RELEASE NOTES SYSTEMSOFTWARE 7.2.1

Release Notes - Systemsoftware 7.2.1
Version 0.9

Ziel und Zweck

Dieses Dokument beschreibt neue Funktionen, Änderungen und behobene Fehler in **Systemsoftware 7.2.1**.

Haftung

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

Die Informationen in diesem Dokument können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Änderungen finden Sie unter www.bintec.de.

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.bintec.de.

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

Bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
France

Telephone: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Wichtige Informationen

Bitte lesen Sie die folgenden Informationen zu Systemsoftware 7.2.1 aufmerksam, um Probleme beim Update oder bei der Verwendung der Software zu vermeiden.

1.1 Gültigkeit

Folgende Geräte werden von **Systemsoftware 7.2.1** unterstützt:

- **Bingo DSL II**
- **X1000 II**
- **X1200 II**
- **X2100**
- **X2250**
- **X2300**
- **X2500**
- **X2400**
- **X4x00**
- **X8500**
- **VPN line.**

1.2 Funktionsumfang

X.25 und H.323 sind für folgende Geräte aus dem Funktionsumfang der IPSec-Versionen entfernt worden:

- **X1000 II**
- **X1200 II**

- **X2100**
- **X2300**
- **X2400**
- **X2500**
- **X4x00.**

1.3 Update-Probleme

Aufgrund von Änderungen in **Systemsoftware 7.2.1** wird unter Umständen die Konfiguration des Event Schedulers durch das Update verändert.

Hinweis

Wenn Sie den Event Scheduler nicht verwenden oder die Konfiguration Ihres Event Schedulers keine Zeitbedingungen enthält, treffen die folgenden Informationen nicht auf Ihren Update-Vorgang zu.

Unter zwei Bedingungen müssen Sie die Event-Scheduler-Konfiguration von **Systemsoftware 7.2.1** nach dem Update manuell anpassen:

Sie haben die Bedingung "daily" verwendet und wollen eine Konfiguration z. B. per TFTP laden

Wenn ein von Ihnen konfigurierter Event auf der Bedingung *daily* beruht (***CONDITION*** = *daily*, zuvor als *dayly* falsch geschrieben), so wird das Update korrekt durchgeführt. Wenn Sie jedoch eine zuvor gesicherte Konfiguration per TFTP wieder einspielen wollen, so schlägt der Download der Konfiguration fehl. Wenn es unumgänglich ist, eine Konfiguration per TFTP zu laden, öffnen Sie die Konfigurationsdatei mit einem Texeditor und ersetzen Sie alle Vorkommen von "dayly" durch "daily". Die Konfiguration sollte sich nun laden lassen.

Sie verwenden eine andere Zeitbedingung und wollen Systemsoftware 7.2.1 mit der auf dem Gateway gesicherten Konfiguration betreiben

Für bestimmte zeitbasierte Events wird ein Update die Konfiguration wie folgt ändern:

ursprünglicher Wert	geänderter Wert
sat-sun	mon_sat
day1	sat_sun
day2	day1
day3	day2
...	...
day31	day30

Konfigurationen auf Basis einzelner Wochentage werden nicht verändert.

Die Veränderung findet lediglich während des Updates der Systemsoftware statt, d. h. wenn Sie die Konfiguration auf einem TFTP-Server gesichert haben und per TFTP Download zurückspielen, werden die Werte korrekt in die MIB übertragen.

1 Wichtige Informationen

2 Neue Funktionen

Systemsoftware 7.2.1 enthält eine Reihe neuer Funktionen, die den Leistungsumfang gegenüber Systemsoftware 7.1.12 erheblich erweitern:

2.1 PKCS#12-Unterstützung

Systemsoftware 7.2.1 unterstützt den Import von PKCS#12-Zertifikaten für das IPSec-Zertifikatsmanagement. PKCS#12-Zertifikate können nun sowohl über die `cert`-Applikation als auch über das Setup Tool importiert werden.

PKCS#12 unterstützt die Übertragung persönlicher Identifikationsdaten wie privater Schlüssel und Zertifikate in einer Reihe von Sicherheitsmechanismen (PKI und Passwortschutz). **Systemsoftware 7.2.1** unterstützt die zur initialen Konfiguration sinnvollen Passwort-Mechanismen. Der Import eines PKCS#12-Zertifikats erfolgt auf die gleiche Art und Weise wie die eines anderen Zertifikats, d. h. es kann entweder von einem TFTP-Server heruntergeladen oder per Copy/Paste in das Setup Tool oder die Konsole kopiert werden. In beiden Fällen werden die zum Entschlüsseln des Zertifikats benötigten Passwörter interaktiv abgefragt (`cert` stellt eine Option zur direkten Übergabe eines Passwortes zur Verfügung).

2.1.1 Import über das Setup Tool

Der Import über das Setup Tool erfolgt im Menü zum Download eines Zertifikates, also ***IPSec ➜ Certificate and Key Management ➜ Own/CA/Peer Certificate ➜ DOWNLOAD***:

```
BINTEC X2300s Setup Tool        Funkwerk Enterprise Communications GmbH
[IPSEC][CERTMGMT][OWN][GETCERT]: IPsec Configuration -
                              Get Certificate        MyGateway

   Import a Certificate/CRL using:  TFTP

      Type of certificate: Own Certificate



    Server:
    Name:                                              auto
            START                                    EXIT
```

Hinweis

Der Vorgang des Imports ist im Benutzerhandbuch Ihres Gateways beschrieben. Sie können das Zertifikat entweder von einem TFTP-Server laden oder es per Copy/Paste in das entsprechende Menüfenster kopieren.

Wenn das Gateway ein passwortgesichertes PKCS#12-Zertifikat erkennt, fragt es die notwendigen Passwörter interaktiv ab:

```
BINTEC X2300s Setup Tool        Funkwerk Enterprise Communications GmbH
[IPSEC][CERTMGMT][OWN][GETCERT]: IPsec Configuration -
                              Get Certificate        MyGateway

 Please Review retrieved Certificate:   [mycert]

 Encountered PKCS#12 password authenticated envelope



 please enter password for outer envelope       __________
```

Nacheinander fragt das Gateway die im Zertifikat enthaltenen Schlüssel ab (Outer Envelope, Internal Safe und Shrouded Key - es bleibt das jeweils zuletzt eingegebene Passwort stehen, so dass Sie es nur einmal eingeben müssen, sofern alle Passwörter indentisch sind).

