RELEASE NOTES SYSTEMSOFTWARE 7.2.2

Release Notes - Systemsoftware 7.2.2
Version 0.9

Ziel und Zweck

Dieses Dokument beschreibt neue Funktionen, Änderungen und behobene Fehler in **Systemsoftware 7.2.2**.

Haftung

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

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

1 Wichtige Informationen

Bitte lesen Sie die folgenden Informationen zu Systemsoftware 7.2.2 aufmerksam, um Probleme beim Update oder bei der Verwendung der Software zu vermeiden.

1.1 Gültigkeit

Systemsoftware 7.2.2 steht ausschließlich für folgende Geräte zur Verfügung und kann auf anderen Geräten nicht eingesetzt werden:

- **X2301**
- **X2302**
- **X2301w**
- **X2302w**.

Viele der hier beschriebene Funktionen finden sich für Geräte anderer Produktreihen in **Systemsoftware 7.2.1**.

1.2 Inkompatibilität

Konfigurationen, die unter **Systemsoftware 7.2.2** erstellt oder gesichert werden, sind zu allen älteren Versionen unserer Systemsoftware inkompatibel. Beachten Sie unbedingt die folgenden Hinweise zum Update und zu den Möglichkeiten eines Downgrades.

1.2.1 Vorbereitung und Update

Gehen Sie folgendemaßen vor, um ein Update auf **Systemsoftware 7.2.2** vorzubereiten und durchzuführen:

1. Sichern Sie die aktuelle Boot-Konfiguration. Verwenden Sie eine der folgenden Möglichkeiten:
   a) Geben Sie auf der SNMP Shell `cmd=save path=boot.alt` ein. Dies sichert die aktuelle Boot-Konfiguration im Flash ROM Ihres 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 7.2.2** wie gewohnt durch und starten Sie das Gateway neu.
   Das Gateway startet mit der neuen Software, die Boot-Konfiguration ist konvertiert und nicht mehr mit älteren Versionen der Systemsoftware kompatibel.

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 FLAH 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.

1 Wichtige Informationen

2 Neue Funktionen

Systemsoftware 7.2.2 enthält eine Reihe neuer Funktionen, die den Leistungsumfang gegenüber Systemsoftware 7.1.15 erheblich erweitern:

2.1 PKCS#12-Unterstützung

Systemsoftware 7.2.2 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 7.2.2** 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 X2302 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 X2302 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 X2302 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):

```
X2302:> 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

X2302:>
```

Der Import per TFTP-Download erfolgt folgendermaßen:

```
X2301:> 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

X2301:>
```

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 7.2.2 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 X2302 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 X2302 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 X2302 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 7.2.2 bietet die Möglichkeit, die vier Switch Ports von X2301(w) und X2302(w) 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).

Das Ethernet-Menü wurde den neuen Funktionen entsprechend angepasst:

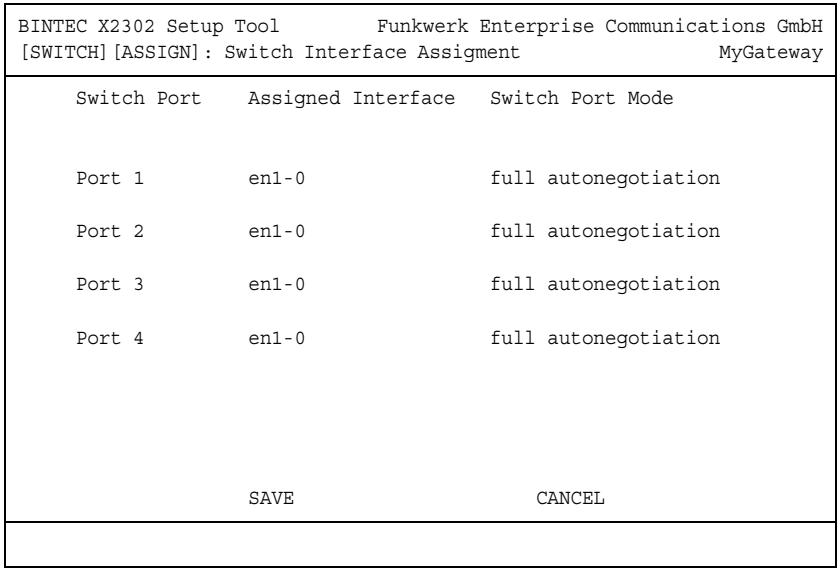
```
BINTEC X2302 Setup Tool          Funkwerk Enterprise Communications GmbH
[SWITCH]: Fast Ethernet Configuration                            MyGateway

    Fast Ethernet/en1-0>


    Switch Configuration >


              EXIT
```

Nach dem Update auf **Systemsoftware 7.2.2** 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:



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 7.2.2** 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 Universal Plug and Play

Universal Plug and Play (UPnP) ermöglich es einem Client im LAN, ein NAT-aktives Gateway zu Portfreigaben und -mappings zu veranlassen, die für aktuelle Messenger-Dienste wie Real-Time-Videokonferenzen notwendig sind. Systemsoftware 7.2.2 unterstützt UPnP.

