# Release Notes Systemsoftware-Release 7.1.1

März 2004

Version 1.0

## Systemsoftware-Release 7.1.1

Dieses Dokument beschreibt neue Funktionen, Änderungen, behobene und bekannte Fehler von Systemsoftware-Release 7.1.1.

# 1 Wichtige Informationen

## 1.1 Einschränkungen beim Downgrade

Es ist nicht möglich, direkt von Systemsoftware-Release 7.1.1 auf eine frühere Version des Systemsoftware zurückzukehren.

Konfigurationen, die unter Systemsoftware-Release 7.1.1 erstellt werden, sind mit älterer Systemsoftware nicht kompatibel.

Sichern Sie die Konfiguration Ihres Routers auf einem PC, bevor Sie ein Upgrade vornehmen.

Ein stufenweiser Downgrade ist möglich:

- Sichern Sie die Konfiguration Ihres Routers auf einem PC, bevor Sie auf Systemsoftware-Release 7.1.1 upgraden. Informationen zum externen Sichern einer Konfiguration finden Sie im Handbuch Ihres Routers im Kapitel "Konfigurationsmanagement".
- Nun können Sie das Upgrade vornehmen und ggf. dennoch zu Ihrer alten Systemsoftware zurückkehren. Nach dem Downgrade müssen Sie die zu dieser Systemsoftware passende Konfigurationen auf den Router zurückspielen. Informationen zu den notwendigen Schritten finden Sie im Handbuch Ihres Routers.

Beachten Sie, dass Ihnen nach einem Downgrade bestimmte Funktionen nicht mehr zur Verfügung stehen werden.

Weitere Informationen zu Beschränkungen beim Up- oder Downgrade sowie die Dokumentation Ihres Routers finden Sie unter www.bintec.de

## 1.2 Funktionsumfang

Systemsoftware-Release 7.1.1 führt eine Vielzahl neuer Funktionen und Optimierungen ein. Folgende Besonderheiten sind zu beachten:

### 1.2.1 Einschränkungen

- Für **X1000** und **X1200** steht kein IPSec-Release der Systemsoftware-Release 7.1.1 zur Verfügung.
- **BinGO! DSL II** ist ebenso wie **BinGO! DSL** nicht IPSec-fähig.
- Ebenso stehen die folgenden, in Systemsoftware-Release 7.1.1 neuen Funktionen für **X1000, X1200, BinGO! DSL** und **X3200** nicht zur Verfügung:
  - SSH Login
  - Content Filtering
  - IP Load Balancing.
- **X8500** unterstützt derzeit kein Content Filtering.

### 1.2.2 Erweiterungen

**X1000 II IPSec** und **X1200 II IPSec** stellen eine Reihe von Funktionen wieder zur Verfügung, die aus älteren IPSec-Releases für **X1000** und **X1200** entfernt werden mussten:

- Bridging
- X.25
- XoT
- AoDI
- H.323

- Encrypted ISDN Login
- RIP

Darüber hinaus stehen für **X1000 II** und **X1200 II** folgende Funktionen zum ersten Mal zur Verfügung:

- PPPoE-Server (auch für **BinGO! DSL II**)
- OSPF
- RADIUS PPP Authentication
- BRRP
- Frame Relay (mit entsprechender Lizenz)
- IPSec Peers über RADIUS

## 1.3 Software-Image-Namen

Die Bezeichnungen der Software-Images haben sich dahingehend geändert, dass der eigentlichen Release-Kennung die Bezeichnung des Gerätes vorangestellt wird. Werden Ihre Router mittels des Konfigurationswerkzeugs XAdmin konfiguriert, so müssen Sie zunächst noch die alten Image-Namen verwenden. Dazu löschen Sie lediglich die Gerätekennung aus dem Namen: "X1x00II-b7101.x2x" wird so zu "b7101.x2x".

## 1.4 BRICKware Wizard

Ab Release 7.1.1 unterstützt unsere Systemsoftware den **BRICKware** Configuration Wizard nicht mehr. Ein neuer, HTML-basierter Configuration Wizard wird mit Systemsoftware Release 7.1.3 eingeführt, das kurze Zeit nach Systemsoftware-Release 7.1.1 zur Verfügung stehen wird.