Danach wird das Zertifikat zur Kontrolle im Klartext angezeigt:

```
BINTEC X2300s Setup Tool        Funkwerk Enterprise Communications GmbH
[IPSEC][CERTMGMT][OWN][GETCERT]: IPsec Configuration -
                                Get Certificate        MyGateway

Please Review retrieved Certificate:   [mycert]

Encountered PKCS#12 password authenticated envelope                    =
Certificate =                                                          |
 SerialNumber = 1                                                      |
 SubjectName = <CN=certtest, OU=no_dept., O=FEC GmbH, C=DE>            |
 IssuerName = <MAILTO=noob@fec.com, CN=Openssl Test-CA OU=no_dept      |
   O=FEC GmbH, L=Nuernberg, ST=Bayern, C=DE>                           |
 Validity =                                                            |
    NotBefore = 2004 Oct  5th, 08:07:36 GMT                            |
    NotAfter  = 2005 Oct  5th, 08:07:36 GMT                            |
 PublicKeyInfo =                                                       |
   Algorithm name (X.509) : rsaEncryptionv                             v

                 IMPORT
```

Durch Bestätigen mit ***IMPORT*** wird das Zertifikat installiert und Sie gelangen zurück in das Menü zur Eingabe bzw. zum Download des Zertifikats. Dieses können Sie nun mit ***EXIT*** verlassen und gelangen dann zur Übersicht der installierten Zertifikate.

2.1.2 Import mittels "cert"

Die Applikation `cert`, die von auf der SNMP Shell aufgerufen wird, wurde ebenfalls erweitert, um PKCS#12-Zertifikate zu unterstützen. PKCS#12-Zertifikate werden automatisch erkannt, ggf. enthaltene Passwörter werden interaktiv abgefragt.

Der Import erfolgt folgendermaßen (per Copy/Paste importiertes Zertifikats):

```
X2300:> cert get -p console test
Please enter certificate data:>

<Die SNMP Shell zeigt die kodierten Zertifikatsdaten an>

cert: Encountered PKCS#12 password authenticated envelope

please enter password for outer envelope (empty password cancels) >
please enter password for internal safe (empty password cancels) >
please enter password for shrouded key (empty password cancels) >
Received 2 certificate(s) 1 key(s). Accept all? (y/n) > y

X2300:>
```

Der Import per TFTP-Download erfolgt folgendermaßen:

```
X2300:> cert get -p tftp://<Server IP Adresse>/1.pem test
cert: Encountered PKCS#12 password authenticated envelope

please enter password for outer envelope (empty password cancels) >
please enter password for internal safe (empty password cancels) >
please enter password for shrouded key (empty password cancels) >
Received 2 certificate(s) 1 key(s). Accept all? (y/n) > y

X2300:>
```

Mittels der Option `-P <Passwort>` kann bereits bei der Eingabe des Befehls ein Passwort an die Applikation übergeben werden. Dieses wird allerdings auf alle Schlüssel angewendet, so dass die Option nur bei indentischen Passwörtern für Outer Envelope, Internal Safe und Shrouded Key sinnvoll ist.

2.2 TCP-Download-Kontrolle

Eine zunehmende Anzahl von Netzwerkdiensten erfordert es, dass Daten nicht nur so schnell wie möglich, sondern auch mit konstanter Transferrate ausgetauscht werden können (so z. B. VoIP). Systemsoftware 7.2.1 verfügt über einen Mechanismus, mit dem entsprechende Probleme vor allem bei ADSL-Verbindungen umgangen werden können.

Grundsätzlich kann man auf zwei Wegen sicherstellen, dass Datenströme, die eine geringe Latenz erfordern, nicht behindert werden: Zum einen ist es möglich, die allgemein zur Verfügung gestellte Downloadrate für TCP-Verbindungen herabzusetzen, so dass eine gesicherte Bandbreite für die Daten einer High Priority QoS Queue zur Verfügung steht. Zum anderen ist es möglich, die

zur Verfügung stehende Bandbreite optimal auszunutzen, indem man den Upload von TCP-ACK-Paketen im Upstream asynchroner DSL-Verbindungen bevorzugt. Dies stellt sicher, dass keine Verzögerungen aufgrund der geringen Upload-Bandbreite von ADSL-Verbindungen auftreten.

Beide Mechanismen lassen sich im Menü ***IP ➜ BANDWIDTH MANAGEMENT (TDRC / LOAD BALANCING / BOD) ➜ TCP DOWNLOAD RATE CONTROL (TDRC)*** konfigurieren. Mit ***ADD/EDIT*** gelangen Sie in das Menü zur Konfiguration (der Screenshot zeigt nicht die Defaultwerte):

```
BINTEC X2300s Setup Tool        Funkwerk Enterprise Communications GmbH
[IP][TDRC][EDIT]: Configure TCP Download Rate Control        MyGateway

  Interface              50000   ethoa50-0

  Optimize Download Rate via TCP ACK prioritisation      no
  (recommended for ADSL)

  TDRC Mode      disabled

  Maximum TCP Download Rate (kbits/s)          1024

  Control all TCP Services                     no
  Select TCP Services >

         SAVE                                CANCEL
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Interface	Hier wählen Sie aus, auf welches Interface die Konfiguration angewendet werden soll.
Optimize Download Rate via TCP ACK prioritisation	Hier wählen Sie aus, ob die Downloadrate optimiert werden soll, indem TCP-ACK-Pakete im Upstream bevorzugt behandelt werden. Wenn Sie hier *yes* wählen, werden die folgenden Felder nicht mehr angezeigt. Mögliche Werte sind *yes*, und *no*, Defaultwert ist *no*.

Feld	Bedeutung
TDRC Mode	Nur wenn ***Optimize Download Rate via TCP ACK prioritisation*** = *no*. Hier wählen Sie den Mechanismus der TDRC (TCP Download Rate Control), mögliche Werte sind: ■ *static (fixed maximum rate for TCP download)* (Defaultwert) - Die Dowload-Rate für TCP-Verbindungen wird statisch auf den in ***Maximum TCP Download Rate (kbits/s)*** definierten Wert begrenzt. ■ *dynamic (maximum rate less amount of high priority traffic)* - Die Download-Rate wird auf einen dynamisch errechneten Wert begrenzt. Dieser errechnet sich aus dem in ***Maximum TCP Download Rate (kbits/s)*** definierten Wert, von dem die Bandbreite abgezogen wird, die aktuell im Moment des Dazukommens oder Wegfallens einer TCP-Verbindung für den QoS-High-Priority-Verkehr auf diesem Interface benötigt wird. Diese Einstellung setzt eine QoS-Konfiguration für das ausgewählte Interface voraus. ■ *disabled* - Die TCP Download Rate wird nicht begrenzt.
Maximum TCP Download Rate (kbits/s)	Hier geben Sie die maximale Bandbreite für TCP-Download-Verbindungen an. Mögliche Werte sind *1* bis *100000*, der Defaultwert ist *1024*.

Feld	Bedeutung
Control all TCP Services	Hier wählen Sie aus, ob die eingestellte Download-Kontrolle auf alle TCP-Verbindungen angewendet werden soll. Mögliche Werte sind *yes*, und *no*, Defaultwert ist *yes*.

Tabelle 2-1: ***IP ➜ BANDWIDTH MANAGEMENT (TDRC / LOAD BALANCING / BOD) ➜ TCP DOWNLOAD RATE CONTROL (TDRC) ➜ ADD/EDIT***

Wenn Sie für ***CONTROL ALL TCP SERVICES*** *no* ausgewählt haben, gelangen Sie über ***SELECT TCP SERVICES*** zur Konfiguration derjenigen Dienste, die der TDRC unterworfen werden sollen (der Screenshot zeigt die Voreingestellten Dienste):

