Release Notes System-Software Release 6.2.2 X-Generation

Juli 2002

System-Software Release 6.2.2

Dieses Dokument beschreibt neue Funktionen, Änderungen, behobene und bekannte Fehler der System-Software Release 6.2.2.

Inhaltsverzeichnis

1 Wichtige Hinweise

Beachten Sie, daß Konfigurationen, die Sie unter System-Software Release 6.2.2 erstellen, nicht abwärtskompatibel sind! Sie sollten vor dem Update auf System-Software Release 6.2.2 Ihre alte Konfiguration sichern, um diese im Falle eines "Rollback" auf das Release 6.1 wieder einspielen zu können.

Eine Anleitung zum Sichern und Wiedereinspielen einer Konfiguration mit dem Setup Tool finden Sie im Handbuch Ihres Routers im Kapitel "Konfigurationsmanagement".

Sollten Sie mit System-Software Release 6.2.2 IPSec-Konfigurationen realisieren, beachten Sie, daß die Gegenstelle, zu der Sie einen Tunnel aufbauen wollen, ebenfalls unter System-Software Release 6.2.2 laufen muß, sofern es sich um ein BinTec-Gerät handelt.

2 Aktualisierung der Systemsoftware

- Laden Sie System-Software Release 6.2.2 von unserem Webserver (www.bintec.de) herunter.
- Aktualisieren Sie die Software auf Ihrem Router. Eine Anleitung finden Sie im Kapitel "Software-Update durchführen" im Handbuch Ihres Routers.

Wenn Sie die System-Software Ihres Routers aktualisieren, sollten Sie erwägen, auch die neueste Version der BRICKware for Windows auf Ihrem PC zu installieren. Sie können diese ebenfalls von unserem Webserver herunterladen.

Wenn Sie **X4000** von einem früheren Softwarestand als 6.1.2 (also 5.1.6 oder früher) auf System-Software Release 6.2.2 aktualisieren wollen, müssen Sie den BOOTmonitor und die Logik(en) Ihres Gerätes aktualisieren:

Sie können Ihre Software zunächst mit dem 6.1.2 BLUP (BinTec Large Update) aktualisieren. Dieses enthält alle notwendigen Dateien. Wenn Sie das BLUP eingespielt haben, können Sie, wie im Handbuch Ihres Routers beschrieben, auf System-Software Release 6.2.2 aktualisieren.

Bei der Aktualisierung mit dem BLUP ist lediglich ein einziger Aktualisierungsvorgang notwendig. Sie können sich die notwendigen Dateien sowie die Anleitungen zur Aktualisierung der Software bei www.bintec.de herunterladen.

3 Neue Funktionen

BinTec hat seit dem Software Release 6.1 den Funktionsumfang der Router der X-Generation um folgende Funktionen erweitert:

- DHCP Client (Kapitel 3.1, Seite 10)
- H.323 (Kapitel 3.2, Seite 11)
- Neue BinTec-IPSec-Version (Kapitel 3.3, Seite 11)
- XoT – X.25 über TCP/IP (Kapitel 3.4, Seite 12)
- Dynamic DNS (Kapitel 3.5, Seite 15)
- Dynamic VPN (PPPT) (Kapitel 3.6, Seite 22)
- Dynamic IPSec (Kapitel 3.7, Seite 25)
- MPPC und STAC Hardwarekompression (Kapitel 3.8, Seite 26)
- BAP/BACP: Kanalbündelung bei Sammelrufnummern (Kapitel 3.9, Seite 27)
- V.120 (Kapitel 3.10, Seite 30)
- Multi-NAT (Kapitel 3.11, Seite 31)
- Konfigurierbares ICMP-Verhalten (Kapitel 3.12, Seite 37)
- RIP und OSPF deaktivierbar (Kapitel 3.13, Seite 38)
- Automatische Kabelerkennung an X.21-Schnittstellen (Kapitel 3.14, Seite 39)
- Weekly Schedule (Kapitel 3.15, Seite 44)
- CAPI Supplementary Services (Kapitel 3.16, Seite 46)

3.1 DHCP Client

Ab der System-Software Release 6.2.2 ist es möglich, die IP-Konfiguration eines Ethernet-Interfaces nicht nur manuell vorzunehmen, sondern auch von einem DHCP-Server dynamisch zu beziehen.

Diese Einstellung kann für jedes Ethernet-Interface vorgenommen werden. Wenn Sie im Feld ***IP-CONFIGURATION*** eines Menüs zur Konfiguration eines Ethernet-Interfaces als Wert *DHCP* auswählen, ändert sich das Menü z. B. wie folgt:

```
BinTec Router Setup Tool                        BinTec Communications AG
[LAN]: Configure Ethernet Interface                              MyRouter

          IP-Configuration            DHCP
               local IP-Number
               local Netmask
               DHCP MAC Address       000Af000000

               Encapsulation          Ethernet II
               Mode                   Auto


          Bridging                    disabled


                     SAVE                                  CANCEL

Use <Space> to select
```

Die Felder für die lokale IP-Adresse und Netzmaske sind zwar noch sichtbar, aber Sie können hier keine Änderungen mehr vornehmen.

Als neues Feld erscheint das Feld **DHCP MAC Address**. Hier geben Sie die MAC-Adresse des Ethernet-Interfaces ein, das Sie gerade konfigurieren. Mit Hilfe der MAC-Adresse kann Ihr Router im LAN eindeutig identifiziert werden, auch wenn er noch keine IP-Adresse zugewiesen bekommen hat. Im allgemeinen brauchen Sie hier allerdings keinen Eintrag zu machen, der Router verwendet dann die in die Hardware "eingebrannte" MAC Adresse.

Manche Provider verwenden Hardware-unabhängige MAC-Adressen, um ihren Clients IP-Adressen dynamisch zuzuweisen. Sollte Ihnen Ihr Provider eine

MAC-Adresse zugewiesen haben, so tragen Sie diese in das entsprechende Feld ein. Eine Beschreibung der Konfiguration für die Anbindung an das Internet in diesem Fall (Verwendung von z. B. Ethernet oder IPoA) finden Sie im Handbuch **Basiskonfiguration**.

Je nach Routertyp bzw. Ausstattung des Routers mit Erweiterungskarten kann diese Option in unterschiedlichen Menüs relevant sein, so z. B. in den Menüs ***ATM*** ➧ ***IPoA*** bzw. ***Ethernet (PPPoE,...)*** ➧ ***IP*** von **X2300i**, dem Menü ***CM-10BT*** von **X1200** oder im Menü ***X4E-100BT, Fast Ethernet*** einer Ethernet-Erweiterungskarte für **X4000**.

3.2 H.323

System-Software Release 6.2.2 bietet zum ersten Mal eine Implementierung des H.323-Protokolls. Damit sind vielfache Anwendungen im Bereich "Voice over IP" (VoIP) möglich. Die implementierte Software gliedert sich derzeit in einen H.323 Proxy und einen Gatekeeper. Diese ermöglichen z. B. Unterstützung von IP-Telephonen oder kompletten VoIP-Anlagen.

Eine detaillierte Beschreibung der H.323-Funktionen finden Sie im Software-Reference-Kapitel "H.323", das Sie von unserem Webserver (www.bintec.de) herunterladen können.

3.3 Neue BinTec-IPSec-Version

Die von BinTec angebotene IPSec-Lösung liegt nun in der Version 2.1.1 vor. Die Änderungen, die diese Implementierung mit sich gebracht hat, sind umfangreich. Sie können die vorgenommenen Änderungen und Ergänzungen dem Software-Reference-Kapitel "IPSec" entnehmen, das Sie von unserem Webserver (www.bintec.de) herunterladen können. Gleichzeitig mit der IPSec-Software liegt dort für Sie eine Vorabversion dieses Kapitels bereit, die neue Dokumentation wird Ende Juli vollständig sein.

Wesentliche neue Funktionen sind:

- einfache Grundkonfiguration mit Hilfe eines Wizards
- Dynamic IPSec – IPSec mit dynamischen IP-Adressen (siehe Kapitel 3.7, Seite 25)
- Integration neuer Verschlüsselungsalgorithmen (Twofish und Rijndael/AES) sowie neuer Hash-Algorithmen (RipeMD 160 und Tiger 192)
- Peer-spezifische Konfiguration von IKE und IPSec

3.4 XoT – X.25 über TCP/IP

Mit XoT können X.25 Pakete auch über ein IP-Netz versendet werden. Hierbei werden X.25-Pakete in TCP-Pakete "verpackt" und dann über ein IP-Netz versendet.

XoT steht auf folgenden Geräten nicht zur Verfügung:

- **X1000**
- **X1200**
- **X3200**

Bei der Konfiguration muß zunächst der Port definiert werden, auf dem der Router XoT-Verbindungen annimmt. Der Default-Port hierfür ist 1998, aber die BinTec-Implementierung läßt eine freie Portauswahl zu, um individuelle Konfigurationen zu unterstützen. Die Festlegung des Ports erfolgt in ***X.25*** ➧ ***STATIC SETTINGS*** im Feld **XOT TCP Port**. Alle Pakete, die an diesem Port ankommen, werden an den XoT-Dienst weitergeleitet. Dort werden sie entsprechend der Konfiguration der XoT-Interfaces verarbeitet.