# 2 Neue Funktionen

Systemsoftware-Release 7.1.1 enthält die folgenden neuen Funktionen:

- 2.1: "Unterstützung neuer X8500-Boards"
- 2.2: "IPSec Interface Concept"
- 2.3: "Content Filtering"
- 2.4: "IP Load Balancing"
- 2.5: "ATM-Redesign"
- 2.6: "Analog-/GSM-Interface"
- 2.7: "Email Alert"
- 2.8: "SSH Login"
- 2.9: "GRE (Generic Routing Encapsulation)"

## 2.1 Unterstützung neuer X8500-Boards

Ab Release 7.1.1 unterstützt die Systemsoftware die neu eingeführten Boards von **X8500**: Das **X8E-1/2E3** für einen oder zwei E3-Anschlüsse sowie das neue System-Board **X8A-SYS-VPN**. Informationen zur Konfiguration und zum Einbau finden Sie im Downloadbereich von **X8500** bei www.bintec.de.

## 2.2 IPSec Interface Concept

Die Konfiguration von IPSec-Peers war bisher lediglich über Traffic Lists möglich. Dadurch war eine vollständige Nutzung der Konfigurationsoptionen, wie sie für WAN-Partner zur Verfügung stehen, nicht möglich. Systemsoftware-Release 7.1.1 IPSec führt eine grundlegend neue Art der IPSec-Konfiguration

ein, die diesen Nachteil ausgleicht. Die gewohnte Art der Peer-Konfiguration über Traffic Lists steht weiterhin zur Verfügung.

Im neuen Konfigurationskonzept entspricht ein IPSec-Peer einem virtuellen Interface. Damit stehen u. a. die folgenden Funktionen zur Behandlung von IPSec-Verbindungen zur Verfügung:

- NAT und IPSec
- Routing-Protokolle wie RIP
- Rerouting
- weitere Sicherheitsfunktionen wie SIF und TAF, Filterlisten
- IP Accounting für IPSec-Peers
- weitere Funktionen, die zur Konfiguration von WAN-Partnern zur Verfügung stehen.

Die Konfiguration eines auf Traffic Lists basierenden IPSec-Peers hat sich nur geringfügig geändert (siehe "Änderungen bei der Konfiguration der Traffic Lists", Seite 16), Informationen zur Konfiguration von Traffic Lists finden Sie im IPSec-Handbuch bzw. den entsprechenden Release Notes.

### 2.2.1 IKE- und IPSec-Profile

Die Einstellungen, die bestimmen, wie Phase 1 und Phase 2 eines Tunnelaufbaus durchgeführt werden, sind in Systemsoftware-Release 7.1.1 in **Profilen** abgelegt. Diese Profile stehen in all den Konfigurationskontexten zur Verfügung, an denen Einstellungen bisher isoliert vorgenommen werden mussten. D. h., dass ein Profil, das in einem bestimmten Kontext erstellt wird (z. B. bei der Anpassung eines Peers), auch in anderen Kontexten (zum Beispiel bei der Definition der Default-Einstellungen für Phase 1 und Phase 2 im IPSec-Hauptmenü) zur Verfügung steht.

Das Menü zur Konfiguration von Profilen findet sich im Setup Tool an drei Stellen:

- ***IPSec*** ➧ ***IKE (Phase 1)/IPSec (Phase 2) Defaults edit*** im Kontext der Festlegung des Default-Profils, das für jeden Peer gilt, sofern keine Peer-spezifischen Einstellungen vorgenommen werden.
- ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT** ➧ ***Peer specific Settings*** ➧ ***IKE (Phase 1)/IPSec (Phase 2) Profile: edit*** im Kontext der Peer-spezifischen Einstellungen.
- ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT** ➧ ***Traffic List Settings*** ➧ **APPEND/EDIT** im Kontext der Konfiguration vonTraffic Lists (nur für Phase-2-Profile).

Die Menüs sind in allen Kontexten identisch, ein Profil, das in einem Kontext erstellt wird, steht auch in allen anderen zur Verfügung.

Da für die IPSec-Konfiguration ein Profil vorhanden sein muss (auch wenn dies später nicht verwendet werden soll), sollte der IPSec-Wizard zur Erstellung eines ersten Peers verwendet werden. Dadurch ist sichergestellt, dass ein funktionsfähiges Profil existiert.

Erstellen Sie ein neues Profil im Setup Tool, sind im entsprechenden Menü die meisten Parameter auf den Wert *default* gestellt. Dies bedeutet, dass für den entsprechenden Parameter die Werte des Profils übernommen werden, das im IPsec-Hauptmenü als Default-Profil ausgewählt ist.

