Release Notes System-Software-Release 6.2.5 X-Generation

Oktober 2002

System-Software-Release 6.2.5

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

Dies ist eine Vorabversion der Release Notes 6.2.5. Obwohl die enthaltenen Information mit größter Sorgfalt erarbeitet wurden, ist nicht auszuschließen, daß uns Fehler unterlaufen sind.

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 44.

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 7)
- IPSec-Callback (Kapitel 2.2, Seite 20)
- PPTP-Passthrough (Kapitel 2.3, Seite 25)
- Bündelung von PRI-Hypperchannels (Kapitel 2.4, Seite 26)
- Erweiterung der RIP-Implementierung (Kapitel 2.5, Seite 30)
- Zeitgesteuerte Ausführung von Shell-Befehlen (Kapitel 2.6, Seite 41)
- Modem-Update (Kapitel 2.7, Seite 44)

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.

Gegenüber der sogenannten statischen Paketfilterung hat eine SIF mit dynamischer Paketfilterung einen entscheidenden Vorteil: Die Entscheidung, ob ein Paket weitergeleitet wird, wird nicht lediglich aufgrund von Quell- und Zieladressen oder Ports gefällt. Vielmehr wird bei dynamischer Paketfilterung der Zustand (*state*) der Verbindung zu einem Partner überprüft. Es werden nur solche Pakete weitergeleitet, die zu einer aktiven Verbindung gehören. Nur wenn die Kontrolle der Quell- und Zieladresse, des Services (Protokoll und Portnummern) und des Status der Verbindung positiv ausfällt, wird ein Paket weitergeleitet. Pakete, die keiner bestehenden Verbindung zugeordnet werden können, wie "Echo Requests" (Pings), werden daher ignoriert.

Dabei leitet die SIF auch Pakete weiter, die zu einer aktiven "Tochterverbindung" gehören: Die Aushandlung einer FTP- Verbindung findet z. B. über den

Port 21 statt, der eigentliche Datenaustauch 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. Systeme wie "Network Address Translation" (NAT) und "IP Access Lists" (IPAL) erfordern einen größeren Konfigurationsaufwand als die Einrichtung der SIF.

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 und dann auf dem direktesten Weg realisieren.

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. Zwar kann man Interfaces ähnlich wie Quell- und Zieladresse auch bei der Konfiguration der SIF als Filterkriterium verwenden. Eine weitere Differenzierung aufgrund von Quell- und Zieladresse eines Pakets wie bei NAT und IPAL ist dann aber nicht mehr möglich.

Grundsätzlich werden aber die selben Filterkriterien auf den Datenverkehr anwenden:

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

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

henfolge, in der sie auch vom Router vorgenommen werden. Die Reihenfolge orientiert sich dabei an einem am Router von außen ankommenden Paket.

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.

SIF

Auf die NAT-Filterung folgt die Filterung durch die "Stateful Inspection Firewall". Da NAT jeden Zugriff auf das LAN von außen unterbindet, werden Genehmigungen, die in der SIF konfiguriert werden, auf die NAT-Konfiguration übertagen. D. h., daß man bei der Konfiguration von NAT erwünschte Verbindungen von außen nicht bedenken muß, wenn man eine SIF-Konfiguration plant. Die SIF sondert alle Pakete aus, die nicht explizit 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 folgerndermaßen:

- 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 Pass-Regel zutrifft, wird es weitergeleitet.

- Alle Pakete, auf die keine Regel zutrifft, werden nach Kontrolle aller vorhandenen Regeln ohne Fehlermeldung an den Sender abgewiesen.

"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.

2.1.2 Konfiguration

Eine grundlegende Konfiguration, die dennoch ein hohes Maß an Sicherheit bietet, kann folgendermaßen aussehen:

- NAT wird ohne weitere Konfiguration auf allen Interfaces eingeschaltet, die Zugang zum WAN haben. Dadurch werden alle Verbindungen aus dem WAN zum LAN unterbunden, die nicht angefordert worden sind. Darüber hinaus wird NAT zur Adreßumsetzung benötigt.
- Die SIF wird so konfiguriert, daß aller Verkehr, der von außen zugelassen werden soll, durch entsprechende Regeln gestattet wird. Zugleich kann unerwünschter Verkehr von innen nach außen unterbunden werden.
- Eine Konfiguration der "IP Access Lists" ist in diesem Fall nicht notwendig.

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 Filter                          MyRouter

Stateful Inspection Filter List

Pos.      Source      Destination      Service      Action

  1       LAN_EN1     WAN_ISP          http         accept
  2       WAN_ISP     LAN_EN1          ftp          deny


            ADD          DELETE           SAVE           EXIT

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

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 FIREWALL*** ➧ **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 Alias für die Quelladresse 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 FIREWALL*** ➧ **ADD/EDIT** ➧ ***EDIT ADDRESSES***.