```
BINTEC X2300s Setup Tool        Funkwerk Enterprise Communications GmbH
[IP][TDRC][SERVICES]: Configure TCP Services          MyGateway

 TCP Port                                  Status

    80              HTTP                    builtin
    443             HTTPS                   builtin
    20              FTP Data                builtin
    110             POP3                    builtin
    143             IMAP2                   builtin



     ADD                DELETE               EXIT
```

Mit ***ADD*** gelangen Sie zur Konfiguration weiterer Dienste:

```
BINTEC X2300s Setup Tool        Funkwerk Enterprise Communications GmbH
[IP][TDRC][SERVICES][ADD]: Configure TCP Services          MyGateway

     TCP Service Port              1
     Status                        enabled
     Alias Name (Description)


           SAVE                                    CANCEL
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
TCP Service Port	Hier geben Sie den TCP-Port des entsprechenden Dienstes ein. Mögliche Werte sind *1* bis *65535*, der Defaultwert ist *1*.
Status	Hier wählen Sie aus, ob der konfigurierte Dienst tatsächlich kontrolliert werden soll. Mögliche Werte sind *enabled* und *disabled*, Defaultwert ist *enabled*.
Alias Name (Description)	Hier geben Sie eine beliebige Beschreibung für den Dienst ein, die maximale Länge der Eingabe ist 20 Zeichen.

Tabelle 2-2: ***IP ➜ BANDWIDTH MANAGEMENT (TDRC / LOAD BALANCING / BOD) ➜ TCP DOWNLOAD RATE CONTROL (TDRC) ➜ ADD/EDIT ➜ SELECT TCP SERVICES ➜ ADD***

2.3 Trennung von Switch Ports

Systemsoftware 7.2.1 bietet die Möglichkeit, die vier Switch Ports von X2300s und X2300is logisch voneinander zu trennen und wie vier eigenständige Ethernet Interfaces zu konfigurieren.

Die Trennung der Switch Ports voneinander erlaubt eine jeweils vollständig eigenständige Konfiguration der entstandenen Interfaces. Die Konfigurationsoptionen sind dabei mit denen identisch, die auch zur Konfiguration eines einzelnen Ethernet-Interfaces zur Verfügung stehen (Informationen zur Ethernet-Konfiguration finden Sie in Ihrem Benutzerhandbuch).

Hinweis

Diese Funktion steht nur für Geräte ab einer bestimmten Seriennummer zur Verfügung:

X2300is: alle Geräte ab Seriennummer X2Y25...

X2300s: alle Geräte ab Seriennummer X2Z25...

Das Ethernet-Menü wurde den neuen Funktionen entsprechend angepasst:

```
BINTEC X2300s Setup Tool        Funkwerk Enterprise Communications GmbH
[SWITCH]: Fast Ethernet Configuration                          MyGateway

    Fast Ethernet/en1-0>


    Switch Configuration >


              EXIT
```

Nach dem Update auf **Systemsoftware 7.2.1** ist der Switch noch immer im Single-Interface-Modus. d. h. für alle Switch Ports gilt die gleiche Konfiguration.

Hinweis

Beachten Sie, dass die Konfiguration des Interface ***MODE*** nicht mehr im Menü zur Konfiguration des Interfaces stattfindet, sondern im Menü ***SWITCH CONFIGURATION***.