Wie bei früheren Versionen der IPSec-Software ist es nach wie vor notwendig, den nicht-interaktiven Teil des IPSec-Wizards einmal zu durchlaufen, da erst dadurch die IKE- und IPSec-Proposals und entsprechende Profile zur Verfügung gestellt werden.

### 2.2.2 Peer-Konfiguration

Das Menü zum Erstellen eines Peers (gleich welchen Typs) sieht in Systemsoftware-Release 7.1.1 folgendermaßen aus:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[IPSEC][PEERS][ADD]                                            MyRouter

     Description:
     Admin Status:      up        Oper Status:   dormant

     Peer Address:
     Peer IDs:
     Pre Shared Key:    *

     IPSec Callback >
     Peer specific Settings >

     Virtual Interface: no
     Traffic List Settings >

                          SAVE                          CANCEL
```

Es enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Description** | Hier geben Sie eine beliebige Beschreibung des Peers an. Die maximale Länge des Eintrags beträgt 255 Zeichen. |

| Feld | Bedeutung |
|---|---|
| **Admin Status** | Hier wählen Sie den Zustand aus, in den Sie den Peer nach dem Speichern der Konfiguration versetzen wollen. Die Einstellung gilt für jede Art von Peer.<br>Zur Verfügung stehen:<br>■ *up* - Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung.<br>■ *down* - Der Peer steht nach dem Speichern der Konfiguration zunächst nicht zur Verfügung.<br>■ *dialup* - Nach dem Speichern wird einmalig ein Tunnel aufgebaut. Dabei werden alle möglichen Verbindungsarten (also auch Callback) berücksichtigt.<br>■ *callback* - Nach dem Speichern wird ein Tunnel zum Peer aufgebaut. Dabei wird so verfahren, als sei ein initialer Callback-Ruf bereits eingegangen. |
| **Oper Status** | Hier wird der derzeitige Zustand des Peers angezeigt. Das Feld ist nicht editierbar. |
| **Peer Address** | Hier geben Sie die offizielle IP-Adresse des Peers bzw. seinen auflösbaren Host-Namen ein. Die Eingabe kann in bestimmten Konfigurationen entfallen.<br>Weitere Informationen finden Sie im IPSec-Handbuch. |

| Feld | Bedeutung |
|---|---|
| **Peer IDs** | Hier geben Sie die ID des Peers ein. Die Eingabe kann in bestimmten Konfigurationen entfallen.<br>Auf dem Peer-Router entspricht diese ID der **Local ID** (***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** ➧ ***IKE (PHASE 1) DEFAULTS: EDIT*** ➧ **ADD/EDIT**).<br>Weitere Informationen finden Sie im IPSec-Handbuch. |
| **Pre Shared Key** | Nur bei Authentisierung über Preshared Keys.<br>Hier geben Sie den mit dem Peer vereinbarten Passphrase ein.<br>Die **Authentication Method** kann im Menü ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** ➧ ***IKE (PHASE 1) DEFAULTS: EDIT*** für den Peer angepasst werden. |
| **Virtual Interface** | Hier legen Sie fest, ob der Peer wie bisher mit einer Traffic List oder als virtuelles Interface geführt wird.<br>Zur Verfügung stehen:<br>■ *no* - Verbindungen zum Peer werden über eine Traffic List gesteuert.<br>■ *yes* - Der Peer wird als virtuelles Interface erstellt. Der Datenverkehr, der über dieses Interface geroutet wird, wird vollständig verschlüsselt.<br>Default ist *no*. |

Tabelle 2-1: ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **APPEND/EDIT**

Die Anpassung des Peers erfolgt in den folgenden Menüs:

- ***IPSEC CALLBACK*** (Informationen zur Konfiguration des IPSec Callback finden Sie in den Release Notes zum Systemsoftware Release 6.2.5.)
- ***PEER SPECIFIC SETTINGS*** (siehe Kapitel 2.2.3, Seite 18)
- ***TRAFFIC LIST SETTINGS*** (für **Virtual Interface** = *no*, Informationen zur Konfiguration von Traffic Lists finden Sie im IPSec-Handbuch)
- ***INTERFACE IP SETTINGS*** (für **Virtual Interface** = *yes*, siehe Kapitel 2.2.4, Seite 24).

### Änderungen bei der Konfiguration der Traffic Lists

Obwohl die Konfiguration von Traffic Lists weitgehend gleich geblieben ist, kommen zur Einstellung des *protect*-Modus der Traffic Lists ebenfalls IPSec-Profile zum Einsatz:

```
BinTec Router Setup Tool                  BinTec Access Networks GmbH
[IPSEC][PEERS][Traffic][ADD]: Edit Traffic Entry              MyRouter

    Description:

     Protocol:      dont-verify

     Local:
          Type: net   Ip: 192.168.1.0         / 24

     Remote:
          Type: net   Ip: 192.168.2.0        / 24

     Action:        protect

     Profile          default              edit >


                    SAVE                                CANCEL
```

Die Anwendung der Profile erfolgt wie in Kapitel 2.2.3, Seite 18 beschrieben.

Darüber hinaus lassen sich die IKE- und IPSec-Einstellungen auf Traffic Lists basierender Peers im Menü ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** für den Peer allgemein anpassen.

### 2.2.3 IKE- und IPSec-Einstellungen

Das Menü ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** enthält die Optionen zur Anpassung der IKE- und IPSec-Einstellungen für den Peer:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[IPSEC][PEERS][EDIT][SPECIAL]: IPSec Peer Special Settings    MyRouter

 Special settings for p1

     IKE (Phase 1) Profile:   default                 edit >
     IPsec (Phase 2) Profile: default                 edit >

     Select Different Traffic List >

                          SAVE                          CANCEL
```

Dieses Menü erlaubt die Auswahl von zuvor definierten Profilen für Phase 1 und Phase 2. Der Wert *default* steht dabei für das im IPSec-Hauptmenü, Feld **IKE (Phase 1)/IPSec (Phase 2) Defaults**, eingestellte Profil.

Das Menü ***SELECT DIFFERENT TRAFFIC LIST*** ist nur dann zugänglich, wenn ein Peer mit Traffic Lists angelegt wird.

#### Phase-1-Profil

Das Menü zur Konfiguration eines Phase-1-Profils ist bei der Peer-Konfiguration über das Menü ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** ➧ ***IKE (PHASE 1) PROFILE: EDIT*** ➧ **ADD/EDIT** zugänglich:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[IPSEC][PEERS][ADD][SPECIAL][PHASE1][ADD]                      MyRouter

 Description (Idx 0) :
   Proposal              :  none/default
   Lifetime              :  use default
   Group                 :  default
   Authentication Method :  default
   Mode                  :  default
   Heartbeats            :  default
   Block Time            :  -1
   Local ID              :
   Local Certificate     :  none
   CA Certificates       :

   View Proposals >
   Edit Lifetimes >

                         SAVE                          CANCEL
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Description** | Informationen zu diesen Parametern finden Sie im IPSec-Handbuch, Kapitel 3.4.3. |
| **Proposal** | |
| **Lifetime** | |
| **Group** | |
| **Authentication Method** | |
| **Mode** | |

| Feld | Bedeutung |
|---|---|
| **Heartbeats** | Hier wählen Sie, ob und in welcher Weise IPSec Heartbeats verwendet werden.<br>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.<br>Zur Verfügung stehen:<br>■ *default* - Der Router verwendet die Einstellung des Default-Profils.<br>■ *none* - Der Router sendet und erwartet keinen Heartbeat.<br>■ *expect* - Der Router erwartet einen Heartbeat vom Peer, sendet selbst aber keinen.<br>■ *send* - Der Router erwartet keinen Heartbeat vom Peer, sendet aber einen.<br>■ *both* - Der Router erwartet einen Heartbeat vom Peer und sendet selbst einen.<br>Ab Systemsoftware-Release 7.1.1 werden Heartbeats für Phase 1 und Phase 2 getrennt konfiguriert. Wenn Interoperabilität mit älterer Software zu gewährleisten ist, müssen für Phase 1 und Phase 2 die gleichen Werte konfiguriert werden. |

| Feld | Bedeutung |
|---|---|
| **Block Time** | Hier legen Sie fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist. Dies betrifft nur lokal initiierte Aufbauversuche.<br>Zur Verfügung stehen Werte von *-1* bis *86400* (Sekunden), der Wert *-1* (Defaultwert) bedeutet die Übernahme des Wertes im Defaultprofil, der Wert *0*, dass der Peer in keinem Fall blockiert wird. |
| **Local ID** | Informationen zu diesen Parametern finden Sie im IPSec-Handbuch, Kapitel 3.4.3. |
| **Local Certificate** | |
| **CA Certificates** | |

Tabelle 2-2: ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT** ➧ ***Peer specific Settings*** ➧ ***IKE (Phase 1) Profile: edit*** ➧ **ADD/EDIT**

Die Menüs ***View Proposals*** und ***Edit Lifetimes*** unterscheiden sich nicht von denen der IPSec-Software Version 6.3.4 (Informationen finden Sie im IPSec-Handbuch, Kapitel 3.4.3).

