***MULTICAST*** gelangen Sie in folgende Untermenüs:

- ***INTERFACES***
- ***FORWARDING***
- ***IGMP***
- ***PIM***
- ***MSDP***.

Interfaces

Im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***INTERFACES*** sehen Sie die aktiven Multicast-Schnittstellen Ihres Geräts und deren Nutzung.

Forwarding

Im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***FORWARDING*** ➜ ***ADD/EDIT*** können Sie eine einfache Weiterleitung von Paketen an eine Multicast-Gruppe einrichten.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][FORWARDING]: Add/Edit Rule                          MyGateway


  Group Address
  Status                        active


  Source Interface              none
  Destination Interface         none


            SAVE                                CANCEL
```

Das Menü ***IP*** ➜ ***MULTICAST*** ➜ ***FORWARDING*** ➜ ***ADD/EDIT*** enthält folgende Felder:

Parameter	Wert
Group Address	IP-Adresse der Gruppe, für die dieser Eintrag gilt. Die Adresse muss im Bereich 224.0.0.0 - 239.255.255.255 liegen. Mit der Adresse 224.0.0.0 können Sie alle Multicast-Pakete spezifizieren.
Status	Aktiviert oder deaktiviert den Eintrag. Mögliche Werte: ■ *active* (Standardwert): Der Eintrag ist aktiv, die Datenpakete werden weitergeleitet. ■ *inactive*: Der Eintrag ist nicht aktiv, er wird nicht berücksichtigt.
Source Interface	Schnittstelle, an der die Datenpakete empfangen werden sollen. ***SOURCE INTERFACE*** und ***DESTINATION INTERFACE*** müssen unterschiedliche Schnittstellen sein.
Destination Interface	Schnittstelle, an welche die Datenpakete weitergeleitet werden sollen. ***SOURCE INTERFACE*** und ***DESTINATION INTERFACE*** müssen unterschiedliche Schnittstellen sein.

Tabelle 2-12: Felder im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***FORWARDING*** ➜ ***ADD/EDIT***

Hinweis

Stellen Sie sicher, dass sich Ihre Einstellungen unter ***FORWARDING*** nicht mit Schnittstellen überschneiden, die gleichzeitig für IGMP oder PIM konfiguriert sind. Pakete für Gruppen, die unter ***FORWARDING*** konfiguriert sind, werden auch dann weitergeleitet, wenn sie von IGMP oder PIM an den Schnittstellen explizit abbestellt wurden.

IGMP

Im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** legen Sie fest, ob IGMP aktiviert werden soll. Sie können angeben, ob IGMP nur in der Version 3 betrieben werden soll oder

ob der Kompatibilitätsmodus verwendet werden soll. Der Kompatibilitätsmodus führt zu einer automatischen Anpassung der IGMP Version, die an dieser Schnittstelle verwendet wird. Damit können an der jeweiligen Schnittstelle neben Hosts mit Version 3 auch Hosts mit Version 2 oder Version 1 betrieben werden. Darüber hinaus können Sie festlegen, an welchen Schnittstellen IGMP benutzt werden soll.

Das Menü enthält Beispielwerte.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][IGMP]: IGMP Configuration                          MyGateway


Status        auto                    Advanced >
Mode          compat

Interface     Status          Mode
-------------------------------------------------------------------------
en1-0         acitve          routing









SAVE      ADD      DELETE      EXIT
```

Das Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** enthält folgende Felder:

Parameter	Wert
Status	Bestimmt, ob IGMP benutzt werden soll. Mögliche Werte: ■ *auto* (Standardwert): IGMP ist eingeschaltet. IGMP erzeugt Schnittstellen im Host-Modus, sobald diese von Anwendungen angefordert werden. ■ *down*: IGMP ist ausgeschaltet. ■ *up*: IGMP ist eingeschaltet.

Parameter	Wert
Mode	Bestimmt, in welchem Modus IGMP benutzt werden soll. Mögliche Werte: ■ *compat*: IGMP wird im Kompatibilitätsmodus benutzt, d.h. Hosts, die mit Version 1, Version 2 oder Version 3 arbeiten, werden berücksichtigt. Wenn in einem Netz mehrere Versionen verfügbar sind, wird die Version mit der niedrigsten Versionsnummer (die älteste Version) als gemeinsamer Standard gewählt. ■ *v3only* (Standardwert: Ausschließlich IGMP Version 3 wird benutzt, d.h. nur V3 Hosts werden berücksichtigt.

Tabelle 2-13: Felder im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP***

Im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADD/EDIT*** können Sie die Schnittstellen festlegen, an denen IGMP benutzt werden soll.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][IGMP][INTERFACE]: Configure IGMP Interface        MyGateway



Interface                           en1-0
Status                              active
Mode                                routing

Query Interval (s)                  125
Max Response Time (ms)              10000
Robustness                          2
Last Member Query Interval (ms)     1000
StateLimit (msg/s)                  0

ProxyIfIndex                        none



SAVE     CANCEL
```

Das Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADD/EDIT*** enthält folgende Felder:

Parameter	Wert
Interface	Wählen Sie die Schnittstelle, über die IGMP Queries ausgesandt werden sollen und an der auf Antworten gewartet werden soll. Wählen Sie dazu die Schnittstelle, hinter der sich die Multicast-Empfänger verbergen.
Status	Aktiviert oder deaktiviert IGMP an der gewählten Schnittstelle. Mögliche Werte: ■ *active* (Standardwert): Der Eintrag ist aktiv, IGMP wird an der gewählten Schnittstelle benutzt. ■ *inactive*: Der Eintrag ist nicht aktiv, IGMP wird an der gewählten Schnittstelle nicht benutzt.
Mode	Wählen Sie aus, ob die hier definierte Schnittstelle im Host-Modus und im Routing-Modus oder nur im Host-Modus arbeiten soll. Mögliche Werte: ■ *routing* (Standardwert): Die Schnittstelle wird im Routing- und im Host-Modus betrieben. ■ *host-only*: Die Schnittstelle wird ausschließlich im Host-Modus betrieben.
Query Interval	Geben Sie den Zeitraum in Sekunden ein, in dem IGMP Queries versendet werden sollen. Mögliche Werte: *0* .. *600*. Standardwert: *125*.

Parameter	Wert
Max Response Time (ms)	Geben Sie für das Senden von Queries an, in welchem Zeitraum in Millisekunden Hosts auf jeden Fall antworten müssen. Die Hosts wählen aus diesem Zeitraum zufällig eine Verzögerung, bis die Antwort gesendet wird. Damit können Sie bei Netzen mit vielen Hosts eine Streuung und somit eine Entlastung erreichen. Mögliche Werte: *0* .. *25500*. Standardwert: *10000*.
Robustness	Wählen Sie den Multiplikator zur Steuerung interner Timer-Werte aus. Mit einem höheren Wert kann z. B. in einem verlustreichen Netzwerk ein Paketverlust kompensiert werden. Durch einen zu hohen Wert kann sich aber auch die Zeit zwischen dem Abmelden und dem Stopp des eingehenden Datenverkehrs erhöhen (Leave Latency). Mögliche Werte: Ganze Zahlen *2* .. *8*. Standardwert: *2*.
Last Member Query Interval (ms)	Zeitraum in Millisekunden, der auf Antwort nach einer Query an eine Gruppe gewartet wird. Wenn Sie den Wert verkleinern, wird schneller erkannt, ob das letzte Mitglied eine Gruppe verlassen hat und somit keine Pakete mehr für diese Gruppe an diese Schnittstelle weitergeleitet werden müssen.
StateLimit	Legt die maximale Anzahl von Queries bzw. Reports pro Sekunde für die gewählte Schnittstelle fest.

Parameter	Wert
ProxyIfIndex	Hier können Sie entscheiden, ob Ihr Gerät die IGMP-Meldungen der Hosts an dieser Schnittstelle über eine andere Proxy Schnittstelle weiterleiten soll. Wenn Sie wollen, dass die IGMP-Meldungen der Hosts weitergeleitet werden, wählen Sie die Schnittstelle Ihres Geräts, die als IGMP Proxy dienen soll. In der Regel muss an dieser Schnittstelle auch IGMP aktiv sein.

Tabelle 2-14: Felder im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADD/EDIT***

Über das Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** gelangen Sie in das Untermenü

- ***ADVANCED***.

Das Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** enthält folgende Felder:

Parameter	Wert
Max Groups	Legt die maximale Anzahl der insgesamt möglichen Gruppen sowohl intern als auch in Reports fest. Standardwert: *64*.
Max Sources	Legt für eine Gruppe sowohl die maximale Anzahl der Quellen fest, die in den Reports der Version 3 spezifiziert sind, als auch die maximale Anzahl der intern verwalteten Quellen pro Gruppe. Standardwert: *64*.
StateLimit	Legt die maximale Anzahl der insgesamt möglichen eingehenden Queries bzw. Reports pro Sekunde fest. Standardwert: *0*.

Tabelle 2-15: Felder im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED***

Über das Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** gelangen Sie in folgende Untermenüs:

- ***STATIC GROUPS***
- ***MONITOR***
- ***ACL***.

Im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** ➜ ***STATIC GROUPS*** können Sie statische Gruppen anlegen. Pakete an diese Gruppen werden auf der jeweiligen Schnittstelle immer weitergeleitet, auch wenn eine bestimmte Gruppe nicht explizit bestellt wurde. Das Menü enthält folgende Felder:

Parameter	Wert
Group Address	IP-Adresse der statischen Gruppe. Hier können Sie eine IP-Multicast-Adresse eingeben.
Interface	Schnittstelle, an der Daten an die Gruppe weitergeleitet werden sollen. IGMP muss auf dieser Schnittstelle aktiv sein.
Status	Bestimmt, ob die statische Gruppe aktiv sein soll. Mögliche Werte: ■ *active* (Standardwert): Die statische Gruppe ist aktiv. ■ *inactive*: Die statische Gruppe ist nicht aktiv.

Tabelle 2-16: Felder im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP***➜ ***ADVANCED*** ➜ ***STATIC GROUPS***

Im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** ➜ ***MONITOR*** können Sie bestimmte IGMP Parameter überwachen, die sich auf eine Schnittstelle beziehen. Das Menü enthält folgende Felder:

Parameter	Wert
Interface	Zeigt die Schnittstelle, an der IGMP aktiv ist.

Parameter	Wert
Compat Version	Zeigt die aktuell benutzte IGMP Version.
Querier	Zeigt den Router, der als Querier dient und die Queries sendet.
V1 ExpiryTime(s)	Sollte in Ihrem Netzwerk ein V1 Host existieren, wird IGMP im Kompatibilitätsmodus mit Version 1 betrieben. Wenn sich in der Zeitspanne ***V1 EXPIRYTIME(S)*** kein V1 Host meldet, wird auf V2 bzw. V3 umgeschaltet.
ExpiryTime(s)	Zeigt die Gültigkeitsdauer des Queriers, wenn Ihr Gateway aktuell nicht als Querier dient. Der Wert *0* zeigt, dass Ihr Gateway Querier ist.
V2 ExpiryTime(s)	Sollte in Ihrem Netzwerk ein V2 Host existieren, wird IGMP im Kompatibilitätsmodus mit Version 2 betrieben. Wenn sich in der Zeitspanne ***V2 EXPIRYTIME(S)*** kein V2 Host meldet, wird auf V3 umgeschaltet.
Joins	Zeigt die Anzahl der empfangenen Anmeldungen zu Gruppen (Joins) an der entsprechenden Schnittstelle.
Wrong Queries	Zeigt die Anzahl der empfangenen fehlerbehafteten Queries an der entsprechenden Schnittstelle.
Group	Zeigt die Anzahl und die IP-Adressen der Gruppen.

Tabelle 2-17: Felder im Menü ***IP ➜ MULTICAST ➜ IGMP ➜ ADVANCED ➜ MONITOR***

Im Menü ***IP ➜ MULTICAST ➜ IGMP ➜ ADVANCED ➜ MONITOR ➜ GROUP*** können Sie bestimmte IGMP Parameter überwachen, die sich auf eine Gruppe beziehen.

Das Menü enthält folgende Felder:

Parameter	Wert
Group	Zeigt die IGMP Gruppe.
LastReporter	Zeigt den letzten Host, der einen Report für diese Gruppe geschickt hat.
Mode	Zeigt den IGMP-Filter-Modus. Mögliche Werte: ■ EXCLUDE: Pakete von den angegebenen Quellen werden von der Übermittlung ausgeschlossen. ■ INCLUDE: Pakete von den angegebenen Quellen werden für die Übermittlung zugelassen.
V1HostExpiryTime(s)	Zeigt die Dauer der Gruppenzugehörigkeit, wenn sich ein Host mit IGMP Version 1 an der Gruppe angemeldet hat.
ExpiryTime(s)	Zeigt die Dauer der Gruppenzugehörigkeit.
V2HostExpiryTime(s)	Zeigt die Dauer der Gruppenzugehörigkeit, wenn sich ein Host mit IGMP Version 2 an der Gruppe angemeldet hat.
included / excluded Source	Zeigt abhängig vom Wert des Feldes ***Mode*** die IP-Adressen der Quellen, die für die Datenübermittlung erlaubt werden bzw. von der Datenübermittlung ausgeschlossen sind.

Tabelle 2-18: Felder im Menü ***IP*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ ***Advanced*** ➜ ***Monitor*** ➜ ***Group***

Im Menü ***IP*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ ***Advanced*** ➜ ***ACL*** können Sie mit Hilfe von Regeln Reports und Pakete von bestimmten Hosts für bestimmte Gruppen

akzeptieren bzw. zurückweisen. Sie können die Reihenfolge der Regeln ändern oder Regeln löschen.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][IGMP]: ACL Configuration                            MyGateway


Press 'u' to move ACL up or press 'd' to move ACL down.

Pos    Interface   Sender          Group           Type      Action

  0    en1-0       192.168.0.1/24  224.0.0.0/4     traffic   deny
  1    any         0.0.0.0/0       224.1.2.3/32    traffic   deny




    ADD              DELETE           SAVE             CANCEL
```