Sie können die Konfiguration des Switches im Menü ***SWITCH CONFIGURATION*** ändern:

```
BINTEC X2300s Setup Tool        Funkwerk Enterprise Communications GmbH
[SWITCH][ASSIGN]: Switch Interface Assigment                    MyGateway

     Switch Port    Assigned Interface   Switch Port Mode

     Port 1         en1-0                full autonegotiation
     Port 2         en1-0                full autonegotiation
     Port 3         en1-0                full autonegotiation
     Port 4         en1-0                full autonegotiation




                    SAVE                      CANCEL
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Switch Port	Hier wird der jeweilige Switch-Port angezeigt. Die Numerierung entspricht der der Ports auf der Rückseite des Gateways.
Assigned Interface	Hier können Sie dem Switch Port ein Ethernet Interface zuordnen. Zur Auswahl stehen vier Interfaces, *en1-0* bis *en1-3*. In der Grundeinstellung ist allen Switch Ports das Interface *en1-0* zugeordnet. Die vor dem Update auf **Systemsoftware 7.2.1** vorhandene Ethernet-Konfiguration wird auf das Interface mit der Bezeichnung *en1-0* übertragen. Wenn Sie kein solches Interface erstellen, wird die Konfiguration nicht übernommen.

Feld	Bedeutung
Switch Port Mode	Hier wählen Sie den Modus aus, in dem das Interface betrieben werden soll. Mögliche Werte sind: ■ *full autonegotiation* (Defaultwert) ■ *auto 100 mbps only* ■ *auto 10 mbps only* ■ *auto 100 mbps/full duplex* ■ *auto 100 mbps/half duplex* ■ *auto 10 mbps/full duplex* ■ *auto 10 mbps/half duplex* ■ *fixed 100 mbps/full duplex* ■ *fixed 100 mbps/half duplex* ■ *fixed 10 mbps/full duplex* ■ *fixed 10 mbps/half duplex* ■ *suspend* - Das Interface wird auf *disabled* gesetzt und von der Stromversorgung ausgenommen. ■ *disabled* - Das Interface wird angelegt, bleibt aber inaktiv.

Tabelle 2-3: ***XEY-100SW, FAST ETHERNET → SWITCH CONFIGURATION***

Nach der Konfiguration des Switches, ändert sich das Menü ***XEY-100SW, FAST ETHERNET*** und zeigt die soeben zugewiesenen Ethernet Interfaces an. Sie könne nun jedes Interface einzeln konfigurieren.

Bei der Konfiguration sollten Sie Folgendes beachten: Die Aufteilung des Switches in mehrere Ethernet Interfaces ist eine logische, d. h. die maximal Bandbreite, die über alle Switch Ports oder Ethernet Interfaces zur Verfügung steht bleibt in der Summe unverändert (100 Mbit/s Full Duplex). Wenn Sie also z. B.

alle Switch Ports voneinander trennen, verfügt jedes der entstehenden Interfaces nur über einen Teil der vollen Bandbreite.

Wenn Sie mehrere der Switch Ports zu einem Interface zusammenfassen, so besteht zwischen den Ports dieses Interfaces die volle Bandbreite von 100 Mbit/s Full Duplex.

2.4 Neue HTML-Wizard-Funktionen

Der Bintec-HTML-Wizard zur Gatewaykonfiguration verfügt über eine Reihe neuer Funktionen, die auch komplexere Konfigurationsaufgaben wie die Konfiguration der Firewall über den Wizard erlauben.

Folgende Funktionen sind hinzugeführt worden:

- Konfiguration der Stateful Inspection Firewall (im Advanced-Modus)
- Konfiguration mehrerer LAN-LAN-Verbindungen
- Country Profiles zur Voreinstellung häufig verwendeter ISPs bei der Internet-Konfiguration.

Eine ausführliche Online-Hilfe informiert Sie bei der Konfiguration über die notwendigen Einstellungen.

2.5 Cisco LMI

Mit Systemsoftware 7.2.1 ist Cisco LMI für Frame Relay verfügbar.

Im Menü ***FR*** ➜ ***LINK CONFIGURATION*** ➜ ***ADD/EDIT*** kann für ***LINE MANAGEMENT*** nun der Wert *original_lmi* ausgewählt werden.

2.6 Neue Trace-Tool-Funktionen

Systemsoftware 7.2.1 stellt eine neue Filtermöglichkeit sowie Unterstützung von X.25-over-ISDN-Interfaces zur Verfügung.

Die Trace-Applikation ist um die Möglichkeit erweitert worden, den Verkehr von und zu bzw. zwischen bestimmten IP-Adressen im LAN aufzuzeichnen. Dazu wurden folgende Optionen eingeführt:

```
-S      set source IP address filter (LAN only)
-U      set destination IP address filter (LAN only)
-Ba,b   filter IP packets between a and b (LAN only)
```

Darüber hinaus lassen sich nun auch X.25-over-ISDN-Interfaces (Interface-Indices 27000 bis 29999) tracen.

2.7 Konfigurierbare IP-Accounting-Meldungen

Systemsoftware 7.2.1 stellt eine Möglichkeit zur Verfügung, die Syslog-Meldungen des IP Accountings den eigenen Bedürfnissen anzupassen.

Mittels der Variablen ***biboAdmAcctlogFormat*** ist es möglich, folgende Informationen nach Belieben zusammen zu stellen:

```
%d      Date the session opened; in DD.MM.YY format.
%t      Time the session opened: in HH:MM:SS format
%a      session age in seconds
%c      protocol type
%i      source IP address
%r      source port
%f      source interface index
%I      destination IP address
%R      destination port
%F      destination interface index
%p      outgoing packets
%o      outgoing octets
%P      incoming packets
%O      incoming octets
%s      message sequence counter
%%      '%'
```

Das gewünschte Format kann mit dem Befehl

```
biboAdmAcctlogFormat="<fmt>"
```

gefolgt von

```
cmd=save
```

konfiguriert werden.

3 Änderungen

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

3.1 QoS - Monitoring-Menü

Systemsoftware 7.2.1 führt ein Menü zur Überwachung von QoS-Funktionen ein.

Im Menü ***MONITORING AND DEBUGGING*** ➜ ***IP QOS*** werden QoS-spezifische statistische Information für Interfaces angezeigt, für die Quality of Service konfiguriert wurde. Die Werte können nicht verändert werden.

```
X2300s Setup Tool                          Bintec Access Networks GmbH
[MONITOR][IP QOS]: IP QoS Interface Monitoring                MyGateway

  Interface                          en1-0
  Operational Status                 up

  Nominal Transmit Rate              2048000
  Maximum Transmit Rate              192000

  Received Packets                   1075
  Received Octets                    66650

  Transmit Packets                   2334382
  Transmit Octets                    144731684

  QoS Policy Statistics >


  EXIT
```

Folgende Werte werden angezeigt:

Feld	Wert
Interface	Auswahl des Interfaces, für das QoS konfiguriert wurde und dessen QoS-Statistik angezeigt werden soll.
Operational Status	Zeigt den Betriebszustand des gewählten Interfaces an.
Nominal Transmit Rate	Die maximale Gesamtdatenübertragungsrate in Bits pro Sekunde.
Maximum Transmit Rate	Die für dieses Interface spezifizierte maximale Datenrate in Bits pro Sekunde in Senderichtung (siehe Benutzerhandbuchkapitel **QoS** im Untermenü ***Interfaces and Policies*** ➜ *<Interface>* ➜ ***QoS Scheduling and Shaping***)
Received Packets	Die Anzahl der über das ausgewählte Interface empfangenen Pakete seit dem letzten Wechsel in den *up*-Status.

Feld	Wert
Received Octets	Die Anzahl der über das ausgewählte Interface empfangenen Oktetts seit dem letzten Wechsel in den *up*-Status.
Transmit Packets	Die Anzahl der über das ausgewählte Interface gesendeten Pakete seit dem letzten Wechsel in den *up*-Status.
Transmit Octets	Die Anzahl der über das ausgewählte Interface gesendeten Oktetts seit dem letzten Wechsel in den *up*-Status.

Tabelle 3-1: Felder im Menü ***IP QoS***

3.1.1 Untermenü QoS Policy Statistics

Im Folgenden wird das Untermenü *QoS Policy Statistics* beschrieben.

Standardmäßig wird bei Aufruf des Menüs ***Monitoring and Debugging*** ➜ ***QoS Policy Statistics*** eine Übersicht über die Verteilung der gesamten Bandbreite in Form eines Balkendiagramms angezeigt.