Die wesentlichen Parameter werden im Menü ***X.25*** ➧***XoT*** ➧**ADD/EDIT** konfiguriert:

```
BinTec Router Setup Tool                          BinTec Communications AG
[X.25][XOT][EDIT]: XOT Configuration                                MyRouter


   Interface Name                                 xot1

   Allow Incoming XOT Calls                       yes
   Incoming Partner Source IP Address             5.5.5.5
   Mask                                           255.255.255.255

   Outgoing Partner Destination IP Address        6.6.6.6
   Destination Port                               1998

   Max Number of XOT Links                        5
   MTU                                            1456


                  SAVE                                    CANCEL
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Interface Name	Hier geben Sie einen beliebigen Namen (max. 25 Zeichen) für das XoT-Interface ein.
Allow Incoming XOT Calls	Definiert, ob eingehende XoT-Verbindungen zugelassen werden sollen oder nicht. Mögliche Werte: ■ *yes*: Auf diesem Interface werden eingehende XoT-Pakete angenommen. ■ *no*: Auf diesem Interface werden keine eingehenden XoT-Verbindungen akzeptiert (wohl aber können Verbindungen nach außen aufgebaut werden).

Feld	Bedeutung
Incoming Partner Source IP Address	Definiert die IP-Adresse des XoT-Partners, der XoT-Pakete sendet. Dieses Feld ist nur sichtbar, wenn Sie eingehende XoT-Verbindung auf diesem Interface zugelassen haben. Wenn Sie als IP-Adresse *0.0.0.0* eingeben, werden Verbindungen von beliebigen IP-Adressen akzeptiert.
Mask	Die zu der IP-Adresse (**Incoming Partner Source IP Address**) gehörende Netzmaske. Dieses Feld ist nur sichtbar, wenn Sie eingehende XoT-Verbindung auf diesem Interface zugelassen haben. Sie haben die Möglichkeit, keine IP-Adresse anzugeben, aber eine Netzmaske zu spezifizieren. Dann werden Verbindungen von allen IP-Adressen aus dem von der Netzmaske spezifizierten Adreßbereich akzeptiert.
Outgoing Partner Destination IP Address	Hier geben Sie die IP-Adresse des XoT-Partners an, an den XoT-Pakete gesendet werden sollen.
Destination Port	Definiert den Port, an welchen die XoT-Pakete gesendet werden. Stellen Sie sicher, daß der Empfänger des Pakets auch tatsächlich auf diesem Port XoT-Pakete annimmt.
Max Number of XOT Links	Definiert die maximale Anzahl ein-und ausgehender XoT-Verbindungen zu diesem XoT-Partner.
MTU	Definiert die maximale Größe der zu sendenden Pakete (in bit). Mögliche Werte: *576* bis *8180*.

Tabelle 3-1: ***X.25*** ➧ ***XOT*** ➧ **ADD/EDIT**

Damit ein- und ausgehende XoT-Pakete weitergegeben werden können, muß noch eine entsprechende Route im Menü ***X.25*** ➧***ROUTING*** angelegt werden. Außerdem ist eine Konfiguration der X.25-spezifischen Parameter des XoT-Interfaces im Menü ***X.25*** ➧***LINK CONFIGURATION*** empfehlenswert.

Informationen zur Konfiguration einer X.25-Route und zu den Einstellungen im Menü ***LINK CONFIGURATION*** finden Sie in der Software Reference, Kapitel "X.25". Sie können die Software Reference von www.bintec.de herunterladen.

3.5 Dynamic DNS

Der Einsatz dynamischer IP-Adressen hat den Nachteil, daß ein Host im Netz nicht mehr aufgefunden werden kann, sobald sich seine IP-Adresse geändert hat. Dynamic DNS sorgt dafür, daß Ihr Router auch nach einem Wechsel der IP-Adresse noch erreichbar ist.

DynDNS ist ausschließlich für die Anwendung auf solche Interfaces gedacht, die eine dynamische IP-Adresse zugewiesen bekommen. Statische IP-Adressen werden nicht propagiert.

Folgende Schritte sind zur Einrichtung notwendig:

- Registrierung eines Host-Namens bei einem DynDNS-Provider
- Konfiguration des Routers

Registrierung

Bei der Registrierung des Host-Namens legen Sie einen individuellen Benutzernamen für den DynDNS-Dienst fest, z. B. ***dyn_client***. Dazu bieten die Service Provider unterschiedliche Domainnamen an, so daß sich ein eindeutiger Host-Name für Ihren Router ergibt, z. B. ***dyn_client.provider.com***. Der DynDNS-Provider übernimmt es für Sie, alle DNS-Anfragen bezüglich des

Hosts ***dyn_client. provider.com*** mit der dynamischen IP-Adresse Ihres Routers zu beantworten.

Damit der Provider stets über die aktuelle IP-Adresse Ihres Routers informiert ist, kontaktiert der Router beim Aufau einer neuen Verbindung den Provider und propagiert seine derzeitige IP-Adresse. System-Software Release 6.2.2 ermöglicht es Ihnen, diesen Service zu nutzen.

Konfiguration des Routers

Die Konfiguration erfolgt in ***IP*** ➧ ***DynDNS***. Im ersten Menüfenster finden Sie eine Aufstellung der bereits konfigurierten DynDNS-Services. Darüber hinaus gelangen Sie von hier in die Untermenüs ***IP*** ➧ ***DynDNS*** ➧ **ADD/EDIT** und ***IP*** ➧ ***DynDNS*** ➧ ***DynDNS Provider List***.

Das Menü **ADD/EDIT** sieht folgendermaßen aus:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IP][DYNDNS][ADD]: Dynamic DNS Service                          MyRouter


          Host
          Interface
          User
          Password

          Provider
          MX
          Wildcard                  off
          Permission                enabled


                    SAVE                                  CAN
```

In diesem Menü konfigurieren Sie einen DynDNS-Service. Die Felder haben folgende Bedeutung:

Feld	Bedeutung
Host	Hier geben Sie Ihren vollständigen Host-Namen für diesen Service ein, also z. B. ***dyn_client.provider.com***.
Interface	Definiert das WAN-Interface, dessen IP-Adresse über den DynDNS-Service propagiert werden soll (i. allg. das des Internet Service Providers).
User	Definiert den Benutzernamen, mit dem Sie sich bei Ihrem DynDNS-Provider anmelden.
Password	Hier geben Sie das Paßwort ein, mit dem Sie sich bei Ihrem DynDNS-Provider authentisieren.
Provider	Definiert einen der vorkonfigurierten Provider. Im unkonfigurierten Zustand stehen Ihnen bereits sechs Dienste zur Auswahl, deren Protokolle unterstützt werden. Im Menü ***IP*** ➧ ***DynDNS*** ➧ ***Edit DynDNS Provider*** können Sie weitere Provider eintragen und konfigurieren.
MX	Definiert einen weiteren Hostnamen, an den E-Mails weitergeleitet werden, wenn der gerade konfigurierte Host keine Mail empfangen soll. Erkundigen Sie sich bei Ihrem Provider nach diesem Service und stellen Sie sicher, daß Emails von dem als MX eingetragene Host angenommen werden können.

Feld	Bedeutung
Wildcard	Hier können Sie eine zusätzliche DNS-Namensauflösung innerhalb Ihres Netzes aktivieren. Dafür müssen Sie in Ihrem Netz einen DNS-Server betreiben. Die möglichen Werte sind: ■ *on*: Die zusätzliche Namensauflösung ist aktiviert. ■ *off*: Die zusätzliche Namensauflösung ist deaktiviert.
Permission	Hier können Sie den soeben konfigurierten DynDNS-Service ein- bzw. ausschalten. Die möglichen Werte sind: ■ *enabled* ■ *disabled*

Tabelle 3-2: ***IP*** ➧ ***DynDNS*** ➧ **ADD/EDIT**

Im Menü ***IP*** ➧ ***DynDNS*** ➧ ***DynDNS Provider List*** können Sie weitere DynDNS-Provider konfigurieren und editieren. Die voreingestellten Provider (*dyndns*, *stat dyndns*, *ods*, *hn*, *dyns* und *orgdns*) können Sie nicht editieren und auch nicht löschen.

Das Menü zum Hinzufügen bzw. Editieren der Einträge sieht folgendermaßen aus:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IP][DYNDNS][DYNDNS PROVIDER][ADD]: Edit DynDNS Provider      MyRouter


