Release Notes System-Software-Release 6.2.5 X-Generation

November 2002

System-Software-Release 6.2.5

Dieses Dokument beschreibt neue Funktionen, Änderungen, behobene und bekannte Fehler von System-Software-Release 6.2.5.

System-Software-Release 6.2.5 ist bisher in drei Versionen erschienen: Patch 1, Patch 2 und Patch 4. Diese Release Notes beziehen sich im allgemeinen auf alle drei Versionen. Wo eine Funktion oder eine Fehlerbehebung nur in Patch 4 zur Verfügung steht, ist dies entsprechend vermerkt.

Inhaltsverzeichnis

1 Einleitung

Mit System-Software-Release 6.2.5 stellt BinTec ein neues Element des BinTec-Sicherheitskonzepts vor: die Stateful Inspection Firewall (SIF). Darüber hinaus finden sich in diesem Release weitere neue Funktionen sowie eine Reihe von Problembehebungen.

1.1 Aktualisierung der System-Software

Um Ihren Router auf System-Software-Release 6.2.5 zu aktualisieren, gehen Sie folgendermaßen vor:

- Laden Sie System-Software-Release 6.2.5 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 6.2.5 aktualisieren wollen, müssen Sie zunächst den BOOTmonitor und die Logik(en) Ihres Gerätes aktualisieren:

- Aktualisieren Sie Ihre Software mit dem 6.1.2 BLUP (BinTec Large Update).
  Dieses enthält alle notwendigen Dateien.
- Wenn Sie das BLUP eingespielt haben, aktualisieren Sie, wie im Handbuch Ihres Routers beschrieben, auf System-Software-Release 6.2.5.

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.

1.1.1 Aktualisierung der Modemlogik

Für die Verwendung von Modemmodulen auf einem Router der **X4000-Familie** oder auf **X8500** unter System-Software-Release 6.2.5 ist es notwendig, die Logik der Modemmodule zu aktualisieren. Sie können die notwendigen Dateien von unserem Webserver (www.bintec.de) herunterladen. Wie Sie die Aktualisierung der Modemlogik vornehmen, erfahren Sie in Kapitel 2.7, Seite 47.

2 Neue Funktionen

BinTec hat seit dem Release 6.2.2 den Funktionsumfang der Router der X-Generation um folgende Funktionen erweitert:

- Stateful Inspection Firewall (Kapitel 2.1, Seite 9)
- IPSec-Callback (Kapitel 2.2, Seite 22)
- PPTP-Passthrough (Kapitel 2.3, Seite 28)
- Bündelung von PRI-Timeslots zu Hyperchannels (Kapitel 2.4, Seite 29)
- Erweiterung der RIP-Implementierung (Kapitel 2.5, Seite 34)
- Zeitgesteuerte Ausführung von Shell-Befehlen (Kapitel 2.6, Seite 45)
- Modem-Update (Kapitel 2.7, Seite 47)
- **X8500-S3** (Kapitel 2.8, Seite 47)

2.1 Stateful Inspection Firewall

Mit einer Stateful Inspection Firewall (SIF) ergänzt BinTec den Funktionsumfang von System-Software-Release 6.2.5 um eine aktuelle Sicherheitsfunktion.

Zusätzlich zur sogenannten statischen Paketfilterung hat eine SIF durch dynamische Paketfilterung einen entscheidenden Vorteil: Die Entscheidung, ob ein Paket weitergeleitet wird, kann entweder aufgrund von Quell- und Zieladressen oder Ports gefällt werden. Oder sie kann mittels dynamischer Paketfilterung aufgrund des Zustands (*state*) der Verbindung zu einem Partner gefällt werden. Es können also auch solche Pakete weitergeleitet werden, die zu einer bereits aktiven Verbindung gehören. Dabei akzeptiert die SIF auch Pakete, die zu einer "Tochterverbindung" gehören: Die Aushandlung einer FTP- Verbindung findet z. B. über den Port 21 statt, der eigentliche Datenaustausch kann aber über einen völlig anderen Port erfolgen.

2.1.1 SIF und andere Sicherheitsfunktionen

BinTecs Stateful Inspection Firewall fügt sich wegen ihrer einfachen Konfiguration gut in die bestehende Sicherheitsarchitektur der BinTec-Router ein. Systemen wie Network Address Translation (NAT) und IP Access Lists (IPAL) gegenüber ist der Konfigurationsaufwand der SIF sehr gering.

Da SIF, NAT und IPAL gleichzeitig im System aktiv sind, muß man auf mögliche Wechselwirkungen achten: Wenn ein beliebiges Paket von einer der Sicherheitsinstanzen verworfen wird, so geschieht dies unmittelbar, d. h. es ist irrelevant, ob es von einer anderen Instanz zugelassen werden würde. Daher sollte man den eigenen Bedarf an Sicherheitsfunktionen genau analysieren.

Der wesentliche Unterschied zwischen SIF und NAT/IPAL besteht darin, daß die Regeln der SIF grundsätzlich global angewendet werden, d. h. nicht auf ein Interface beschränkt sind. Als Filterkriterien stehen Quelladresse bzw. Quellinterface und Zieladresse bzw. Zielinterface zur Verfügung.

Grundsätzlich werden aber die selben Filterkriterien auf den Datenverkehr angewendet wie bei NAT und IPAL:

- Quell- und Zieladresse des Pakets (mit einer zugehörigen Netzmaske), alternativ Filterung aufgrund des Interfaces bei der SIF
- Dienst (vorkonfiguriert, z. B. Echo, FTP, HTTP)
- Protokoll
- Portnummer(n)

Um die Unterschiede in der Paketfilterung zu verdeutlichen, folgt eine Aufstellung der einzelnen Sicherheitsinstanzen und ihrer Funktionsweise:

NAT

Eine der Grundfunktionen von NAT ist die Umsetzung lokaler IP-Adressen Ihres LANs in die globalen IP-Adressen, die Ihnen von Ihrem ISP zu gewiesen werden, und umgekehrt. Dabei werden zunächst alle von außen initiierten Verbindungen abgeblockt, d. h. jedes Paket, daß der Router nicht einer bereits

bestehenden Verbindung zuordnen kann, wird abgewiesen. Auf diese Art kann eine Verbindung lediglich von innen nach außen aufgebaut werden. Ohne explizite Genehmigungen wehrt NAT jeden Zugriff aus dem WAN auf das LAN ab.

IP Access Lists

Hier werden Pakete ausschließlich aufgrund der oben aufgeführten Kriterien zugelassen oder abgewiesen, d. h. der Zustand der Verbindung wird in der Regel nicht berücksichtigt.

SIF

Die SIF sondert alle Pakete aus, die nicht explizit oder implizit zugelassen werden. Dabei gibt es sowohl einen "deny", bei dem keine Fehlermeldung an den Sender des zurückgewiesenen Pakets ausgegeben wird, als auch einen "reject", bei dem der Sender über die Ablehnung des Pakets informiert wird.

Die Bearbeitung eingehender Pakete erfolgt folgendermaßen:

- Zunächst überprüft die SIF, ob ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann. Ist dies der Fall, wird es weitergeleitet. Kann das Paket keiner bestehenden Verbindung zugeordnet werden, wird überprüft, ob eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden). Ist dies der Fall, wird das Paket ebenfalls akzeptiert.
- Wenn das Paket keiner bestehenden und auch keiner zu erwartenden Verbindung zugeordnet werden kann, werden die SIF-Filterregeln angewendet: Trifft auf das Paket eine Deny-Regel zu, wird es abgewiesen, ohne daß eine Fehlermeldung an den Sender des Pakets geschickt wird; trifft eine Reject-Regel zu, wird das Paket abgewiesen und eine ICMP-Host-Unreachable-Meldung an den Sender des Paktes ausgegeben. Nur wenn auf das Paket eine Accept-Regel zutrifft, wird es weitergeleitet.
- Alle Pakete, auf die keine Regel zutrifft, werden nach Kontrolle aller vorhandenen Regeln ohne Fehlermeldung an den Sender abgewiesen.

2.1.2 Konfiguration

Im folgenden Kapitel werden die Menüs, in denen Sie die SIF konfigurieren, beschrieben. Weitere Informationen zu NAT und IP Access Lists finden Sie im Handbuch Ihres Routers.

BinTec hat die SIF mit einer benutzerfreundlichen Konfiguration versehen, in der die Regeln mittels definierbarer Aliase übersichtlich dargestellt und definiert werden können. Die Konfiguration erfolgt in ***IP*** ➧ ***STATEFUL INSPECTION***.

Das erste Menüfenster sieht z. B. folgendermaßen aus:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IP][STATEFUL INSPECTION]: Stateful Filters                      MyRouter

Stateful Inspection Filter List

Pos.     Source     Destination     Service     Action

  1      LAN_EN1    WAN_ISP         http        accept
  2      WAN_ISP    LAN_EN1         ftp         deny


   Use <Ctrl-u> to move filter up, <Crtl-d> to move filter down

          ADD         DELETE          SAVE          CANCEL
```

In der Liste dieses Menüfensters sind alle konfigurierten Filterregeln dargestellt. Die Abfolge der Filterregeln in der Liste ist relevant: Die Regeln werden der Reihe nach auf jedes Paket angewendet, bis eine Regel zutrifft. Kommt es zu Überschneidungen, d. h. trifft für ein Paket mehr als eine Regel zu, wird lediglich die erste Regel ausgeführt. Wenn also die erste Regel ein Paket zurückweist, während eine später es zuläßt, so wird es abgewiesen. Ebenso bleibt eine Deny-Regel ohne Auswirkung, wenn ein entsprechendes Paket zuvor von einer anderen Regel zugelassen wird.

Filterregel hinzufügen

Wenn Sie eine Filterregel für die SIF hinzufügen oder eine bestehende editieren wollen, können Sie dies im Menü ***IP*** ➧ ***STATEFUL INSPECTION*** ➧ **ADD/EDIT** tun:

```
BinTec Router Setup Tool                    BinTec Communications AG
[IP][STATEFUL INSPECTION][ADD]: Stateful Filter              MyRouter