```
X2300s Setup Tool                          Bintec Access Networks GmbH
[MONITOR][IP QOS][STATISTICS]: QoS Bandwidth                  MyGateway
                               Distribution (en1-0)

load          ::: agreed      XXX agreed but bounded     *** overbooked
  ^
  |       42        41   19
  + 100
  |
  |
  |
  |
  |       :::       ***
  |       :::       ***
  |       :::       ***
  |       :::       ***  ***
  |       :::       XXX  XXX
  +-------------------------------------------------------------->
HP   1    2    3    DEF                          classes

  EXIT


 (d)istribution   (c)lasses   (t)os   (i)nterface statistics
```

Das Diagramm zeigt den prozentualen Anteil der einzelnen konfigurierten QoS-Paket-Klassen an der genutzten Gesamtbandbreite. Die Balken enthalten die Bandbreitenverteilung der QoS-Paket-Klassen.

Die grafisch unterschiedliche Darstellung der Balken hat folgende Bedeutung:

- *agreed*: Anteil der Pakete innerhalb der für diese QoS-Paket-Klasse garantierten Bandbreite.
- *agreed but bounded*: Anteil der Pakete innerhalb der für diese QoS-Paket-Klasse maximal garantierten Bandbreite.
- *overbooked*: Überbuchung der garantierten (not bounded) bzw. maximalen (bounded) Bandbreite. Diese Überbuchung ist nur zulässig im "not bounded"-Modus.

Weiterhin können detaillierte statistische Werte angezeigt werden. Die Anzeige können Sie wie in der Hilfezeile beschrieben mit folgenden Befehlen wechseln:

- *c* = Classes: Klassenbezogene Anzeige der statistischen Werte
- *t* = TOS: TOS-bezogene Anzeige der statistischen Werte

- *i* = Interface Statistics: Interface-bezogene Anzeige der statistischen Werte.

Mit der Schaltfläche **RESET STATISTICS** werden im jeweiligen Fenster sämtliche Werte auf *0* gesetzt.

CLASSES

```
X2300s Setup Tool                          Bintec Access Networks GmbH
[MONITOR][IP QOS][STATISTICS]: QoS Class                      MyGateway
                               Statistics (en1-0)

Class Pkts Send   Dropped Queued Octs Send    Dropped  Queued

DEF        0       0       0          0         0        0
N 1        0       0       0          0         0        0
N 2        167550  355049  22         6702000   19172646 880
N 3        292021  735122  405        11680840  39696588 16200
HP         1969580 0       13         78783200  0        520









  EXIT                    RESET STATISTICS

 (d)istribution      (c)lasses      (t)os      (i)nterface statistics
```

Folgende Werte werden angezeigt:

Feld	Wert
Class	Die ID der konfigurierten QoS-Paket-Klasse. Die Abkürzungen vor den Einträgen haben folgende Bedeutung: ■ N = normal ■ HP = High Priority ■ DEF = Default

Feld	Wert
Pkts	Anzahl der Pakete dieser QoS-Paket-Klasse: ■ *Send*: gesendete Pakete ■ *Dropped*: verworfene Pakete ■ *Queued*: Pakete in der Warteschlange
Octs	Anzahl der Oktetts dieser QoS-Paket-Klasse: ■ *Send*: gesendete Oktetts ■ *Dropped*: verworfene Oktetts ■ *Queued*: Oktetts in der Warteschlange

Tabelle 3-2: Felder im Menü ***QoS Policy Statistics → Classes***

TOS

```
X2300s Setup Tool                          Bintec Access Networks GmbH
[MONITOR][IP QOS][STATISTICS]: TOS Statistics                MyGateway
                               (en1-0)

TOS OutPkts OutOctets InPkts InOctets PktsDropped OctetsDropped

00    0       0        0       0          0           0
01    0       0        1135    68100      0           0

  EXIT                    RESET STATISTICS

 (d)istribution      (c)lasses      (t)os      (i)nterface statistics
```

Folgende Werte werden angezeigt:

Feld	Wert
TOS	Der Wert im TOS-Feldes des IP-Paketes

Feld	Wert
OutPkts	Anzahl der gesendeten Pakete mit dem unter TOS angegebenen Wert.
OutOctets	Anzahl der gesendeten Oktetts mit dem unter TOS angegebenen Wert.
InPkts	Anzahl der empfangenen Pakete mit dem unter TOS angegebenen Wert.
InOctets	Anzahl der empfangenen Oktetts mit dem unter TOS angegebenen Wert.
PktsDropped	Anzahl der verworfenen Pakete mit dem unter TOS angegebenen Wert.
OctetsDropped	Anzahl der verworfenen Oktetts mit dem unter TOS angegebenen Wert.

Tabelle 3-3: Felder im Menü ***QoS Policy Statistics ➜ TOS***

Interface Statistics

```
X2300s Setup Tool                          Bintec Access Networks GmbH
[MONITOR][IP QOS][STATISTICS]: QoS Interface                MyGateway
                               Statistics (en1-0)