          Name
          Server
          Path
          Port                          80

          Protocol                      dyndns

          Minimum Wait (sec)            300


                     SAVE                                  CANCEL
```

Prinzipiell können Sie beliebige DynDNS-Provider eintragen. Da aber viele Provider proprietäre Protokolle zur Abwicklung des Services entwickelt haben, müssen Sie sicherstellen, daß der von Ihnen gewählte Provider eines der von BinTec unterstützten Protokolle verwendet (siehe Tabelle 3-3, Seite 21).

Das **ADD/EDIT** Menü hat folgende Felder:

Feld	Bedeutung
Name	Hier können Sie dem Provider einen beliebigen Namen geben.
Server	Hier geben Sie den (auflösbaren) Host-Namen des Servers an, auf dem der DynDNS-Service des Providers läuft.

Feld	Bedeutung
Path	Hier geben Sie den Pfad auf dem Server des Providers ein, auf dem das Skript zur Aktualisierung der IP-Adresse Ihres Routers zu finden ist. Fragen Sie Ihren Provider nach dem zu verwendenden Pfad.
Port	Hier geben Sie den Port an, auf dem Ihr Router den Server Ihres Providers ansprechen soll. Erfragen Sie den entsprechenden Port bei Ihrem Provider.
Protocol	Hier wählen Sie eines der implementierten Protokolle aus. Es stehen zur Verfügung – *dyndns* (www.dyndns.org) – *static dyndns* (www.dyndns.org) – *ods* (http://www.ods.org) – *hn* (http://hn.org) – *dyns* (http://dyns.cx) – *GnuDIP HTML* (http://gnudip2.sourceforge.net) – *GnuDIP TCP* (http://gnudip2.sourceforge.net)

Feld	Bedeutung
Minimum Wait	Hier geben Sie die Zeitdauer (in Sekunden) an, die der Router mindestens wartet, bevor er seine aktuelle IP-Adresse erneut beim DynDNS-Provider propagieren kann. Der Default-Wert ist auf 300 Sekunden eingestellt.

Tabelle 3-3: ***IP*** ➧ ***DynDNS*** ➧ ***Edit DynDNS provider*** ➧ **ADD/EDIT**

Mit *GnuDIP* ist ein Protokoll implementiert, das den als Freeware zur Verfügung stehenden GnuDIP-Server unterstützt. Mit diesem ist es möglich, einen eigenen DynDNS-Service anzubieten.

Beachten Sie, daß Sie einen relativ langen Shorthold (ca. 120 Sekunden) für das Interface einstellen sollten, über das die DynDNS-Verbindungen realisiert werden. Denn die Aktualisierung der IP-Adresse beim DynDNS-Provider dauert unter Umständen relativ lange. Wenn der Shorthold greift und die Verbindung beendet wird, bevor die IP-Adresse erfolgreich beim Provider aktualisiert werden konnte, bleibt der DynDNS-Service auf Ihrem Router u. U. wirkungslos.

Wenn Sie Verbindungen zum Internet über eine Flatrate aufbauen, stehen Ihnen weitere Möglichkeiten zur Verfügung, den Shorthold an Ihre Bedürfnisse anzupassen. Informationen dazu finden Sie im Handbuch Ihres Routers unter dem Stichwort "Shorthold".

DynDNS ermöglicht es also, daß Hosts mit dynamischen IP-Adressen eine Peer-to-Peer Verbindung z. B. über das Internet aufbauen. Dies ist von entscheidender Bedeutung in PPTP/VPN-Szenarien, in denen der Responder oder beide Peers lediglich über dynamische IP-Adressen verfügen. Unter diesen Umständen konnte der VPN-Tunnel bisher nicht aufgebaut werden, weil die Adresse eines der Tunnelendpunkte nicht bekannt war.

Nun kann sich nicht mehr lediglich eine Filiale mit dynamischer IP-Adresse in der Firmenzentrale einloggen, sondern die Firmenzentrale kann die Filiale ebenfalls (auch per Callback) erreichen. Darüber hinaus können Filialen mit der Zentrale oder auch untereinander PPTP-Tunnel aufbauen und sensible Daten sicher austauschen.

3.6 DynVPN (PPTP)

DynVPN erlaubt es, PPTP-VPNs auch dann zu realisieren, wenn beide Teilnehmer lediglich über eine dynamische IP-Adresse verfügen oder die Rolle des Initiators nicht festgelegt ist. Denn wenn nur einer der beiden Partner eine dynamische IP-Adresse hat, so mußte der Aufbau des VPN-Tunnels stets von diesem angestoßen werden. Ist eine feste "Rollenverteilung" nicht möglich, muß eine Möglichkeit geschaffen werden, wie sich beide Partner im Netz "finden" können, ohne die IP-Adresse des anderen von vornherein zu kennen (für den Fall, daß beide Partner dynamische IP-Adressen haben, ist dies völlig unumgänglich).

DynDNS bietet die Möglichkeit, die eigene dynamische IP-Adresse z. B. im Internet zu propagieren und so über einen bestimmten Host-Namen identifizierbar zu sein. Dabei ist es wesentlich, daß alle Teilnehmer, die unter Umständen für einen anderen Teilnehmer initiativ erreichbar sein sollen, DynDNS bereits konfiguriert haben.

Die Konfiguration eines VPN-Partners, der über einen DynDNS-Hostnamen erreicht werden soll, unterscheidet sich nicht grundlegend von der Konfiguration eines VPN-Partners mit fester IP-Adresse. Im Menü ***VPN*** ➧ ***IP*** ist eine Reihe von Optionen hinzugekommen, die dynamische VPNs ermöglichen.

Das Menü sieht für einen bereits konfigurierten VPN-Partner folgendermaßen aus:

```
BinTec Router Setup Tool                        BinTec Communications AG
[VPN][ADD][IP]: IP Configuration (dyn_partner)                  MyRouter

 Dynamic VPN                              yes

  VPN Partner's IP Address                 dyn_partner.dyndns.org

  local IP Address                         10.2.2.1

  Partner's LAN IP Address                 10.1.1.0
  Partner's LAN Netmask                    255.255.240.0

  Advanced Settings >

                    SAVE                                  CANCEL
```

Feld	Bedeutung
Dynamic VPN	Hier aktivieren oder deaktivieren Sie den DynDNS-Service für diesen VPN-Partner.
VPN Partner's IP Address	Definiert im Falle eines dynamischen VPNs den Host-Namen des VPN-Partners, mit dem dieser bei seinem DynDNS-Provider registriert ist.
local IP Address	Definiert die lokale IP-Adresse des virtuellen VPN-Interfaces an, das Sie gerade konfigurieren. Es handelt sich hierbei um eine frei wählbare IP-Adresse des privaten Adreßbereichs.
Partner's LAN IP Address	Definiert die lokale IP-Adresse des LANs, das hinter dem VPN-Tunnel liegt.
Partner's LAN Netmask	Definiert die zur **Partner's LAN IP Address** gehörende Netzmaske.

Tabelle 3-4: ***VPN*** ➧**ADD/EDIT** ➧***IP***

Sollte Ihr Router bei der Eingabe des Host-Namens in das Feld **VPN Partner's IP Address** die Warnung ausgeben, daß der Host-Name nicht auflösbar ist, so haben Sie entweder den DynDNS-Host-Namen des Partners noch nicht konfiguriert oder Ihr Router kann nicht auf das Internet zugreifen, um den Host-Namen beim DynDNS-Provider aufzulösen.

Konfigurieren Sie den DynDNS-Service, bevor Sie ein dynamisches VPN einrichten.

Sollten Sie ein Szenario konfigurieren wollen, in dem zwei Partner, die nicht permanent online sind, einander erreichen können, so können Sie zusätzlich im Menü ***VPN*** ➧**ADD/EDIT** ➧***ADVANCED SETTINGS*** die Option *yes (callback via VPN)* für das Feld **Callback** aktivieren. Der eine Partner kann dann durch einen ISDN-Ruf bei dem anderen Partner den Aufbau eines VPN-Tunnels über das

Internet anstoßen, selbst wenn dieser augenblicklich gar nicht online ist. Dabei erkennt der Router den anklopfenden Partner anhand von dessen Rufnummer und baut (je nach der Konfiguration des Routings, im allgemeinen aber über das Internet) einen VPN-Tunnel zu der durch den DynDNS-Service propagierten IP-Adresse auf. Die Authentisierung der VPN-Partner erfolgt wie bei einem statischen VPN durch die in ***VPN*** ➧**ADD/EDIT** ➧***PPP*** konfigurierte PPP-Authentisierung.

Die WAN-Nummern, die der Router für den Callback kennen muß, geben Sie im Menü ***VPN*** ➧***WAN-NUMBERS*** ein (dieses Menü erscheint nur bei aktiviertem Callback). Dies entspricht dem Menü ***WAN PARTNER*** ➧**ADD/EDIT** ➧***WAN NUMBERS***. Weitere Informationen zu den WAN-Nummern finden Sie im Handbuch Ihres Routers.

Beachten Sie, daß Sie für einen Callback die entsprechende Option auf den Routern beider Partner aktvieren müssen.

3.7 Dynamic IPSec

Bisher unterlag die Absicherung von Datenverkehr mit IPSec den selben Einschränkungen wie diejenige mit PPTP-VPNs: Wenn einer der Peers lediglich über eine dynamische IP-Adresse verfügte, mußte dieser den Aufbau eines IPSec-Tunnels initiieren. Mit dynamischen IP-Adressen auf beiden Seiten war IPSec überhaupt nicht möglich.

System-Software Release 6.2.2 ermöglicht es, den oben beschriebenen DynDNS-Service auch für IPSec zu nutzen. Dazu ist es notwendig, einen entsprechenden DynDNS-Service zu konfigurieren (siehe Kapitel 3.5, Seite 15) und bei der Peer-Konfiguration anstelle einer IP-Adresse den Host-Namen anzugeben, mit dem der Peer beim DynDNS-Service registriert ist. Sobald der Router des Peers seine derzeitige IP-Adresse propagiert, kann Ihr eigener Router diesen Host-Namen auflösen und somit eine Verbindung zu einem Peer mit dynamischer IP-Adresse auch initiieren.

Der Eintrag des Host-Namens anstelle einer IP-Adresse erfolgt bei der Peer-Konfiguration im Menü ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT**:

```
BinTec Router Setup Tool                    BinTec Communications AG
[IPSEC][PEERS][ADD]: IPsec Configuration -
                     Configure Peer List                    MyRouter

     Description:
     Peer Address:
     Peer IDs:




                        SAVE              CANCEL
```

Im Feld **Peer Address** können Sie nun anstelle einer IP-Adresse auch den DynDNS-Host-Namen eingeben.

Beachten Sie, daß es auch bei der Anwendung des DynDNS-Services auf IPSec nicht möglich ist, die Authentisierung der Phase 1 mit *preshared_keys* im *id_protect* Modus durchzuführen.

Weitere Konfigurationsschritte sind im Menü ***IPSec*** nicht notwendig.

3.8 MPPC- und STAC-Hardwarekompression

Ab System-Software Release 6.2.2 unterstützt BinTec auf allen Ressourcenmodulen, die mit einem entsprechenden HiFn-Chip ausgestattet sind (XTR-Enc und XTR-VPN), MPPC, MS-STAC und STAC-Kompression.

3.9 BAP/BACP: Kanalbündelung bei Sammelrufnummern

Ab System-Software Release 6.2.2 kann von einem ISP auch dann Kanalbündelung gewährleistet werden, wenn dieser die ankommenden Rufe auf mehrere Router verteilt: Dem Client, der sich einwählt und einen weiteren B-Kanal anfordert, wird eine bestimmte ISDN-Nummer übermittelt. Diese wird für jeden Router der Zentralseite individuell vergeben, so daß die Rufe mehrerer Kanäle über diese Rufnummer tatsächlich auf demselben Router terminiert werden. Der Aufbau des zusätzlichen B-Kanals wird durch eine Art Callback realisiert: Der Client fordert einen weiteren B-Kanal an. Daraufhin fordert die Zentralseite einen Ruf mit der individuellen Rufnummer des Routers an, mit dem der Client bereits aktuell verbunden ist.

In diesem Szenario ist der Client der aktive Teilnehmer, d. h. die Kontrolle und die Verantwortung (Kosten für Kanalbündelung) liegen bei diesem. Die Zentralseite akzeptiert alle Anfragen des Clients, solange diese in Übereinstimmung mit der WAN-Partner-Konfiguration des Routers stehen.

Folgende neue Parameter wurden eingeführt:

- die MIB-Tabelle **pppDialProfile**
- die Werte *bap_client* und *bap_server* für die Variable **BodMode** in der **pppExtIfTable**

Konfiguration der pppDialProfileTable

Die Konfiguration der in dieser Tabelle enthaltenen Parameter ist nur serverseitig notwendig und nicht in das Setup Tool integriert. Sie muß in der SNMP-Shell vorgenommen werden.

Die **pppDialProfileTable** enthält die folgenden Variablen:

Variable	Bedeutung
Index	Der Wert wird automatisch generiert und bezeichnet das zu konfigurierende Dialout-Profil.
Descr	Hier geben Sie eine Beschreibung des Dialout-Profils ein.
BapNumber	Hier geben Sie die Rufnummer ein, mit der der Rückruf des Clients erfolgen soll.
BapSubAddress	Hier bestimmen Sie die BAP-Subadresse, die für eine BAP-Call-Response oder einen Callback-Request verwendet werden soll.
BapLkType	Hier bestimmen Sie den Link-Type, der für eine BAP-Call-Response oder einen Callback-Request verwendet werden soll.
StkMask	Hier bestimmen Sie die ISDN-Stack-Maske. Ein Wert von *0* deaktiviert jeden Dialup, ein Wert von *-1* läßt einen Dialup über jeden verfügbaren ISDN-Stack zu.
CallbackL1Prot	Hier bestimmen Sie das Layer-1-Protokoll, das für den Callback verwendet wird. Der Wert *initial (1)* bedeutet, daß das Layer-1-Protokoll des ersten Rufs verwendet wird.

Tabelle 3-5: **pppDialProfileTable**

Die Konfiguration dieses Services auf der Zentralseite erfordert folgende Einstellungen:

- Einstellungen in der **pppDialProfileTable**:
  Hier sind die beiden Variablen **BapNumber** und **BapLkType** mit bestimmten Werten zu versehen:

- Für **BapNumber** müssen Sie eine nur diesem Router zugeordnete Rufnummer angeben. Diese wird dem Client für den "Callback" übermittelt.
- Für **BapLkType** muß der Wert *isdn* eingestellt sein.
- Die Werte der anderen Variablen hängen vom Umfeld der Zentralseite ab.

Konfiguration der pppExtIfTable

Die Konfiguration der Variable **pppExtIfBodMode** muß sowohl server- als auch clientseitig erfolgen. Sie kann im Setup Tool vorgenommen werden. Serverseitig muß darüber hinaus die Variable **pppExtIfDialProfileIndex** konfiguriert werden.

- Serverseitige Einstellungen:
  - Die Variable **pppExtIfBodMode** in der **pppExtIfTable** muß den Wert *bap_server* haben. Dazu können Sie den Wert für den entsprechenden WAN-Partner im Setup Tool einstellen. Dies geschieht im Menü ***WAN-PARTNER*** ➧ **ADD/EDIT** ➧ ***ADVANCED SETTINGS*** ➧ ***EXTENDED INTERFACE SETTINGS (OPTIONAL)*** mit der Einstellung **Mode** = *BAP, Dialup Server Mode*.
    Alternativ können SIe den Wert über die SNMP-Shell einstellen.
  - Die Variable **pppExtIfDialProfileIndex** muß als Wert die Indexnummer des Eintrags in der **pppDialProfileTable** annehmen, dessen Einstellungen verwendet werden sollen. Diesen Wert können Sie nicht im Setup Tool einstellen.
- Clientseitige Einstellungen:
  Die Variable **pppExtIfBodMode** in der **pppExtIfTable** muß den Wert *bap_client* haben.
  Dazu ist im Menü ***WAN-PARTNER*** ➧ **ADD/EDIT** ➧ ***ADVANCED SETTINGS*** ➧ ***EXTENDED INTERFACE SETTINGS (OPTIONAL)*** der Wert des Felds **Mode** auf *BAP, Dialup Client Mode* zu setzen.

Grundsätzlich muß auf beiden Seiten Kanalbündelung wie im Handbuch Ihres Routers beschrieben aktiviert sein (***WAN PARTNER*** ➧ **ADD/EDIT** ➧

ADVANCED SETTINGS, **Channel Bundling** = *dynamic* oder *static*, **Total Number of Channels** *>1*).

Wenn die Einwahlauthentisierung über einen RADIUS-Server erfolgt, müssen bei der Konfiguration des RADIUS-Servers die BinTec-spezifischen Attribute verwendet werden. Dazu muß in der Users-Datei ein Eintrag angelegt werden, der die notwendigen Einträge in der **pppExtIfTable** erzeugt.

3.10 V.120

V.120 wird verwendet, um sich mit einem Mobiltelefon bei einem Router einzuwählen. Für die Verbindung des Mobiltelefons zur Schaltstelle des Telefon-Providers wird HSCSD verwendet, für die ISDN-Verbindung vom Telefon-Provider zum Router V.120. Damit erfüllt V.120 weitgehend die gleichen Zwecke wie V.110, ermöglicht allerdings höhere Transfergeschwindigkeiten.

Um V.120 für eingehende Rufe zu verwenden, ist keinerlei spezielle Konfiguration notwendig: Der Router erkennt das Protokoll automatisch und behandelt die Pakete entsprechend. Allerdings kann der Router seinerseits nicht unter Verwendung von V.120 ein Mobiltelefon anrufen; dies ist mit V.110 möglich.

Wenn Sie den Router an einer Nebenstellenanlage betreiben, kann es vorkommen, daß die Telefonanlage den Dienst verfälscht, mit dem ein Ruf eingeht. Für diesen Fall kann im Menü ***WAN*** ➧ ***INCOMING CALL ANSWERING*** eine MSN (Multiple Subscriber Number) fest für den V.120-Dienst vergeben werden. Alle Rufe, die auf dieser Rufnummer eingehen, werden dann als V.120-Rufe behandelt.

Wenn Sie auf Ihrem Router einen WAN-Partner anlegen wollen, der ausschließlich auf V.120-Rufe reagiert, so können Sie dies bei der Konfiguration dieses WAN-Partners in ***WAN PARTNER*** ➧ **ADD** entsprechend einstellen: Setzen Sie den Wert für das Feld **Encapsulation** auf *Async PPP over V.120 (HSCSD)*. Bedenken Sie aber, daß über dieses Interface dann ausschließlich V.120-Verbindungen möglich sind.

3.11 Multi-NAT (Network Address Translation)

System-Software Release 6.2.2 bietet eine Erweiterung der NAT-Implementierung, die die NAT-Konfiguration für Netze mit mehr als einer externen IP-Adresse erleichtert. Zuvor konnte lediglich auf einzelne IP-Adressen umgesetzt werden, und die Umsetzung mehrerer IP-Adressen bedeutete einen erhöhten Konfigurationsaufwand. System-Software Release 6.2.2 führt zwei neue Variablen ein, **ExtMask** in der **ipNat Out Table** und **IntMask** in der **IP NatPresetTable**. Diese ermöglichen es, ganze IP-Netze umzusetzen. Dies ist relevant, wenn Sie von Ihrem Provider mehr als eine IP-Adresse zugewiesen bekommen. Mithilfe der neuen Variablen können z. B. die IP-Adressen eines externen IP-Adreß-Pools auf lokale Adressen des LAN übersetzt werden. Dabei muß sichergestellt sein, daß die IP-Adressen, die der Router aufgrund der eingegebenen Netzmaske errechnet, auch tatsächlich im Adreßbereich des LAN liegen.

Die Konfiguration kann im Setup Tool vorgenommen werden, die entsprechenden Menüs sind ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **EDIT** ➧ ***REQUESTED FROM OUTSIDE*** ➧ **ADD/EDIT** und ***REQUESTED FROM INSIDE*** ➧ **ADD/EDIT**.

Das Menü für eingehende Verbindungen sieht z. B. folgendermaßen aus:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IP][NAT][CONFIG][OUTSIDE][EDIT]: NAT - sessions from OUTSIDE MyRouter

  Service                     user defined
  Protocol                    any

  Remote Address
  Remote Mask


  External Address            2.3.4.0
  External Mask               255.255.255.240
  External Port               any

  Internal Address            192.168.1.0
  Internal Mask               255.255.255.240
  Internal Port               any

                   SAVE                                  CANCEL
```

Die Menüs des Setup Tools erlauben eine sehr präzise Konfiguration. Folgende Einstellungen können vorgenommen werden:

Feld	Bedeutung
Service	Dienst, der für Verbindungen zu einem definierten Host oder einer Gruppe von Hosts in einem LAN im Menü ***REQUESTED FROM OUTSIDE*** ➧ **EDIT/ADD** definiert wird. Dienst, für den die im Menü ***REQUESTED FROM INSIDE*** ➧ **EDIT/ADD** definierte IP-Adressen-Abbildung durchgeführt wird. Mögliche Werte: ■ *ftp* ■ *telnet* ■ *smtp* ■ *domain/udp* ■ *domain/tcp* ■ *http* ■ *nntp* ■ *user defined* (wenn Sie keinen der vordefinierten Dienste verwenden)

Feld	Bedeutung
Protocol	Nur bei **Service** = *user defined*. Definiert das Protokoll. Mögliche Werte: ■ *icmp* ■ *tcp* ■ *udp* ■ *gre* ■ *esp* ■ *ah* ■ *l2tp* ■ *any*
Remote Address	Optional. IP-Adresse des Hosts oder der Gruppe von Hosts im entfernten Netzwerk. Bei eingehenden Verbindungen werden nur Pakete dieses Hosts/dieser Gruppe angenommen.
Remote Mask	Netzmaske von **Remote Address** im entfernten Netzwerk. Die Angabe der Netzmaske stellt sicher, daß eingehende Verbindungen aus dem gesamten entfernten Netzwerk zugelassen werden.