Source                      ANY
Destination                 ANY
Edit Addresses>

Service                     any
Edit Service>

Action                      accept

                SAVE                    CANCEL
```

Die Felder des Menüs haben die folgende Bedeutungen:

Feld	Bedeutung
Source	Hier können Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets auswählen. Der Router liest die Liste bestehender WAN- und LAN-Interfaces aus und bietet diese als Voreinstellung an. Einen neuen Alias erstellen Sie in ***IP*** ➧ ***STATEFUL INSPECTION*** ➧ **ADD/EDIT** ➧ ***EDIT ADDRESSES***.

Feld	Bedeutung
Destination	Hier können Sie einen der vorkonfigurierten Alias für das Ziel des Pakets auswählen. Der Router liest die Liste bestehender WAN- und LAN-Interfaces aus und bietet diese als Voreinstellung an. Einen neuen Alias erstellen Sie in ebenfalls ***IP*** ➧ ***STATEFUL INSPECTION*** ➧ **ADD/EDIT** ➧ ***EDIT ADDRESSES***.
Service	Hier können Sie einen der vorkonfigurierten Dienste auswählen, dem das zu filternde Paket zugeordnet sein muß. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: ■ *ftp* ■ *telnet* ■ *smtp* ■ *dns* ■ *http* ■ *nntp* ■ *internet* ■ *netmeeting* Im Menü ***IP*** ➧ ***STATEFUL INSPECTION*** ➧ **ADD/EDIT** ➧ ***EDIT SERVICES*** können Sie weitere Dienste konfigurieren.

Feld	Bedeutung
Action	Hier wählen Sie die Aktion, die auf ein gefiltertes Paket angewendet werden soll. Die möglichen Werte sind: ■ *accept* ■ *deny* ■ *reject* Sowohl bei *reject* als auch bei *deny* wird das Paket abgewiesen; bei *deny* jedoch, ohne daß eine Fehlermeldung an den Sender des Pakets ausgegeben wird.

Tabelle 2-1: ***IP*** ➧ ***STATEFUL INSPECTION*** ➧ **ADD/EDIT**

Die vorkonfigurierten Dienste unter **Service** decken die wesentlichen Applikationen bereits ab. Zusätzlich sind drei weitere, komplexe Voreinstellungen verfügbar:

- *any*
  Eine Regel mit dieser Einstellung trifft auf jedes Paket zu, das zu einer Verbindung mit einem bestimmten Adreßalias gehört.
- *internet*
  Dieser Alias faßt folgende Dienste zusammen: *dns*, *http*, *http (SSL)*, *smtp*, *pop3*, *pop3 (SSL)*, *nntp*,*nntp (SSL)* sowie *echo*. Er dient vor allem einer einfachen Absicherung des üblichen Internet-Datenverkehrs.
- *netmeeting*
  Dieser Alias umfaßt alle Einstellungen, die zur Verwendung von Microsoft NetMeeting erforderlich sind.

Adreßalias hinzufügen

Wenn Sie einen weiteren Adreßalias anlegen oder einen bestehenden editieren wollen, können Sie dies im Menü ***IP*** ➧ ***STATEFUL INSPECTION*** ➧

ADD/EDIT ➧ ***EDIT ADDRESSES***. Die auf dem Router konfigurierten Interfaces werden angezeigt:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IP][STATEFUL INSPECTION][ADDRESSES]: Alias Addresses          MyRouter

Alias Address List:

  Alias            IP-Address         IP-Mask             Interface

  ANY               0.0.0.0           0.0.0.0              any
  LAN_EN1           ------            ------               en1
  LAN_EN1-SNAP      ------            ------               en1-snap
  WAN_DIALIN        ------            ------               dialin
  WAN_ISP           ------            ------               isp
  WAN_SI3-0         ------            ------               si3-0
  WAN_SI3-1         ------            ------               si3-1

            ADD             DELETE            EXIT
```

In diesem Fenster werden alle konfigurierten Aliase aufgelistet. Durch **ADD** oder die Auswahl eines bestehenden Eintrags gelangen Sie in das Menü ***IP*** ➧ ***STATEFUL INSPECTION*** ➧ **ADD/EDIT** ➧ ***EDIT ADDRESSES*** ➧ **ADD/EDIT**:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IP][STATEFUL INSPECTION][ADDRESSES][ADD]: Alias Addresses     MyRouter

Alias

Mode              interface

Interface         en1


                       SAVE               CANCEL
```

Das Feld **Interface** ist sichtbar, wenn Sie als Wert für **Mode** *interface* gewählt haben.

Wenn Sie unter **Mode** *address* gewählt haben, werden die Felder **IP-Address** und **IP-Mask** sichtbar

Die Felder des Menüs haben die folgenden Bedeutungen:

Feld	Bedeutung
Alias	Hier geben Sie einen Aliasnamen ein, den Sie einrichten wollen.
Mode	Hier geben Sie an, ob Sie eine IP-Adresse (*address*) oder ein Interface (*interface*) mit dem Alias bezeichnen wollen
IP-Address	Nur, wenn Sie für **Mode** den Wert *address* gewählt haben. Hier geben Sie die IP-Adresse ein, für die der Alias gelten soll.
IP- Mask	Nur, wenn Sie für **Mode** den Wert *address* gewählt haben. Hier geben Sie die zur IP-Adresse des Hosts gehörende Netzmaske ein.
Interface	Nur, wenn Sie für **Mode** den Wert *interface* gewählt haben. Hier wählen Sie das Interface aus, über das Pakete empfangen und gesendet werden. Sie können unter allen konfigurierten WAN-Partnern und LAN-Interfaces wählen.

Tabelle 2-2: ***IP*** ➧ ***STATEFUL INSPECTION*** ➧ **ADD/EDIT** ➧ ***EDIT ADDRESSES*** ➧ **ADD/EDIT**

Wird zur Konfiguration des Alias eine IP-Adresse verwendet, wird **Interface** automatisch auf *any* gesetzt; wird ein Interface angegeben, werden **IP-Address** und **IP-Mask** nicht dargestellt.

Dienstalias hinzufügen

Wenn Sie einen weiteren Dienstalias definieren oder einen bestehenden editieren wollen, können Sie dies im Menü ***IP*** ➧ ***STATEFUL INSPECTION*** ➧ **ADD/EDIT** ➧ ***EDIT SERVICES*** tun.

Es wird eine Liste von über 60 vorkonfigurierten Dienstaliasen angezeigt:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IP][STATEFUL INSPECTION][SERVICES]: Alias Services            MyRouter

Alias Service List

 Alias          Protocol      Port/Range     ICMP Type

 any            any                                                    =
 apple-qt       tcp           458/1                                    |
 auth           tcp           113/1                                    |
 bootp          tcp           67/2                                     |
 chargen        tcp           19/1                                     |
 clients_1      udp/tcp       1024/3975                                |
 clients_2      udp/tcp       32768/32768                              |
 daytime        tcp           13/1                                     |
 discard        tcp           9/1                                      |
 dns            tcp           53/1                                     |
 echo           icmp          any                                      |
 exec           tcp           512/1                                    v

     ADD               DELETE             EXIT
```

Durch **ADD** oder die Auswahl eines bestehenden Eintrags gelangen Sie in das Menü ***IP*** ➧ ***STATEFUL INSPECTION*** ➧ **ADD/EDIT** ➧ ***EDIT SERVICES*** ➧ **ADD/EDIT**:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IP][STATEFUL INSPECTION][SERVICES][ADD]: Alias Services       MyRouter