### Phase-2-Profil

Ebenso wie für die Phase 1 können Sie Profile für die Phase 2 des Tunnelaufbaus definieren.

Die Konfiguration erfolgt im Menü ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** ➧ ***IPSEC (PHASE 2) PROFILE: EDIT*** ➧ **ADD/EDIT**:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[IPSEC][PEERS][ADD][SPECIAL][PHASE2][ADD]                       MyRouter

   Description (Idx 0) :

   Proposal              :  default
   Lifetime              :  use default
   Use PFS               :  default
   Heartbeats            :  default
   Propagate PMTU        :  default


   View Proposals >
   Edit Lifetimes >


                         SAVE                          CANCEL
```

Das Menü enthält die folgenden Felder:

| Feld | Bedeutung |
|---|---|
| **Proposal** | Informationen zu diesen Parametern finden Sie im IPSec-Handbuch, Kapitel 3.4.3. |
| **Lifetime** | |
| **Use PFS** | |

| Feld | Bedeutung |
|---|---|
| **Heartbeats** | Hier wählen Sie, ob und in welcher Weise IPSec Heartbeats verwendet werden.<br>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.<br>Zur Verfügung stehen:<br>■ *default* - Der Router verwendet die Einstellung des Default-Profils.<br>■ *none* - Der Router sendet und erwartet keinen Heartbeat.<br>■ *expect* - Der Router erwartet einen Heartbeat vom Peer, sendet selbst aber keinen.<br>■ *send* - Der Router erwartet keinen Heartbeat vom Peer, sendet aber einen.<br>■ *both* - Der Router erwartet einen Heartbeat vom Peer und sendet selbst einen.<br>Ab Systemsoftware-Release 7.1.1 werden Heartbeats für Phase 1 und Phase 2 getrennt konfiguriert. Wenn Interoperabilität mit älterer Software zu gewährleisten ist, müssen für Phase 1 und Phase 2 die gleichen Werte konfiguriert werden. |

| Feld | Bedeutung |
|---|---|
| **Propagate PMTU** | Hier wählen Sie aus, ob während der Phase 2 die PMTU (Path Maximum Transfer Unit) propagiert werden soll oder nicht.<br>Zur Verfügung stehen:<br>■ *default* - Der Router verwendet die Einstellung des Default-Profils.<br>■ *no* - Die Path Maximum Transfer Unit wird nicht übermittelt.<br>■ *yes* - Die Path Maximum Transfer Unit wird übermittelt. |

Tabelle 2-3: ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** ➧ ***IPSEC (PHASE 2) PROFILE: EDIT*** ➧ **ADD/EDIT**

Die Menüs ***VIEW PROPOSALS*** und ***EDIT LIFETIMES*** unterscheiden sich nicht von denen der IPSec-Software-Version 6.3.4 (Informationen finden Sie im IPSec-Handbuch, Kapitel 3.4.3).

### 2.2.4 Peer IP-Konfiguration

Die IP-Konfiguration eines Interface Peers erfolgt im Menü ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***INTERFACE IP SETTINGS***. Das Menü ist identisch mit dem zur IP-Konfiguration eines WAN-Partners. Es ist im Zuge der IPSec-Änderungen neu gestaltet worden. Die Änderungen finden Sie in Kapitel 3.2, Seite 81 beschrieben.

## 2.3 Content Filtering

Mit Systemsoftware-Release 7.1.1 führt BinTec URL-basiertes Content Filtering ein. Dieser Dienst verhält sich wie ein lokaler HTTP-Proxy. Er greift zur

Laufzeit auf den Orange Filter der Firma Cobion (http://www.cobion.de) zu und überprüft, wie eine angeforderte Internet-Seite durch den Cobion-Filter kategorisiert worden ist. Die Aktion, die sich aus der Kategorisierung ergibt, wird auf dem Router konfiguriert.

Zum Betrieb des Cobion Orange Filters ist eine Lizenz von Cobion zu erwerben. Im Auslieferungszustand kann über einen bestimmten Status (siehe Tabelle 2-4, Seite 27) eine 30-Tage-Testlizenz generiert werden. Diese ist an die Seriennummer Ihres Routers gebunden und kann nur einmal aktiviert werden.

Grundsätzlich kann der versuchte Aufruf einer URL oder IP-Adresse beim Conten Filtering zu folgenden Reaktionen führen:

- Der Aufruf der angeforderten Seite wird unterbunden.
- Der Aufruf wird zugelassen, aber protokolliert.
- Der Aufruf wird zugelassen, ohne protokolliert zu werden.

### 2.3.1 Basisparameter

Die Konfiguration erfolgt im Menü ***SECURITY*** ➧ ***COBION ORANGE FILTER***:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[SECURITY][ORANGE FILTER]: Static Settings                    MyRouter


          Admin Status        : disable
          Orange Filter Ticket: B1BT

          Ticket Status       :

          Filtered Interface  : none
          History Entries     : 64

          Configure White List >
          Configure Filters >
          View History >

                    SAVE                                CANCEL

Use <Space> to select
```