Im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** ➜ ***ACL*** ➜ ***ADD*** können Sie Regeln anlegen.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][IGMP]: Add/Edit ACL Rule                            MyGateway



   Interface                          en1-0
   Sender Address                     192.168.0.1
   Sender Netmask                     255.255.255.0
   Group Address                      224.0.0.0
   Group Netmask                      240.0.0.0

   Type                               traffic

   Action                             deny



   SAVE      CANCEL
```

Das Menü enthält folgende Felder:

Parameter	Wert
Interface	Interface, für das eine Regel angelegt werden soll.
Sender Address	IP Adresse des Senders. Dies ist beim Typ *report* der Host, der IGMP Nachrichten verschickt. Bei *traffic* Einträgen entspricht diese der Multicast-Quelle.
Sender Netmask	Netzmaske des Senders.
Group Address	IP Adresse der Multicast-Gruppe.
Group Netmask	Netzmaske der Multicast-Gruppe.

Parameter	Wert
Type	Unterscheidet die Art der Pakete. Mögliche Werte: ■ *traffic*: Multicast-Pakete ■ *report*: IGMP Nachrichten.
Action	Bestimmt, was mit den Daten geschehen soll. Mögliche Werte: ■ *deny*: Daten werden zurückgewiesen. ■ *accept*: Daten werden akzeptiert.

Felder im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** ➜ ***ACL*** ➜ ***EDIT***

PIM Im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** können Sie die PIM-Funktionalität ein- oder ausschalten.

Hinweis

Bitte beachten Sie, dass Sie für die Nutzung der PIM-Funktionalität eine gültige Lizenz benötigen.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][PIM]: PIM Configuration                              MyGateway


                Status                  enabled


                Interfaces >
                Rendezvous Points >

                AnycastRP >




                SAVE     EXIT
```

Über das Menü ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** gelangen Sie in folgende Untermenüs:

- ***INTERFACES***
- ***RENDEZVOUS POINTS***
- ***ANYCASTRP***.

Im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** ➜ ***INTERFACES*** ➜ ***ADD/EDIT*** können Sie die Schnittstellen festlegen, an denen PIM benutzt werden soll.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][PIM][INTERFACE]: Configure PIM Interface          MyGateway



Interface             en1-0
Status                active
Mode                  Sparse
Stub Interface        disabled

Role   Router


Hello Interval (s)          30            Propagation Delay (s)    1
Triggered Hello Delay (s)   5             Override Interval (s)    3
Hello HoldTime (s)          180           DR Priority              1
JoinPrune Interval (s)      30
JoinPrune HoldTime (s)      180



SAVE     CANCEL
```

Das Menü ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** ➜ ***INTERFACES*** ➜ ***ADD/EDIT*** enthält folgende Felder:

Parameter	Wert
Interface	Wählen Sie die Schnittstelle, die für PIM benutzt werden soll, d.h. über die Multicast Routing betrieben werden soll.
Status	Aktiviert oder deaktiviert den Eintrag. Mögliche Werte: ■ *active* (Standardwert): PIM ist an dieser Schnittstelle aktiv. ■ *inactive*: PIM ist an dieser Schnittstelle nicht aktiv.
Mode	Modus, der für PIM benutzt werden soll. ■ *Sparse Mode* (Standardwert): PIM wird im Sparse Mode benutzt. ■ *Dense Mode*: Nicht verfügbar.
Stub Interface	Bestimmt, ob die Schnittstelle für PIM Datenpakete genutzt werden soll. Mit diesem Parameter können Sie z. B. eine Schnittstelle für IGMP benutzen, aber vor (gefälschten) PIM Messages schützen. Mögliche Werte: ■ *disabled*: Die Schnittstelle ist für PIM Datenpakete blockiert. ■ *enabled*: Die Schnittstelle ist für PIM Datenpakete freigegeben.

Parameter	Wert
Role	Bestimmt, welche Rolle das Gateway übernehmen soll. Mögliche Werte: ■ *Router*: Das Gateway dient als Router. ■ *RP*: Das Gateway dient als Rendezvous Point.
Hello Interval (s)	Bestimmt, in welchen Zeitabständen (in Sekunden) PIM Hello Messages über diese Schnittstelle gesendet werden. Der Wert *0* bedeutet, dass auf dieser Schnittstelle keine PIM Hello Mesages gesendet werden. Wertebereich: *0* .. *18000*.
Triggered Hello Delay (s)	Bestimmt, wie lange maximal gewartet werden darf, bis eine PIM Hello Message nach einem Sytemstart oder nach einem Neustart eines Nachbarn gesendet wird. Der Wert *0* bedeutet, dass PIM Hello Mesages immer sofort gesendet werden. Wertebereich: *0* .. *60*.
Hello HoldTime (s)	Bestimmt den Wert des Holdtime Feldes in einer PIM Hello Message. Daraus ergibt sich, wie lange ein PIM Router als verfügbar gilt. Sobald die ***HELLO HOLDTIME (S)*** abgelaufen ist und und keine weitere Hello Message empfangen wurde, wird dieser PIM Router als nicht erreichbar betrachtet. Wertebereich: *0* .. *65535*.

Parameter	Wert
JoinPrune Interval (s)	Bestimmt die Häufigkeit, mit der PIM Join/Prune Messages auf der Schnittstelle gesendet werden sollen. Der Wert *0* bedeutet, dass auf dieser Schnittstelle keine periodischen PIM Join/Prune Mesages gesendet werden. Wertebereich: *0* .. *18000*.
JoinPrune HoldTime (s)	Bestimmt den Wert, der in das Holdtime Feld einer PIM Join/Prune Message eingefügt wird. Dies ist die Zeitspanne, die ein Empfänger den Join/Prune State halten muss. Wertebereich: *0* .. *65535*.
Propagation Delay (s)	Bestimmt den Wert, der in das Propagation Delay Feld eingefügt wird. Dieses Feld ist ein Bestandteil der LAN Prune Delay Option in den PIM Hello Messages, die auf dieser Schnittstelle gesendet werden Propagation Delay und Override Interval stellen die sogenannten LAN-Prune-Delay-Einstellungen dar. Sie bewirken eine verzögerte Verarbeitung von Prune-Messages bei Upstream Routern. Wenn ***Propagation Delay (s)*** zu klein ist, kann es zum Abbruch der Übertragung von Multicast-Paketen kommen, bevor ein Downstream Router eine Prune Override Message geschickt hat. Wertebereich: *0* .. *32*.
Override Interval (s)	Bestimmt den Wert, den das Gateway in das Feld Override_Interval der LAN Prune Delay Option einfügt. ***Override Interval (s)*** bestimmt, wie lange ein Downstream Router höchstens warten darf, bis er eine Prune Override Message schickt.

Parameter	Wert
DR Priority	Bestimmt den Wert der Designated Router Priority, der in die Option DR Priority eingefügt wird. Je höher dieser Wert ist, desto größer ist die Wahrscheinlichkeit, dass der entsprechende Router als Designated Router verwendet wird.

Tabelle 2-19: Felder im Menü ***IP ➜ MULTICAST ➜ PIM ➜ INTERFACES ➜ ADD/EDIT***

Im Menü ***IP ➜ MULTICAST ➜ PIM ➜ RENDEZVOUS POINTS ➜ ADD/EDIT*** können Sie festlegen, welcher Rendezvous Point für welche Gruppen zuständig sein soll.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][PIM][RP]: Configure RP                              MyGateway


      Group Range           All Groups


      RP Address
      Precedence            0



       SAVE       CANCEL
```

Das Menü enthält folgende Felder:

Parameter	Wert
Group Range	Hier können Sie alle Gruppen angeben oder ein Multicast-Netzwerksegment spezifizieren.
Group Address	Nur für ***GROUP RANGE*** = *Specify*. IP Adresse des Multicast-Netzwerksegments.

Parameter	Wert
Group Prefix Length	Nur für ***GROUP RANGE*** = *Specify*. Die Netzmaskenlänge des Multicast-Netzwerk-segments. 224.0.0.0/4 bezeichnet das komplette Multi-cast Class D Segment. Wertebereich: *4 .. 32*.
RP Address	IP Adresse des Rendezvous Points
Precedence	Priorität Sie können ganze Zahlen eingeben.

Felder im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** ➜ ***RENDEZVOUS POINTS*** ➜ ***ADD/EDIT***

Im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** ➜ ***ANYCASTRP*** können Sie zwei oder mehr PIM Domänen verbinden und damit die Last zwischen ihnen verteilen. Sie können zwei Gateways als Backup füreinander einsetzen.

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][PIM]: AnycastRP Configuration                       MyGateway


      AnycastRP Address          1.1.1.1
      Local RP Address           192.168.0.1
      Remote RP Address          192.168.1.2
      Via                        MSDP



      SAVE      CANCEL
```

Das Menü enthält folgende Felder:

Parameter	Wert
AnycastRP Address	Virtuelle RP Adresse.

Parameter	Wert
Local RP Address	Lokal vergebene RP Adresse.
Remote RP Address	IP Adresse der RP Peers.
Via	Bestimmt, worüber die PIM Domänen verbunden werden sollen. Mögliche Werte: ■ MSDP ■ PIM Register.

Felder im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** ➜ ***ANYCASTRP***

Hinweis

Bitte beachten Sie, dass für AnycastRP eine zusätzliche virtuelle Adresskonfiguration notwendig ist.

MSDP

Mit MSDP (Multicast Source Discovery Protocol) können Sie mehrere Domänen verbinden, in denen PIM benutzt wird. Dabei verwendet jede Domäne ihren eigenen Rendezvous Point. Im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***MSDP*** können Sie die MSDP-Funktionalität ein- oder ausschalten bzw. im Detail konfigurieren.

Das Menü ***IP*** ➜ ***MULTICAST*** ➜ ***MSDP*** ➜ ***ADD/EDIT*** enthält folgende Felder:

Parameter	Wert
Remote Address	IP-Adresse des Peers.
Local Address	Lokale IP-Adresse.
Status	Aktiviert oder deaktiviert den Eintrag. Mögliche Werte: ■ *active* (Standardwert): Der Eintrag ist aktiv. ■ *inactive*: Der Eintrag ist nicht aktiv.
Retry Interval (s)	Zeitspanne in Sekunden bis zum nächsten Verbindungsversuch, wenn ein Verbindungsversuch fehlgeschlagen ist. Standardwert: *30*.
Holdtime (s)	Zeitspanne in Sekunden, die verstreichen darf, bis ein Peer als inaktiv gilt und getrennt wird. Standardwert: *75*.
KeepAlive (s)	Zeitspanne in Sekunden, in der eine KeepAlive Nachricht gesendet werden muss. Standardwert: *60*.

Tabelle 2-20: Felder im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***MSDP*** ➜ ***ADD/EDIT***

2.18 Stateful Inspection Firewall - Konfiguration vereinfacht

Die Konfiguration der bintec Stateful Inspection Firewall wurde vereinfacht. Schnittstellen, Services und Adressen können Sie jetzt zu Gruppen zusammenfassen. Die interne Verwendung der Alias Namen wurde ebenfalls verbessert.

Die Konfiguration der Gruppen erfolgt im Menü ***SECURITY*** ➜ ***STATEFUL INSPECTION*** in den jeweiligen Untermenüs.

Interface Groups

Im Menü ***Security*** ➜ ***Stateful Inspection*** ➜ ***Edit Interface Groups*** ➜ ***ADD/EDIT*** können Sie Schnittstellen zu Gruppen zusammenfassen. Das Menü besteht aus folgenden Feldern:

Parameter	Wert
Alias	Hier geben Sie einen Namen für die Schnittstellengruppe ein, die Sie konfigurieren wollen.
Interface Alias 1 - 10	Zeigt jeweils die Alias Namen der Schnittstellen Ihres Geräts. Sie können die gewünschten Alias Namen wählen und somit bis zu zehn Schnittstellen zu einer Gruppe zusammenfassen.

Tabelle 2-21: Neue Felder im Menü ***Security*** ➜ ***Stateful Inspection*** ➜ ***Edit Interface Groups*** ➜ ***ADD/EDIT***

Service Groups

Im Menü ***Security*** ➜ ***Stateful Inspection*** ➜ ***Edit Services Groups*** ➜ ***ADD/EDIT*** können Sie Dienste zu Gruppen zusammenfassen. Das Menü besteht aus folgenden Feldern::

Parameter	Wert
Alias	Hier geben Sie einen Namen für die Dienstgruppe ein, die Sie konfigurieren wollen.
Service Alias 1 - 10	Zeigt jeweils die Alias Namen der Dienste, die auf Ihrem Gerät konfiguriert sind. Sie können die gewünschten Dienste wählen und somit bis zu zehn Dienste zu einer Gruppe zusammenfassen.

Tabelle 2-22: Neue Felder im Menü ***Security*** ➜ ***Stateful Inspection*** ➜ ***Edit Interface Groups*** ➜ ***ADD/EDIT***

Address Groups

Im Menü ***Security*** ➜ ***Stateful Inspection*** ➜ ***Edit Address Groups*** ➜ ***ADD/EDIT*** können Sie Adress-Aliase zu Gruppen zusammenfassen. Das Menü besteht aus folgenden Feldern::

Parameter	Wert
Alias	Hier geben Sie einen Namen für die Adress-Alias-Gruppe ein, die Sie konfigurieren wollen.
Interface Alias 1 - 10	Zeigt jeweils die Alias Namen der Schnittstellen, für die auf Ihrem Gerät ein Alias zu einer IP-Adresse oder zu einem IP-Adressbereich konfiguriert ist. Sie können die gewünschten Alias Namen wählen und somit bis zu zehn Aliase zu einer Gruppe zusammenfassen.

Tabelle 2-23: Neue Felder im Menü ***Security*** ➜ ***Stateful Inspection*** ➜ ***Edit Adress Groups*** ➜ ***ADD/EDIT***

2.19 QoS-Klassifizierung in Stateful Inspection Firewall integriert

Mit Systemsoftware 7.8.7 ist die IP-QoS-Klassifizierung in die Konfiguration der Stateful Inspection Firewall integriert.

Dies ermöglicht die Anwendung des SIF-internen Sessionhandlings auch für die Paket-Klassifizierung, wie sie für QoS-Policies nötig ist.

Ein wesentlicher Vorteil ist die leichtere QoS-Konfiguration:

- Es müssen keine einzelnen IP-Paket-Filter mehr konfiguriert werden.
- Paket-Richtung und Zielports können außer Acht gelassen werden.
- Bei voneinander abhängigen Sessions müssen die Querbeziehungen nicht separat konfiguriert werden, z.B. PPTP/GRE, H232/RTP, FTP...).
- Die QoS-Klassifizierung wird nun für alle Datenströme durchgeführt, die nicht von der SIF geblockt werden.

Die Konfiguration erfolgt im Menü ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ **ADD/EDIT**:

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[SECURITY][STATEFUL INSPECTION][ADD]                            MyGateway

   Source              <-- Addresses   select     Addresses       -->
   Destination         <-- Addresses   select     Addresses       -->
   Edit Addresses >

   Service           <-- Services      select      Services        -->
   Edit Services >

   Action          accept


   QoS Priority    default (no special IP QoS handling)


                   SAVE                                  CANCEL
```