Feld	Bedeutung
Remote Port	Nur im Menü ***REQUESTED FROM INSIDE*** ➧ **EDIT/ADD**. Nur bei **Service** = *user defined*. Definiert die Port-Nummer des Dienstes auf dem Host oder der Gruppe von Hosts im entfernten Netzwerk. Mögliche Werte: ■ *any* ■ *specify* ■ *specify range*
Remote Port: Port	Nur bei dem Wert *specify* für **Remote Port**. Port-Nummer des Dienstes auf dem entfernten Host.
Remote Port: Port to Port	Nur bei dem Wert *specify range* für **Remote Port**. Port-Nummernbereich der Dienste auf dem entfernten Host.
External Address	Externe IP-Adresse des BinTec-Routers für diese Schnittstelle. Bei einer externen IP-Netzadresse müssen Sie die externe Netzmaske entsprechend angeben.
External Mask	Netzmaske von **External Address**. Wenn Sie externe und interne IP-Netzadressen verwenden, müssen die Werte für **External Mask** und **Internal Mask** identisch sein.

Feld	Bedeutung
External Port	Nur bei **Service** = *user defined*. Definiert die Port-Nummer des Dienstes des BinTec-Routers für diese Schnittstelle. Mögliche Werte: ■ *any* ■ *specify* ■ *specify range* (nur im Menü ***REQUESTED FROM OUTSIDE*** ➧ **EDIT/ADD**)
External Port: Port	Nur bei dem Wert *specify* für **External Port**. Port-Nummer des Dienstes des BinTec-Routers für diese Schnittstelle.
External Port: Port to Port	Nur im Menü ***REQUESTED FROM OUTSIDE*** ➧ **EDIT/ADD**. Nur bei dem Wert *specify range* für **External Port**. Port-Nummernbereich der Dienste auf dem BinTec-Router für diese Schnittstelle.
Internal Address	IP-Adresse des internen Hosts oder der Gruppe von Hosts in einem Subnetz. Bei einer internen IP-Netzadresse müssen Sie die interne Netzmaske entsprechend angeben.
Internal Mask	Netzmaske von **Internal Address**. Wenn Sie externe und interne IP-Netzadressen verwenden, müssen die Werte für **External Mask** und **Internal Mask** identisch sein.

Feld	Bedeutung
Internal Port	Definiert die Port-Nummer des Dienstes auf dem internen Host oder der Gruppe von Hosts in einem Subnetz. Mögliche Werte: ■ *any* ■ *specify*
Internal Port: Port	Nur bei dem Wert *specify* für **Internal Port**. Port-Nummer des Dienstes auf **Internal Address**.

Tabelle 3-6: ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **EDIT** ➧ ***REQUESTED FROM OUTSIDE*** und ***REQUESTED FROM INSIDE*** ➧ **ADD/EDIT**.

Das Menü für ausgehende (***REQUESTED FROM INSIDE***) Verbindungen entspricht dem für eingehende(***REQUESTED FROM OUTSIDE***). Allerdings kann zusätzlich zu **Remote Address** und zur **Remote Mask** noch der **Remote Port** bestimmt werden (nur wenn Sie als **Service** *user defined* gewählt haben). Stellen Sie sicher, daß der WAN-Partner Pakete des entsprechenden Protokolls auch auf diesem Port annimmt.

3.12 Konfigurierbares ICMP-Verhalten

Ab System-Software Release 6.2.2 ist es möglich, die ICMP-Messages, die der Router sendet, in der **ipIcmpTable** zu konfigurieren. Das Default-Verhalten ist dabei im Vergleich zu früheren Versionen nicht geändert worden. Eine Änderung der Voreinstellungen sollten Sie nur bei Problemen mit dem ICMP-Verhalten Ihres Routers vornehmen.

Folgende ICMP-Messages können in der **ipIcmpTable** aktiviert oder deaktiviert werden (das Beispiel zeigt die Default-Konfiguration):

```
ipIcmpSourceQuench( rw):              enabled
ipIcmpTimeExceededTrans( rw):         enabled
ipIcmpTimeExceededFrag( rw):          enabled
ipIcmpDestUnreachFrag( rw):           enabled
ipIcmpDestUnreachHost( rw):           enabled
ipIcmpDestUnreachHostTcp( rw):        tcp_rst
ipIcmpDestUnreachProto( rw):          enabled
ipIcmpEchoReply( rw):                 enabled
ipIcmpMaskReply( rw):                 enabled
MyRouter:ipIcmp>
```

Eine Sonderstellung nimmt die Variable **ipIcmpDestUnreachHostTcp** ein: Sie modifiziert eine "ICMP Destination Unreachable"-Message so, daß die TCP-Verbindung durch ein entsprechendes Paket beendet wird. Dazu muß **ipIcmpDestUnreachHostTcp** auf den Wert *tcp_rst* gesetzt sein. Ist die Variable auf *icmp* gesetzt, wird lediglich eine "ICMP Destination Unreachable"-Message versendet. Wenn **ipIcmpDestUnreachHost** auf *disabled* gesetzt ist, wird diese Option ignoriert.

Wenn Sie von System-Software Release 6.2.2 BETA auf die finale Version von System-Software Release 6.2.2 aktualisieren, gehen Änderungen, die Sie in der **ipIcmpTable** vorgenommen haben, verloren. Sichern Sie Ihre Konfiguration vor der Aktualisierung und spielen Sie sie anschließend wieder ein.

3.13 RIP und OSPF deaktivierbar

BinTec-Router können Routen sowohl per RIP (Routing Information Protocol) als auch per OSPF (Open Shortest Path First; hierzu ist außer bei **X8500** eine zusätzliche Lizenz notwendig) berechnen. Sie können Ressourcen freigeben, indem Sie den RIP/OSPF-Prozeß deaktivieren. Dies ist sinnvoll, wenn weder RIP noch OSPF genutzt werden und wenn eine Synchronisierung des RIP/OSPF-Prozesses mit den Interface- bzw. Routing-Tabellen nicht notwendig ist.

Der Prozeß konnte bisher nur über die Konfiguration mehrerer Variablen entweder protokollspezifisch oder interface-spezifisch deaktiviert werden. Mit der

neuen Variablen **biboExtAdmProcRouted** ist dies nun auch global möglich, indem man deren Wert auf *disabled* setzt.

3.14 Automatische Kabelerkennung an X.21-Schnittstellen

Ab System-Software Release 6.2.2 werden die Kabeltypen an X.21-Schnittstellen automatisch erkannt, sofern entsprechende Kabel verwendet werden. Dementsprechend hat sich das Menü zur Konfiguration der Schnittstellen geändert. Das Beispiel zeigt das Menü eines seriellen Ports einer **X4300** (***SERIAL-WAN: CM-SERIAL, SERIAL*** ➧ ***UNIT 0: SERIAL***):

```
BinTec Router Setup Tool                        BinTec Communications AG
[SLOT 3 SERIAL]: Configure Serial Interface - Unit 0          MyRouter

     Cable Detection      interface & connector type

     Interface Type       V.35 (autodetected)
     Connector            dte (autodetected)


     Layer 2 Mode         auto

     Interface Leads      disabled

                    SAVE                 CANCEL

Use <Space> to select
```

Das Menü enthält die folgenden Felder:

Feld	Bedeutung
Cable Detection	Definiert, ob die verwendeten Schnittstellen- und Verbindungstypen automatisch erkannt (*autodetected*) oder manuell gesetzt werden sollen. Mögliche Werte: ■ *interface & connector type*: Schnittstellen- und Verbindungstypen werden automatisch erkannt. ■ *interface type*: Nur der Schnittstellentyp wird automatisch erkannt. Der Verbindungstyp muß manuell gesetzt werden. ■ *connector type*: Nur der Verbindungstyp wird automatisch erkannt. Der Schnittstellentyp muß manuell gesetzt werden. ■ *manual*: Sowohl Schnittstellen- als auch Verbindungstyp müssen manuell gesetzt werden.
Interface Type	Definiert den Schnittstellentyp des genutzten Ports. Wenn Sie den Wert *interface type* oder *interface & connector type* für das Feld **Cable Detection** wählen, wird der Schnittstellentyp automatisch erkannt. Der erkannte Wert wird angezeigt, z. B. ***V.35 (autodetected)***. Wenn Sie *connector type* oder *manual* für das Feld **Cable Detection** wählen, müssen Sie das Feld **Interface Type** manuell setzen. Mögliche Werte siehe Tabelle 3-8, Seite 43.

Feld	Bedeutung
Connector	Definiert den Verbindungstyp des genutzten Ports. Wenn Sie den Wert *connector type* oder *interface & connector type* für das Feld **Cable Detection** wählen, wird der Verbindungstyp automatisch erkannt. Der erkannte Wert wird angezeigt, z. B. ***dte (autodetected)***. Wenn Sie *interface type* oder *manual* für das Feld **Cable Detection** wählen, müssen Sie das Feld **Connector** manuell setzen. Mögliche Werte siehe Tabelle 3-9, Seite 44.
Speed	Nur für den Wert *dce* für das Feld **Connector**. Übertragungsrate der Verbindung. Mögliche Werte: ■ *2400 bit/s, 9600 bit/s, 14400 bit/s, 19200 bit/s, 38400 bit/s, 64000 bit/s* ■ *128 kbit/s, 256 kbit/s, 512 kbit/s* ■ *1 Mbit/s, 2 Mbit/s, 4 Mbit/s, 8 Mbit/s* ■ *custom*: Das Feld **Speed: Value (bit/s)** erscheint. Skalierbar von *2400 bit/s* bis *8 Mbit/s*. Der einzustellende Wert ist abhängig von Qualität und Länge des Kabels, vom Verbindungstyp und von der min./max. akzeptierten Geschwindigkeit auf der Gegenseite (DTE). Über eine kurze Distanz von bis zu 5 m und bei Verwendung von abgeschirmten Twisted-Pair-Kabeln sind bis zu 8 Mbit/s möglich. Standardwert: *64000 bit/s*

Feld	Bedeutung
Layer 2 Mode	Definiert den Wert des HDLC-Adreßfelds in gesendeten Kommando-Frames (Schicht 2). Mögliche Werte: ■ *auto* (Standardwert): Die für **Connector** getroffene Auswahl wird übernommen. In der Regel können Sie diese Einstellung übernehmen, z. B. auch bei Zugang zu einem öffentlichen Datennetz (z. B. Datex-P). ■ *dte:* Das Adreßfeld hat den Wert für DTE. ■ *dce:* Das Adreßfeld hat den Wert für DCE.
Interface Leads	Legt fest, ob der Router den Status der Schnittstellenleitung überprüft. Bei beiden Verbindungspartnern sollte der gleiche Wert eingestellt sein. Mögliche Werte: ■ *enabled:* Auf der Signalleitung (I bei X.21, CTS bei V.35) wird die Schicht-1-Signalisierung der Gegenstelle überprüft. Die Überprüfung beeinflußt die Variable **L1State** entsprechend. ■ *disabled* (Standardwert): Die Schicht-1-Signalisierung der Gegenstelle wird nicht überprüft, die physikalische Leitung ist immer "up". Bei dieser Einstellung sollten Sie die Schnittstellenleitung auf andere Weise überwachen, z. B. durch PPP-Keepalive.