  Transmit Packets  2469015
  Transmit Octets   98760600

  Queued Packets    417
  Queued Octets     16680

  Dropped Packets   1090901
  Dropped Octets    43636040




  EXIT                   RESET STATISTICS

 (d)istribution      (c)lasses      (t)os     (i)nterface statistics
```

Folgende Werte werden angezeigt:

Feld	Wert
Transmit Packets	Anzahl der über das ausgewählte Interface gesendeten Pakete.
Transmit Octets	Anzahl der über das ausgewählte Interface gesendeten Oktetts.
Queued Packets	Anzahl der Pakete in der Warteschlange des ausgewählten Interfaces.
Queued Octets	Anzahl der Oktetts in der Warteschlange des ausgewählten Interfaces.
Dropped Packets	Anzahl der an diesem Interface verworfenen Pakete.
Dropped Octets	Anzahl der an diesem Interface verworfenen Oktett.

Tabelle 3-4: Felder im Menü ***QoS Policy Statistics*** ➜ ***Interface Statistics***

3.2 Neue Option beim Setup-Tool-Start

Das Setup Tool kann unter **Systemsoftware 7.2.1** mit der Option `-I` gestartet werden. Diese Option startet das Setup Tool im Menü ***Monitoring and Debugging*** ➜ ***Interfaces*** und gestattet keinen Zugriff auf andere Menüs des Setup Tools.

3.3 Neuer DHCP-Parameter

Mittels der neuen MIB-Variablen ***ipDhcpUseDefaultHostname*** ist es möglich, festzulegen, ob das Gateway in einer DHCP Reply einen Standard-Host-Namen überträgt oder nicht. Ist für ***ipDhcpUseDefaultHostname*** *disabled* ausgewählt, wird kein Hostname übertragen, ist *enabled* ausgewählt, so wird ein vom

Gateway aus der IP-Adresse des Clients generierter Host-Name übertragen. Der Defaultwert ist *enabled*.

3.4 PPTP - Zusätzliche konfigurierbare Parameter

Folgende für PPTP-Kontrollverbindungen relevante Parameter können ab **Systemsoftware 7.2.1** in der ***PPTPPROFILETABLE*** auf der SNMP Shell konfiguriert werden. Einträge in dieser Tabelle sind optional, und so lange keine expliziten Werte vorgegeben werden, werden systeminterne Defaultwerte verwendet.

- ***HOST*** - Wird kein Wert für ***HOST*** angegeben, wir der Wert der Variablen ***SYSNAME*** aus der ***SYSTEMTABLE*** übertragen. Ansonsten wird der hier eingetragene Wert verwendet.
- ***VENDOR*** **-** Wird kein Wert für ***VENDOR*** angegeben, wird eine ID generiert, die sich aus "Bintec" und einem systeminternen Wert aus der ***BIBOADMBOARDTABLE*** zusammensetzt. Ansonsten wird der hier eingetragene Wert verwendet.
- ***FIRMREV*** - Für ***FIRMREV*** = *-1* wird die Firmware-Revision *0* übermittelt, für ***FIRMREV*** = *0* (also auch, wenn kein Eintrag vorgenommen wird) wird die der Systemsoftware entsprechende Revision angegeben. Für jeden anderen Wert (*1* bis *999*) wird genau der eingegebene Wert übermittelt.

3.5 IPSec - Konfigurierbarer Log Level

Mittels der Variable ***CERTGLOBLOGLEVEL*** lässt sich die Detailliertheit der das Zertifikatsmanagement betreffenden Syslog-Meldungen regeln:

Log-Level	Details in der Syslog-Meldung
3	wichtige Ereignisse wie ein ungültiges Zertifikat

Log-Level	Details in der Syslog-Meldung
4	erweiterte Hinweise zu den Ereignissen, die in Level 3 geloggt werden
5	Cache- und Search-Ereignisse
6	detaillierte Meldungen zu erfolgreichen Cache-Ereignissen
7	Ausgabe von Zertifikaten nach erfolgreichen Such-Ereignissen

Tabelle 3-5: Details des Zertifikatsmanagement-Syslogs

Meldungen des Level 3 (und darunter) werden auf dem globalen Syslog-Level *Info* ausgegeben, alle anderen auf dem Level *Debug*.

3.6 BRRP-over-VLAN

Wenn dem physikalischen Interface eines virtuellen Routers keine IP-Konfiguration zugeordnet war (wenn dies z. B. ausschließlich für Bridging verwendet werden sollte), war die Funktion BRRP over VLAN bisher nicht funktionsfähig, weil auf dem Interface keine BRRP Advertisements versendet werden konnten.

Um den Versand von BRRP-Advertisements auf einem anderen Interface zu ermöglichen, wurde ein neuer Parameter eingeführt: ***BRRP*** ➜ ***CONFIGURATION: ADVERTISEMENT INTERFACE***. Er ermöglicht die Auswahl desjenigen Interfaces, über das die BRRP Advertisements gesendet werden sollen.

3.7 NAT - Kontrolle der Session-Anzahl

Wenn die Anzahl der NAT-Sessions auf einem Interface zu groß wurde, konnte es bisher zu einem Reboot des Gateways kommen.

Systemsoftware 7.2.1 ermöglicht die Kontrolle über die maximale Anzahl von NAT-Sessions, die auf einem Interface zugelassen werden. Der Wert wird über

die Variable ***ipExtIfNatMaxSessions*** gesteuert. Wird die maximale Anzahl erreicht, versucht das Gateway zunächst, alte Sessions abzubauen. Gelingt das nicht, werden neue Sessions nicht zugelassen.

3.8 Keepalive Monitoring - Flexibler Default

Mit einer Standardeinstellung von lediglich drei Versuchen, einen Host über einen ICMP Echo Request zu erreichen, hat sich das Keepalive Monitoring als zu unflexibel herausgestellt. Die Anzahl der Versuche kann nun über die Variable ***ipHostsAliveTrials*** frei zwischen *1* und *65535* eingestellt werden.

3.9 BOOTP - CPU-Belastung gesenkt

Das BOOTP NetBIOS Relaying wurde so verändert, dass die CPU-Belastung durch den BOOTP-Service reduziert wird.

3 Änderungen

4 Behobene Fehler

Folgende Fehler sind in Systemsoftware 7.2.1 behoben worden:

4.1 Setup Tool - Änderungen trotz CANCEL

(ID 2211 und 3728)