Das Menü enthält folgende Felder für die QoS-Klassifizierung:

Feld	Bedeutung
QoS Priority	Wählen Sie aus, mit welcher Priorität die von dem Filter spezifizierten Daten sendeseitig behandelt werden. Mögliche Werte: ■ *default (no special IP QoS handling)* (Standardwert): Keine Priorität. ■ *low latency (highest priority)*: Low Latency Transmission (LLT), d.h. Behandlung der Daten mit der geringstmöglichen Latenz, z. B. Standardmodus für VoIP-Daten (sofern dies nicht schon anderweitig festgelegt wurde, z. B. im Menü ***VoIP***). ■ *high* ■ *medium* ■ *low*.
QoS Class ID	Nur für QoS ***Priority*** = *high*, *medium* oder *low*. Legt die QoS-Paket-Klasse fest. Mögliche Werte: *1* (Standardwert) bis *255*.

Tabelle 2-24: ***Security*** ➜ ***Stateful Inspection*** ➜ ***Edit Filters*** ➜ ***Add/Edit***

Hinweis

Beachten Sie, dass wie gewohnt im Menü ***QoS*** ➜ ***Interfaces and Policies*** für jede Schnittstelle die gewünschten Regeln für die Klassifizierung der Daten festgelegt werden müssen.

2.20 QoS - Schicht 2 Unterstützung

Systemsoftware 7.8.7 unterstützt Schicht 2 Priorisierung entsprechend IEEE 802.1p.

Sie finden die Parmeter dazu in den Menüs ***Security*** ➜ ***Access Lists*** ➜ ***Filters*** ➜ ***ADD/EDIT***, ***QoS*** ➜ ***IP Filters*** ➜ ***ADD/EDIT*** und ***QoS*** ➜ ***IP Classification and Signaling*** ➜ ***ADD/EDIT*** ➜ ***Signaling (TOS/DSCP - Level 2)***.

2.21 Neue DynDNS-Provider selfHOST und NO-IP

Mit Systemsoftware 7.8.7 stehen die DynDNS-Provider selfhost und NO-IP zur Verfügung.

2.22 ISDN-Login unterstützt ISDN Subadressen

Mit Systemsoftware 7.8.7 unterstützt `isdnlogin` sowohl die eigene ISDN Subadresse als auch gerufene ISDN Subadressen.

2.23 RADIUS - Gleichzeitige Nutzung mehrerer Wählverbindungen und MLPPP

Mit Systemsoftware 7.8.7 können Sie mehrere Wählverbindungen mit derselben ID und demselben Passwort zusammen mit Channel Bundling (MLPPP) unter RADIUS nutzen.

2.24 VoIP Traffic zwischen Telefonanlagen

Mit Systemsoftware 7.8.7 können Sie im Menü *VoIP* ➜ *Dynamic Bandwidth Control* ➜ *ADD* im Feld *Mode* den Wert *always* einstellen, um VoIP Traffic zwischen zwei Telefonanlagen zu optimieren.

2.25 ISAKMP Configuration Method (IKE Config Mode)

Mit Systemsoftware 7.8.7 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 dynamische Zuteilung einer 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-Adressbereich an. Wählen Sie dazu das Setup Tool Menü ***IP*** ➜ ***IP Address Pools*** ➜ ***Pools*** ➜ **ADD**. Geben Sie einen eindeutigen, ganzzahligen ***Identifier*** und im Feld ***Description*** einen Namen für den Adress-Bereich ein. Geben Sie im Feld ***IP Address*** die erste IP-Adresse des Bereichs ein und im Feld ***Number of Consecutive Addresses*** die Anzahl der IP-Adressen, die der Bereich enthalten soll. Ergänzen Sie die Eingaben nach Wunsch. Speichern Sie den angelegten IP-Adressbereich mit **SAVE**. Mit **ADD** können Sie weitere IP-Adressbereiche anlegen.
   Die angelegten IP-Adressbereiche stehen zur Verfügung.
2. Wählen Sie IKE Config Mode aus und ordnen Sie den gewünschten IP-Adressbereich zu. Wählen Sie dazu das Setup Tool Menü ***IPSec*** ➜ ***Configure Peers*** ➜ **APPEND** und setzen Sie ***Virtual Interface*** = *yes*. Wählen Sie das Untermenü ***Interface IP Settings*** ➜ ***Basic IP-Settings*** und setzen Sie ***IP Transit Network*** = *IKE Config Server Mode*. Wählen Sie im Feld ***IP Address Pool*** den gewünschten IP-Adressbereich, ergän-

zen Sie die Einstellungen nach Ihren Wünschen und speichern Sie mit **SAVE**.

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

2.26 SSH Client

Ab Systemsoftware 7.8.7 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.

2.27 IGMP Host für lokale Applikationen

Systemsoftware 7.8.7 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.

Dieser Automatismus ist standardmäßig im Setup Tool im Menü ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** mit ***STATUS*** = *auto* eingestellt.

Falls der IGMP-Status auf *up* steht (***STATUS*** = *up)*, müssen Sie die jeweiligen Schnittstellen manuell für IGMP Host konfigurieren. Wird eine Schnittstelle im "Nur-Host-Modus" betrieben (***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ **ADD** mit ***MODE*** = *host-only*), 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 (***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ **ADD** mit ***MODE*** = *routing*).

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

2.28 STunnel Unterstützung

Systemsoftware 7.8.7 unterstützt STunnel. Sie können 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.

Parameter	Wert
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*.
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 2-25: 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.
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	IP-Adresse des Gateways Der Standardwert ist *127.0.0.1*.

Parameter	Wert
Internal port	Interner Port, der entsprechend der Einstellung im Feld ***INTERNAL MODE*** verwendet wird.
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 2-26: 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
Maximun 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 2-27: Felder im Menü ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** ➜ ***(ADVANCED) TIMER SETTINGS***

2.29 VLAN Priorisierung

Wenn ab **Systemsoftware 7.8.7** Daten mit VLAN Priorisierung entsprechend IEEE 802 empfangen werden, werden diese akzeptiert und weiterverarbeitet.

2.30 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.

2.31 DNS - Bailiwick Checking

Mit **Systemsoftware 7.8.7** wurde Bailiwick Checking hinzugefügt, d.h. es können in DNS-Anworten keine ungefragt mitgelieferten Einträge (Additional Resource Records) eingeschleust werden.

2.32 Standleitung - Bündel

Um Standleitungs-Schnittstellen zu einem Bündel kombinieren zu können, wurde im Setup Tool Menü ***PRI2-x*** für die Einstellung ***ISDN SWITCH TYPE*** = *leased line, 1 Hyperchannel (G.703 + G.704)* bzw. ***ISDN SWITCH TYPE*** = *leased line, G.703 (unstructured, no G.704)* das neue Feld ***BUNDLE NUMBER*** hinzugefügt. ***BUNDLE NUMBER*** = 0 bedeutet, dass kein Bündel angelegt wird. Eine ***BUNDLE NUMBER*** zwischen 1 und 255 weist die jeweilige Schnittstelle einem Bündel mit der angegebenen Nummer zu.

2.33 OSPF

Im Setup Tool Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***OSPF*** ➜ ***INTERFACES*** ➜ **EDIT** wurde das neue Feld ***PERFORM DEMAND PROCEDURES*** mit den Werten *yes* (Standardwert) und *no* eingeführt. Das neue Feld bildet die MIB-Variable ***IFDEMAND*** der MIB-Tabelle ***OSPFIFTABLE*** im Setup Tool ab.

2.34 HTTPS hinzugefügt

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

2.35 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.

2.36 Bandwidth on Demand (BoD) erweitert

Ab **Systemsoftware 7.8.7** 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.

2.37 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.

2.38 IPSec - Extended Authentication (XAuth) verfügbar

Mit Systemsoftware 7.8.7 steht Extended Authentication für IPSec (XAuth) zur Verfügung, eine zusätzliche Authentifizierungsmethode für Benutzer eines IPSec-Tunnels.

Das Gateway kann bei Nutzung von XAuth zwei verschiedene Rollen übernehmen, es kann als Server oder als Client dienen:

- Das Gateway fordert als Server einen Berechtigungsnachweis an.
- Das Gateway weist als Client seine Berechtigung nach.

Im Server-Modus können sich mehrere Benutzer über XAuth authentifizieren, z. B. Nutzer von Apple iPhones. Die Berechtigung wird entweder anhand einer Liste oder über einen RADIUS Server geprüft. Bei Verwendung eines Einmalpasswords (One Time Password, OTP) kann die Passwortüberprüfung von einem Token Server übernommen werden (z. B. beim Produkt SecOVID von Kobil), der hinter dem RADIUS Server installiert ist.

Wenn über IPSec eine Firmenzentrale mit mehreren Filialen verbunden ist, können mehrere Peers konfiguriert werden. Je nach Zuordnung verschiedener XAuth-Profile kann ein bestimmter Benutzer den IPSec-Tunnel über verschiedene Peers nutzen. Das ist zum Beispiel nützlich, wenn ein Angestellter abwechsend in verschiedenen Filialen arbeitet, jeder Peer eine Filiale repräsentiert und der Angestellte jeweils vor Ort Zugriff auf den Tunnel haben will.

Nachdem IPSec IKE (Phase 1) erfolgreich beendet ist und bevor IKE (Phase 2) beginnt, wird XAuth realisiert.

Wenn XAuth zusammen mit IKE Config Mode verwendet wird, werden zuerst die Transaktionen für XAuth und dann diejenigen für IKE Config Mode durchgeführt.

XAuth Server

Wenn Sie Ihr Gateway als XAuth Server konfigurieren wollen, können Sie die Authentifizierung über einen RADIUS Server oder lokal durchführen lassen.

XAuth Server mit Authentifizierung über RADIUS

Wenn Sie einen RADIUS Server nutzen wollen, konfigurieren Sie diesen für XAuth.