Tabelle 3-7: ***X21[x]***

Das Feld **Interface Type** enthält die folgenden Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
unknown (autodetected)	Es ist kein Kabel an dem Port angeschlossen, oder das angeschlossene Kabel unterstützt die automatische Erkennung (autodetection) nicht.
none	Der Port wird nicht genutzt.
X.21 (term)	V.11 auf allen Leitungen, 120 Ohm Abschluß-widerstand an kritischen Leitungen.
V.35	V.35 auf kritischen Leitungen, V.28 auf unkriti-schen Leitungen.
V.36	V.11 auf kritischen Leitungen, V.10 auf unkriti-schen Leitungen.
X.21bis	V.28 auf allen Leitungen.
X.21 (not term)	Nicht terminiertes V.11 auf allen Leitungen.
RS-449	V.11 auf kritischen Leitungen, V.10 auf unkriti-schen Leitungen.
RS-530	V.11 auf kritischen Leitungen, V.10 auf unkriti-schen Leitungen.

Tabelle 3-8: **Interface Type**

Wenn Sie ein X.21-Kabel verwenden, das die automatische Erkennung unterstützt, wird automatisch der Wert *X.21 (term)* ausgewählt. Sollten Sie dennoch keine Terminierung wünschen, müssen Sie die automatische Erkennung deaktivieren und die Konfiguration von Hand vornehmen.

Das Feld **Connector** enthält die folgenden Auswahlmöglichkeiten:

Mögliche Werte	Bedeutung
unknown (autodetected)	Es ist kein Kabel an dem Port angeschlossen, oder das angeschlossene Kabel unterstützt die automatische Erkennung (autodetection) nicht.
dte	Die Pins sind als DTE-Schnittstelle belegt. Diese Einstellung ist z. B. notwendig, wenn der Router an ein öffentliches Datennetz wie Datex-P angeschlossen ist.
dce	Die Pins sind als DCE-Schnittstelle belegt.

Tabelle 3-9: **Connector**

3.15 Weekly Schedule (Dialup)

System-Software Release 6.2.2 bietet die Möglichkeit, für jeden Dialup-WAN-Partner einen Zugangsplan zu erstellen, der regelt, wann und für wie lange Verbindungen über dieses Interface aufgebaut werden können. Dieser Plan wird im Menü ***WAN PARTNER*** ➧ **ADD/EDIT** ➧ ***WEEKLY SCHEDULE*** eingerichtet. Dort haben Sie die Möglichkeit, die Überwachung zu aktivieren bzw. zu deaktivieren.

Wenn Sie die Überwachung aktivieren (**Surveillance** *on*), wird folgendes Menü angezeigt:

```
BinTec Router Setup Tool                          BinTec Communications AG
[WAN][ADD][SCHEDULE]: Weekly Schedule                              MyRouter

         Surveillance  on

 (S)un:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]
 (M)on:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]
 (T)ue:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]
 (W)ed:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]
 T(h)u:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]
 (F)ri:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]
 S(a)t:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]

                    SAVE                                  CANCEL

Use <Space> to select
Enter up to 4 time windows each day as [BB:BB-EE:EE] (B/E: begin/end at
hh:mm)
```

Für jeden Wochentag haben Sie die Möglichkeit, vier Zeitfenster zu definieren, in denen eine Verbindung mit diesem WAN-Partner aufgebaut werden kann. Wenn bei einer bestehenden Verbindung das Ende der konfigurierten Zeitspanne erreicht wird, wird die Verbindung beendet. Ein Wiederaufbau wird erst zugelassen, wenn das nächste Zeitfenster erreicht ist.

Wird die Überwachung zum ersten Mal aktiviert (der Default-Wert ist *off*), so ist für jeden Tag der Zeitraum von 00:00 bis 24:00 Uhr freigeschaltet, um uneingeschränkte Verbindungen sicherzustellen.

Die Buchstaben, die in den Abkürzungen für die Wochentage in Klammern gesetzt sind, können verwendet werden, um direkt zum gewünschten Tag zu gelangen. Drücken Sie einfach die entsprechende Taste auf der Tastatur.

Sollten Sie die Zugangsmöglichkeiten genauer festlegen wollen, so können Sie in der **isdnScheduleTable** auch mehr als vier Zeitfenster konfigurieren. Dabei ist folgendes zu beachten: Auch wenn in den MIB-Tabellen mehr als vier Zeitfenster definiert worden sind, werden im Setup-Tool lediglich die ersten vier angezeigt. Es erscheint eine Warnmeldung: Wenn Sie **SAVE** drücken, werden die Einträge in der MIB gelöscht und lediglich durch die vier im Setup Tool sichtbaren ersetzt.

3.16 CAPI Supplementary Services

Mit der System-Software Release 6.2.2, stellt BinTec Communications AG folgende Supplementary Services zur Verfügung:

- Hold/Retrieve (Halten/Wiederannehmen)
- ECT (Explicit Call Transfer, Vermitteln von Gesprächen)
- Call Forwarding (Rufumleitung)
- Call Deflection (Rufweiterleitung)

Die Supplementary Services werden in der Vermittlungsstelle des Telefonnetzbetreibers oder in einer zwischengeschalteten Telefonanlage ausgeführt.

4 Änderungen

- Funktionsumfang von **X1000**/**X1200** und **X3200** mit IPSec (Kapitel 4.1, Seite 47)
- S_2M-Konfiguration (Kapitel 4.2, Seite 48)
- X.25 PAD (Kapitel 4.3, Seite 52)
- Verbesserte Kompatibilität mit SNMP-Managern (Kapitel 4.4, Seite 52)
- Konfiguration serieller Schnittstellen (Kapitel 4.5, Seite 53)
- Zeitdarstellung beim `ps`-Befehl (Kapitel 4.6, Seite 53)
- Neue Option `-r` für `rtlookup` (Kapitel 4.7, Seite 53)
- Lösung für ADSL-Modem-Problem (Kapitel 4.8, Seite 54)

4.1 Funktionsumfang von X1000/X1200 und X3200 mit IPSec

Da die neue IPSec-Software aufgrund des erheblich erweiterten Funktionsumfangs sehr umfangreich ist, mußten für die IPSec-Versionen von System-Software Release 6.2.2 von **X1000** bzw. **X1200** sowie von **X3200** einige Änderungen bei den sonstigen Funktionen vorgenommen werden. Folgende Funktionen stehen in der IPSec-Version von System-Software Release 6.2.2 daher nicht mehr zur Verfügung:

- verschlüsselter ISDN-Login (`dhkeyd`, `icrypt`, `dhkey`)
- RIP (Routing Information Protocol) daemon (`routed`)
- Web Based Monitoring (`httpd`)
- Bridging (`bridged`, `bridgemux`)

Darüber hinaus stehen das Command-Line-Interface `cli.cmd` und die Debug-Funktion `profile` sowie die ISDN-Approval-Funktion `zul` nicht mehr zur Verfügung.

Beachten Sie, daß der H.323 Proxy und der H.323 Gatekeeper in der IPSec-Version von System-Software Release 6.2.2 nicht enthalten sein können.

4.2 S_2M-Konfiguration

Die Konfiguration eines S_2M- (PRI-)Anschlusses ist in zwei Punkten erweitert worden. Die Handhabung mehrerer PRI-Erweiterungskarten (z. B. in einer **X8500**) ist dadurch erleichtert und die Kompatibilität mit speziellen Dienstanbietern sichergestellt worden.

4.2.1 Statusanzeige

Das Menü zur Konfiguration eines S_2M- Anschlusses enthält zusätzlich zu den Feldern und Submenüs zur Konfiguration eine Statusanzeige.

Im folgenden Beispiel wird das Menü der ersten PRI-Schnittstelle in Steckplatz 5 (`SLOT 5 UNIT 0 ISDN S2M`) einer **X8500** dargestellt:

```
BinTec Router Setup Tool                        BinTec Communications AG
[SLOT 5 UNIT 0 ISDN S2M]: Configure ISDN S2M Interface        MyRouter

Status

    ISDN Switch Type     detected Euro ISDN S2M user profile (TE)
    Layer 1              active
    Layer 2              established
    License usage        1 PRI  (not used: PRI: 0, G.703: 0)

Configuration

    ISDN Switch Type     autodetect on bootup
    ISDN Line Framing    standard (CRC4)


    Incoming Call Answering >

                    SAVE                    CANCEL

Use <Space> to select
```

Der obere Teil des Menüs gibt Statusinformationen zu ISDN-Protokoll und Layer-Aktivität des PRI-Ports und zur Lizenzverwendung der Erweiterungskarte an. Das Feld **License usage** zeigt an, welche Lizenz für die aktuelle Konfiguration verwendet wird und wieviele der von Ihnen aktivierten Lizenzen auf dieser Erweiterungskarte noch zur Verfügung stehen (*not used)*. In unserem Beispiel sind alle vier PRI-Schnittstellen lizenziert und konfiguriert (*not used: PRI: 0, G.703: 0*). So würde eine PRI-Erweiterungskarte mit zwei PRI-Lizenzen und nur einer schon konfigurierten PRI-Schnittstelle anzeigen: *not used: PRI: 1, G.703: 0*. Weitere Details zu Statusinformationen erhalten Sie in Tabelle 4-1, Seite 51.