Dieses Menü erlaubt die Konfiguration grundlegender Parameter sowie den Zugang zu den weiteren Konfigurationsmenüs. Es enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Admin Status** | Hier können Sie das Filter aktivieren. Die verfügbaren Einstellungen sind:<br>■ *disable* - Content Filtering ist deaktiviert (Defaultwert).<br>■ *enable* - Content Filtering ist aktiviert.<br>■ *enable 30 day demo ticket* - der Router fordert von Cobion eine Demo-Lizenz an. |

| Feld | Bedeutung |
|---|---|
| **Orange Filter Ticket** | Hier tragen Sie die Nummer der erworbenen Cobion-Lizenz ein. Die voreingestellte, von Cobion vergebene Kennung bezeichnet den Gerätetyp. |
| **Expiring Date** | Dieses Feld wird nur angezeigt, wenn eine Lizenz eingetragen und überprüft worden ist. Es zeigt das Ablaufdatum der Lizenz an und kann nicht editiert werden. |
| **Ticket Status** | Hier wird das Ergebnis der letzten Gültigkeitsprüfung des Lizenz angezeigt. Die Gültigkeit der Lizenz wird alle 23 Stunden überprüft. |
| **Filtered Interface** | Hier wählen Sie aus, für welches der vorhandenen Ethernet-Interfaces Content Filtering aktiviert werden soll. Es kann lediglich ein Interface spezifiziert werden. Die Aufrufe, die über dieses Interface gehen, werden dann vom Content Filtering überwacht.<br>Defaultwert ist *none*. |
| **History Entries** | Hier definieren Sie die Anzahl an Einträgen, die in der Content Filtering History gespeichert werden sollen.<br>Verfügbar sind ganze Zahlen zwischen *1* und *512*, der Defaultwert ist *64*. |

Tabelle 2-4: ***SECURITY*** ➧ ***COBION ORANGE FILTER***

Abgesehen von der Konfiguration der grundlegenden Parameter erlaubt das Menü ***SECURITY*** ➧ ***COBION ORANGE FILTER*** Zugriff auf folgende Menüs:

- ***CONFIGURE WHITE LIST*** zur Konfiguration von URLs, die unabhängig von der Kategorisierung durch Cobion aufgerufen werden können.
- ***CONFIGURE FILTERS*** zur Konfiguration der Aktionen, die aufgrund der Kategorisierung durch Cobion vorgenommen werden soll.

- ***VIEW HISTORY*** zur Einsicht in die gespeicherten URL-Aufrufe.

### 2.3.2 White List konfigurieren

Das Menü ***SECURITY*** ➧ ***COBION ORANGE FILTER*** ➧ ***CONFIGURE WHITE LIST*** enthält eine Liste derjenigen URLs bzw. IP-Adressen, die auch dann aufgerufen werden können, wenn sie aufgrund der Filterkonfiguration und der Klassifizierung im Cobion Filter blockiert würden (das Beispiel enthält beliebige Werte, in der Defaultkonfiguration sind keine Einträge enthalten):

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[SECURITY][ORANGE FILTER][WHITE LIST]: Url List                MyRouter

 White List:

    Url / Address
    192.168.1.253
    192.168.1.254
    www.bintec.de
    www.cobion.de