Feld	Bedeutung
Destination	Hier können Sie einen der vorkonfigurierten Alias für die Zieladresse 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 Firewall*** ➧ **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* ■ *domain/udp* ■ *domain/tcp* ■ *http* ■ *nntp* ■ *netmeeting* Im Menü ***IP*** ➧ ***Stateful Inspection Firewall*** ➧ **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 FIREWALL*** ➧ **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 FIREWALL*** ➧

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 FIREWALL*** ➧ **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 Namen für den Alias 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 des Hosts ein, für den 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 die Pakete des Hosts empfangen und gesandt werden. Sie können unter allen konfigurierten WAN-Partnern wählen.

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

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

Dienstalias hinzufügen

Wenn Sie einen weiteren Dienstalias definieren oder einen bestehenden editieren wollen, können Sie dies im Menü ***IP*** ➧ ***STATEFUL INSPECTION FIREWALL*** ➧ **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 FIREWALL*** ➧ **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	Hiergeben 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 ggf. den Port an, über den der Dienst läuft. Nicht alle Protokolle sind portspezifisch; die Angabe eines Ports entfällt dann.
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 FIREWALL*** ➧ **ADD/EDIT** ➧ ***EDIT SERVICES*** ➧ **ADD/EDIT**

Syslog Messages

Wenn eine der konfigurierten Regeln auf ein Paket zutrifft, und wenn die daraufhin ausgeführte Aktion entweder *deny* oder *reject* ist, so wird ein Syslog-Eintrag erzeugt. Für die Einträge existieren zwei Detailstufen, *info* und *debug*. Die protokollierten Details unterscheiden sich wie folgt:

- *info*
  Auf dieser Ebene werden lediglich der Quell- und der Zielalias sowie der Dienstalias des abgewiesenen Pakets angegeben.
- *debug*
  Auf dieser Ebene werden Quell- und Ziel-IP-Adresse sowie der Port des abgewiesenen Pakets angegeben.

Die Syslog-Messages werden so ausgegeben, wie es im Menü ***SYSTEM*** konfiguriert ist.

SIF Reject Table

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

Die **ipSifAliasRejectTable** enthält folgende Variablen:

Variable	Bedeutung
Index	Die Indexnummer des Eintrags. Sie wird automatisch vergeben.
Source	Die Quell-IP-Adresse des abgewiesenen Pakets.
Destination	Die Ziel-IP-Adresse des abgewiesenen Pakets.
Rejects	Anzahl der abgewiesenen Pakete dieser Verbindung.
Silence	Zeit in Sekunden, während derer keine Pakete abgewiesen wurden.

Variable	Bedeutung
PortLo	Niedrigster Port, an den abgewiesene Pakete gesendet wurden.
PortHigh	Höchster Port, an den abgewiesene Pakete gesendet wurden.

Tabelle 2-4: **ipSifAliasRejectTable**

Die Einträge in der **ipSifAliasRejectTable** sind nicht statisch: Wenn 3600 Sekunden lang kein Paket abgewiesen wird, werden die Einträge als Syslog-Nachricht ausgegeben und anschließend 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 Host-Namens. Die Konfiguration der IP-Adresse des Peers ist nicht notwendig.

Der DynDNS-Dienst signalisiert aber nicht, daß 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-Rufes 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 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 ISDN-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 Eintrag 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 Router reagiert weder auf eingehende ISDN-Rufe von noch initiiert er ISDN-Rufe zu diesem Peer.
passive	Der Router reagiert lediglich auf eingehende ISDN-Rufe und initiiert ggf. den Aufbau eines IPSec-Tunnels zum Peer. Es werden keine ISDN-Rufe an den Peer abgesetzt, um diesen zum Aufbau eines IPSec-Tunnel zu veranlassen.
active	Der Router setzt einen ISDN-Ruf an den Peer ab, um diesen zum Aufbau eines IPSec-Tunnels zu veranlassen. Auf eingehende ISDN-Rufe reagiert der Router nicht.
both	Der Router reagiert auf eingehende ISDN-Rufe und setzt ISDN-Rufe an den Peer ab. 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**

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 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 Peer Ihren Router ruft (Calling Party Number), und für das Feld **OUT** die Nummer, unter der Ihr Router den Peer ruft (Called Party Number).

Im allgemeinen werden die beiden Nummern identisch sein. Unter bestimmten Umständen 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: 091112345      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.

2.2.1 IPSec-Heartbeat

Um feststellen zu können, ob eine 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.