1. Wählen Sie dazu im Setup Tool das Menü ***IP*** ➜ ***REMOTE AUTHENTCATION (RADIUS/TACACS+)*** ➜ ***RADIUS AUTHENTICATION AND ACCOUNTING*** ➜ **ADD**.
2. Wählen Sie ***PROTOCOL*** = eXtended *AUTHentication*.
3. Geben Sie im Feld ***GROUP DESCRIPTION NEW*** den gewünschten Gruppennamen für den RADIUS Server ein.
4. Ändern und ergänzen Sie die übrigen Einstellungen für den RADIUS Server nach Wunsch und speichern Sie die Einstellungen mit **Save**.
   Der RADIUS Server für XAuth wird angelegt.

Legen Sie ein passendes Profil an.

1. Wählen Sie dazu ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND** ➜ ***PEER SPECIFIC SETTINGS***. ➜ ***XAUTH PROFILE*** ➜ **edit** ➜ **ADD**.
2. Geben Sie einen eindeutigen, ganzzahligen ***INDEX*** ein.
3. Geben Sie im Feld ***DESCRIPTION*** eine Beschreibung für das XAuth-Profil ein.
4. Wählen Sie ***ROLE*** = *server*.
5. Wählen Sie ***MODE*** = *radius*, wählen Sie im Feld ***AAASERVERGROUP*** die gewünschte RADIUS-Server-Gruppe aus und speichern Sie die Einstellungen mit **SAVE**.
   Das Profil mit RADIUS Server wird angelegt.

Legen Sie einen IPSec-Peer für XAuth an.

1. Wählen Sie dazu ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND**.
2. Geben Sie im Feld ***DESCRIPTION*** eine Beschreibung für den Peer ein.
3. Wählen Sie **Peer specific Settings**.
4. Wählen Sie im Feld ***XAUTH PROFILE*** das gewünschte Profil.
5. Ändern und ergänzen Sie die übrigen Einstellungen für den IPSec-Peer nach Wunsch und speichern Sie die Einstellungen mit **SAVE**.
   Der IPSec-Peer wird angelegt.

XAuth Server mit lokaler Authentifizierung

Wenn Sie lokal über eine Gruppenzuordnung authentifizieren lassen wollen, können Sie ein XAuth-Profil mit einer entsprechenden Benutzergruppe definieren.

1. Wählen Sie dazu ***IPSec*** ➜ ***Configure Peers*** ➜ **APPEND** ➜ ***Peer specific Settings*** ➜ ***XAUTH Profile*** ➜ **edit** ➜ **ADD**.
2. Geben Sie im Feld ***Index*** einen eindeutigen, ganzzahligen Wert ein.
3. Geben Sie im Feld ***Description*** eine Beschreibung für das XAuth-Profil ein.
4. Wählen Sie ***Role*** = *server*.
5. Wählen Sie ***Mode*** = *local*.
6. Geben Sie im Feld ***UserListGroupId*** einen ganzzahligen Wert ein.
7. Wählen Sie ***View UserList***.
   Sie sehen die Benutzerliste mit der eingegebenen ***UserListGroupId***.
8. Fügen Sie weitere Benutzer mit der Schaltfläche **ADD** hinzu. Geben Sie für jeden Eintrag ***Name*** und ***Password***.ein.
9. Speichern Sie jeden Benutzer mit **SAVE**.
   Das XAuth-Profil wird mit der definierten Benutzergruppe angelegt.

Legen Sie einen IPSec-Peer für XAuth an.

1. Wählen Sie dazu ***IPSec*** ➜ ***Configure Peers*** ➜ **APPEND**.
2. Geben Sie im Feld ***Description*** eine Beschreibung für den Peer ein.
3. Wählen Sie **Peer specific Settings**.
4. Wählen Sie das gewünschte Profil im Feld ***XAUTH Profile***.
5. Ändern und ergänzen Sie die übrigen Einstellungen für den IPSec-Peer nach Wunsch und speichern Sie die Einstellungen mit **SAVE**.
   Der IPSec-Peer wird angelegt.

XAuth Client

Wenn Sie Ihr Gateway als XAuth Client konfigurieren wollen, gehen Sie folgendermaßen vor:

Legen Sie ein Profil für XAuth im Client-Modus an.

1. Wählen Sie dazu ***IPSec*** ➜ ***Configure Peers*** ➜ **APPEND** ➜ ***Peer specific Settings*** ➜ ***XAUTH Profile*** ➜ **edit** ➜ **ADD**.

2. Geben Sie im Feld ***INDEX*** einen eindeutigen, ganzzahligen Wert ein.
3. Geben Sie im Feld ***DESCRIPTION*** eine Beschreibung für das XAuth-Profil ein.
4. Wählen Sie ***ROLE*** = *client*.
5. Geben Sie im Feld ***NAME*** den gewünschten Benutzernamen ein.
6. Geben Sie das Passwort für den Benutzer ein und speichern Sie die Einstellungen mit **SAVE**.
   Das Profil wird angelegt.

Legen Sie einen IPSec-Peer für XAuth an.

1. Wählen Sie dazu ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND**.
2. Geben Sie im Feld ***DESCRIPTION*** eine Beschreibung für den Peer ein.
3. Wählen Sie **Peer specific Settings**.
4. Wählen Sie das gewünschte Profil im Feld ***XAUTH PROFILE***.
5. Ändern und ergänzen Sie die übrigen Einstellungen für den IPSec-Peer nach Wunsch und speichern Sie die Einstellungen mit **SAVE**.
   Der IPSec-Peer wird angelegt.

2.39 IPSec - Dynamic Bandwidth Control verfügbar

Mit Systemsoftware 7.8.7 können Sie im Menü *VOIP* ➜ *DYNAMIC BANDWIDTH CONTROL* ➜ *ADD* im Feld *INTERFACE* auch IPSec Schnittstellen auswählen.

2.40 IPSec - Start Mode für IPSec Peers

Systemsoftware 7.8.7 unterstützt einen neuen Start Modus für IPSec Peers.

Um sicher zu stellen, dass ein Tunnel unmittelbar nach Einschalten des Gateways aktiviert wird, ist für die Peer-Konfiguration ein neuer Parameter eingeführt worden. Das Menü ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** ➜ ***PEER SPECIFIC SETTINGS*** erlaubt jetzt die Auswahl zwischen dem ***START MODE*** *Always*

Up und dem ***START MODE*** *On demand*. Wird ***START MODE*** *Always Up* gewählt, versucht das Gateway, einen Tunnel sofort nach Beendigung des Bootvorgangs herzustellen.

2.41 IPSec - Dynamic Peer und IKE Config Mode

Ab **Systemsoftware 7.8.7** kann der "Dynamic Peer Mode" zusammen mit IKE Config Mode verwendet werden.

2.42 IPSec - Dynamic Peer und XAUTH

Ab **Systemsoftware 7.8.7** kann der "Dynamic Peer Mode" zusammen mit XAUTH verwendet werden.

3 Änderungen

Folgende Änderungen sind in Systemsoftware 7.8.7 vorgenommen worden, um Leistung und Bedienbarkeit zu verbessern:

3.1 Konfigurationsdatei - Format geändert

Das Dateiformat der Konfigurationsdatei wurde erweitert, um eine Verschlüsselung zu erlauben sowie die Kompatibilität beim Zurückspielen der Konfiguration auf das Gateway in unterschiedliche Versionen der Systemsoftware sicherzustellen.

Das neue Format ist ein CSV-Format; es kann problemlos gelesen und modifiziert werden. Außerdem können Sie z. B. mithilfe von Microsoft Excel die entsprechenden Dateien in übersichtlicher Form einsehen.

Sicherungsdateien der Konfiguration können vom Administrator verschlüsselt abgelegt werden. Bei Versand der Konfiguration per E-Mail (z. B. für Supportzwecke) können vertrauliche Konfigurationsdaten bei Bedarf komplett geschützt werden.

Im Menü ***CONFIGURATION MANAGEMENT*** können Sie mit den Kommandos *put* und *get* wie gewohnt Dateien an einen TFTP-Host übertragen bzw. von diesem holen.

Wenn Sie mit dem Kommando *put* eine Konfigurationsdatei auf einen TFTP-Host übertragen wollen, können Sie bestimmen, ob die Konfigurationsdatei unverschlüsselt oder verschlüsselt gespeichert werden soll oder ob das alte Format verwendet werden soll. Da bei einer Konfigurationsdatei im alten Format ein Wiedereinspielen auf das Gerät nur bei gleicher Software-Version garantiert ist, wird das alte Format nicht mehr empfohlen.

Bei dem Kommando *get* kann das System das jeweilige Dateiformat erkennen. Bei verschlüsseltem Format muss selbstverständlich das Passwort beim Einspielen angegeben werden.

Im Menü ***CONFIGURATION MANAGEMENT*** wurden für das neue Dateiformat die Eingabemöglichkeiten im Feld ***TFTP FILE NAME*** erweitert.

Feld	Bedeutung
TFTP File Name	Nur für ***OPERATION*** = *put (FLASH -> TFTP)*. *get (TFTP -> FLASH)*, *state (MEMORY -> TFTP)*. Name der Konfigurationsdatei auf dem TFTP-Server. Über das Format des Dateinamens können Sie steuern, welches Format für die Konfigurationsdatei benutzt wird. Mögliche Formate: ■ *config.cf*: Bisheriges Format V0, unverschlüsselt. Für *config* können Sie einen beliebigen Namen eingeben. ■ *pwd:config.cf*: Neues Format V1, verschlüsselt. Für *pwd* können Sie ein beliebiges Passwort eingeben, für *config* einen beliebigen Namen. ■ *:config.cf*: Neues Format V1, unverschlüsselt. Für *config* können Sie einen beliebigen Namen eingeben.

Mit dem Programm *cf_convert.exe* können Sie Konfigurationsdateien des Formats V1 in solche des Formats V0 konvertieren und umgekehrt. Sie können bei bekanntem Passwort mit diesem Programm auch verschlüsselte Dateien entschlüsseln. Sie finden es unter www.funkwerk-ec.com.

Die grundlegende Verwendung des Programms *cf_convert.exe* ist folgendermaßen:

```
cf_convert

usage: cf_convert [-options]  infile [outfile]

   infile:  input filename (or "stdin")
   outfile: output filename (or "stdout" or none)

Options:
        -p <pwd>:     decryption password
        -o <version>: 0 or 1: output format version
        -v:           increment verbosity

Examples:
  cf_convert -p passwd router.cf router.csv: decrypt file
  cat infile | cf_convert -p passwd stdin | ..: usage within pipe
```

3.2 DHCP-Implementierung ergänzt

Aufgrund der Neuimplementierung der IP-Adressbereiche (Pools) (siehe Seite 23) ist die DHCP-Implementierung umstrukturiert und ergänzt worden.

DHCP Das neue Menü ***IP ➜ IP ADDRESS POOLS ➜ DHCP*** ersetzt das Menü ***IP ➜ IP ADDRESS POOL LAN (DHCP)***.

Das Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Parameter	Wert
Interface	Schnittstelle, welcher ein Adressbereich zugewiesen werden soll. Wenn ein DHCP-Request über ***INTERFACE*** eingeht, wird eine der Adressen aus dem Adressbereich zugeteilt. Sie können hier eine Schnittstelle wählen.
Pool	Zeigt die Bezeichnung der im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** definierten IP-Adressbereiche. Die jeweilige Bezeichnung wird dort im Feld ***DESCRIPTION*** festgelegt. Sie können hier einen Adressbereich wählen.
Assignment Mode	Bestimmt, welche Clients aus dem Adressbereich bedient werden sollen. Mögliche Werte: ■ *local* (Standardwert): Clients im lokalen Netz werden Adressen aus dem Adressbereich zugewiesen. ■ *relay*: Clients, die über einen Relay Server anfragen, werden Adressen aus dem Adressbereich zugewiesen. ■ *local/relay*: Sowohl Clients aus dem lokalen Netz als auch Clients, die über einen Relay Server anfragen, werden Adressen aus dem Adressbereich zugewiesen.
Lease Time (minutes)	Legt fest, wie lange eine Adresse aus dem Adressbereich einem Host höchstens zugewiesen werden soll. Mögliche Werte: *1* .. *300*. Standardwert: *120*.

Parameter	Wert
Gateway	Legt fest, welche IP-Adresse dem DHCP-Client als Gateway übermittelt werden soll. Wenn hier keine IP-Adresse eingetragen ist, wird die im Feld ***INTERFACE*** definierte IP-Adresse übertragen.
First TFTP Server	Standard-TFTP-Server, über den IP-Telefone ihre Konfiguration erhalten. Ist das Feld ***FIRST TFTP SERVER*** = *0.0.0.0*, so wird der Wert des Feldes ***SECOND TFTP SERVER*** benutzt. Sind die Felder ***FIRST TFTP SERVER*** = *0.0.0.0* und ***SECOND TFTP SERVER*** = *0.0.0.0*, so ist kein TFTP-Server verfügbar.
Second TFTP Server	Alternativer TFTP-Server, über den IP-Telefone ihre Konfiguration erhalten. Ist das Feld ***SECOND TFTP SERVER*** = *0.0.0.0*, so wird der Wert des Feldes ***FIRST TFTP SERVER*** benutzt. Sind die Felder ***FIRST TFTP SERVER*** = *0.0.0.0* und ***SECOND TFTP SERVER*** = *0.0.0.0*, so ist kein TFTP-Server verfügbar.
Radius Accounting	Protokolliert die IP-Adressvergabe und die Nutzung der IP-Adressen mithilfe eines RADIUS-Servers. Mögliche Werte: ■ *disabled* (Standardwert): IP-Adressvergabe und -nutzung wird nicht protokolliert. ■ *enabled*: IP-Adressvergabe und -nutzung wird protokolliert.
Radius Group Id	Gibt die Gruppe an, aus welcher der RADIUS-Server stammen soll. Mögliche Werte: *1 .. 999999*.