Die Konfiguration des Gateways erfolgt über wenige Paramater im Menü ***IP*** ➜ ***UPnP***:

```
BINTEC X2302 Setup Tool          Funkwerk Enterprise Communications GmbH
[IP][UPNP]: UPnP Configuration                                  MyGateway

     UPnP status                          disabled

     TCP port number for UPnP             5678

          SAVE                             CANCEL
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
UPnP status	Hier wählen Sie aus, wie das Gateway mit UPnP Requests aus dem LAN verfährt. Mögliche Werte sind: ■ *disabled* (Defaultwert) - Das Gateway verwirft UPnP Requests, NAT-Freigaben werden nicht vorgenommen. ■ *restricted* - Das Gateway erlaubt Portfreigaben und -mappings nur für den jeweils anfragenden Host. ■ *enabled* - Das Gateway nimmt die UPnP-Freigaben für das lokale Netz vor.
TCP port number for UPnP	Hier tragen Sie die Nummer des Ports ein, auf dem das Gateway auf UPnP-Anfragen lauscht. Mögliche Werte sind *1* bis *65535*, der Defaultwert ist *5678*.

Tabelle 2-4: ***IP ➜ UPnP***

2.5 SNMP V.2/V.3

Systemsoftware 7.2.2 unterstützt neben SNMP V. 1 nun ebenfalls die SNMP Versionen 2(c) und 3. SNMP V. 3 bietet vor allem die Möglichkeit, die übertragenen Daten zu authentisieren und zu verschlüsseln.

Achtung!

Die Konfiguration Ihres Gateways ist nach einem Update auf Systemsoftware 7.2.2 nicht mehr mit älteren Softwareversionen kompatibel, d. h. ein direktes Downgrade auf eine frühere Systemsoftware ist nicht möglich.

Befolgen Sie die HInweise in “Vorbereitung und Update” auf Seite 5 **und** “Downgrade” auf Seite 6**.**

SNMP V.1 und V. 2 unterstützen eine Zugangskontrolle über die bekannten SNMP-Communities (*admin*, *write*, *read*), während SNMP V. 3 drei unterschiedliche Access Level mit entsprechenden Sicherheitsstufen unterstützt:

- no authentication, no privacy (encryption): *noAuthNoPriv*
- authentication (MD5 oder SHA1): *authNoPriv*
- authentication and privacy (DES oder AES): *authPriv*

Darüber hinaus unterstützt SNMP V. 3 eine "echte" User-Verwaltung. Aktuell sind drei den SNMP-Communities entsprechende User mit festen Sicherheitsstufen vorkonfiguriert:

- *admin* - Vollzugriff mit MD5-Authentisierung und DES-Verschlüsselung (*authPriv*)
- *write* - Schreibzugriff mit MD5-Authentisierung (*authNoPriv*)
- *read* - Lesezugriff mit MD5-Authentisierung (*authNoPriv*).

Die Verschlüsselung und Authentisierung der übetragenen SNMP-Daten wird bei der Verwendung von SNMP V. 3 vom Gateway automatisch durchgeführt. Die verwendeten Schlüssel entsprechen den Benutzer-Passwörtern, sie müssen mindesten 8 Zeichen lang sein (die Benutzer-Passwörter sollten daher wenigstens diese Länge haben). Ist ein Benutzerpasswort kürzer als acht Zeichen so muss es im SNMP-Kommando wiederholt werden, also *bintecbintec* anstelle von *bintec* (siehe auch das Beispiel für ein entsprechendes SNMP-Kommando: Alle SNMP-Versionen).

Die Konfiguration der neuen SNMP-Parameter erfolgt vorwiegend auf der SNMP Shell, lediglich ***SNMPADMINVERSION*** kann über das Menü ***IP*** ➜ ***SNMP*** eingestellt werden. Folgende MIB Tabellen sind unter **Systemsoftware 7.2.2** vorhanden:

- ***SNMP***
- ***SNMPADMIN***
- ***SNMPENGINE***
- ***USMSTATS.***

Informationen zu den Tabellen und den enthaltenen Parametern können Sie der mit der Software veröffentlichten HTML-MIB-Dokumentation entnehmen.

Relevant für die Konfiguration ist vor allem ***SNMPADMIN***. Hier ist in erster Linie folgender Parameter von Bedeutung:

Parameter	Bedeutung
snmpAdminVersion(rw)	Dieser Parameter definiert, welche SNMP-Versionen das Gateway für externe SNMP-Verbindungen zur Verfügung stellt. Mögliche Werte sind: ■ *All* (Defaultwert) - Das Gateway akzeptiert SNMP V. 1, 2c und 3. ■ *None* - Das Gateway akzeptiert keine externen SNMP-Befehle, d. h. der SNMP-Zugriff ist nur noch auf der Konsole des Getways aus möglich (z. B. per SSH oder über die serielle Schnittstelle). ■ *v1 (0)* - Das Gateway akzeptiert nur SNMP V. 1. ■ *v2c (1)* - Das Gateway akzeptiert nur SNMP V. 2c. SNMP-Version 2c unterstützt 64bit Counter und Zugriffskontrolle über SNMP Communities. ■ *v3 (2)* - Das Gateway akzeptiert nur SNMP V. 3 mit "echter" User-Verwaltung und Zugangskontrolle durch Access Level. Bei der Eingabe des gewünschten Wertes ist, es möglich, einzelne Werte miteinander über das Pipe-Zeichen ("|") miteinander zu verknüpfen. Wenn also eine Unterstützung von SNMP V.1 und V. 3 gewünscht ist, kann das durch die Eingabe von `snmpAdminVersion=v1|v3` realisiert werden.

Tabelle 2-5: ***SNMPADMIN***: ***SNMPADMINVERSION***

SNMP-Kommandos haben also in den unterschiedlichen Versionen z. B. folgende Form:

SNMP V.1