Alias

Protocol         icmp

ICMP Type        echo


                   SAVE               CANCEL
```

Das Feld **ICMP Type** ist sichtbar, wenn Sie unter **Protocol** *icmp* gewählt haben.

Wenn Sie unter **Protocol** *tcp*, *udp* oder *udp/tcp* gewählt haben, sind die Felder **Port** und **Range** sichtbar.

Die Felder des Menüs haben die folgenden Bedeutungen:

Feld	Bedeutung
Alias	Hier geben Sie einen Alias für den Dienst ein, den Sie konfigurieren wollen.
Protocol	Hier wählen Sie das Protokoll aus, auf dem der Dienst basiert. Es stehen 28 Protokolle zur Auswahl.
ICMP Type	Nur wenn Sie für **Protocol** den Wert *icmp* gewählt haben. Der Wert dieses Felds ist werkseitig auf *echo* gesetzt. Diese Einstellung deckt die sogenannten Pings ab.
Port	Nur wenn Sie für **Protocol** den Wert *tcp*, *udp/tcp* oder *udp* gewählt haben. Hier geben Sie den Port an, über den der Dienst läuft.
Port Range	Nur, wenn Sie für **Protocol** den Wert *tcp*, *udp/tcp* oder *udp* gewählt haben. Hier geben Sie an, wieviele Ports der Dienst verwendet. Mögliche Werte sind *1* bis *65535*. Wenn Sie keinen Wert eingeben, nimmt der Router den Wert *1* als Default an.

Tabelle 2-3: ***IP*** ➧ ***Stateful Inspection*** ➧ **ADD/EDIT** ➧ ***Edit Services*** ➧ **ADD/EDIT**

Syslog-Meldungen

Wenn eine der konfigurierten Regeln auf ein Paket zutrifft, wird je nach Konfiguration ein Syslog-Eintrag erzeugt. SIF-Syslogs werden auf den Syslog-Levels *info* und *debug* ausgegeben.

Die protokollierten Details unterscheiden sich wie in den folgenden Abschnitten dargestellt.

Info

Auf diesem Syslog-Level werden ausschließlich abgewiesene Verbindungen protokolliert. Die ausgegebenen Meldung gliedert sich wie folgt:

`SIF: <action> packet from <source> to <destination> with Service <service>.`

Quelle, Ziel und Service werden jeweils mit dem zugehörigen Alias angegeben, die Aktionen mit `Reject` bzw. `Ignore`.

Wenn mehr als 10 Pakete mit derselben Quelle und demselben Ziel innerhalb einer Sekunde abgewiesen worden sind, wird eine Warnung ausgegeben. Ausgegeben wird der Quellalias, der Zielalias sowie die Anzahl der in der letzten Sekunde abgewiesenen Pakete.

Debug

Auf diesem Syslog-Level werden folgende Ereignisse protokolliert:

- Annehmen eines Paketes
- Abweisen/Ignorieren eines Paketes
- Entfernen eines Eintrags aus der **ipSifRejectTable**
- Fragmentation Timeout
- Session Timeout

Im Debug-Modus werden nicht nur die Adress- bzw. Dienstaliase angezeigt, sondern ebenfalls die IP-Adressen, Portnummern und das Protokoll der entsprechenden Verbindung.

Die Ausgabe der Syslog-Meldungen erfolgt gemäß der allgemeinen Konfiguration im Menü ***System***.

Durch die Protokollierung der SIF-Aktivität im Debug-Modus wird u. U. eine große Anzahl an Meldungen erzeugt. In diesem Fall sollten Sie die Meldungen nicht auf der seriellen Konsole ausgeben lassen, da dies zu einer Beeinträchtigung des Zugriffs auf Ihren Router führen kann.

Informationen zur Einrichtung eines externen Log-Hosts finden Sie im Handbuch Ihres Routers.

SIF Reject Table

Für jede von der SIF abgewiesene Verbindung wird ein Eintrag in der **ipSifRejectTable** erzeugt. Diese ist nicht über das Setup Tool zugänglich. Die Einträge können als Grundlage für die Analyse möglicher Angriffe dienen.

Die **ipSifRejectTable** enthält folgende Variablen:

Variable	Bedeutung
Index	Die Indexnummer des Eintrags. Sie wird automatisch vergeben.
Source	Die Quell-IP-Adresse abgewiesener Pakete.
Destination	Die Ziel-IP-Adresse abgewiesener Pakete.
Rejects	Anzahl der abgewiesenen Pakete dieser Verbindung.
Silence	Zeit in Sekunden, während derer keine Pakete abgewiesen wurden.
PortLo	Niedrigster Port, an den abgewiesene Pakete adressiert waren.

Variable	Bedeutung
PortHigh	Höchster Port, an den abgewiesene Pakete adressiert waren.

Tabelle 2-4: **ipSifRejectTable**

Die Einträge in der **ipSifRejectTable** sind nicht statisch: Wenn für einen Eintrag 3600 Sekunden lang kein Paket abgewiesen wird, wird eine entsprechende Syslog-Nachricht ausgegeben und anschließend der Eintrag aus der Tabelle gelöscht.

2.2 IPSec-Callback

Um Hosts, die nicht über feste IP-Adressen verfügen, eine sichere Verbindung über das Internet zu ermöglichen, unterstützt BinTec seit dem Release 6.2.2 den DynDNS-Dienst. Dieser Dienst ermöglicht die Identifikation eines Peers anhand eines durch DNS auflösbaren Host-Namens. Die Konfiguration der IP-Adresse des Peers ist nicht notwendig.

Der DynDNS-Dienst signalisiert aber nicht, ob ein Peer wirklich online ist, und kann einen Peer nicht veranlassen, eine Internetverbindung aufzubauen, um einen IPSec-Tunnel über das Internet zu ermöglichen. Diese Möglichkeit wird mit dem IPSec-Callback geschaffen: Mit Hilfe eines direkten ISDN-Rufs bei einem Peer kann diesem signalisiert werden, daß man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den ISDN-Ruf veranlaßt, eine Verbindung aufzubauen. Dieser ISDN-Ruf verursacht (je nach Einsatzland) keine Kosten, da der ISDN-Ruf vom Router nicht angenommen werden muß. Die Identifikation des Anrufers durch dessen ISDN-Rufnummer genügt als Information, um einen Tunnelaufbau zu initiieren.

Um diesen Dienst einzurichten, muß zunächst im Menü ***WAN*** ➧ ***INCOMING CALL ANSWERING*** eine Rufnummer für den IPSec-Callback konfiguriert werden. Dazu steht für das Feld **Item** der neue Wert *IPSec* zur Verfügung. Dieser Ein-

trag sorgt dafür, daß auf diese Nummer eingehende Rufe an den IPSec-Dienst geleitet werden.

Die weitere Konfiguration erfolgt im Menü ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **APPEND/EDIT**. Dort findet sich das neue Feld **ISDN Callback**. Es kann die folgenden Werte annehmen:

Mögliche Werte	Bedeutung
disabled	Der ISDN-Callback ist deaktiviert. Der lokale Router reagiert weder auf eingehende ISDN-Rufe noch initiiert er ISDN-Rufe zum entfernten Router.
passive	Der lokale Router reagiert lediglich auf eingehende ISDN-Rufe und initiiert ggf. den Aufbau eines IPSec-Tunnels zum Peer. Es werden keine ISDN-Rufe an den entfernten Router abgesetzt, um diesen zum Aufbau eines IPSec-Tunnel zu veranlassen.
active	Der lokale Router setzt einen ISDN-Ruf an den entfernten Router ab, um diesen zum Aufbau eines IPSec-Tunnels zu veranlassen. Auf eingehende ISDN-Rufe reagiert der Router nicht.
both	Der Router kann auf eingehende ISDN-Rufe reagieren und ISDN-Rufe an den entfernten Router absetzen. Der Aufbau eines IPSec-Tunnels wird sowohl ausgeführt (nach einem eingehenden ISDN-Ruf) als auch veranlaßt (durch einen ausgehenden ISDN-Ruf).

Tabelle 2-5: **ISDN Callback**

Wenn Sie den IPSec-Callback für zwei Peers verwenden wollen, die beide mit dynamischen IP-Adressen operieren, müssen Sie den Wert *both* einstellen.

Je nachdem, welchen Wert Sie wählen, ändert sich das Menü erneut und ermöglicht die Eingabe der ISDN-Rufnummern für ein- bzw. ausgehende ISDN-Rufe für die Felder **IN** und **OUT**. Wenn Sie für **ISDN Callback** den Wert *both* gewählt haben, müssen Sie eine Nummer für eingehende ISDN-Rufe angeben und eine, die der Router wählt, um den entfernten Peer zum Aufbau eines IPSec-Tunnels zu veranlassen.

Bedenken Sie, daß hier immer die Nummer des entfernten Routers eingetragen wird. D. h daß für das Feld **IN** die Nummer angegeben wird, von der aus der entfernte Router den lokalen Router ruft (Calling Party Number), und für das Feld **OUT** die Nummer, unter der der lokale Router den entfernten Router ruft (Called Party Number).

Im allgemeinen werden die beiden Nummern bis auf die führende "0" identisch sein. Diese darf für das Feld **IN** nicht mit eingegeben werden.

Unter bestimmten Umständen (z. B. beim Betrieb des Routers an einer Telefonanlage mit Rufnummernunterdrückung)) kann es notwendig sein, unterschiedliche Nummern anzugeben. Fragen Sie den Systemadministrator nach den zu konfigurierenden Rufnummern.

Das Menü ***IPSec*** ➧ ***Configure Peers*** ➧ **ADD/EDIT** sieht folgendermaßen aus, wenn Sie den Callback in beiden Richtungen aktivieren:

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


     Description:    test-peer
     Peer Address:   test-peer.dyndns.org
     Peer IDs:       test-peer
     Pre Shared Key: **********
     ISDN Callback: both       IN: 91112345      OUT: 091112345



                           SAVE              CANCEL
```

Wenn Sie einen Callback für einen Peer eingerichtet haben, wird dieser stets ausgeführt. Bei aktivem Callback wird daher, sobald ein IPSec-Tunnel benötigt wird, der Peer durch einen ISDN-Ruf veranlaßt, diesen zu initiieren. Bei passivem Callback wird immer dann ein Tunnelaufbau zum Peer initiiert, wenn ein ISDN-Ruf auf der entsprechenden Nummer eingeht. Auf diese Weise wird sichergestellt, daß beide Peers erreichbar sind und die Verbindung über das Internet zustande kommen kann. Es wird lediglich dann kein Callback ausgeführt, wenn bereits SAs (Security Associations) vorhanden sind, der Tunnel zum Peer also bereits besteht.

Wenn ein Tunnel zu einem Peer aufgebaut werden soll, wird vom IPSec-Daemon zunächst das Interface aktiviert, über das der Tunnel realisiert werden soll. Sofern auf dem lokalen Router DynIPSec konfiguriert ist, wird dann die IP-Adresse propagiert und erst dann der ISDN-Ruf an den entfernten Router abgesetzt. Auf diese Art ist sichergestellt, daß der entfernte Router den lokalen auch tatsächlich erreichen kann, wenn er den Tunnelaufbau initiiert.

2.2.1 IPSec-Heartbeat

Um feststellen zu können, ob eine Security Association (SA) noch gültig ist oder nicht, hat BinTec einen IPSec-Heartbeat implementiert. Dieser sendet bzw. empfängt je nach Konfiguration Signale, bei deren Ausbleiben die SA als ungültig verworfen wird. Die Pakete, die der Router aufgrund dieser Signalisierung sendet und empfängt, werden nicht als IPSec-Pakete gezählt, d. h. eine SA bleibt nicht allein aufgrund des gesendeten oder empfangenen Heartbeats aktiv.

Auch der PPP-Shorthold wird durch gesendete Heartbeat-Pakete nicht zurückgesetzt.

Der Heartbeat wird in zwei der IPSec-Menüs konfiguriert:

- In ***IPSEC*** ➧ ***ADVANCED SETTINGS*** ➧ ***HEARTBEAT*** werden die Default-Parameter gesetzt.
- In ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** können bestimmte Default-Parameter für einzelne Peers angepaßt werden.

Das Menü ***IPSec*** ➧ ***Advanced Settings*** ➧ ***Heartbeat*** enthält die folgenden Felder:

Feld	Bedeutung
Heartbeat	Hier bestimmen Sie, in welcher Weise der Router mit Heartbeats verfährt. Mögliche Werte: ■ *none*: Der Router sendet und erwartet keinen Heartbeat, die Funktion steht nicht zur Verfügung. ■ *expect:* Der Router erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. ■ *send*: Der Router erwartet keinen Heartbeat vom Peer, sendet aber einen. In diesem Fall werden eingehende Heartbeat-Pakete als normale IPSec-Pakete behandelt und verlängern somit die SA-Lifetime. ■ *both*: Der Router erwartet einen Heartbeat vom Peer und sendet selbst einen.
Interval	Hier geben Sie an, in welchen Abständen der Router Heartbeats sendet bzw. erwartet. Der Wert wird in Sekunden angegeben.
Tolerance	Hier geben Sie ein, wieviele Heartbeats ausfallen dürfen, bevor eine SA verworfen wird.

Tabelle 2-6: ***IPSec*** ➧ ***Advanced Settings*** ➧ ***Heartbeat***

Im Menü ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT** kann die Art des Heartbeats für den jeweiligen Peer angepaßt werden. Es enthält lediglich das Feld **Heartbeat** mit den oben beschriebenen Werten. Zusätzlich findet sich dort der Wert *default*. In dieser Einstellung verwendet der Router für den Peer die

Einstellungen, die im Menü ***IPSec*** ➧ ***Advanced Settings*** ➧ ***Heartbeat*** konfiguriert wurden.