Parameter	Wert
Alive Check	Überprüft, ob die Clients, denen eine IP-Adresse aus dem IP-Adressbereich zugewiesen wurde, noch erreichbar sind. Mögliche Werte: ■ *enabled*: Überprüft die Erreichbarkeit der Clients. ■ *disabled*: Überprüft die Erreichbarkeit der Clients nicht. Standardwert: dis*abled*.
Alive Test Period (seconds, 0=disabled)	Legt einen Zeitraum (in Sekunden) fest, nach dem überprüft wird, ob die Clients, denen eine IP-Adresse aus dem Adressbereich zugewiesen wurde, noch erreichbar sind. Mögliche Werte: *0* .. *65535*. Standardwert: *0*. Wenn hier der Wert *0* gesetzt ist, wird kein Alive-Test durchgeführt.
Admin State	Einschalten oder Ausschalten der Zuordnung des IP-Adressbereichs zur gewählten Schnittstelle. Mögliche Werte: ■ *enabled* (Standardwert): Die Zuordnung zwischen IP-Adressbereich und Schnittstelle ist aktiv. ■ *disabled*: Die Zuordnung zwischen IP-Adressbereich und Schnittstelle ist nicht aktiv.

Tabelle 3-1: Neue Felder im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT***

IP Address Pool WAN (PPP)

Das Menü ***IP*** ➜ ***IP ADDRESS POOL WAN (PPP)*** wurde nach ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***IP ADDRESS POOL WAN (PPP)*** verschoben.

Assigned IP Addresses

Das Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***ASSIGNED IP ADDRESSES*** zeigt Ihnen eine Liste der reservierten IP-Adressen mit zusätzlichen Informationen..

Parameter	Wert
IP Address	Zeigt die reservierte IP-Adresse.
User Type	Für ***ENTRY TYPE*** = *dynamic*. Zeigt das Subsystem, welches den Eintrag angelegt hat. Für ***ENTRY TYPE*** = *manual*. Zeigt das Subsystem, welches die IP-Adresse zuweisen darf. Mögliche Werte: ■ *DHCP* (Standardwert): Subsystem DHCP. ■ *other*: Anderes Subsystem. ■ *none*: Der Eintrag kann nicht reserviert werden.
Type	Entry Type Zeigt, wie die IP-Adresse zugewiesen wurde. Mögliche Werte: ■ *dynamic*: Die IP-Adresse wurde dynamisch zugewiesen. Der Eintrag wurde automatisch durch das System erstellt. ■ *manual* (Standardwert): Die IP-Adresse wurde manuell durch den Administrator zugewiesen. Manuelle Einträge werden in der Konfigurationsdatei gespeichert.

Parameter	Wert
PhysAddr	Physical Address Für ***ENTRY TYPE*** = *dynamic*. Zeigt die MAC-Adresse des Clients. Für ***ENTRY TYPE*** = *manual* und ***USER TYPE*** = *DHCP*. Zeigt die physikalische Adresse, welche mit der Adresse im DHCP-Request übereinstimmen muss. Sie wird gezeigt, wenn sie konfiguriert ist und angefordert wurde.
Host Name	Für ***ENTRY TYPE*** = *dynamic*. Zeigt einen Hostnamen, wenn ein solcher in der Adressanfrage enthalten ist. Für ***ENTRY TYPE*** = *manual* und ***USER TYPE*** = *DHCP*. Zeigt den Hostnamen des Clients, wenn ein Hostname konfiguriert wurde.

Parameter	Wert
State	Status Diese Anzeige dient Support-Zwecken. Mögliche Werte: ■ *in*: init: initialer Wert. ■ *ch*: checking: Überprüft die Nutzung einer IP-Adresse (dies ist einer von mehreren temporären Zuständen). ■ *aw*: awrequest: Überprüft die Nutzung einer IP-Adresse (dies ist einer von mehreren temporären Zuständen). ■ *rc*: requestcheck: Überprüft die Nutzung einer IP-Adresse (dies ist einer von mehreren temporären Zuständen). ■ *cx*: checkexpired: Überprüft die Nutzung einer IP-Adresse (dies ist einer von mehreren temporären Zuständen). ■ *fo*: foreign: die IP-Adresse wird von einem anderen System benutzt. ■ *ow*: own: die IP-Adresse wird vom Router benutzt. ■ *re*: reserved: die IP-Adresse ist für einen bestimmten Client reserviert. ■ *al*: allocated: die IP-Adresse ist aktuell einem Client zugewiesen.

Tabelle 3-2: Neue Felder im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***ASSIGNED IP ADDRESSES***

Das Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***ASSIGNED IP ADDRESSES*** ➜ ***ADD/EDIT*** dient dazu, IP-Adressen zu vergeben oder bereits bestehende Einträgen zu ändern.

Im Menü ***IP ➜ IP ADDRESS POOLS ➜ ASSIGNED IP ADDRESSES*** können Sie sehen, ob und wie bestimmte IP-Adressen genutzt werden.

In diesem Menü können Sie die Art der Zuweisung einer IP-Adresse komfortabel ändern. Sie können z. B. eine IP-Adresse, die einem Client über DHCP zugewiesen ist, diesem Client fest zuweisen. Dazu müssen Sie in der Liste den gewünschten Eintrag mit der **Leertaste** wählen, um ihn zu markieren. Mit der Eingabe *s* weisen Sie die aktuelle IP-Adresse fest zu. Sie können aber auch umgekehrt fest zugewiesene Adressen für DHCP freigeben. Dazu müssen Sie den Listeneintrag wählen und *f* eingeben.

In früheren Softwareversionen war die Möglichkeit, einzelne IP-Adressen manuell zu vergeben, implizit im Menü ***IP ➜ IP ADDRESS POOL LAN (DHCP)*** enthalten.

Das Menü ***IP ➜ IP ADDRESS POOLS ➜ ASSIGNED IP ADDRESSES ➜ ADD/EDIT*** enthält folgende Felder:

Parameter	Wert
IP Address	Reservierte IP-Adresse. Sie können hier alle IP-Adressen eingeben, die in den unter ***IP ➜ IP ADDRESS POOLS ➜ POOLS*** definierten Adressbereichen enthalten sind.
User Type	Verwendung der IP-Adresse. Mögliche Werte: ■ *DHCP* (Standardwert): Die IP-Adresse wird für DHCP verwendet. ■ *other*: Die IP-Adresse wird für ein anderes Subsystem verwendet. ■ *none*: Die IP-Adresse wird nicht verwendet.
Entry Type	Zuweisen der IP-Adresse. Mögliche Werte: ■ *dynamic*: Die IP-Adresse wird dynamisch zugewiesen. Sie können bereits bestehende Einträge, bei denen die IP-Adresse manuell vergeben wurde, für dynamische IP-Adressvergabe freigeben. ■ *manual* (Standardwert): Die IP-Adresse wird manuell für einen bestimmten Client reserviert. Diese manuellen Einträge werden in der Konfigurationsdatei gespeichert.

Parameter	Wert
Client Identifier	Nur für ***User Type*** = *DHCP*. Identifiziert den Client. Für ***Entry Type*** = *manual*. Wenn Sie hier einen Wert eintragen, wird das Feld ***Physical Address*** ignoriert. Sie können aber auch das Feld ***Physical Address*** alternativ zum Feld ***Client Identifier*** verwenden. Für ***Entry Type*** = *dynamic*. ***Client Identifier*** wurde vom DHCP Client mitgesendet. Mögliche Werte: Hexadezimale Zahlen. Maximale Zeichenzahl: 20.
Physical Address	Nur für ***User Type*** = *DHCP*. Für ***Entry Type*** = *manual*. Hier können Sie die physikalische Adresse des Clients eintragen. Sie muss mit der Adresse im DHCP-Request übereinstimmen. Sie können das Feld ***Physical Address*** alternativ zum Feld ***Client Identifier*** verwenden. Für ***Entry Type*** = *dynamic*. MAC-Adresse des Clients.
Host Name	Nur für ***User Type*** = *DHCP*. Hostname des Clients. Für ***Entry Type*** = *manual*. Hier können Sie einen Hostnamen für den Client eingeben, der mit der Antwort auf eine Adressanfrage geschickt wird. Für ***Entry Type*** = *dynamic*. Hostname, der in einer Adressanfrage enthalten ist.

Parameter	Wert
Use Default Parameters	Sie können bei einer Gruppe von optionalen Parametern entweder Standardwerte benutzen oder die Parameter selbst festlegen. Dazu werden die Parameter verborgen oder angezeigt. ■ *yes* (Standardwert): Verbirgt die optionalen Parameter. Es werden Standardwerte benutzt. ■ *no*: Zeigt die optionalen Parameter. Sie können die Parameter festlegen.
LeaseTime	Für ***USE DEFAULT PARAMETERS*** = *no*. Legt fest, wie lange eine Adresse aus dem Adressbereich für einem Host reserviert wird. Standardwert: *-1*. Der Standardwert übernimmt den im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** eingegebenen Wert.
Gateway	Für ***USE DEFAULT PARAMETERS*** = *no*. Legt fest, welche IP-Adresse dem Client als Gateway übermittelt werden soll. Standardwert: *255.255.255.255*. Der Standardwert übernimmt den Eintrag aus dem Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT***. Der Wert *0.0.0.0* übermittelt die Adresse des nächsten Gateways, d.h. entweder die IP-Adresse der Schnittstelle oder die IP-Adresse des Relay Servers.

Parameter	Wert
Primary DNS	Für ***USE DEFAULT PARAMETERS*** = *no*. Hier können Sie die IP-Adresse eines globalen Domain Name Servers eingeben. Wenn im Feld ***PRIMARY DOMAIN NAME SERVER*** oder im Feld ***SECONDARY DOMAIN NAME SERVER*** ein Wert gesetzt ist, werden die entsprechenden Einträge im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ ***ADD/EDIT*** ignoriert. Standardwert: *255.255.255.255*. Der Standardwert übernimmt den entsprechenden Eintrag aus dem Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ ***ADD/EDIT***. Sind die Felder ***PRIMARY DOMAIN NAME SERVER*** = *0.0.0.0* und ***SECONDARY DOMAIN NAME SERVER*** = *0.0.0.0*, so wird die Einstellung von ***IP*** ➜ ***STATIC SETTINGS*** benutzt, wenn im Menü ***IP*** ➜ ***DNS*** für das Feld ***DHCP ASSIGNMENT*** = *global* gesetzt ist.

Parameter	Wert
Secondary DNS	Für ***USE DEFAULT PARAMETERS*** = *no*. Hier können Sie die IP-Adresse eines alternativen Domain Name Servers eingeben. Wenn im Feld ***PRIMARY DOMAIN NAME SERVER*** oder im Feld ***SECONDARY DOMAIN NAME SERVER*** ein Wert gesetzt ist, werden die entsprechenden Einträge im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ ***ADD/EDIT*** ignoriert. Standardwert: *255.255.255.255*. Der Standardwert übernimmt den entsprechenden Eintrag aus dem Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ ***ADD/EDIT***. Sind die Felder ***PRIMARY DOMAIN NAME SERVER*** = *0.0.0.0* und ***SECONDARY DOMAIN NAME SERVER*** = *0.0.0.0*, so wird die Einstellung von ***IP*** ➜ ***STATIC SETTINGS*** benutzt, wenn im Menü ***IP*** ➜ ***DNS*** für das Feld ***DHCP ASSIGNMENT*** = *global* gesetzt ist.
Primary TFTP Server	Für ***USE DEFAULT PARAMETERS*** = *no*. Hier können Sie die IP-Adresse eines Standard-TFTP-Servers eingeben, über den IP-Telefone ihre IP-Adresse und ihre Konfiguration erhalten sollen. Standardwert: *255.255.255.255*. Der Standardwert übernimmt den Eintrag aus dem Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT***. Wenn im Feld ***PRIMARY TFTP SERVER*** oder im Feld ***SECONDARY TFTP SERVER*** ein Wert gesetzt ist (nicht 255.255.255.255), so werden die entsprechenden Werte im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT*** ignoriert.