Der Heartbeat wird in zwei der IPSec-Menüs konfiguriert:

- In ***IPSec*** ➧ ***Advanced Settings*** ➧ ***Heartbeat*** werden die Default-Paramter gesetzt.
- In ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT** können bestimmte Default-Paramter 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. ■ *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 können zunächst einmal in NAT (Network Address Translation) nicht voneinander getrennt werden. Pakete, die als Antwort auf eine Anfrage seitens des LANs 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 von LAN her kommenden Pakets eine "externe GRE Context Number" zu und kann somit vom WAN kommende 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-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 frei konfigurierbar, d. h. die zur Verfügung stehenden "Timeslots" können zu mehreren PPP-Multilink-Kanalbündeln zusammengefaßt werden. Bisher war nur ein einziges Kanalbündel mit allen "Timeslots" möglich.

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
```

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.
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 die gewünschten 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. Dieser Wert wird automatisch gesetzt.

Feld	Bedeutung
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 "Stopkanal" auswählen wollen, können Sie dies hier tun.
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 "Stopkanal" für ein Kanalbündel verwenden wollen, können Sie hier eine differenzierte Zuweisung vornehmen.

Feld	Bedeutung
X.75 Layer 2 Mode	Hier definieren Sie, wie sich das Interface, das durch dieses Kanalbündel entsteht, beim Verbindungsaufbau verhält. Mögliche Werte: ■ *dte* ■ *dce*
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-Prozesses vorgenommen:

- Triggered RIP wurde implementiert(Kapitel 2.5.1, Seite 31).
- die Konfigurationsmöglichkeiten für den RIP-Prozeß wurden erweitert (Kapitel 2.5.2, Seite 33).

2.5.1 Triggered RIP

Durch häufige Updates der **ipRouteTable** verursachter Datenverkehr kann unter Umständen erheblich 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.
RIP V2 Triggered	RIP V2 Nachrichten werden gemäß RFC 2091 gesendet.

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 einesetzen, sofern Ihr Netzwerk es zuläßt.

2.5.2 Konfiguration des RIP-Prozesses

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-Prozesses. Im Menü ***IP*** findet sich das neue Untermenü ***ROUTING PROTOCOLS***. Dieses zeigt den Status des Route 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 den RIP-Prozeß:

```
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 weiter 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 grundelegenden Parameter des RIP-Prozesses. 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 einer Route die maximale Metrik von *16* zugeordnet, d. h. die Route hat nur eine minimale Relevanz. 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 Zustände 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 einen "Poisened Reverse" erhält. 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 selben Einstellungen verwenden.

Filter

Im Menü ***IP*** ➧ ***ROUTING PROTOCOLS*** ➧ ***RIP*** ➧ ***FILTER*** können Sie exakt festlegen, wie Routen vom Routing-Prozeß 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 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 Adress** 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, der 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*.
Direction	Hier bestimmen Sie, ob das Filter für den Export oder den Import von Routen gilt. Die möglichen Werte sind: ■ *import* ■ *export*

Feld	Bedeutung
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 Shell-Befehlen

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

Eine Aufstellung der verfügbaren Befehle erhalten Sie, wenn Sie in 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 in 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 2-12, Seite 41).

Wenn Sie einen konfigurierten Timeout korrigieren wollen, beachten Sie, daß Sie den Timeout für den entsprechenden Eintrag (`inx`) ändern. Andernfalls fügen Sie einen weiteren Eintrag hinzu, anstatt einen bestehenden zu ändern. Dies kann zu Komplikationen führen.

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**.
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" in 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 in 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 (XTR-S, XTR-M, XTR-2M, XTR-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 laden. Sie benötigen die folgenden Dateien:

- Für **X4000-Familie**
  - (die Bezeichnungen der Dateien stehen derzeit noch nicht fest)
- Für **X8500/**
  - (die Bezeichnungen der Dateien stehen derzeit noch nicht fest)

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

```
update modem <tftpserver> <filename>.
```

Nachdem Sie die neue Modemlogik eingespielt haben, ist diese sofort betriebsbereit. Ein Neustart des Routers ist nicht notwendig.

3 Änderungen

3.1 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 Arbeit.

5 Bekannte Probleme

Folgende Probleme mit System-Software-Release 6.2.5 sind uns bekannt:

- H.232 und Stateful Inspection Firewall
- TFTP-Operationen mit Konfigurationsdateien

5.1 H.232 und Stateful Inspection Firewall

Die gleichzeitige Verwendung der H.323-Implementierung und der Stateful Inspection Firewall (SIF) ist derzeit nicht möglich.

5.2 TFTP-Operationen mit Konfigurationsdateien

Unter System-Software-Release 6.2.5 ist es möglich, mehrzeilige Banner in das Setup Tol zu integrieren. Dies führt jedoch derzeit dazu, daß Konfigurationen, die derartige Banner enthalten, nicht per TFTP in der Router zurückgespielt werden können.

5 Bekannte Probleme