     ADD                 DELETE              EXIT
```

Über die Schaltfläche **ADD** kann man weitere URLs oder IP-Adressen der Liste hinzufügen. Die Länge eines Eintrags ist auf 60 Zeichen begrenzt. Adressen, die in der White List geführt sind, werden automatisch zugelassen. Die Konfiguration eines entsprechenden Filters ist nicht notwendig.

### 2.3.3 Filter konfigurieren

Im Menü ***SECURITY*** ➧ ***COBION ORANGE FILTER*** ➧ ***CONFIGURE FILTERS*** konfigurieren Sie, welche URLs und IP-Adressen auf welche Weise behandelt werden sollen. Grundsätzlich gibt es dabei unterschiedliche Ansätze: Zum einen kann man eine Filterliste anlegen, die nur Einträge für solche Adressen anlegen, die blockiert bzw. protokolliert werden sollen. In diesem Fall ist es notwendig, am

Ende der Filterliste einen Eintrag vorzunehmen, der alle Zugriffe, auf die kein Filter zutrifft, gestattet. Wenn Sie nur Einträge für solche Adressen anlegen, die zugelassen werden sollen, ist eine Änderung des Default-Verhaltens nicht notwendig.

Wenn Sie Filter konfiguriert haben, werden diese gemäß ihrer Priorität durchlaufen, d. h. wenn für eine Adresse mehr als eine Kategorie zutrifft, wird das erste zutreffende Filter angewendet.

Wenn bei konfigurierten Filtern eine Adresse zu keinem der Filter passt, so wird sie blockiert. Um dieses Verhalten zu ändern ist ein Filter der Kategorie "Default behaviour" erforderlich, der derartige Adressen ggf. zulässt.

Die Konfiguration der Filter erfolgt im Menü ***Security*** ➧ ***Cobion Orange Filter*** ➧ ***Configure Filters***. Zunächst wird eine Liste der bereits konfigurierten Filter angezeigt (das Beispiel enthält beliebige Werte, in der Defaultkonfiguration sind keine Filter enthalten).

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
SECURITY][ORANGE FILTER][FILTER]: Filter List                  MyRouter

   Content Filter List:

Category                        Day          Start  Stop   Action   Prio

No valid license ticket         Everyday      00:00  23:59  allow       1
Unknown URL                     Everyday      00:00  23:59  allow      10
Anonymous Proxies               Everyday      00:00  23:59  block      20
Criminal Activities             Everyday      00:00  23:59  block      21
Pornography / Nudity            Everyday      00:00  23:59  block      22
Drugs                           Everyday      00:00  23:59  block      23
Other Category                  Everyday      00:00  23:59  logging    30
Orange Server not reachable     Everyday      00:00  23:59  logging    35
Default behaviour               Everyday      00:00  23:59  allow     100


     ADD                DELETE              EXIT
```

Über die Schaltfläche **ADD** gelangen Sie in das Menü zur Filterkonfiguration:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[SECURITY][ORANGE FILTER][FILTER][ADD]                          MyRouter

  Category :  Anonymous Proxies

          Day       :  Everyday
          From      :  [0 :0 ]   To : [23:59]
          Action    :  block
          Priority  :  0