Parameter	Wert
Secondary TFTP Server	Für ***USE DEFAULT PARAMETERS*** = *no*. Hier können Sie die IP-Adresse eines alternativen TFTP-Servers eingeben, über den IP-Telefone ihre IP-Adresse und ihre Konfiguration erhalten sollen. Standardwert: *255.255.255.255*. Der Standardwert übernimmt den Eintrag aus dem Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT***. Wenn im Feld ***PRIMARY TFTP SERVER*** oder im Feld ***SECONDARY TFTP SERVER*** ein Wert gesetzt ist (nicht 255.255.255.255), so werden die entsprechenden Werte im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT*** ignoriert.
Alive Test Period	Für ***USE DEFAULT PARAMETERS*** = *no*. Legt einen Zeitraum (in Sekunden) fest, nach dem überprüft wird, ob die Clients, denen eine IP-Adresse zugewiesen wurde, noch erreichbar sind. Falls ein Client nicht mehr erreichbar ist, kann die IP-Adresse anderweitig vergeben werden. Mögliche Werte: *0* .. *65535*. Standardwert: *-1*. Der Standardwert übernimmt den Wert aus dem Feld ***ALIVE TEST PERIOD*** im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT***. Ist ***ALIVE INTERVAL*** = *0* gesetzt, so findet keine Überprüfung statt.

Parameter	Wert
Radius Accounting	Für ***USE DEFAULT PARAMETERS*** = *no*. Protokolliert die IP-Adressvergabe und die Nutzung der IP-Adressen mit Hilfe eines RADIUS-Servers. Mögliche Werte: ■ *default* (Standardwert): Übernimmt den Wert aus dem Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT***. ■ *enabled*: IP-Adressvergabe und -nutzung wird protokolliert. ■ *disabled*: IP-Adressvergabe und -nutzung wird nicht protokolliert.
Radius Group Id	Für ***USE DEFAULT PARAMETERS*** = *no*. Gibt die Gruppe an, aus welcher der RADIUS-Server stammen soll. Standardwert: *-1*. Der Standardwert übernimmt den Wert aus dem Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT***.

Tabelle 3-3: Neue Felder im Menü ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***ASSIGNED IP ADDRESSES*** ➜ ***ADD/EDIT***

3.3 DNS - Lokale Name Server

Zusätzlich zu globalen Name Servern können Sie jetzt lokale Name Server festlegen, über die bestimmte Einträge aufgelöst werden sollen. Die Konfiguration lokaler Name Server erfolgt im Menü ***IP*** ➜ ***DNS*** ➜ ***FORWARDED DOMAINS*** ➜ ***ADD/EDIT***.

Das Menü ***IP*** ➜ ***DNS*** ➜ ***FORWARDED DOMAINS*** ➜ ***ADD/EDIT*** enthält folgende zusätzlichen Felder:

Parameter	Wert
Forward to	Bestimmt, wohin ein Host Name zur Namensauflösung geschickt werden soll. Mögliche Werte: ■ *Interface* (Standardwert): Legt den WAN Partner fest, zu dem zur Namensauflösung eine Verbindung aufgebaut werden soll. ■ *Nameserver*: Legt fest, dass ein bestimmter Name Server zur Namensauflösung benutzt werden soll.
Primary	Nur für ***FORWARD TO*** *Nameserver*. IP-Adresse eines Domain Name Server, über den der angegebene Eintrag aufgelöst werden soll.
Secondary	Nur für ***FORWARD TO*** *Nameserver*. IP-Adresse eines alternativen Domain Name Server.

Tabelle 3-4: Neue Felder im Menü ***IP*** ➜ ***DNS*** ➜ ***FORWARDED DOMAINS*** ➜ ***ADD/EDIT***

3.4 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 7.8.7** 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.

3.5 DNS Query IDs zufallsgeneriert

Ab **Systemsoftware 7.8.7** werden aus Sicherheitsgründen die DNS Query IDs zufallsgeneriert.

3.6 MIB-Variable DNSNegotiation geändert

Mit **Systemsoftware 7.8.7** wurde in der MIB-Tabelle ***biboPPPDNS*** die MIB-Variable ***DNSNegotiation*** geändert.

In der MIB-Variable ***DNSNegotiation*** werden mit den Werten *enabled* und *dynamic_client* keine WINS Adressen mehr angefordert bzw. verwandelt. Wenn WINS Adressen angefordert werden sollen, steht der Wert *dynamic_client_with_wins* zur Verfügung.

3.7 MGCP Proxy Support beendet

Die Unterstützung des MGCP Proxy wird ab **Systemsoftware 7.8.7** eingestellt.

3.8 Verhalten von ISDN Schnittstelle mit aktivem NAT geändert

Mit **Systemsoftware 7.8.7** wurde das Verhalten von ISDN Schnittstellen mit aktivem NAT bei TCP Sessions geändert.

Bisher wurden alle NAT Einträge gelöscht, wenn sich der Zustand der ISDN Schnittstelle von *down* auf *up* geändert hatte.

Jetzt wird überprüft, ob die IP-Adresse identisch geblieben ist. In diesem Fall bleiben die NAT Einträge erhalten.

3.9 Application Level Gateway geändert

Mit **Systemsoftware 7.8.7** werden die Application Level Gateways nicht mehr Endgeräte basiert sondern Session basiert genutzt.

Die Menüs ***VoIP*** ➜ ***Application Level Gateway*** ➜ ***MGCP Terminal configuration*** und ***VoIP*** ➜ ***Application Level Gateway*** ➜ ***SIP Terminal configuration*** wurden daher entfernt.

3.10 Spanning Tree Algorithmus entfernt

Mit **Systemsoftware 7.8.7** wurde der Spanning Tree Algorithmus aus der Funktion Bridging entfernt.

3.11 Mögliche Anzahl von NAT Sessions vergrößert

Bisher war die Anzahl NAT Ports für jedes Protokoll (TCP, UDP, ICMP) auf 4000 begrenzt.

Mit **Systemsoftware 7.8.7** kann jeder globale Pool dynamisch in 500er Schritten bis zur maximalen Größe von 32500 wachsen.

3.12 IPSec - Bezeichnung geändert

Im Menü ***IPSec*** ➜ ***Configure Peers*** ➜ ***APPEND*** ➜ ***Peer specific Settings*** wurde *p2* in *Peer No. 2* umbenannt.

3.13 Ping-Funktion ergänzt

Ab **Systemsoftware 7.8.7** kann in ausgehenden IP-Paketen das sogenannte Don't-Fragment-Flag gesetzt werden. Geben Sie dazu *ping -M <IP-Adresse>* ein.

3.14 Standardwert für Anzahl der NAT Ports vergrößert

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

3.15 NAT - Pass-Through hinzugefügt

Ab **Systemsoftware 7.8.7** können Sie mit Hilfe der neuen MIB-Tabelle ***ipNatExcludeTable*** einen Teil des Datenverkehrs von NAT ausnehmen, d.h. NAT Pass-Through konfigurieren.

3.16 UDP Portnummern zufallsgeneriert

Ab **Systemsoftware 7.8.7** 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 zugeordnet.

3.17 Verarbeitung leerer IP-Adressen geändert

Bisher wurde bei leerer IP-Adresse automatisch *0.0.0.0* angezeigt. Wenn eine MIB-Tabelle eine leere IP-Adresse liefert, wird diese ab sofort als leer angezeigt.

Das System prüft, ob die Eingabe einer IP-Adresse erforderlich ist. Gegebenenfalls erscheint ein Hinweis.

3.18 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.

3.19 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.

3.20 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.

3.21 MIB-Tabellen für AUX Port neu organisiert

Wegen der neuen Funktion Serial over IP und um die Übersichtlichkeit zu verbessern wurden für den AUX Port die beiden neuen MIB-Tabellen ***AUXCONFIGTABLE*** und ***AUXSTATTABLE*** angelegt, die Tabelle ***TTYPROFILETABLE*** wurde entfernt. Die Tabelle ***TTYIFTABLE*** enthält jetzt die neue MIB-Variable ***CURRENTMODE***, die Variable ***MODE*** wurde um den Wert *soip* ergänzt; einige Einträge dieser Tabelle wurden in die Tabelle ***AUXSTATTABLE*** bzw. in die Tabelle ***AUXCONFIGTABLE*** verschoben.

3.22 RADIUS Server - Gruppenkonfiguration vereinfacht

In der MIB-Tabelle ***RADIUSSERVERTABLE*** wurde die MIB-Variable ***GROUPDESCR*** hinzugefügt, um eine Gruppe von RADIUS Servern, die über die Variable ***GROUPID*** zusammengefasst wurden, komfortabler "ansprechen" zu können.

4 Gelöste Probleme

Die folgenden Probleme sind in Systemsoftware 7.8.7 gelöst worden:

4.1 IP - Speicherverlust

(ID 4832)

Inkorrektes Löschen von Sessions konnte zu einem Speicherverlust und zum Neustart des Gateways führen.

Dieses Problem ist gelöst worden.

4.2 Setup Tool Absturz

(ID 8020)

Es konnte vorkommen, dass der Aufruf des Menüs ***System*** ➜ ***Schedule & Monitor*** ➜ ***Keepalive Monitoring (Hosts & Ifc)*** zum Absturz des Setup Tools führte.

Das Problem ist gelöst worden.

4.3 Stacktrace bei bestimmtem Wert für Encapsulation

(ID 7819)

In der MIB-Tabelle ***biboPPPTable*** verursachte der veraltete Wert ***Encapsulation*** = *x25_ppp* einen Stacktrace. Es existierten folgende weitere veraltete Werte:

x31_bchan, *x75btx_ppp*, *x25_nosig*, *x25_ppp_opt*, *x25_pad*, *x25_noconfig*, *x25_noconfig_nosig* und *ipoa*.

Das Problem ist gelöst worden, die veralteten Werte sind entfernt worden.

4.4 Stacktrace bei Triggered RIP Meldungen

(ID n/a)

Das Senden von Triggered RIP Meldungen verursachte einen Stacktrace.

Das Problem ist gelöst worden.

4.5 Probleme mit dem System nach 194 Tagen

(ID 7309)

Nach 194 Tagen konnte man sich auf dem System zwar weiterhin einloggen, aber keine Kommandos ausführen und das Setup Tool nicht aufrufen.

Das Problem ist gelöst worden.

4.6 Email Alert Probleme

(ID n/a)

Unbeabsichtigte Einträge in der MIB-Tabelle ***ipSifExpectTable***, mittels SNMP nicht sichtbar, verursachten unter Umständen schlechte IP Performance.

Das Problem ist gelöst worden.

4.7 Email Alert unvollständig abgeschaltet

(ID 3240)

Mit ***USERALERTADMINSTATUS*** = *disable* wurde der Email Alert nicht vollständig deaktiviert.

Das Problem ist gelöst worden.

4.8 Ausschließlich Ziffern für Called Party Number

(ID 786)

Bei der Eingabe einer Called Party Number waren ausschließlich Ziffern verfügbar.

Das Problem ist gelöst worden, Sie können jetzt auch andere alphanumerische Zeichen eingeben.

4.9 Bootconfig - Encapsulation Wert nicht gespeichert

(ID 7675)

Wurde im Menü ***WAN PARTNER*** ➜ **ADD** im Feld ***ENCAPSULATION*** der Wert *HDLC Framing (only IP)* gewählt, so wurde dieser Wert nicht in der Bootkonfiguration gespeichert sondern für ***ENCAPSULATION*** war nach dem Speichern der Wert *PPP* gesetzt.

Das Problem ist gelöst worden.

4.10 HTTP - Systeminformation nicht korrekt

(ID 8345)

Auf der entsprechenden HTTP Seite wurden in den Systeminformationen falsche Angaben zu S2M Schnittstellen angezeigt.

Das Problem ist gelöst worden.

4.11 MS-CHAP Authentifizierungsfehler zwischen Windows-Clients und Router

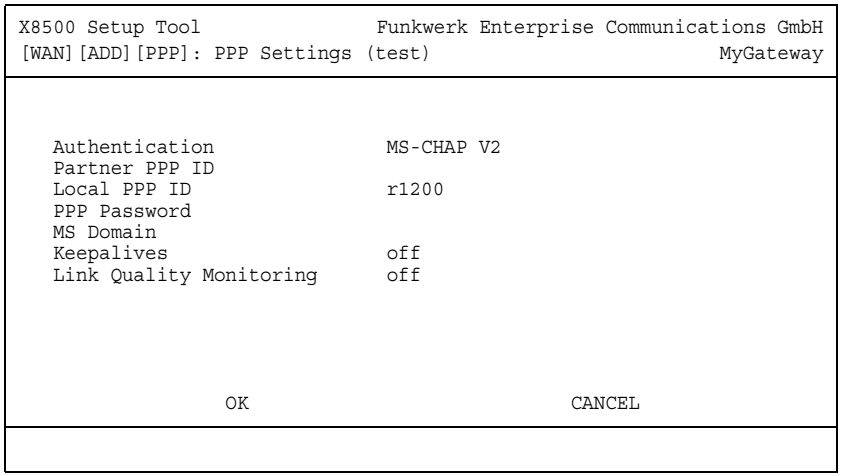
(ID 2318)

Die Authentifizierungsverhandlung zwischen Windows-Clients und dem Router konnte bei PPP- oder PPTP-Verbindungen fehlschlagen, wenn der Login-Name zusammen mit dem Domänennamen verwendet wurde, z. B. DEVELOPMENT\Developer.