2.3 PPTP-Passthrough

Das für PPTP-Verbindungen genutzte erweiterte GRE-Protokoll (Generic Routing Encapsulation) arbeitet nicht portspezifisch, d. h. die PPTP-Verbindungen unterschiedlicher Hosts im gleichen LAN können zunächst einmal durch NAT (Network Address Translation) nicht voneinander getrennt werden. Pakete, die als Antwort auf eine Anfrage eines Hosts im LAN eingehen, können daher keinem bestimmten Zielhost zugeordnet werden.

Um mehreren PPTP-Endpunkten (Hosts) eine Verbindung zu einem VPN-Server über einen Router hinweg zu ermöglichen, hat BinTec zusätzlich zu NAT ein PPTP-Passthrough implementiert. Ähnlich wie beim NAT-Port-Mapping werden hierbei GRE Context Numbers einander zugeordnet: Der Router weist der internen GRE Context Number eines vom LAN her kommenden Pakets eine externe GRE Context Number zu und kann somit vom WAN kommende Antwort-GRE-Pakete einer bestimmten PPTP-Verbindung zuordnen. Nach dem Abbau der GRE-Verbindung wird die zugeordnete GRE Context Number wieder freigegeben.

Dieses Vorgehen funktioniert nur für ausgehende Verbindungen, d. h. es kann nach wie vor lediglich eine einzelne PPTP-Verbindung von außen nach innen aufgebaut werden. Die Zuordnung zu einem Host im LAN erfolgt über die NAT-Konfiguration, denn bei eingehenden PPTP-Paketen kann der Router die externe GRE Context Number nach wie vor keiner internen zuordnen. Es wird lediglich die externe IP-Adresse auf eine interne Adresse umgesetzt.

Beachten Sie, daß NAT entsprechend konfiguriert sein muß, um eingehende Verbindungen zu akzeptieren. Das gilt auch für eingehende PPTP-Verbindungen.

PPTP-Passthrough wird im Menü ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **EDIT** ein- oder ausgeschaltet: Für das Feld **PPTP Passthrough** kann entweder der Wert *yes* oder *no* gewählt werden. Wie NAT selbst erfolgt die Anwendung von PPTP-Passthrough Interface-spezifisch.

2.4 Bündelung von PRI-Timeslots zu Hyperchannels

Bisher konnten die Kanäle eines S_{2M}-Anschlusses lediglich mit PPP-Multilink auf Layer-2 gebündelt werden. BinTec hat dem die Möglichkeit hinzugefügt, Kanäle bereits auf dem physikalischen Layer zu bündeln. Darüber hinaus sind jetzt auch PPP-Multilink-Kanalbündel im Setup Tool frei konfigurierbar, d. h. die zur Verfügung stehenden Timeslots können zu mehreren PPP-Multilink-Kanalbündeln zusammengefaßt werden. Bisher war im Setup Tool nur ein einziges Kanalbündel mit allen Timeslots möglich.

Die in diesem Kapitel beschriebene Funktion steht nur für Festverbindungen (leased lines) zur Verfügung.

Zur Konfiguration der Kanalbündel ist es notwendig, im Menü der PRI-Schnittstelle den **ISDN Switch Type** *leased line, chan. B1..B31* einzustellen. Das neue Untermenü ***BUNDLE CONFIGURATION*** wird dadurch zugänglich. Im ersten Fenster sehen Sie eine Aufstellung der bereits konfigurierten Kanalbündel.

Timeslots (sogenannte Zeitscheiben oder Zeitfenster) unterteilen die zur Verfügung stehenden 2 MBit Bandbreite einer S_{2M}-Verbindung in logische Kanäle. Im folgenden wird nicht zwischen Timeslots und den Kanälen unterschieden, da der Unterschied für die Konfiguration ohne Belang ist.

Wenn Sie z. B. keine physischen Kanalbündel definiert haben, sondern alle Kanäle in PPP-Multilink-Bündel zusammengefaßt haben, sieht das Menü folgendermaßen aus (im Beispiel das Menü einer X4E-2PRI-Erweiterungskarte):

```
BinTec Router Setup Tool                        BinTec Communications AG
[MODULE X4E-2PRI][BUNDLE]: Bundle Configuration                 MyRouter

 Type       Name       Timeslots                                 Channels
 PPP        bundle4    01 - 31                                     31




                      DELETE            EXIT
```

Timeslots, die keinem Kanalbündel zugeordnet sind, können für 64 Kbit Festverbindungs-WAN-Partner genutzt werden.

Das Übersichtsfenster enthält die folgenden Felder:

Feld	Bedeutung
Type	Hier wird die Art des Kanalbündels angezeigt. Die möglichen Werte sind: ■ *PPP*: Die Kanäle werden als PPP-Multilnk-Kanäle gebündelt. ■ *Physical*: Die Kanäle werden als physikalische Hyperchannels gebündelt.

Feld	Bedeutung
Name	Hier wird der Name angezeigt, der diesem Kanalbündel gegeben wurde.
Timeslots	Hier werden die logischen Kanäle (Timeslots) angezeigt, die zu diesem Kanalbündel zusammengefügt werden.
Channels	Hier wird die Anzahl der gebündelten Kanäle angezeigt.

Tabelle 2-7: ***BUNDLE CONFIGURATION***

Indem Sie einen bestehen Eintrag oder **ADD** wählen, gelangen Sie in das Untermenü ***BUNDLE CONFIGURATION*** ➧ **ADD/EDIT**. Hier können Sie das gewünschte Kanalbündel konfigurieren.

Das Menü sieht folgendermaßen aus, wenn Sie keine physikalischen Kanalbündel definiert, sondern alle Kanäle zu einem PPP-Multilink-Bündel zusammengefaßt haben:

```
BinTec Router Setup Tool                        BinTec Communications AG
[MODULE X4E-2PRI][BUNDLE][EDIT]:Bundle Configuration          MyRouter


  Bundle Type           PPP Multilink
  Interface Name        bundle1
  From Timeslot         1
  To Timeslot           31

  Used 31 Timeslots:

     1 <X>    6 <X>    11 <X>    16 <X>    21 <X>    26 <X>    31 <X>
     2 <X>    7 <X>    12 <X>    17 <X>    22 <X>    27 <X>
     3 <X>    8 <X>    13 <X>    18 <X>    23 <X>    28 <X>
     4 <X>    9 <X>    14 <X>    19 <X>    24 <X>    29 <X>
     5 <X>   10 <X>    15 <X>    20 <X>    25 <X>    30 <X>

  X.75 Layer 2 Mode     DTE
  Bundle Id             1

                SAVE                            CANCEL
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Bundle Type	Hier definieren Sie den Typ des Kanalbündels. Die möglichen Werte sind: ■ *PPP Multilink* ■ *Physical (Hyperchannel)*
Interface Name	Zeigt den Namen des Interfaces an, das im Menü ***WAN Partner*** durch das Kanalbündel entsteht.
From Timeslot	Zeigt den ersten der für dieses Kanalbündel verwendeten Kanäle an. Wenn Sie eine Konfiguration wählen, bei der nicht zusammenhängende Kanäle verwendet werden, wird der erste verwendete Kanal angezeigt und mit dem Vermerk *customized* versehen, z. B. ***6 customized***. Wenn Sie einen bestimmten "Startkanal" auswählen wollen, können Sie dies hier tun.
To Timeslot	Zeigt den letzten der für dieses Kanalbündel verwendeten Kanäle an. Wenn Sie eine Konfiguration wählen, bei der nicht zusammenhängende Kanäle verwendet werden, wird der letzte verwendete Kanal angezeigt und mit dem Vermerk *customized* versehen, z. B. ***31 customized***. Wenn Sie einen bestimmten "Endkanal" auswählen wollen, können Sie dies hier tun.

Feld	Bedeutung
Used x Timeslots	Zeigt die Summe der verwendeten Kanäle an sowie eine Liste, welche Kanäle im einzelnen verwendet worden sind. Wenn Sie nicht alle Kanäle zwischen einem bestimmten Start- und einem bestimmten "Endkanal" für ein Kanalbündel verwenden wollen, können Sie hier eine differenzierte Zuweisung vornehmen.
X.75 Layer 2 Mode	Hier definieren Sie, wie sich das Interface, das durch dieses Kanalbündel entsteht, beim Verbindungsaufbau verhält. Mögliche Werte: ■ *dte* ■ *dce* Diesen Parameter brauchen Sie nur dann zu konfigurieren, wenn Sie X.75 im Layer 2 verwenden.
Bundle Id	Hier teilen Sie dem Kanalbündel eine eindeutige ID-Nummer zu. Mögliche Werte sind *1* bis *255*. Als Default-Wert wird die Nummer des ersten verwendeten Kanals genommen.

Tabelle 2-8: ***BUNDLE CONFIGURATION*** ➧ **ADD/EDIT**

Bei der Konfiguration der Kanalbündel (ob PPP Multilink oder physikalisches Bündel) gibt es prinzipiell keine Einschränkungen, was die Aufteilung der Kanäle angeht: Sowohl die Konfiguration vieler kleiner Kanalbündel als auch unterschiedlicher Typen (PPP Multilink oder physikalisches Bündel) ist möglich.

2.5 Erweiterung der RIP-Implementierung

Um den durch RIP-Updates (RIP = Routing Information Protocol) erzeugten Datenverkehr präzise steuern zu können, hat BinTec zwei Erweiterungen des RIP vorgenommen:

- Triggered RIP wurde implementiert(Kapitel 2.5.1, Seite 34).
- die Konfigurationsmöglichkeiten des RIP wurden erweitert (Kapitel 2.5.2, Seite 36).

2.5.1 Triggered RIP

Durch häufige Updates der **ipRouteTable** verursachter Datenverkehr kann unter Umständen erhebliche Ausmaße annehmen. BinTec hat gemäß RFC 2091 neben RIPV1 und RIPV2 auch das sogenannte Triggered RIP implementiert. Dieses sorgt dafür, daß Updates der **ipRouteTable** nur noch unter genau definierten Umständen und nicht unbedingt nach einer bestimmten Zeit durchgeführt werden.

Gemäß RFC 2091 werden mit Triggered RIP Updates der **ipRouteTable** nur unter den folgenden Bedingungen gesendet bzw. angenommen:

- Wenn die **ipRouteTable** durch neue Informationen von einem Interface verändert wird.
- Wenn eine spezifische Anfrage nach eine Routing-Update eingeht ("Update Request").
- Wenn sich die Erreichbarkeit eines Hops von "nicht erreichbar" nach "erreichbar" ändert.
- Wenn das Gerät eingeschaltet wird, um sicherzustellen, daß zumindest ein Update gesendet bzw. angefordert wird.

Im ersten Fall werden lediglich die letzten Änderungen gesendet, in den weiteren Fällen der gesamte Inhalt der **ipRouteTable**.

Triggered RIP wird interfacespezifisch im Menü ***WAN PARTNER*** ➧ **ADD/EDIT** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** konfiguriert:

```
BinTec Router Setup Tool                    BinTec Communications AG
[WAN][ADD][IP][ADVANCED]: Advanced Settings                  MyRouter


  RIP Send                            RIP V2 Triggered
  RIP Receive                         RIP V2 Triggered

  Van Jacobson Header Compression     off
  Dynamic Name Server Negotiation     yes


  IP Accounting                       off
  Back Route Verify                   off
  Route Announce                      up or dormant
  Proxy Arp                           off

                OK                                CANCEL
```

Relevant sind die Felder **RIP Send** und **RIP Receive**. Für sie stehen die folgenden neuen Werte zur Verfügung:

Mögliche Werte	Bedeutung
RIP V1 Triggered	RIP V1 Nachrichten werden gemäß RFC 2091 gesendet, empfangen und verarbeitet.
RIP V2 Triggered	RIP V2 Nachrichten werden gemäß RFC 2091 gesendet, empfangen und verarbeitet.

Tabelle 2-9: **RIP Send/RIP Receive**

Beachten Sie, daß "gemischte" Konfigurationen (z. B. **RIP Send** *RIP V1* und **RIP Receive** *RIP V1 Triggered*) nicht funktionieren, da die Header-Formate der beiden Protokolle inkompatibel sind.

Aufgrund der größeren Effizienz von RIP V2 sollten Sie dieses einsetzen, sofern Ihr Netzwerk es zuläßt.

2.5.2 Konfiguration des Routing Information Protokolls

Durch RFC 2453 ist das Routing Information Protocol erheblich erweitert worden. System-Software-Release 6.2.5 trägt diesen Erweiterungen Rechnung und ermöglicht eine präzise Konfiguration des RIP. Im Menü ***IP*** findet sich das neue Untermenü ***ROUTING PROTOCOLS***. Dieses zeigt den Status des Routing-Daemon (**Routed**) an und ermöglicht seine Aktivierung bzw. Deaktivierung.

Die möglichen Zustände des Routing-Daemons sind:

- *running:* Für Interfaces, die entsprechend konfiguriert sind, werden RIP-Updates je nach Konfiguration gesendet und empfangen
- *stopped*: RIP-Updates werden können weder gesendet noch empfangen werden.

Die Einstellung *stopped* hebt die Einstellungen auf, die in den Feldern **RIP Send** und **RIP Receive** im Menü ***WAN PARTNER*** ➧ **ADD/EDIT** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** konfiguriert worden sind. Auch wenn für ein Interface RIP-Updates vorgesehen sind, werden diese dann nicht ausgeführt.

Darüber hinaus ermöglicht das Menü ***IP*** ➧ ***ROUTING PROTOCOLS*** den Zugriff auf die Untermenüs ***RIP*** und ***OSPF*** (OSPF ist nur mit einer entsprechenden Lizenz verfügbar).

Das Menü ***RIP*** ist neu und enthält die erweiterten Konfigurationsmöglichkeiten für RIP:

```
BinTec Router Setup Tool                    BinTec Communications AG
[IP][ROUTING][RIP]: RIP configuration                       MyRouter

               UDP port                          520

               Static Settings >

               Timer >

               Filter >


               SAVE                              CANCEL
```

Die Einstellungsmöglichkeit des UDP-Ports, der für das Senden und Empfangen von RIP-Updates verwendet wird, ist lediglich für Testzwecke von Bedeutung. Eine Veränderung der Einstellung kann dazu führen, daß der Router auf einem Port sendet und lauscht, auf dem keine weiteren Router (Hops) reagieren. Der Default-Wert *520* sollte eingestellt bleiben.

Vom Menü ***IP*** ➧ ***ROUTING PROTOCOLS*** ➧ ***RIP*** gelangen Sie in drei weitere Untermenüs, in denen Sie die Art und Weise, in der RIP-Updates gehandhabt werden, genau festlegen können:

- Static Settings
- Timer
- Filter

Static Settings

Im Menü ***IP*** ➧ ***ROUTING PROTOCOLS*** ➧ ***RIP*** ➧ ***STATIC SETTINGS*** konfigurieren Sie die grundlegenden Parameter des RIP. Es enthält die folgenden Felder:

Feld	Bedeutung
Default Route distribution	Hier bestimmen Sie, ob die Default-Route Ihres Routers über RIP-Updates propagiert werden soll. Die möglichen Werte sind: ■ *disabled* ■ *enabled* Der Default-Wert ist *enabled*.
Poisoned Reverse	Bei einem **Poisened Reverse** wird eine gelernte Route über alle Interfaces propagiert. Über das Interface, über das der Router die Route gelernt hat, propagiert er diese mit der Metric 16 (="Netz ist nicht erreichbar"). Der Default-Wert ist *disabled*.
RFC 2453 variable timer	Hier können Sie bestimmen, ob für die in RFC 2453 beschriebenen Timer diejenigen Werte verwendet werden sollen, die Sie im Menü ***IP*** ➧ ***ROUTING PROTOCOLS*** ➧ ***RIP*** ➧ ***TIMER*** konfigurieren können. Die möglichen Werte sind: ■ *disabled* ■ *enabled* Der Default-Wert ist *enabled*. Wenn Sie den Wert *disabled* wählen, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.

Feld	Bedeutung
RFC 2091 variable timer	Hier können Sie bestimmen, ob für die in RFC 2091 beschriebenen Timer diejenigen Werte verwendet werden sollen, die Sie im Menü ***IP*** ➧ ***ROUTING PROTOCOLS*** ➧ ***RIP*** ➧ ***TIMER*** konfigurieren können. Die möglichen Werte sind: ■ *disabled* ■ *enabled* Der Default-Wert ist *disabled*. Wenn Sie den Wert *disabled* belassen, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.

Tabelle 2-10: ***IP*** ➧ ***ROUTING PROTOCOLS*** ➧ ***RIP*** ➧ ***STATIC SETTINGS***

Die Timer, die im Menü ***STATIC SETTINGS*** aktiviert werden können, werden im Menü ***IP*** ➧ ***ROUTING PROTOCOLS*** ➧ ***RIP*** ➧ ***TIMER*** konfiguriert.

Timer

In diesem Menü können Sie die Timer konfigurieren, die von RFC 2091 und RFC 2453 für die unterschiedlichen Ereignisse innerhalb der Liftetime einer Route vorgesehen sind.

Das Menü gliedert sich in die Felder zur Konfiguration des RIP-V2-Timers (RFC 2453) und des Triggered-RIP-Timers (RFC 2091):

```
BinTec Router Setup Tool                    BinTec Communications AG
[IP][ROUTING][RIP][TIMER]: RIP timer configuration           MyRouter


               Timer for RIP V2 (RFC 2453)
               ---------------------------
               Update Timer                        30
               Route Timeout                       180
               Garbage Collection Timer            120

               Timer for Triggered RIP (RFC 2091)
               ----------------------------------
               Hold down timer                     120
               Retransmission timer                5


               SAVE                                CANCEL
```

Das Menü enthält die folgenden Felder (alle Timer werden in Sekunden angegeben):

Feld	Bedeutung
Update Timer	Nach Ablauf dieses Zeitraums wird ein RIP-Update gesendet. Der Default-Wert ist *30*.
Route Timeout	Nach dem letzten Update einer Route wird der **Route Timeout** aktiviert. Nach dessen Ablauf wird die Route deaktiviert und der **Garbage Collection Timer** gestartet. Der Default-Wert ist *180*.

Feld	Bedeutung
Garbage Collection Timer	Der **Garbage Collection Timer** wird gestartet, sobald der Route Timeout abgelaufen ist. Nach Ablauf dieses Zeitraums wird die ungültige Route aus der **ipRouteTable** gelöscht, sofern kein Update für die Route mehr eingeht. Der Default-Wert ist *120*.
Hold down timer	Der **Hold down timer** wird aktiviert, sobald der Router eine Route erhält, die mit einem Poisened Reverse propagiert wurde. Nach Ablauf dieses Zeitraums wird die Route ggf. aus der **ipRouteTable** gelöscht. Der Default-Wert ist *120*.
Retransmission timer	Nach Ablauf dieses Zeitraums werden Update-Request- bzw. Update-Response-Pakete erneut versendet, bis ein Update-Flush- bzw. Update-Acknowledge-Paket eintrifft. Der Default-Wert ist *5*.

Tabelle 2-11: ***IP*** ➧ ***ROUTING PROTOCOLS*** ➧ ***RIP*** ➧ ***TIMER***

Die genaue Funktionsweise der Timer im RIP ist komplex. Detaillierte Informationen entnehmen Sie bitte den RFCs 2453 (u. a. Abschnitt 3.8) und 2091 (u. a. Abschnitt 6).

Wenn Sie für die Timer andere Werte verwenden, als die in den RFCs vorgesehenen, sollten alle Router in Ihrem Netzwerk die gleichen Einstellungen verwenden.

Filter

Im Menü ***IP*** ➧ ***ROUTING PROTOCOLS*** ➧ ***RIP*** ➧ ***FILTER*** können Sie exakt festlegen, wie Routen vom **Routed** exportiert oder importiert werden.

Im ersten Menüfenster sehen Sie eine Auflistung der bereits konfigurierten Filter:

```
BinTec Router Setup Tool                      BinTec Communications AG
[IP][ROUTING][RIP][FILTER]: RIP Distribution Filter           MyRouter

  Interface  Direction  State    IP-Address      Netmask         Priorit

  en1        import     enabled  10.1.1.0        255.255.255.0       1



     ADD                 DELETE               EXIT
```

Die angezeigten Felder entsprechen den im Untermenü **ADD/EDIT** konfigurierbaren. Unter **State** wird der für die Variable **Distribution** konfigurierte Wert angezeigt.

Das Menü ***IP*** ➧ ***ROUTING PROTOCOLS*** ➧ ***RIP*** ➧ ***FILTER*** ➧ **ADD/EDIT** sieht folgendermaßen aus:

```
BinTec Router Setup Tool                      BinTec Communications AG
[IP][ROUTING][RIP][FILTER][ADD]: Define RIP Filter            MyRouter


          Interface                                 en1
          IP-Address
          Netmask
          Priority                                  1
          Direction                                 import
          Distribution                              disabled
          Metric1 offset on interface up            0
          Metric1 offset on interface dormant       0


                    SAVE                            CANCEL
```

Zur Konfiguration der Filter enthält das Menü folgende Felder:

Feld	Bedeutung
Interface	Hier bestimmen Sie, für welches Interface die zu konfigurierende Regel gilt.
IP-Address	Hier geben Sie die IP-Adresse ein, auf die die Regel angewendet werden soll. Die Adresse kann sowohl im LAN als auch im WAN liegen. Die Regeln für eingehende und ausgehende RIP-Pakete (Import oder Export) werden für dieselbe IP-Adresse getrennt konfiguriert. Sie können einzelne Host-Adressen ebenso angeben wie Netzadressen.
Netmask	Hier geben Sie die Netzmaske von **IP Address** ein.
Priority	Hier geben Sie die Priorität ein, mit der das Filter angewendet werden soll. Gibt es unterschiedliche Filter mit sich überlappenden IP-Adreßbereich, so wird dasjenige Filter zuerst ausgeführt, das die höhere Priorität hat. So läßt sich eine einzelne Host-Route aus einem eigentlich gesperrten IP-Adreßbereich importieren, wenn die Regel, die dies zuläßt, eine höhere Priorität hat als diejenige, die den Adreßbereich sperrt. Mögliche Werte sind *1* bis *16*, wobei *1* der höchsten Priorität entspricht. Der Default-Wert ist *1*.

Feld	Bedeutung
Direction	Hier bestimmen Sie, ob das Filter für den Export oder den Import von Routen gilt. Die möglichen Werte sind: ■ *import* ■ *export*
Distribution	Hier bestimmen Sie, ob der Export bzw. Import von Router durch dieses Filter zugelassen oder gesperrt werden soll. Die möglichen Werte sind: ■ *enabled* ■ *disabled* Der Default-Wert ist *disabled*.
Metric1 offset on interface up	Hier geben Sie an, ob und in welchem Umfang die Metrik einer importierten oder exportierten Route geändert werden soll, wenn das betroffene Interface aktiv (*up*) ist. Die möglichen Werte sind *-16* bis *16*. Der Default-Wert ist *0*.
Metric1 offset on interface dormant	Hier geben Sie an, ob und in welchem Umfang die Metrik einer importierten oder exportierten Route geändert werden soll, wenn das betroffene Interface inaktiv (*down*) ist. Die möglichen Werte sind *-16* bis *16*. Der Default-Wert ist *0*.

Tabelle 2-12: ***IP*** ➧ ***ROUTING PROTOCOLS*** ➧ ***RIP*** ➧ ***FILTER*** ➧ **ADD/EDIT**

2.6 Zeitgesteuerte Ausführung von Aktionen

System-Software-Release 6.2.5 ermöglicht es, alle Aktionen mit einem Countdown zu steuern, die sich auf der SNMP-Shell in der Form `cmd=<action>` eingeben lassen.

Eine Aufstellung der verfügbaren Aktionen erhalten Sie, wenn Sie auf der SNMP-Shell `cmd?` eingeben.

Es handelt sich nicht um direkt ausgeführte Shell-Befehle, sondern um Einträge, die in der **biboAdmConfigTable** für die Variable **Cmd** gemacht werden. Die entsprechenden Operationen werden der Reihe nach ausgeführt.

Wenn Sie auf der SNMP-Shell z. B. die Zeile `cmd=reboot timeout=120` eingeben, wird ein Eintrag in der **biboAdmConfigTable** erstellt. Dieser sieht folgendermaßen aus:

```
x4000:> cmd=reboot timeout=120
00: biboAdmConfigCmd.9( rw):            reboot
00: biboAdmConfigTimeout.9( rw):        120
x4000:> biboadmconfig

inx Cmd(*rw)         Object(rw)       Path(rw)         PathNew(rw)
    Host(rw)         State(ro)        File(rw)         Timeout(rw)

 00 reboot            .0.0
    0.0.0.0           delayed                           120

x4000:biboAdmConfigTable>
```

In diesem Fall wird nach 120 Sekunden ein Neustart des Routers durchgeführt. Nachdem der Timeout eingetragen worden ist, kann er bis zum Ablauf jederzeit korrigiert werden. Dazu werden der Variable **Timeout** bestimmte Typen von Werten zugewiesen (siehe Tabelle 2-13, Seite 46).

Wenn Sie einen konfigurierten Timeout korrigieren wollen, beachten Sie, daß Sie den Timeout für den entsprechenden Eintrag (`inx`) ändern.

Die folgenden Wertebereiche stehen für die Variable **Timeout** zur Verfügung:

Variablenwert	Bedeutung
positive Werte	Z. B. *120* Der Timeout wird auf den eingegebenen Zahlenwert in Sekunden eingestellt. Der Countdown beginnt sofort nach Bestätigung mit **Enter**. Der Wert wird als 32bit-Integer angegeben.
0	Der Wert 0 führt zur unmittelbaren Ausführung des Befehls nach der Bestätigung mit **Enter**.
negative Werte	Z. B. *-1* Jeder negative Wert führt dazu, daß ein zuvor gestarteter Timeout unmittelbar gestoppt wird. Die Höhe des Wertes hat keine Auswirkung auf die Funktion.

Tabelle 2-13: **Timeout**

Shortcut für `cmd=reboot`

Darüber hinaus können die Tabelleneinträge `cmd=reboot` und `timeout=<sekunden>` auch über einen Shortcut auf der SNMP-Shell erstellt werden.

Dies geschieht mittels des Befehlskürzels `h`:

```
x4000:> h ?

Usage:
    h               Display currently scheduled halt.
    h 0             Cancel  currently scheduled halt.
    h HHH:MM        Schedule a halt command in HHH hours MM minutes.