Die Felder unter **Status** können nicht modifiziert werden. Sie zeigen den aktuellen Status der PRI-Schnittstelle. Die Felder haben folgende Bedeutung:

Feld	Bedeutung
Status: ISDN Switch Type	Zeigt das aktuell gültige Protokoll dieses Ports und den Status der ISDN-Autokonfiguration. Mögliche Werte: ■ *autodetection is waiting to run*: Der Router wartet, bis Layer 1 aktiv wird. Dann wird die Autokonfiguration gestartet. ■ *autodetection is running*: Die ISDN-Autokonfiguration wird gerade durchgeführt. ■ *detected <any switch type name>*: Das angegebene Protokoll wurde durch die ISDN-Autokonfiguration erkannt und ist aktiv. ■ *<any switch type name>*: Zeigt das aktuell konfigurierte ISDN-Protokoll.
Status: Layer 1	Zeigt den physischen Zustand des PRI-Ports an. Mögliche Werte: ■ *active*: Layer 1 ist OK. ■ *no signal*: Möglicherweise kein Kabel oder keine Lizenz vorhanden. ■ andere Angaben: Defektes Kabel oder falscher Wert für **ISDN Line Framing**.
Status: Layer 2	Zeigt den Status des Layer-2-Protokolls LAPD des D-Kanals. Mögliche Werte: ■ *connecting*: Layer 2 ist nicht verbnden. ■ *established*: Layer 2 ist verbunden.

Feld	Bedeutung
Status: License usage	Zeigt, welche Lizenz diesem Port aktuell zugewiesen ist. Mögliche Werte: ■ *license missing*: Für das konfigurierte ISDN-Protokoll wird eine Lizenz benötigt, die nicht verfügbar ist. Alle verfügbaren Lizenzen werden gerade von anderen Ports der Erweiterungskarte genutzt. ■ *not used*: Für die aktuelle Konfiguration wird keine Lizenz benötigt (oder eine für diese Erweiterungskarte verfügbare Lizenz wird nicht genutzt). ■ *1 PRI*: Für diese Schnittstelle wird eine PRI-Lizenz verwendet. ■ *1 G.703*: Für diese Schnittstelle wird eine G.703-Lizenz verwendet.

Tabelle 4-1: ***PRI[x]***: Statusinformationen

4.2.2 Channel Selection

Um die Kompatibilität auch mit speziellen Dienstanbietern zu gewährleisten, ist für den **ISDN Switch Type** *Euro ISDN S2M user profile (TE)* eine weitere Option vorgesehen: Wenn Sie den Switch Type entsprechend setzen, können Sie einen Wert für die neue Variable **Channel Selection** wählen. Diese definiert, wie der B-Kanal für einen abgehenden Ruf ausgewählt wird. Die möglichen Werte sind:

- *standard (any channel)*: (Voreinstellung) Das (TK-)Netz wählt den zu verwendenden Kanal.

- *no channel identification*: System-Software Release 6.2.2 sendet keine IE-Kanalidentifizierung (IE=information element). Das (TK-)Netz wählt den zu verwendenden Kanal.
- *submit preferred channel*: System-Software Release 6.2.2 wählt den zu verwendenden Kanal und signalisiert diesen dem (TK-)Netz.

In aller Regel können Sie den Default-Wert eingestellt lassen. Lediglich in wenigen Sonderfällen ist eine Anpassung der Einstellung notwendig. Wenden Sie sich an Ihren Provider, um zu erfahren, ob ein spezieller Wert eingestellt werden muß.

4.3 X.25 PAD

Die X.25-PAD-Funktionalität steht lediglich dann zur Verfügung, wenn die Verbindung über ein asynchrones Layer-1-Protokoll (*V.110* oder *Modem*) aufgebaut wird. Dabei war es bisher notwendig, einen eigenen WAN-Partner mit dem entsprechenden Protokoll einzurichten. Darüber hinaus mußte eine MSN für den X.25-PAD-Dienst reserviert werden. Eine simultane Verwendung von X.25 und X.25 PAD auf einem Interface war daher nicht möglich.

Die Erkennung des Layer-1-Protokolls ist automatisiert worden. Wenn das tatsächlich verwendete Layer-1-Protokoll einer Verbindung mit einem beliebigen X.25-WAN-Partner ein asynchrones ist, wird automatisch X.25 PAD aktiviert. Anderenfalls wird X.25 native verwendet. Die Notwendigkeit der Bindung einer MSN ausschließlich auf den X.25-PAD-Dienst entfällt.

4.4 Verbesserte Kompatibilität mit SNMP-Managern

Für die Variable **biboAdmSnmpVersion** sind drei neue Werte entstanden, *version1p1*, *version1p1_compat* und *version1p1_auto*. Mit der Version 1p1 ist

die Kompatibilität der BinTec SNMP-Implementierung mit SNMP-Managern wie HP OpenView stark verbessert worden.

Beachten Sie, daß ab System-Software Release 6.2.2 die Default-Einstellung *version1p1_auto* ist. In dieser Einstellung wird Version 1p1 verwendet, wenn dies möglich ist. Ansonsten wird Version 1p1 im Kompatibilitätsmodus (*version1p1_compat*) verwendet.

Wenn Sie SNMP-Manager wie HP OpenView verwenden, sollten Sie den Wert von **biboAdmSnmpVersion** in bereits bestehenden Konfigurationen ändern und *version1p1_auto* einstellen.

4.5 Konfiguration serieller Schnittstellen

In System-Software Release 6.2.2 hat es Änderungen der MIB-Tabellen gegeben, die die Konfiguration serieller WAN-Schnittstellen betreffen. Daher kann es beim Update auf System-Software Release 6.2.2 dazu kommen, daß sich die Konfiguration der Schnittstellen ungewollt ändern.

Nach einem Update auf System-Software Release 6.2.2 sollten Sie die Konfiguration entsprechende Schnittstellen überprüfen und ggf. wiederherstellen.

4.6 Zeitdarstellung beim Kommando `ps`

Bei Verwendung des Befehls `ps` auf der SNMP Shell erfolgen alle Zeitangaben (`time`, `ktime`, `utime`) nun auf die Hundertstel Sekunde genau.

4.7 Neue Option `-r` für `rtlookup`

Wenn das Default-Interface für ein zu routendes Paket inaktiv (`dormant`, `down` oder `blocked`) war, es aber ein Backup-Interface für dieses Paket gab, war es bisher nicht möglich, mit dem Befehl `rtlookup` dieses Backup-Interface ange-

zeigt zu bekommen. Mit der Option `-r` wird dieses nun angezeigt, wenn es verwendet wird.

4.8 Lösung für ADSL-Modem-Problem

Alcatels Implementierung von PPTP/GRE (Point to Point Tunnelling Protocol/Generic Routing Encapsulation) kann zu fehlerhaften "Acknowledgement Numbers" und damit zu blockierten PPTP-Interfaces führen.

Folgender Workaround ist implementiert: Es gibt nun einen konfigurierbaren Timer (**pptpProfileMaxBlockTime**, der Wert wird in Millisekunden bis *10000* eingegeben), nach dessen Ablauf eine blockierte PPTP-Verbindung und die zugehörige Kontrollverbindung über den TCP Port 1723 beendet wird. Andernfalls könnten Versuche, die Verbindung zur Alcatel-Gegenstelle wieder aufzunehmen, scheitern.

5 Behobene Fehler

System-Software Release 6.2.2 korrigiert eine Reihe von Fehlern, die im Release 6.1.2 aufgetreten sind:

5.1 Schwachstelle in der SNMP-Implementierung

Unter System-Software 6.1.2 waren BinTec-Router anfällig für eine Schwachstelle des SNMP-Protokolls im Zusammenhang mit der Verarbeitung von SNMP-Requests. Unter bestimmten Umständen konnten unsere Geräte unter Ausnutzung dieser Schwachstelle zum Absturz bzw. zum Reboot gebracht werden.

Weitere Informationen sowie eine Beschreibung, wie man die Schwachstelle umgehen kann, finden SIe hier:
http://www.cert.org/advisories/CA-2002-03.html.

Das Problem ist gelöst worden.

5.2 SNMP-Shell

In der SNMP-Shell wurde beim Einloggen mit einer nicht vorgesehenen Bezeichnung für eine SNMP-Community (`admin`, `read`, `write` sind vorgesehene Werte) eine endlose Tabelle mit Nullen angezeigt.

Das Problem ist gelöst worden. Es wird jetzt eine Fehlermeldung ausgegeben, daß die eingegebene Community nicht existiert.

5.3 Absturz durch Syslog-Level-Debug

Wenn das Syslog-Level des Routers auf den Wert *debug* gestellt war, stürzte das System ab, sobald All-Zero-Pakete eintrafen. Dieses Problem wurde von einem Fehler in den Syslog-Messages hervorgerufen.

Das Problem ist gelöst worden.

5.4 IPSec und Backroute Verification

Unter Umständen kam es vor, daß IPSec-Pakete von der Funktion der "Backroute Verification" ausgesondert wurden.

Dieses Problem wurde davon verursacht, daß als Quell-Interface eines IPSec-Paketes dasjenige Interface angenommen wird, von dem das ursprüngliche Pa-

ket stammt. Wenn das IPSec-Paket dann über ein anderes Interface geroutet wurde als das Quell-Interface (IPSec-Pakete werden über alle verfügbaren Interfaces geroutet), kam es zu einer Kollision mit der "Backroute Verification".

Das Problem ist gelöst worden. IPSec-Pakete können daher in jedem Fall über beliebige Interfaces geroutet werden.