Das Problem ist gelöst worden.

Bei MS-CHAP V1 wird der ganze Identifikationsname (Domänenname und Login-Name) für die Authentifizierung verwendet.

Bei MS-CHAP V2 wird nur der Login-Name für die Authentifizierung verwendet. Der Domänenname wird separat überprüft. Dazu ist der Domänenname ggf. in das neue Feld ***MS DOMAIN*** einzugeben. Das Feld wird nur angezeigt, wenn ***AUTHENTICATION*** = *MS-CHAP*, *MS-CHAP V2* oder *CHAP* + *PAP* + *MS-CHAP*.



4.12 RADIUS - Irrtümliche Verwendung von MS-CHAPv2 statt MS-CHAPv1

(ID 7016)

Bei Authentisierung über einen RADIUS Server mit *MS-CHAP V1* wurde beim Rückruf irrtümlich *MS-CHAP V2* verwendet.

Das Problem ist gelöst worden.

4.13 RADIUS - Reload mit zwei Servern fehlgeschlagen

(ID 6873)

Wenn bei zwei RADIUS Servern der eine mit Reload Intervall (MIB-Variable ***RELOADINTERVAL*** in der MIB-Tabelle ***RADIUSSERVERTABLE***) konfiguriert wurde und der zweite ohne, so wurde beim Wechsel vom Server mit Reload Intervall zum Server ohne Reload Intervall keine Reload mehr durchgeführt.

Das Problem ist gelöst worden.

4.14 RIP - Next-Hop-Information nicht gesendet

(ID 4165)

Die Next-Hop-Information wurde in Routenankündigungen nicht mitgesendet (RFC 2453).

Das Problem ist gelöst worden.

4.15 RIP - Unzuässige Metric 0 in Triggered Updates

(ID 7542)

Triggered Update Pakete enthielten Routen mit dem unzulässigen Metric-Wert *0*.

Das Problem ist gelöst worden.

4.16 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.

4.17 DNS - Namensauflösung fehlgeschlagen

(ID 6916)

Es konnte vorkommen, dass nach einigen Tagen plötzlich die Namensauflösung auf dem Gerät nicht mehr funktionierte.

Das Problem ist gelöst worden.

4.18 DNS Request fehlgeschlagen

(ID n/a)

Der erste DNS Request, der an das System geschickt wurde, hielt das System an.

Das Problem ist gelöst worden.

4.19 CAPI - Unbeabsichtigter Neustart des Systems

(ID 7257)

Nach einem Verbindungsaufbau mit der Meldung "... Outgoing call established" konnte es zu einem unbeabsichtigten Neustart des Geräts kommen.

Das Problem ist gelöst worden.

4.20 CAPI - Falsche Versionsnummer

(ID 4965)

Für CAPI wurden die Versionsnummern 1.1 und 2.0 angegeben. Das Gerät unterstützt jedoch nur noch CAPI 2.0

Das Problem ist gelöst worden.

4.21 NAT-Einträge fälschlicherweise gelöscht

(ID n/a)

NAT-Einträge konnten gelöscht werden, auch wenn die IP-Adresse sich nicht geändert hatte. Dieses wurde bei PPP-Verbindungen mit dynamischem Client beobachtet, konnte aber auch bei anderen Verbindungen passieren.

Das Problem ist gelöst worden.

4.22 PPP - Unvollständige CLID-Überprüfung

(ID 6528 - nur für Geräte mit ISDN)

Unvollständige CLID-Überprüfung konnte dazu führen, dass Rufe auch dann angenommen wurden, wenn die Calling Party Number falsch war.

Das Problem ist gelöst worden.

4.23 PPP - Multi-User-Einträge nicht beachtet

(ID 5650)

Bei der Entscheidung, ob eine eingehender Ruf angenommen wird oder nicht, wurden Multi-User-Einträge in der ***BIBOPPPTABLE*** nicht beachtet.

Das Problem ist gelöst worden.

4.24 PPP - Benutzung mehrerer Wählverbindungen fehlgeschlagen

(ID 8411)

Wenn für eine PPP Schnittstelle mehrere Wählverbindungen konfiguriert waren und die erste nicht verfügbar war, wurde nicht auf die anderen Nummern zurückgegriffen.

Das Problem ist gelöst worden.

4.25 PPP - Authentisierung bei Festverbindungen fehlgeschlagen

(ID 7536)

Bei PPP Festverbindungen war die Authentisierung fehlgeschlagen.

Das Problem ist gelöst worden.

4.26 PPP - Unbeabsichtigter Neustart des Systems

(ID n/a)

Während des Verbindungsaufbaus konnte es zu einem unbeabsichtigten Neustart des Geräts kommen.

Das Problem ist gelöst worden.

4.27 Multilink PPP - Datenpaket-Reihenfolge nicht korrekt

(ID 8428)

Mit Multilink-PPP wurden kleine Datenpakete nicht in der korrekten Reihenfolge transportiert.

Das Problem ist gelöst worden.

4.28 PPPoE und Ethernet Schnittstellen - Probleme mit ext. DSL-Modems

(ID 9225)

Wenn die MIB-Variable ***MaxTxRate*** in der Tabelle ***qosIfTable*** geändert worden war und in der Tabelle ***ifTable*** die Variable ***OperStatus*** = *up* war, wurde in der Tabelle ***ifTable*** die MIB-Variable ***Speed*** für PPPoE und Ethernet Schnittstellen nicht angepasst. Das führte zu Latenzproblemen in Szenarien mit externen DSL-Modems.

Das Problem ist gelöst worden.

4.29 PPPoE Probleme

(ID 10668)

Es konnte vorkommen, dass beim Aufbau einer PPPoE Session Probleme auftraten, wenn der BRAS des Providers nicht entsprechend RFC 2516 arbeitete.

Das Problem ist gelöst worden.

4.30 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.

4.31 Multilink PPPoE - Panic

(ID 8512)

Mit einer Last größer 10 MBit/s konnte es bei Multilink Verbindungen mit zwei oder mehr PPPoE Links zu einer Panic kommen.

Das Problem ist gelöst worden.

4.32 PPTP - Falscher Wert im Feld via IP Interface

(ID 3105)

Wenn im Menü ***PPTP ➜ ADD ➜ IP ➜ Basic IP-Settings*** die Felder ***PPTP VPN Partner's IP Adress***, ***via IP Interface***, ***Remote IP Address*** und ***Remote Netmask*** gesetzt waren und nach dem Speichern dieser Konfiguration dieses Menü erneut aufgerufen wurde, wurde für das Feld ***via IP Interface*** irrtümlich der Wert *AUTO* angezeigt.

Darüber hinaus wurde beim erneuten Setzen des Feldes ***via IP Interface*** nach dem Speichern die Hostroute zur ***PPTP VPN Partner's IP Address*** verdoppelt.

Die Probleme sind gelöst worden.

4.33 PPTP-Verbindungsaufbau schlug fehl

(ID 10379)

Es konnte vorkommen, dass der Aufbau von PPTP-Verbindungen fehlschlug, wenn sie von außen initiiert wurden und wenn IP Load Balancing verwendet wurde.

Das Problem ist gelöst worden.

4.34 PPTP Verbindungsaufbau scheiterte

(ID 2787)

Es konnte vorkommen, dass der Aufbau von PPTP-Verbindungen fehlschlug, wenn sie von außen initiiert wurden, wenn das Gateway Tunnel-Endpunkt war und wenn PPTP Passthrough eingeschaltet war.

Das Problem ist gelöst worden.

4.35 MPPE für X.21 Leased Line Verbindungen fehlgeschlagen

(ID 7767)

MPPE konnte nicht als Encryption für Leased Line Verbindungen über X.21 verwendet werden.

Das Problem ist gelöst worden.

4.36 BRRP - Konfiguration des virtuellen Routers nicht korrekt

(ID 8262)

Im Menü ***BRRP*** ➜ ***CONFIGURATION*** ➜ ***ADD*** wurden nach Setzen oder Ändern des Feldes ***VIRTUAL ROUTER ID*** die Felder ***VIRTUAL INTERFACE***, ***MASTER IP-ADDRESS***, ***MAC-ADDRESS*** auf den Standardwert zurückgesetzt.

Das Problem ist gelöst worden.

4.37 BRRP - falsche IP-Adresse

(ID 10112)

Im Setup Tool Menü ***BRRP*** ➜ ***MONITORING*** wurde fälschlicherweise die IP-Adresse der physikalischen Schnittstelle statt der IP-Adresse der virtuellen Schnittstelle angezeigt.

Das Problem ist gelöst worden.

4.38 Inkonsistenz Layer 2 Mode

(ID 1737)

Der Wert des Layer 2 Mode wurde für Festverbindungen irrtümlich aus der MIB-Tabelle ***PPP*** entnommen und nicht aus der Tabelle ***ISDNCHTABLE*** oder der Tabelle ***X21IFTABLE***.

Das Problem ist gelöst worden.

4.39 SIF und NAT - Extended-Passive-FTP-Verbindungen blockiert

(ID 7197)

Obwohl eine Allow-Regel für FTP-Verbindungen angelegt war, blockierte die SIF die Datenverbindungen einer Extended-Passive-FTP-Verbindung.

Das Problem ist gelöst worden.

4.40 SIF - Unbeabsichtigte Filterung

(ID n/a)

Lokal erzeugter Datenverkehr wurde von der SIF auch bei deaktiviertem Local Filtering blockiert. Dies konnte auch bei gänzlich ausgeschalteter SIF geschehen, sofern sich Deny-Regeln in der Konfiguration der SIF befanden.

Das Problem ist gelöst worden.

4.41 SIF - Standardeinträge nicht geladen

(ID n/a)

Die Standardeinträge der ***ipSifAliasServiceTable*** und der ***ipSifAliasAddressTable*** wurden u. U. dann nicht geladen, wenn auf dem Gateway mehrere Konfigurationen abgelegt waren.

Das Problem ist gelöst worden.

4.42 SIF - Unbeabsichtigte Blockierung des Datenverkehrs

(ID n/a)

Durch instabile bzw. inkonsistente Einträge in den MIB-Tabellen ***ipSifAliasAddressTable*** und ***ipSifAliasTable*** konnte es vorkommen, dass der Datenverkehr blockiert wurde.

Das Problem ist gelöst worden.

4.43 SIF - Entfernen einer Service Group verursachte Stacktrace

(ID 7751)

Bei der Konfiguration einer Stateful Inspection Firewall verursachte das Entfernen einer Service Group einen Stacktrace.

Das Problem ist gelöst worden.

4.44 SIF funktionierte mit Interface Groups nicht korrekt

(ID 8934)

Wenn eine Stateful Inspection Firewall zusammen mit Interface Groups konfiguriert war, funktionierten die Filter nicht korrekt.

Das Problem ist gelöst worden.

4.45 SIF - Unerwartete MIB Tabelleneinträge

(ID 6194)

In der MIB-Tabelle ***ipSifAliasAddressTable*** traten unerwartete Tabelleneinträge auf.

Das Problem ist gelöst worden.

4.46 SIF - Systemabsturz während der Registrierung bei einem Provider

(ID 6016)

Während des Versuchs sich bei einem Provider mit falscher IP-Adresse zu registrieren konnte es zum Systemabsturz kommen.

Das Problem ist gelöst worden.

4.47 SIF - Speicherprobleme bei vielen Sessions

(ID 9221)

Da mit einer SIF die Anzahl der Sessions unbegrenzt war, stürzte das System bei einer großen Zahl von Sessions wegen Speicherproblemen ab.

Das Problem ist gelöst worden.

4.48 SIF - Zweiter Befehl Put fehlgeschlagen

(ID 8542)

Mit einer SIF schlug bei zwei aueinanderfolgenden Befehlen Put über TFTP der zweite Befehl Put fehl.

Das Problem ist gelöst worden.

4.49 SIF - Source Port Überprüfung nicht funktionsfähig

(ID n/a)

In der MIB-Tabelle ***ipSifAliasServiceTable*** schlug die Überprüfung der MIB-Variable ***SourcePort*** fehl.

Das Problem ist gelöst worden.

4.50 SIF - Adressaliase versehentlich gelöscht

(ID 7689)

Bei einer SIF wurden während der PPP inband Authentication Adressaliase versehentlich gelöscht.

Das Problem ist gelöst worden.

4.51 SIF - Stacktrace bei der Konfiguration

(ID 11405)

Bei der Konfiguration der Services der SIF kam es zu einem Stacktrace und das Setup wurde beendet.

Das Problem ist gelöst worden.

4.52 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.

4.53 IPSec - Unbeabsichtigter Neustart

(ID 8395)

Bei einem IPSec Peer mit Trafic Lists und wenn Host Routen, z. B. für Einloggen von außen, eingetragen waren, konnte es zu einem Neustart des Geräts kommen.

Das Problem ist gelöst worden.

4.54 IPSec - Panic

(ID 7218)

Gelegentlich wurde auf der Konsole die Meldung "improper state 5" ausgegeben. Es folgte eine Panic.

Das Problem ist gelöst worden.