x4000:>
```

Die Verwendung dieses Befehls auf der SNMP-Shell führt zu den entsprechenden Einträgen in der **biboAdmConfigTable**. Dabei ist zu beachten:

- Der Wert *0* hat folgende Bedeutung:
  Die Eingabe von `h 0` führt zum Abbruch eines bereits gestarteten Timers, entspricht also einem negativen Wert für die Variable **Timeout** in der **biboAdmConfigTable** (es wird der Wert *-1* eingetragen).
  Einen unmittelbaren Neustart können Sie also nur mittels des Tabelleneintrags `cmd=reboot` herbeiführen, nicht aber durch die Verwendung von `h`.
- Die Eingabe eines negativen Wertes ist nicht möglich, da der Abbruch des Timeouts durch `h 0` erreicht wird.

2.7 Modem-Update

Mit System-Software-Release 6.2.5 ist es möglich, die Firmware der Modem-Ressourcenmodule (XT-S, XT-M, XT-2M, XT-L) von Geräten der **X4000-Familie** und **X8500** zu aktualisieren.

Die aktuellen Logik-Dateien können Sie vom Download-Bereich Ihres Routers auf www.bintec.de downloaden.

Um die Firmware zu aktualisieren, loggen Sie sich auf Ihrem Router ein. Die grundsätzliche Update-Prozedur ist in Ihrem Handbuch im Kapitel Software-Update durchführen beschrieben. Die zu verwendende Syntax ist:

`modem update <tftpserver> <filename>`.

2.8 X8500-S3

Mit der **X8500-S3** steht eine kleinere Produktvariante der **X8500** zur Verfügung, Die Hardware ist identisch, doch können nur drei der acht vorhandenen Einschübe mit Erweiterungskarten versehen werden. Mittels einer Upgrade-Lizenz können jederzeit die verbleibenden fünf Einschübe freigeschaltet werden.

X8500-S3 bietet genau wie die **X8500-S8** die Möglichkeit, zwei Netzteile redundant zu betreiben und ist ebenfalls Hot-Swap-fähig.

3 Änderungen

Neben neuen Features sind Änderungen bzw. Erweiterungen des Funktionsumfangs in folgende Bereich von System-Software-Release 6.2.5 eingegangen:

- Bezeichnug der Ressourcenmodule (Kapitel 3.1, Seite 49)
- Gratuitous ARP (Kapitel 3.2, Seite 50)
- ANSI T1.617 D LMI für Frame Relay (Kapitel 3.3, Seite 50)
- State Transitions für PPP-Callback (Kapitel 3.4, Seite 50)
- IPSec (Kapitel 3.5, Seite 51)
- Frame Relay mit **X2100** (Kapitel 3.6, Seite 53)
- Minipad (Kapitel 3.7, Seite 53)
- Anzeige der Default-Route (Kapitel 3.8, Seite 54)
- Lizenzanzeige (Kapitel 3.9, Seite 54)
- Wizard-Unterstützung für BinGO! DSL (Kapitel 3.10, Seite 54)
- STAC-Kompression (Kapitel 3.11, Seite 54)
- Zugang zum OSPF-Menü (Kapitel 3.12, Seite 55)

3.1 Bezeichnug der Ressourcenmodule

Bisher wurden die BinTec-Ressourcenmodule zur Erweiterung der Funktionalität modularer Router unter dem Kürzel "XTR-" geführt. Dieses Kürzel wird von einem anderen Unternehmen als geschützer Name beansprucht. Anstelle von "XTR-" werden wir in Zukunft "XT-" verwenden, also z. B. XT-ENC anstelle von XTR-ENC für das Hardware-Encryption-Modul.

3.2 Gratuitous ARP

Wenn sich die MAC-Adresse eines Gerätes im Netzwerk ändert, kann dieses ein sogenanntes Gratuitous ARP Packet senden, um die neue MAC-Adresse im Netz zu propagieren. Diese Pakete wurden bisher von BinTec-Routern ignoriert. Dadurch konnte es zu Paketverlusten kommen, wenn Daten an ein Gerät gesendet wurden, dessen MAC-Adresse sich geändert hatte.

Die Implementierung des ARP (Address Resolution Protocol) ist vollständig RFC-konform und Gratuitous ARP Packets werden angenommen und ausgewertet.

3.3 ANSI T1.617 D LMI für Frame Relay

Mit System-Software-Release 6.2.5 ist ANSI T1.617 D LMI für Frame Relay verfügbar.

Der ANSI-Standard T1.617 definiert den Austausch zwischen einem entfernten Frame-Relay-Terminal und der Netzkomponente (Router), über die sich das Terminal mit dem Netzwerk (LAN) verbindet.

3.4 State Transitions für PPP-Callback

Die Zustandsübergänge für den Callback Expected Mode sind vereinfacht worden, um für den Benutzer transparentere Zustandsabbildungen zu schaffen.

Wenn der initiale abgehende Ruf angenommen und die PPP-Aushandlung erfolgreich gewesen sind, wird ein Callback so lange erwartet, wie im Menü ***WAN PARTNER*** ➧ **ADD/EDIT** ➧ ***ADVANCED SETTINGS*** für das Feld **Delay after Connection Failure (sec)** konfiguriert.

Tritt ein Fehler während des Verbindungsaufbaus auf, so führen folgende Fehler zu folgenden Aktionen und Interface-Zuständen:

Fehler	Aktion	resultierender Zustand
keine Rufnummer konfiguriert	Interface wird blokkiert, ggf. nach Ausführung der konfigurierten Anzahl an Neuversuchen	**ifOperStatus** ist *blocked* für den konfigurierten **Delay after Connection Failure (sec)**; **IfAdminStatus** ist *up*
keine Route zum PPTP-Zielhost		
keine Antwort		
initialer Ruf akzeptiert, aber keine PPP-Aushandlung wird gestartet	Interface wird blokkiert, nachdem die Verbindung beendet worden ist	
initialer Ruf akzeptiert, aber keine Aushandlung der PPP-Authentisierung wird gestartet		
initialer Ruf akzeptiert, aber PPP-Authentisierung scheitert		

Tabelle 3-1: Fehler, Aktionen und Interface-Zustände im Callback Expected Mode

In allen Zuständen werden eingehende Rückrufe akzeptiert.

3.5 IPSec

An der BinTec-IPSec-Implementierung wurden in System-Software-Release 6.2.5 die folgenden Änderungen vorgenommen:

3.5.1 SA-Management

Das Management bestehender Security Associations ist in zwei Punkten angepaßt worden:

- Die neue Variable **ipsecGlobContUniqueIds** kann dazu genutzt werden, alle SAs zu löschen (wenn **ipsecGlobContUniqueIds** auf *true* gesetzt ist), die die gleichen Phase-1-IDs haben. Bisher wurden obsolete SAs anhand der Phase-1-IP-Adresse identifiziert, was bei dynamischem IPSec nicht möglich ist und daher zu "toten" SAs auf dem Router der Zentralseite geführt hat. Die Identifikation anhand der IP-Adresse kann nach wie vor vorgezogen werden, indem man **ipsecGlobContUniqueIds** auf *false* setzt.
- Da ein Peer nun über seine ID identifiziert wird, kann die Zentralseite eine IPSec-Aushandlung auch mit einem dynamischen Peer und auch ohne DynDNS-Hostnamen initiieren, wenn eine SA für den Peer bereits besteht.

3.5.2 PMTU-Discovery

Ab System-Software-Release 6.2.5 kann im Setup Tool die PMTU-Discovery (Path Maximum Transfer Unit Discovery) auch für IPSec aktiviert bzw. deaktiviert werden. Mittels PMTU wird die maximale Größe eines zu sendenden Pakets bestimmt

Im Zusammenhang mit IPSec ist diese Funktion vor allem aus Leistungsgründen relevant. Bei deaktivierter PMTU-Discovery kommt es dazu, daß Pakete fragmentiert werden, was zu einem Leistungsverlust führt. Die Aktivierung der Option setzt allerdings voraus, daß ICMP-Pakete (Typ 3 "Host Unreachable") ungehindert übertragen werden können. Ist das nicht der Fall (z. B. weil sie von einer Firewall ausgefiltert werden), ist kein Datentransfer möglich.

Die Option findet sich im Menü ***IPSec*** ➧ ***Advanced Settings***.

Diese Änderung steht nur in System-Software-Release 6.2.5 Patch 4 zur Verfügung.

3.6 Frame Relay mit X2100

Ab System-Software-Release 6.2.5 ist die Enkapsulierung Frame Relay ohne Lizenz verwendbar. In früheren Versionen der System-Software konnte es beim Abspeichern eines mit dem Setup Tool erstellten WAN-Partners zu Problemen kommen. Sollten Sie derartige Probleme haben, aktualisieren Sie bitte die Software Ihres Routers.

Diese Änderung steht nur in System-Software-Release 6.2.5 Patch 4 zur Verfügung.

3.7 Minipad

Ein mit `minipad` abgesetzter X.25-Ruf enthielt bisher nur dann die lokale X.25-Adresse, wenn diese manuell im Minipad-Argument angegeben wurde. Dieses Verhalten wurde folgendermaßen geändert:

Wenn eine lokale X.25 Adresse konfiguriert ist,

- wird diese per Default übertragen
- wird sie nur dann nicht übertragen, wenn das Minipad-Argument mit einem "/" nach der Zieladresse endet, z. B. ***123/***
- wird eine andere als die für die Variable **x25LocalAddr** eingestellte übertragen, wenn im Argument eine abweichende Adresse angegeben wird. So wird z. B. mit dem Argument ***123/456*** die ***456*** als lokale Adresse übertragen, auch wenn für **x25LocalAddr** ***789*** konfiguriert ist.

Wenn **x25LocalAddr** unkonfiguriert ist, wird weiterhin auch keine lokale Adresse übetragen, wenn sie nicht manuell im Argument angegeben wird.

3.8 Anzeige der Default-Route

Bisher war es nicht möglich, mittels des Shell-Befehls `rtlookup` die aktuelle Default-Route zu identifizieren. Der Befehl `rtlookup` unterstützt nun diese Funktion mit der Option `-D`. Die Verwendung ist also folgende: `rtlookup -D` (ohne Angabe einer Adresse).

3.9 Lizenzanzeige

Wenn in einen Router eine Softwareversion eingespielt wurde, die eine lizenzierte Funktion nicht unterstützte (z. B. IPSec), so wurde in der Spalte **Used for** irreführenderweise *no hardware* angezeigt. Diese Anzeige ist geändert worden, es erscheint in der Spalte **Used for** *Software* und in der Spalte **State** *unsupported*.

3.10 Wizard-Unterstützung für BinGO! DSL

Der Configuration Wizard der BRICKware for Windows unterstützt BinGO! DSL.

3.11 STAC-Kompression

Bisher konnte STAC-Datenkompression im Configuration Wizard auch für PPPoE-Verbindungen ausgewählt werden, obwohl dies von ISPs nicht unterstützt wird. Die entsprechende Option kann nun im Wizard nicht mehr ausgewählt werden, wenn eine PPPoE-Verbindung angelegt wird.

3.12 Zugang zum OSPF-Menü

Wenn Sie OSPF nutzen, finden Sie das Menü zur Konfiguration nicht mehr direkt im Menü ***IP***, sondern als Untermenü im Menü ***IP*** ➧ ***ROUTING PROTOCOLS***. An der Konfiguration selbst hat sich nichts geändert.

4 Bugfixes

In System-Software-Release 6.2.5 sind folgende Fehler, bzw. Fehler aus den folgenden Bereichen beseitigt worden:

- VoIP (Kapitel 4.1, Seite 57)
- IPSec (Kapitel 4.2, Seite 58)
- VoIP und Stateful Inspection (Kapitel 4.3, Seite 61)
- Neustart mit STAC-Kompression (Kapitel 4.4, Seite 62)
- ICMP Messages und NAT (Kapitel 4.5, Seite 62)
- CHAP-MD5-Authentisierung (Kapitel 4.6, Seite 62)
- PRI-Menü (Kapitel 4.7, Seite 63)
- MPPC und MPPE (Kapitel 4.8, Seite 63)
- Neustart mit OSPF (Kapitel 4.9, Seite 63)
- Software-FAX (Kapitel 4.10, Seite 64)
- Leased Line (Kapitel 4.11, Seite 64)
- Falsche Netzmaske bei NAT-Einträgen (Kapitel 4.12, Seite 64)
- RIP V2 (Kapitel 4.13, Seite 65)
- CAPI-Fehler (Kapitel 4.14, Seite 65)

4.1 VoIP

Folgende Fehler in der VoIP-Implementierung sind beseitigt worden:

4.1.1 Behandlung von Aliasen und E.164-Nummern

Wenn ein VoIP-Ruf über eine H.323-Adresse gestartet wurde, und kurz darauf ein Ruf mit einer E.164-Nummer gestartet werden sollte, reagierte der Gatekeeper nicht auf den zweiten Ruf.