Nachdem Änderungen im Menü ***WAN PARTNER*** mittels **CANCEL** oder **Esc Esc** verworfen worden waren, wurden diese bei einem späteren Sichern des WAN Partners dennoch durchgeführt und gesichert.

4.2 Factory Reset - Fehlfunktion

(ID 3068)

Das Zurücksetzen der Gateway-Konfiguration, indem man das Gerät drei bzw. fünf Mal aus- und wieder einschaltet, funktionierte nicht.

4.3 Setup Tool - "Individual Distribution Ratio" nicht konfigurierbar

(ID 3169)

Wenn man *individual for all interfaces of the group* für das Feld ***DISTRIBUTION RATIO*** im Menü ***IP LOAD BALANCING OVER MULTIPLE INTERFACES*** auswählte, wurden die für die Interfaces eingegebenen Werte nicht in allen Fällen korrekt übernommen.

4.4 DNS - Unerwünschte Namen im Cache

(ID 3364)

Gelegentlich wurde vom DNS Proxy nur der Fully Qualified Domain Name (FQDN, z. B. moon8.bintec.de) gespeichert, nicht aber der Canonical Name (CNAME, z. B. www.bintec.de).

4.5 Setup Tool - Cobion Filter nicht deaktiviert

(ID 3434)

Setzte man ***Security*** ➜ ***Cobion Organge Filter:Admin Status*** auf *disable*, nachdem der Filter zuvor einmal aktiviert worden war, so wurde dieser nicht vollständig deaktiviert und Websites weiterhin gemäß der Filterkonfiguration blockiert.

4.6 IPSec - Session Count falsch

(ID 3487)

Aktivierte man IP Load Balancing für IPSec-Verbindungen, wurden mehr Sessions gezählt als wirklich für die IPSec-Tunnel benötigt wurden.

4.7 RIP - TOS Signaling nicht möglich

(ID 3491)

Es war nicht möglich, das TOS-Feld von RIP-Paketen für das TOS Signaling anzupassen.

4.8 Bridging - Leistungsverlust

(ID 3525)

Bei einer ETHoA-Verbindung mit *bridged-fcs*- oder *bridged-no-fcs*-Encapsulierung sank die Leistung des Gateways kontinuierlich.

4.9 Setup Tool - Routing-Einträge korrupt

(ID 3576)

Wenn man im Menü ***IP*** ➜ ***ROUTING*** ➜ ***ADD/EDIT*** einen Routing-Eintrag mit einem Transitnetzwerk bearbeitete, wurde der Routen-Typ dennoch als *route without transit network* angezeigt. Bestätigte man dann die Änderung mit ***SAVE***, ging die Transitnetz-Konfiguration verloren.

4.10 Ethernet - Empfang großer Pakete fehlerhaft

(ID 3583)

Der Empfang von Ethernet-Paketen mit einer Größe von mehr als 1518 Bytes wurde nicht korrekt initialisiert und ausgeführt.

4.11 Bridging - Bridge-Filter nicht anwendbar

(ID 3584)

Der Bridge-Filtermechanismus arbeitete nicht zuverlässig, weil eine falsche Interpretation der Länge des konfigurierten Filters ein adäquates Matching verhinderte.

4.12 Setup Tool - Einträge nicht gespeichert

(IDs 3343 und 3605)

Wenn man in ***IP*** ➜ ***DNS*** ➜ ***FORWARDED DOMAINS*** ➜ ***ADD*** vorgenommene Änderungen bestätigte, wurden diese nicht in der MIB gespeichert. Gelegentlich wurde ein Stack Trace ausgegeben, aber das Gateway wurde nicht neu gestartet.

4.13 Setup Tool - Verwendung von „_“ nicht möglich

(ID 3619)

Wenn man in einem der DynDNS-Menüs einen Hostnamen eingab, so war die Verwendung von „_“ (Unterstrich) nicht möglich, obwohl es sich um ein für FQDNs akzeptables Zeichen handelt.

4.14 Setup Tool - Session-Abbruch

(ID 3661)

Beim Öffnen des Menüs ***MONITORING AND DEBUGGING*** ➜ ***MESSAGES*** wurde die Setup Tool Session beendet. Die Syslog-Meldungen konnten weiterhin auf der SNMP Shell ausgegeben werden.

4.15 ARP - Falscher ARP Tell

(ID 3671)

Wenn ein Gateway über mehrere Interfaces verfügte (z. B. ein physikalisches und ein virtuelles), konnte es zu falschen ARP Tells kommen, bei denen die IP-

Adresse des einen und die MAC-Adresse des anderen Interfaces verwendet wurde.

4.16 Setup Tool - Load-Balancing-Konfiguration falsch gesichert

(ID 3680)

Bei der Konfiguration von ***IP LOAD BALANCING OVER MULTIPLE INTERFACES*** mit ***DISTRIBUTION POLICY*** *service/source-based routing* wurden falsche Werte in die ***IPEXTRTTABLE*** geschrieben. Das konnte zu einer Fehlfunktion des Load Balancings führen.

4.17 SSHD - Verbindung nicht mehr möglich

(ID 3694)

Nach einer gewissen Zeit war eine Verbindung zum Gateway über SSH nicht mehr möglich. Dies konnte durch einen Speicherverlust auftreten oder nach einem Wechsel der IP-Adresse des Gateways.

4.18 PPPoE - Problem mit mehreren PPP Access Servern

(ID 3698)

Wenn ein Gateway so konfiguriert wurde, dass es zwei PPPoE Access Server nutzte, konnte der PPP Layer nicht aufgebaut werden.

4.19 Setup Tool - IPSec-Wizard-Einstellungen nicht korrekt gespeichert

(ID 3733)

Obwohl der Setup Tool IPSec Wizard während der Konfiguration einer Verbindung mit PSK zur Authentisierung nach einer ***LOCAL ID*** fragte, wurde diese nicht korrekt gespeichert. Wenn man die IPSec-Menüs öffnete, wurde der IPSec Wizard erneut gestartet.

4.20 PPPoE - Verbindungsaufbau erfolglos

(ID 3756)

Wegen eines zu kurzen Timeouts konnten bestimmte Arten von PPPoE-Verbindungen (z. B. Funkverbindungen) nicht hergestellt werden.

4.21 HTML Setup Tool - GO Button fehlt

(ID 3757)

Durchlief man den Setup Tool IPSec Wizard, so verschwand der ***GO***-Button zur Bestätigung der Einstellungen nach der Eingabe einer ***LOCAL ID***.

4.22 DynDNS - Reboot mit GnuDIP

(ID 3762)

Bei der Verwendung von DynDNS mit dem GnuDIP-HTML-Protokoll kam es zu einem Reboot des Gateways.

4.23 Setup Tool - Stack Trace in IP Menü

(ID 3774, 3793, 3794)