4.55 IPSec - Panic

(ID 10155)

Wurde beim Certificate Enrollment über SCEP ein Subject Name in falscher Notation eingegeben, kam es zu einer Panic.

Das Problem ist gelöst worden.

4.56 IPSec - Panic ohne Reboot

(ID 10024)

Wenn ein IPSec Peer mit Traffic-Listen-Eintrag oder ein Traffic-Listen-Eintrag gelöscht wurde, trat eine Panic ohne Reboot auf.

Das Problem ist gelöst worden.

4.57 IPSec - Falscher Wert der MIB-Variablen LifeSeconds

(ID 7825)

Wenn der Wert 65535 der MIB-Varible ***LIFESECONDS*** in der MIB-Tabelle ***IKEPROFILETABLE*** überschritten war, wurde ein falscher Wert verwendet.

Das Problem ist gelöst worden.

4.58 IPSec - Falsche Namensauflösung von IPSec Peers

(ID 5754)

Bei Peers mit mehreren Hostnamen wurden bei der Namensauflösung falsche IP-Adressen zugeordnet.

Das Problem ist gelöst worden.

4.59 IPSec - RADIUS-Reload fehlgeschlagen

(ID 5379)

Wenn ein RADIUS Reload der IPSec Peers sehr häufig durchgeführt wurde, schlug er nach einer gewissen Laufzeit des Gateways fehl.

Das Problem ist gelöst worden.

4.60 IPSec - Dynamischer Peer nicht funktionsfähig

(ID n/a)

Wenn ein Dynamischer Peer auf einem virtuellen Interface konfiguriert wurde, war die Konfiguration nicht funktionsfähig. Ein Peer auf Basis von Traffic-Listen war funktionsfähig.

Das Problem ist gelöst worden.

4.61 IPSec - Automatischer CRL-Import über Event Scheduler nicht möglich

(ID n/a)

Ein über den Event Scheduler gesteuerter Import von CRLS war nicht möglich, da über den Scheduler die Bestätigung des Imports nicht erfolgte.

Das Problem ist gelöst worden.

4.62 IPSec - Kein RIP

(ID 7486)

RIP funktionierte über einen IPSec Tunnel nicht.

Das Problem ist gelöst worden.

4.63 IPSec - Phase 2 nicht initiiert

(ID 3432)

Wenn das Interface der Source Route down war, wurde Phase 2 nicht initiiert.

Das Problem ist gelöst worden.

4.64 IPSec - Phase-2-Aushandlung funktionierte nicht

(ID 7284)

Nach Silent Disconnect funktionierte die Phase 2 Aushandlung nicht.

Das Problem ist gelöst worden.

4.65 IPSec - Phase-2-Aushandlung scheiterte

(ID 10877)

Unter bestimmten Bedingungen wurde für die Phase-2-Aushandlung eine falsche Netzmaske versucht, und die Aushandlung scheiterte dementsprechend.

Das Problem ist gelöst worden.

4.66 IPSec - Phase-2-Bundles - lokales Netz nicht übertragen

(ID 11409)

Bei IPSec Phase-2-Bundles wurde das lokale Netz nicht übertragen, wenn keine lokale IP-Adresse auf dem Router konfiguriert war.

Das Problem ist gelöst worden.

4.67 IPSec - Interface Zurücksetzen nicht möglich

(ID 3232)

Das Zurücksetzen eines IPSec Interfaces im Menü ***MONITORING AND DEBUGGING*** ➜ ***INTERFACES*** ➜ ***<INTERFACE>*** ➜ **EXTENDED** mit der Einstellung ***OPERATION*** > *reset* war nicht möglich.

Das Problem ist gelöst worden.

4.68 IPSec - DELETE Schaltfläche fälschlicherweise angezeigt

(ID 7895)

Im Menü ***IPSEC*** ➜ ***IKE (PHASE 1) DEFAULTS*** ➜ ***<EDIT>*** ➜ **ADD** ➜ ***VIEW PROPOSALS*** wurde fälschlicherweise eine **Delete** Schaltfläche angezeigt. In diesem Menü können jedoch keine Einträge gelöscht werden.

Das Problem ist gelöst worden.

4.69 IPSec - Fehlende Einstellungsmöglichkeit für Twofish-Schlüssellänge

(ID n/a)

Bei der Konfiguration eines IKE- oder IPSec-Proposals fehlte die Möglichkeit, für die Verwendung von Twofish eine Schlüsselänge anzugeben.

Mit **Systemsoftware 7.8.7** ist die Verwendung von 128. 192 und 256 Bit langen Schlüsseln möglich. Nach einer Aktualisierung der Software wird die IPSec-Konfiguration nicht automatisch angepasst, da neue Proposals erstellt werden müssen. Bei einer Neukonfiguration ist die Unterstützung automatisch aktiviert.

4.70 IPSec - Tunnelaufbau

(ID 9004)

Wurde ein IPSec-Tunnel aufgrund eines lokal vom Gateway erzeugten Pakets aufgebaut, so wurde die Phase 2 des Tunnel mit der IP-Adresse des Quellinterfaces und einer 32bit-Netzmaske aufgebaut, anstatt mit den Werten des entsprechenden Subnetzes (z. B. 192.168.1.254/32 anstelle von 192.168.1.0/24). Dadurch konnte es zu Fehlern im Tunnelaufbau vor allem mit Open-Source-IPSec-Lösungen kommen.

Das Problem ist gelöst worden

4.71 IPSec - Irrelevante Menüs angezeigt

(ID 10077)

Im Setup Tool wurden die Menüs für Pre und Post IPSec Rules auch bei einer rein Interface-basierten Konfiguration angezeigt. Eine Konfiguration in diesen Menüs konnte zu unerwarteten Ergebnissen führen.

Das Problem ist gelöst worden.

4.72 IPSec - fehlerhafte Eingabemaske für Feld Block Time

(ID 11840)

Im Setup Tool Menü ***IPSec*** ➜ ***IKE (Phase 1)*** ➜ **Edit** ➜ **ADD** konnte im Feld ***Block Time*** maximal ein vierstelliger Wert eingegeben werden, obwohl der Wertebereich für dieses Feld *-1* bis *86400* beträgt.

Das Problem ist gelöst worden.

4.73 IPSec - Doppelte OSPF Interfaces

(ID 9171)

Bei IPSec mit RADIUS konnte es vorkommen, dass nach einem RADIUS Reload OSPF Interfaces doppelt vorhanden waren.

Das Problem ist gelöst worden.

4.74 IPSec / OSPF - Ungewolltes OSPF Update

(ID 10371)

Kam es während einer IPSec-Verbindung zur Neuaushandlung der Schlüssel, so wurde ungewollt ein OSPF Update ausgelöst. Je nach Konfiguration konnte es dabei zu einer Unterbrechung des Tunnels kommen.

Das Problem ist gelöst worden.

4.75 OSPF - Authentication Type

(ID 2843)

OSPF funktionierte nicht, wenn ***AUTHENTICATION TYPE*** = *md5*.

Das Problem ist gelöst worden.

4.76 OSPF

(ID 7724)

Wenn OSPF auf dem Interface *1000* aktiv war, wurde nur eine LAN Route über Interface *1400* auf dem Interface *1000* propagiert.

Das Problem ist gelöst worden.

4.77 DynVPN Callback via Voice Call fehlgeschlagen

(ID 7578)

Beim Versuch ein DynVPN über einen Voice Call zu initialisieren, erhielten Sie die Meldung "Requested L1 ressources not available".

Das Problem ist gelöst worden.

4.78 X.25-Verbindung fehlgeschlagen

(ID 7960)

Zwischen einem CISCO Gerät und einem bintec Gerät konnte über die X.21-Schnittstellen keine Verbindung hergestellt werden.

Das Problem ist gelöst worden.

4.79 X.25 - Erneute LLC-Verbindung fehlgeschlagen

(ID 3881)

Wenn eine unterbrochene LLC-Verbindung erneut aufgebaut werden sollte, schlug dies fehl.

Das Problem ist gelöst worden.

4.80 SNMP - MIB-Suchoperationen fehlgeschlagen

(ID 4767)

Suchoperationen innerhalb der MIB konnten fehlschlagen.

Das Problem ist gelöst worden.

4.81 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.

4.82 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.

4.83 SNMP Shell - ifoperstatus falsch angezeigt

(ID 4751)

Schnittstellen mit Extended Routes wurden durch `ifoperstatus` mit einem falschen Status angezeigt.

Das Problem ist gelöst worden.

4.84 SNMP Shell - Kommandos nicht richtig ausgeführt

(ID 11448)

Auf der Shell kam es bei Batch-Kommandos dann zu einer Fehlfunktion, wenn ein von der Shell als "extern" interpretiertes Kommando enthalten war.

Das Problem ist gelöst worden.

4.85 Dynamic Bandwidth Control

(ID 7699)

Bei ipoa Schnittstellen funktionierte die bandbreitenabhängige Berechnung der Datenpaketgröße der Funktion Dynamic Bandwidth Control nicht.

Das Problem ist gelöst worden.

4.86 ICMP_TIMESTAMP Messages - Format geändert

(ID n/a)

Wegen eines Fehlers in der Firmware einiger Mitbewerber wurde das Format von ICMP_TIMESTAMP und ICMP_TIMESTAMP_REPLY Messages erweitert.

Jetzt können Funkwerk Geräte mit erweiterten ICMP_TIMESTAMP und ICMP_TIMESTAMP_REPLY Messages "umgehen".

4.87 QoS - Wert für Feld Direction nicht gesetzt

(ID 3656)

Im Menü ***QoS*** ➜ ***IP Classification and Signaling*** ➜ ***ADD/EDIT*** konnte zwar im Feld ***Direction*** ein Wert gewählt werden, er wurde jedoch mit **SAVE** nicht gespeichert und erschien danach nicht in der Liste der Klassifizierungs- und Signalisierungsregeln.

Das Problem ist gelöst worden.

4.88 QoS - High Priority wirkungslos

(ID 11304)

Im Zusammenspiel mit bestimmten SIF-Regeln konnte es dazu kommen, dass eine High Priority Queue nicht entsprechend berücksichtigt wurde.

Das Problem ist gelöst worden.

4.89 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.

4.90 IP Load Balancing - Unvollständige Anzeige der Port Bereiche

(ID 8370)

Wenn im Menü ***IP*** ➜ ***Bandwidth Management (TDRC / Load Balancing / BOD)*** ➜ ***IP Load Balancing over Multiple Interfaces*** ➜ **ADD/EDIT** das Feld ***Distribution Policy*** = *service/source-based routing* gesetzt und für das Feld ***Interface*** ein Wert gewählt war, im Untermenü ***IP Routing List*** beispielsweise das Feld ***Service*** = *client_1* gesetzt war, wurde jeweils nur der erste Wert des entsprechenden Portbereichs angezeigt.

Das Problem ist gelöst worden, die Portbereiche werden vollständig angezeigt.

4.91 VoIP - Registrierung bei 1und1 fehlgeschlagen

(ID 5621)

Mit dem VoIP Telefon snom 190 schlug die Registrierung beim Provider 1und1 fehl.

Das Problem ist gelöst worden.

4.92 Syslog Meldungen mit folgenden Nullen

(ID 8146)

Syslog Meldungen wurden mit nachfolgenden Nullen gesendet.

Das Problem ist gelöst worden.

4.93 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.

4.94 Inkonsistente MIB-Variablen

(ID 7839)

Wenn eine Konfiguration über tftp get geladen wurde, entstanden inkonsistente MIB-Variablen.

Das Problem ist gelöst worden.

4.95 IGMP - Cache-Einträge nicht entfernt

(ID 11356)

Die Cache-Einträge des IGMP Proxys wurden nicht wie vorgesehen gelöscht.

Das Problem ist gelöst worden.

4.96 Ethernet - MAC-Adresse ignoriert

(ID 11245)

Wurde ein Ethernet Interface von "DHCP" auf "Manuell" umgestellt, so wurde eine ggf. spezifizierte MAC-Adresse ignoriert und statt dessen die MAC-Adresse des Ethernet-Chips verwendet.

Das Problem ist gelöst worden.

4.97 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.

4.98 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*.

4.99 Cert - Keine Unterstützung negativer Indices

(ID 11285)

Das `cert`-Tool der SNMP Shell unterstütze keine Zertifikate mit einem negativen Index und ohne Description. Bestimmte Zertifikate werden aber in dieser Form abgespeichert, konnten dann aber nicht manuell gelöscht werden.

Das Problem ist gelöst worden.

4.100 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.

4.101 Kompatibilitätsprobleme mit Konvertern

(ID 10878)

Mit einigen G.703-Konvertern traten an X.21-Schnittstellen Probleme auf.

Die Probleme sind gelöst worden.

4.102 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.

4.103 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.

4.104 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.

4.105 Einträge gelöscht

(ID 10105)

Wenn ein Eintrag für ***ipExtRtTable*** auf der SNMP Shell vorgenommen wurde, wurde dieser bei der nächsten Änderung des entsprechenden Interfaces im Setup-Tool-Menü ***Basic IP Settings*** wieder gelöscht.

Das Problem ist gelöst worden.