Dieses Problem ist gelöst worden. Der Gatekeeper reagiert korrekt auf die unterschiedlichen Adreßformate.

4.1.2 NAT-Einträge

Die NAT-Einträge des H.323-Proxies und des Gatekeepers wurden nicht korrekt vorgenommen: Sie wurden lediglich dann aktualisiert, wenn die NAT-Verbindung bereits bestand.

Dieses Problem ist gelöst worden. Die NAT-Einträge werden korrekt erstellt.

4.1.3 Proxy Location

Im Setup Tool war der Wert des Felds **Location of Proxy** immer auf *inside firewall* gesetzt, unabhängig davon, welcher Wert in der entsprechenden MIB-Tabelle (**voipProxyTable**) gesetzt war. Der Wert konnte im Setup Tool auch nicht verändert werden.

Dieses Problem ist gelöst worden. Der Wert kann im Setup Tool korrekt konfiguriert werden.

4.1.4 H.323-Gateway-Konfiguration

Wenn als H.323-Gateway die IP-Adresse des Routers konfiguriert wurde, kam es zum Absturz des VoIP-Daemons und schließlich des Routers.

Dieses Problem beruhte darauf, daß der VoIP-Daemon in eine Endlosschleife geriet. Es ist gelöst worden, der VoIP-Daemon stürzt nicht mehr ab.

4.2 IPSec

Folgende Fehler der IPSec-Implementierung sind beseitigt worden:

4.2.1 Reboot bei Neukonfiguration

Bei einer Neukonfiguration des IPSec auf der SNMP-Shell konnte es dann zu einem Neustart des Routers kommen, wenn zur selben Zeit eine Phase-2-Aushandlung beendet wurde. Es war unerheblich, ob die Aushandlung erfolgreich oder erfolglos beendet wurde.

Dieses Problem ist gelöst worden. Der IPSec-Daemon stürzt auch unter den beschriebenen Umständen nicht mehr ab.

4.2.2 DynIPSec

Bei der Auflösung der Hostnamen einer DynIPSec-Konfiguration konnte es unter Umständen zu einer Endlosschleife kommen. Der Router startete nicht neu, aber der IPSec-Daemon reagierte nicht mehr.

Dieses Problem ist gelöst worden. Die Namensauflösung wird korrekt durchgeführt.

4.2.3 CRL-Download (1)

Wenn das Zertifikat einer Certificate Authority eine HTTP-Adresse als CRL Distribution Point (CRL=Certificate Revocation List) spezifizierte, scheiterte die Authentisierung in der IKE-Phase 1 unter folgenden Bedingungen:

- die Konfiguration erzwang eine CRL und
- die CRL wurde nicht auf einem anderen Weg geladen (sie lag weder durch statische Konfiguration auf dem Router vor, noch wurde sie als Teil der Phase-1-Aushandlung übertragen)

Darüber hinaus war auch der manuelle CRL-Download nicht möglich.

Dieses Problem beruhte auf nicht zustande kommenden TCP-Verbindungen. Es ist gelöst worden. CRLs können auch von HTTP-Adressen sowie manuell geladen werden.

4.2.4 CRL Download (2)

Beim Download einer CRL (Certificate Revocation List) per HTTP kam es dann zu einer Panic, wenn die HTTP-Verbindung zustande kam, aber die erwartete CRL nicht an der angegebenen Adresse zu finden war.

Dieses Problem beruhte auf einen Fehler im HTTP-Modul. Es ist gelöst worden. Wenn die CRL an der angegebenen Adresse nicht zu finden ist, wird eine Fehlermeldung ausgegeben.

4.2.5 Neue Proposals nach Software-Update

Nach einem Update auf eine neue IPSec-Version konnte es vorkommen, daß trotz eines Aufrufs des IPSec-Wizards neue IKE- und IPSec-Proposals nicht aufgenommen wurden.

Das Problem beruhte darauf, daß die MIB-Tabellen **ikeProposal** und **ipsecProposal** nicht aktualisiert wurden, wenn sie bereits Einträge enthielten.

Wenn man alle vorhandenen Einträge löschte und dann der IPSec-Wizard startete, wurden alle neuen Einträge korrekt vorgenommen.

Dieses Problem ist gelöst worden. Die betreffenden MIB-Tabellen werden korrekt aktualisiert.

4.2.6 Löschen von SAs

Wenn eine SA auf einem Router manuell entfernt wurde, blieb diese auf dem entfernten Router gültig, wenn die Aushandlung eine beliebige SA mit aktiviertem IPComP (IP Payload Compression Protocol) ergeben hatte.

Dieses Problem beruhte auf einer unzureichenden Interpretation der "Delete Notification". Es ist gelöst worden, die SA wird auf beiden Seiten korrekt gelöscht.

4.2.7 Blockade durch unvollständige Konfiguration

Wenn IPSec aktiviert wurde, obwohl weder ein Peerlist-Eintrag noch ein Trafficlist-Eintrag existierten, wurden alle IP-Pakete verworfen. Das geschah auch, wenn die Default-IPSec-Regel im Menü ***IPSec*** ➧ ***Post IPSec Rules*** auf *pass* gesetzt war.

Dieses Problem ist gelöst worden. Wenn die Default-Regel auf *pass* gesetzt ist, führt eine unvollständige IPSec-Konfiguration nicht mehr zu einer Blockade aller IP-Pakete.

4.2.8 IPSec Setup Tool

Wenn die Trafficlist-Einträge gelöscht wurden, die in einem der Menüs ***IPSec*** ➧ ***Pre IPSec Rules/Peer Configuration/Post IPSec Rules*** erstellt worden waren, wurde nicht die nun überflüssige Trennlinie gelöscht, sondern diejenige für die folgende Trafficlist.

Dieses Problem ist gelöst worden. Die Trennlinien werden korrekt gelöscht.

4.2.9 IPSec-Wizard (1)

Bei der Erstellung des Eintrags in die Pre IPSec Rules, der die unverschlüsselte Übertragung des IKE-Verkehrs ermöglicht, meldete der IPSec-Wizard die Verwendung der Aktion *always_plain*. Diese ist jedoch obsolet und in der aktuellen Version der IPSec-Software nicht mehr enthalten. Statt dessen wird als Aktion *pass* verwendet.

Es handelte sich ausschließlich um einen Schreibfehler. Er ist beseitigt worden, und der IPSec-Wizard zeigt korrekt die Verwendung von *pass* an.

4.2.10 IPSec-Wizard (2)

Wenn man im IPSec-Wizard die Funktion **clear config** aufrief, wurde eine Warnung ausgegeben, daß die Einträge der **ipsecPublicKeyTable** gelöscht würden. Dies geschieht jedoch deshalb nicht, damit die Zertifikate nicht ungültig werden, die für einen der Schlüssel in der **ipsecPublicKeyTable** beantragt worden sind. Der Warnhinweis war irreführend.

Dieses Problem ist gelöst worden. Der irreführende Warnhinweis wird nicht mehr ausgegeben.

4.3 VoIP und Stateful Inspection

Bisher kam es zu Problemen bei gleichzeitiger Verwendung von VoIP (Voice over IP) und der BinTec Stateful Inspection Firewall.

Dieses Problem ist gelöst worden. Der VoIP-Daemon unterstützt die Erkennung von "Tochterverbindungen" einer bereits bestehenden Verbindung durch die SIF.

Diese Fehlerbehebung steht nur in System-Software-Release 6.2.5 Patch 4 zur Verfügung.

4.4 Neustart mit STAC-Kompression

Dieses Problem betraf lediglich Geräte, die nicht mit einem HiFn-Chip zur Hardwarekompression ausgestattet sind.

Wenn bei einem BinTec-Router mittels STAC komprimierte Datenpakete eingingen, konnte es dann zum Neustart des Routers kommen, wenn diese Pakete korrupt waren.

Dieses Problem ist behoben worden. Der Neustart wird durch eine Anzahl von Tests verhindert, die die korrekte Form des Paketes verifizieren.

4.5 ICMP Messages und NAT

Network Address Translation war für ICMP-Pakete nicht funktionsfähig. Daher wurden ICMP-Echo-Replies für unterschiedliche Hosts im LAN alle an denjenigen Host innerhalb des LANs gesendet, der die erste ICMP-Echo-Request gesendet hatte.

Dieses Problem ist gelöst worden. Zulässige ICMP-Sessions werden korrekt zugeordnet.

4.6 CHAP-MD5-Authentisierung

Eine CHAP-MD5-Authentisierung scheiterte, wenn der Peer eine CHAP Challenge mit einer anderen Läge als 16 bit sendete, um den Passwort-Hash zu erstellen.

Dieses Problem ist gelöst worden. CHAP-Challenges unterschiedlicher Längen werden korrekt verarbeitet.

4.7 PRI-Menü

Bei **X8500** mit einer PRI-Erweiterungskarte konnte unter System 6.2.2 im Konfigurationsmenü eines PRI-Interfaces die Feldbezeichnung **Clock Mode** mit dem Cursor ausgewählt werden.

Dieses Problem ist gelöst worden. Nur noch die Eingabefelder können mit dem Cursor ausgewählt werden.

4.8 MPPC und MPPE

Bei der Einwahl auf einem BinTec-Router, der mit einem XT-ENC- oder XT-VPN-Resourcenmodul zur Datenkompression und -verschlüsselung ausgestattet ist, konnten MPPC (Microsoft Point to Point Compression) und MPPE (Microsoft Point to Point Encryption) nicht simultan verwendet werden. Es wurden keine Daten über die Verbindung gesendet.

Dieses Problem beruhte auf unvollständiger Verschlüsselung und Fehlern in der Datenübertragung. Es ist gelöst worden. Die Daten werden korrekt komprimiert und übertragen

4.9 Neustart mit OSPF

Bei aktiviertem OSPF (Open Shortest Path First) kam es zu einem Neustart des Routers, wenn im Setup Tool ein WAN-Partner gelöscht wurde.

Dieses Problem ist gelöst worden, das Löschen eines WAN-Partners führt nicht mehr zu einem Neustart des Routers.

4.10 Software-FAX

Es war nicht möglich mit **X2300i** Software-Faxe (z. B. über RVS-COM oder AVM Fritz!fax) zu versenden oder zu empfangen.

Dieses Problem war auf einen Fehler im ISDN-Treiber zurückzuführen. Es ist behoben worden. Faxe können versendet und empfangen werden.

4.11 Leased Line

Nach einem Update auf System-Software-Release 6.2.2 war es nicht mehr möglich mit **X3200** Standleitungen zu verwenden. Darüber hinaus konnten die Parameter der Standleitungskonfiguration weder auf der SNMP-Shell noch im Setup Tool geändert werden.

Dieses Problem ist gelöst worden. Standleitungen sind auch mit **X3200** wieder verwendbar.

4.12 Falsche Netzmaske bei NAT-Einträgen

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

Dieses Problem ist gelöst worden. Bei einem neuen Eintrag werden die korrekten Defaultwerte verwendet.

4.13 RIP V2

Bei Updates der Routing-Tabelle mittels RIP V2 kam es zu folgenden zwei Problemen:

- Der Router versendete RIP-Pakete mit falschen Ziel-IP-Adressen (an nicht angrenzende Hosts).
- Der Router versendete RIP-Pakete mit falscher Quell-IP-Adresse (es wurde nicht die lokale IP-Adresse verwendet, sondern die des ersten Hops).

Diese Probleme sind gelöst worden. Es werden die korrekten IP-Adressen verwendet.

4.14 CAPI-Fehler

Wenn mehrere B-Kanäle von einer CAPI-Applikation genutzt werden sollten, konnten keine Daten transportiert werden.

Dieses Problem beruhte auf Fehlern im Data Flow. Es ist gelöst worden, und CAPI-Applikation können mehrere B-Kanäle nutzen.

5 Bekannte Probleme

Da es im alltäglichen Betrieb trotz umfangreicher Tests zu Problemen mit unserer System-Software kommen kann, hat BinTec eine Mailing-Liste (**release-info**) eingerichtet, durch die Sie laufend über Probleme sowie Lösungen und "Workarounds" informiert werden, die in unseren Labors verifiziert werden konnten. Wenn Sie diese Mailing-Liste abonnieren wollen, können Sie dies auf unseren Internetseiten tun: Sie finden einen entsprechenden Link auf den Downloadseiten von www.bintec.de.