Setzte man in ***IP*** ➜ ***STATIC SETTINGS*** den ***REMOTE CAPI SERVER TCP PORT*** auf *0* und bestätigte mit ***SAVE***, so kam es zu einem Stack Trace, wenn man das Menü erneut öffnete und erneut mit ***SAVE*** bestätigte.

4.24 IPSec - Phase-1-Fehler

(ID 3800)

Die Phase-1-Authentisierung beim Aufbau eines IPSec-Tunnels scheiterte bei der Überprüfung einer Distinguished Name Peer ID.

4.25 ATM - Virtuelles Interface down

(ID 3829)

Erstellte man ein virtuelles PPPoE-Interface im Menü ***ATM*** ➜ ***ETHERNET OVER ATM*** ➜ ***ADD/EDIT*** ➜ ***IP AND BRIDGING*** ➜ ***VIRTUAL INTERFACES***, so wurde dieses Interface nach einem Reboot nicht auf *up* gesetzt.

4.26 Ethernet - Virtuelles Interface geändert

(ID 3840)

Konfigurierte man ein virtuelles Interface, so konnte dies ohne eine IP-Konfiguration nicht gespeichert werden. Die Enkapsulierung wurde vom Gateway beim Verlassen des Menüs von *none* auf *Ethernet II* gesetzt.

4.27 Setup Tool - Falsche MAC-Adresse dargestellt

(ID 3846)

Nach der Eingabe einer MAC-Adresse für eines der Ethernet-Interfaces, zeigten die Menüs zur Konfiguration der verbleibenden Ethernet-Interfaces dieselbe MAC-Adresse an.

4.28 HTML Wizard - Inactivity Timer ohne Wirkung

(ID 3872)

Beim Aufruf des HTML Wizards blieb die Angabe eines Inactivity Timers mit einem Wert über 300 (Sekunden) wirkungslos.

4.29 Bridging - Paketverlust/Datenkorruption

(ID 3875)

Nach der Aktivierung des Bridging war der Datentransfer über die Ethernet Interfaces verlustbehaftet bzw. die Daten korrupt.

4.30 SIF - TCP Sessions unterbrochen

(ID 3895)

Wenn die Stateful Inspection Firewall aktiviert wurde, wurden TCP-Sessions (wie z. B. eine Telnet-Verbindung zum Gateway) unterbrochen, auch wenn ***FULL FILTERING*** auf *disable* gesetzt war.

4.31 Modems - Fehlfunktion wegen Lizenznummer

(ID 3919)

Wenn auf einer **X4300** eine Modemlizenz mit der Nummer *X4AMOD* verwendet werden sollte, wurden keine Verbindungen zugelassen.

Es werden nun alle Lizenzen, die mit *X4*MOD* beginnen, akzeptiert.

4.32 SIF - TCP-Pakete mit ECN verworfen

(ID 3948)

Die Stateful Inspection Firewall verwarf TCP-Pakete, in denen das ECN Flag gesetzt war (ECN=Explicit Congestion Notification).

4.33 HTML Wizard - Nur ISDN-Verbindung auswählbar

(ID 3975)

Auf bestimmten Gateways (z. B. **X1200 II**) konnte es vorkommen, dass bei der Konfiguration eines ISP nur eine ISDN-Verbindung angeboten wurde, nicht aber eine xDSL-Verbindung.

4.34 SSHD - SSHD nicht deaktivierbar

(ID 4024)

Der SSHD war durch Setzen von ***biboExtAdmProcSSHD*** auf *disabled* nicht zu deaktivieren.

4.35 IPSec Wizard - IPSec Proposal nicht zugewiesen

(ID 4048)

Nach einer IPSec-Konfiguration mittels des HTML oder ASCII Wizards war dem Default Profile kein IPSec Proposal zugewiesen.

4.36 QoS - Irreführende Einträge in qosTosStatTable

(ID n/a)

Bei der Aktivierung von QoS auf physikalischen ebenso wie auf virtuellen Interfaces kam es zu falschen Einträgen in die ***QOSTOSSTATTABLE***.

4.37 PPPoE Credits - Panic beim Erreichen des Limits

(ID n/a)

Aktivierte man eine Zeitbegrenzung für PPPoE-Verbindungen, so kam es zu einer Panic des Gateways, wenn das Limit erreicht wurde.

4.38 X25 - Write Queue blockiert

(ID n/a)

Der X.25-Treiber sendete beim Abbau einer Verbindung zu viele Clear Requests bzw. Clear Confirms. Dadurch wurde die Write Queue blockiert und es konnten keine Daten mehr über das X.25 Interface übertragen werden.

4.39 Bridging - Speicherverlust

(ID n/a)

Bei aktiviertem Bridging kam es zu einem Speicherverlust.

4.40 QoS - Keine Einträge in qosTosStatTable

(ID n/a)

Wenn Einträge in die QoS Table von Hand über die SNMP Shell erstellt wurden, konnte es vorkommen, dass das QoS-Modul keine entsprechenden Einträge in der ***QOSTOSSTATTABLE*** vornahm.

4.41 IPSec - CRL Policy zu strikt

(ID n/a)

Wenn ein CA-Zertifikat in der ***CERTTABLE*** nicht als solches markiert war (***CERTISCERT***=*false*), so verlangte das Gateway grundsätzlich nach einer CRL, auch wenn ***CERTNOCRLS*** auf *true* gesetzt war. Diese Einstellung wird nun beachtet.

4.42 Fax - Fehlfunktion mit Mapletree Modems

(ID n/a)

Der Fax Mode war bei der Verwendung von Mapletree Modems nicht funktionsfähig.

4.43 HTML-Konfiguration - Link ohne Optionen

(ID n/a)

Wenn ein Timeout eine HTML Session beendet hatte, wurde der Link zum Aufbau einer neuen Session nicht mit den Optionen der vorhergehenden Session generiert.

4.44 Setup Tool - IPSec Peer nicht gespeichert

(ID n/a)

Es konnte vorkommen, dass eine langsam vorgenommene Peer-Konfiguration nach dem Bestätigen mit ***SAVE*** wieder gelöscht wurde.

4.45 SIF - Erwünschte Verbindungen blokkiert

(ID n/a)

Obwohl die Stateful Inspection Firewall lokal initiierte Verbindungen nicht kontrollierte (***LOCAL FILTER*** = *disable*), wurden lokal auf dem Gateway erzeugte TCP-Verbindungen blockiert.

4.46 QoS - Panic

(ID n/a)

Wenn QoS zur Klassifizierung einer High Priority Queue auf einem LAN-Interface verwendet wurde, und diese Pakete anschließend über ein ETHoA-,

PPPoA-, RPoA- oder PPTP-Interface geroutet wurden, konnte es zu einer Panic kommen.

4.47 Keepalive Monitoring - Fehlfunktion

(ID n/a)

In Abhängigkeit vom zeitlichen Abstand zwischen Statusübergängen konnte es vorkommen, dass Slave-Interfaces ihren Status nicht korrekt änderten.

4 Behobene Fehler