```
$ snmpget -v1 -c bintec 192.168.0.254 iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0

SNMPv2-MIB::sysDescr.0 = STRING: X2302
```

SNMP V.2

```
$ snmpget -v2c -c bintec 192.168.0.254 system.sysDescr.0 system.sysName.0 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus.1000

SNMPv2-MIB::sysDescr.0 = STRING: X2302

SNMPv2-MIB::sysName.0 = STRING: myrouter

IF-MIB::ifOperStatus.1000 = INTEGER: up(1)
```

SNMP V.3

```
$ snmpget -v3 -a MD5 -A publicpublic -u write -l authNoPriv 192.168.0.254 system.sysDescr.0

SNMPv2-MIB::sysDescr.0 = STRING: 2302
```

Alle SNMP-Versionen

```
$ snmpget -m ALL -M /usr/share/snmp/mibs -M /opt/bintec/mib/7.2.2/ -v3 -a MD5 -A bintecbintec -u admin -l authPriv -x DES -X bintecbintec 192.168.0.254 iso.org.dod.internet.private.enterprises.bintec.bibo.admin-2 .snmpAdminMIB.snmpAdmin.snmpAdminVersion.0

BINTEC-ADMIN-MIB::snmpAdminVersion.0 = BITS: E0 v1(0) v2c(1) v3(2)
```

(Die Beispiele wurden mit der Kommmandozeilen-Version von NET-SNMP erstellt. Siehe http://www.net-snmp.org.)

Weiter gehende Informationen zu den SNMP-Versionen finden Sie in den entsprechenden RFCs und Drafts:

- SNMP V.1: RFC 1157
- SNMP V.2c: RFC 1901 – 1908
- SNMP V.3: RFC 3410 – 3418.

2.6 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 hinzugefügt 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.

2.7 Neue Trace-Tool-Funktionen

Systemsoftware 7.2.2 stellt eine neue Filtermöglichkeit.

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)
```

2 Neue Funktionen

3 Änderungen

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

3.1 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 7.2.2 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.

3.2 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 7.2.2 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 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.

4.3 Bridging - Leistungsverlust

(ID 3525)

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

4.4 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.

4.5 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.

4.6 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.

4.7 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.

4.8 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.

4.9 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.

4.10 PPPoE - Verbindungsaufbau erfolglos

(ID 3756)

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

4.11 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***.

4.12 ADSL - Kein Datenverkehr

(ID 3761)

Aufgrund einer extrem hohen Anzahl von Interrupts konnte es zu folgenden Fehlern kommen:

- Das PPP Interface war *dormant* und konnte nicht auf *up* gesetzt werden.
- Auf dem ATM Interface war nur ausgehender Datenverkehr zu verzeichnen.
- Setup Tool und SNMP Shell reagierten nur mit starker Verzögerung.

4.13 DynDNS - Reboot mit GnuDIP

(ID 3762)

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

4.14 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.

4.15 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.

4.16 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.

4.17 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.

4.18 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.

4.19 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).

4.20 SSHD - SSHD nicht deaktivierbar

(ID 4024)

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

4.21 VLAN - Falsches Frame-Format

(ID 4046)

Wenn auf einem ETHoA Interface VLAN Tags angewendet wurden, wurde das Format der ATM Frames verfälscht. Dabei konnte es zu Datenverlust kommen.

4.22 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.

4.23 QoS - TOS geändert

(ID 4148)

Das TOS-Feld einer aus dem LAN ins WAN gehenden Verbindung wurde nicht der Konfiguration gemäß gesetzt.

4.24 Bridging - Speicherverlust

(ID n/a)

Bei aktiviertem Bridging kam es zu einem Speicherverlust.

4.25 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.

4.26 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.

4.27 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.

4.28 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.

4.29 Keepalive Monitoring - Fehlfunktion

(ID n/a)

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

4.30 NAT - WLAN Pakete verworfen

(ID n/a)

TCP-Pakete, die von einem WLAN Interface zu einem WAN Interface (PPPoA oder IPoA) geroutet werden sollten, wurden verworfen, wenn NAT auf dem WAN Interface aktiviert war.