5.5 Closed User Group

Wenn bei einem Dienstanbieter eine Geschlossene Benutzergruppe eingetragen wurde, um anfallende ISDN-Rufe zu kontrollieren, konnte es dazu kommen, daß die Rufe nicht zugelassen wurden. Dies geschah, wenn die Informationen über die Mitglieder der Benutzergruppe nach wie vor vom Dienstanbieter übermittelt, aber im Router ausgewertet werden sollten. Der Router wertete Informationen falsch aus, so daß Rufe der Benutzergruppe nicht mehr erkannt und daher abgelehnt wurden.

Das Problem ist gelöst worden. Die Informationen zur Benutzergruppe werden korrekt verarbeitet.

5.6 Path MTU Discovery und IP-Accounting

PMTU (Path Maximum Transfer Unit) Discovery war nicht funktionstüchtig, wenn gleichzeitig IP-Accounting auf einem Router aktiviert war.

Dieses Problem wurde davon verursacht, daß der PMTU-Discovery-Mechanismus nicht davon ausgeht, daß fragmentierte Pakete auf der Strecke (z. B. aufgrund von NAT oder Access-Control) zusammengefügt werden. Daher kommt es zu Problemen mit dem Dont-Fragment-Bit, das verwendet wird, um kleinere Einheiten als die errechnete PMTU zu markieren.

Das Problem ist gelöst: Das Dont-Fragment-Bit wird nun beim Zusammenfügen der Paketfragmente gelöscht.

5.7 Daten im Flash-ROM beschädigt

Beim Trennen oder Herstellen der Stromversorgung von **X8500** und **X4000** konnte es zu einer Beschädigung der Daten im Flash-Speicher kommen.

Das Problem ist gelöst worden. Gültige Daten werden durch Sector-Lock-Bits geschützt.

5.8 LEDs bei X4E-3BRI-Erweiterungskarte

Bei der X4E-3BRI-Erweiterungskarte waren in der Hardware-Revision 1.2 die rote und die grüne LED vertauscht worden, so daß sich das Signalverhalten der LEDs nicht mit der Beschreibung in der Dokumentation deckte.

Das Problem ist gelöst worden. Der Treiber der LEDs paßt das Signalverhalten der LEDs entsprechend an.

5.9 Logik-Update

Bei einem Logik-Update konnte es passieren, daß die MAC-Adresse des Ethernet-Interfaces, die Seriennummer des Routers sowie ein Teil der Konfiguration gelöscht wurden.

Dieses Problem ist gelöst worden. Die genannten Sektoren bleiben nun unangetastet, und es werden keine Daten überschrieben.

5.10 IP- und Bridge-Menüs im Frame Relay

Die Submenüs ***IP*** und ***BRIDGE*** waren vom Menü ***FR*** ➧ ***MULTIPROTOCOL OVER FRAME RELAY*** ➧ **ADD/EDIT** nicht anzusteuern.

Das Problem ist gelöst worden. Die Menüs lassen sich wieder ansteuern und die darin enthaltenen Einstellungen wieder konfigurieren.

5.11 Kompatibilität zwischen System-Software Release 6.2.2 und älterer Software

Es war nicht möglich, nach einmal erfolgtem Update auf System-Software Release 6.2.2 wieder auf ein älteres Release umzusteigen.

Dieses Problem wurde vom Schreibschutz von System-Software Release 6.2.2 hervorgerufen. Ältere Software-Versionen sind nicht mehr in der Lage, von der neueren Software angelegte Daten zu modifizieren.

Das Problem ist gelöst worden. Der BOOTmonitor und die Update-Shell überprüfen die Software-Version, und nur Software der Version 6.2.x wird geschützt.

5.12 RADIUS-Attribut NAS-Port

Es konnte vorkommen, daß sich eine Accounting-Start-Anfrage auf einem anderen NAS-Port bezog als die Accounting-Stop-Anfrage. Dies führte dazu, daß die Verbindung für das Accounting nicht beendet wurde.

Das Problem ist gelöst worden. Die Accounting-Stop-Anfrage bezieht sich nun auf den richtigen NAS-Port. Das Accounting wird dementsprechend gestoppt.

6 Bekannte Fehler

Unter System-Software Release 6.2.2 treten derzeit noch einige Fehler auf. Wir sind bemüht, diese so schnell wie möglich zu beheben. Sobald Verbesserungen an der Software vorgenommen worden sind, werden diese auf unserem Webserver zur Verfügung stehen. Bitte informieren Sie sich auf www.bintec.de über Software-Updates.

Folgende Fehler treten derzeit noch auf:

- DSL-LED (Kapitel 6.1, Seite 60)
- Beenden einer DSL-Verbindung (Kapitel 6.2, Seite 61)
- PAP-Authentisierung mit einem ACE Radiusserver (Kapitel 6.3, Seite 61)
- Falsche Netzmaske bei NAT-Einträgen (Kapitel 6.4, Seite 61)
- Konfiguration von MPPC (Kapitel 6.5, Seite 62)
- Kompression und Verschlüsselung (Kapitel 6.6, Seite 62)
- V.90-Einwahl mit Acer-Modems (Kapitel 6.7, Seite 62)
- Windows 2000 und 128 bit MPPE (Kapitel 6.8, Seite 62)
- IPSec (Kapitel 6.9, Seite 63)

6.1 DSL-LED

Die Deutsche Telekom AG trennt eine DSL-Verbindung im allgemeinen alle 24 Stunden. Bei der Wiederherstellung der Verbindung kann es vorkommen, daß die DSL-LED eines BinTec-Routers nicht aufleuchtet. Ein erneuter Verbindungsaufbau behebt dieses Problem.

6.2 Beenden einer DSL-Verbindung

Startet man einen BinTec-Router neu, indem man in der SNMP-Shell `cmd=reboot` eingibt, so kann es vorkommen, daß eine bestehende DSL-Verbindung nicht terminiert wird. Es empfiehlt sich, die Verbindung von Hand zu terminieren, zum Beispiel, indem man das entsprechende Interface administrativ deaktiviert und dann wieder aktiviert. Sie können dies im Menü ***MONITORING AND DEBUGGING*** ➧ ***INTERFACES*** tun.

6.3 PAP-Authentisierung mit einem ACE Radiusserver

Wenn ein Windows-PC eine PAP-Authentisierungsanfrage an einen ACE-Radiusserver sendet, wird diese vom Router an den Server weitergeleitet. Nach kurzer Zeit (weniger als zwei Sekunden) sendet der PC eine erneute Anfrage. Der Router leitet auch diese Anfrage weiter, löscht aber dabei die erste. Wenn vom Radiusserver die Freigabe aufgrund der ersten Anfrage erfolgt, kann der Router diese Freigabe nicht mehr zuordnen und die Authentisierung scheitert.

6.4 Falsche Netzmaske bei NAT-Einträgen

Wenn man im Setup Tool einen neuen Eintrag in der **ipNatPresetTable** erstellt (im Menü ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **EDIT** ➧ ***REQUESTED FROM OUTSIDE*** ➧ **ADD**), werden in dem neuen Eintrag die Defaultwerte für **External Mask** und **Internal Mask** vertauscht. Wenn die Werte nicht geändert werden, entsteht u. U. eine nicht funktionsfähige Konfiguration. Werden beide Werte richtig eingegeben, so werden die falschen Defaultwerte überschrieben, und es kommt zu keinen Problemen.

6.5 Konfiguration von MPPC

MPPC kann nicht im Setup Tool aktiviert werden. MPPC kann jedoch aktiviert werden, indem man in der SNMP-Shell den Wert für **Compression** in der **biboPPPTable** auf *MPPC* setzt.

Durch Abspeichern des WAN-Partners im Setup Tool werden alle Werte der MIB-Tabelle überschrieben. Achten Sie darauf, daß Sie den WAN-Partner, für den Sie auf dem oben beschriebenen Weg die MPPC-Kompression aktiviert haben, nicht erneut im Setup Tool abspeichern.

6.6 Kompression und Verschlüsselung

Beim Einsatz von Ressourcenmodulen, die mit einem HiFn-Chip ausgestattet sind (XTR-Enc und XTR-VPN), ist die Kombination von MPPC (Datenkompression) und MPPE (Datenverschlüsselung) nicht funktionsfähig.

6.7 V.90-Einwahl mit Acer-Modems

Acer-Modems können sich nicht mit V.90 bei einem BinTec-Router einwählen, wenn dieser so konfiguriert ist, daß er ausschließlich V.90-Rufe annimmt.

6.8 Windows 2000 und 128 bit MPPE

Verbindungen eines BinTec-Routers und eines PC mit Windows 2000 können nicht mit 128 bit MPPE verschlüsselt und gleichzeitig mit MS-CHAP V1 authentisiert werden. Verwenden Sie MS-CHAP V2 zur Authentisierung.

6.9 IPSec

Im Zusammenhang mit der BinTec-IPSec-Lösung treten derzeit noch einige Probleme auf. Diese beeinträchtigen jedoch nicht die grundlegende IPSec-Funktionalität.

6.9.1 Nicht gelöschte Einträge in der Trafficlist

Wenn man einen IPSec-Peer im Setup Tool löscht, werden die Traffic-Einträge für diesen Peer nicht mitgelöscht. Das kann zu Problemen bei der Neukonfiguration eines Peers führen, da diesem unter Umständen die "verwaisten" Einträge zugeordnet werden.

Wenn Sie einen Peer löschen, sollten Sie die entsprechenden Einträge in der Trafficlist manuell entfernen.

6.9.2 IPSec-Daemon

Wenn die IPSec-Konfiguration eines BinTec-Routers geändert wird, wird der IPSec-Daemon neu initialisiert, damit die Änderungen wirksam werden können. Das geschieht auch, wenn man der Konfiguration einen weiteren Peer hinzufügt. Dadurch werden alle bestehenden Tunnel vorrübergehend abgebaut, und es kann bis zum Ablauf der Phase-2-Lifetime dauern, bis alle Tunnel wiederhergestellt sind.

6 Bekannte Fehler