                     SAVE                                CANCEL
```

Es enthält die folgenden Felder:

| Feld | Bedeutung |
|---|---|
| **Category** | Hier wählen Sie aus, auf welche Kategorie von Adressen/URLs das Filter angewendet werden soll.<br>Zur Auswahl stehen zum einen die Standardkategorien des Cobion-Filters. Darüber hinaus können die Aktionen für folgende Sonderfälle definiert werden:<br>■ *Default behaviour* - Wenn eine Adresse keinem der Filter entspricht, wird sie per Default blockiert. Dieses Verhalten lässt sich mit dieser Kategorie ändern.<br>■ *No valid license ticket* - Wenn die Cobion Lizenz ungültig ist, werden bei aktivem Content Filtering alle Aufrufe unterbunden. Dieses Verhalten lässt sich mit dieser Kategorie ändern, ohne das *Default behaviour* ändern zu müssen. |

| Feld | Bedeutung |
|---|---|
| **Category (Forts.)** | ■ *Orange Server not reachable* - Sollten die Cobion-Server nicht erreichbar sein, wird die mit dieser Kategorie verbundene Aktion angewendet.<br>■ *Other Category* - Manche Adressen sind dem Cobion-Filter bereits bekannt, aber noch nicht kategorisiert. Für derartige Adressen wird die mit dieser Kategorie verbundene Aktion angewendet.<br>■ *Unknown URL* - Wenn eine Adresse dem Cobion-Filter nicht bekannt ist, wird die mit dieser Kategorie verbundene Aktion angewendet. |
| **Day** | Hier wählen Sie aus, an welchen Tagen das Filter aktiv sein soll.<br>Zur Verfügung stehen:<br>■ *Everyday* - Das Filter gilt für jeden Tag der Woche.<br>■ *<Wochentag>* - Das Filter gilt für einen bestimmten Tag der Woche. Es kann pro Filter nur ein Tag ausgewählt werden, für mehrere einzelne Tage müssen mehrere Filter angelegt werden.<br>■ *Monday-Friday* - Das Filter gilt Montags bis Freitags.<br>Default ist *Everyday.* |

| Feld | Bedeutung |
|---|---|
| **From** | Hier geben Sie ein, zu welcher Uhrzeit das Filter aktiviert werden soll. Die Eingabe erfolgt nach dem Schema *hh:mm*.<br>Default ist *0:0*. |
| **To** | Hier geben Sie ein, zu welcher Uhrzeit das Filter deaktiviert werden soll. Die Eingabe erfolgt nach dem Schema *hh:mm*.<br>Default ist *23:59*. |
| **Action** | Hier wählen Sie die Aktion, die ausgeführt werden soll, wenn das Filter auf einen Aufruf zutrifft.<br>Zur Verfügung stehen:<br>■ *block* - Der Aufruf der angeforderten Seite wird unterbunden.<br>■ *logging* - Der Aufruf wird zugelassen, aber protokolliert. Einsicht in die protokollierten Ereignisse ist im Menü ***SECURITY*** ➧ ***COBION ORANGE FILTER*** ➧ ***VIEW HISTORY*** möglich.<br>■ *allow* - Der Aufruf wird zugelassen, ohne protokolliert zu werden.<br>Default ist *block*. |
| **Priority** | Hier weisen Sie dem Filter eine Priorität zu. Die Filter werden gemäß dieser Priorität angewendet.<br>Zur Verfügung stehen alle (ganzzahligen) Werte von *1* bis *999*, ein Wert von *1* entspricht der höchsten Priorität. |

Tabelle 2-5: ***SECURITY*** ➧ ***COBION ORANGE FILTER*** ➧ ***CONFIGURE FILTERS*** ➧ **ADD**

Informationen zu den Standardkategorien des Cobion Orange Filters finden Sie hier: http://www.cobion.de/support/techsupport/dbcategories/). Im Setup Tool werden die englischen Ausdrücke verwendet. Diese finden Sie auf den entsprechenden englischen Seiten.

### 2.3.4 History einsehen

Im Menü ***SECURITY*** ➧ ***COBION ORANGE FILTER*** ➧ ***VIEW HISTORY*** können Sie die aufgezeichnete History des Content Filters einsehen:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[SECURITY][ORANGE FILTER][HISTORY]: History List              MyRouter

History List:

Date   Time     Client       Url               Category           Action

11/12 16:09.52 192.168.0.1 www.xxx.de/       Pornography/Nudity block
11/12 16:09.52 192.168.0.2 www.droge.de/     Drugs              block

                                             EXIT
```

In der History werden alle Aufrufe protokolliert, die durch einen entsprechenden FIlter dafür markiert werden (Aktion = *logging*), ebenso alle abgewiesenen Aufrufe.

## 2.4 IP Load Balancing

Zunehmender Datenverkehr über das Internet erfordert die Möglichkeit, Daten über unterschiedliche Links oder Interfaces senden zu können, um die zur Verfügung stehenden Gesamtbandbreite zu erhöhen. Seitens der Service Provider wird es allerdings zumeist nicht angeboten, mehrere unterschiedliche Interfaces zu einer logischen Verbindung zusammenzufassen. IP Load Balancing

ermöglicht die Verteilung des Datenverkehrs einer logischen Verbindung auf mehrere Links oder Interfaces.

Die Konfiguration erfolgt im Menü IP ➧ ***BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)*** ➧ ***IP LOAD BALANCING OVER MULTIPLE INTERFACES***.

Alle Interfaces, die mittels des Load-Balancing zu einer Interface-Gruppe zusammengefasst werden sollen, müssen Routen mit identischer Metrik haben. Für ein Load Balancing über Internetverbindungen z. B., ist eine Defaultroute mit identischer Metrik für jedes Interface der Gruppe notwendig.

Beim IP Load Balancing wird nur der abgehende Datenverkehr geregelt. Eingehender Datenverkehr wird gemäß des von der Gegenstelle bestimmten Routings behandelt.

Zunächst wird eine Liste der bereits für Load-Balancing konfigurierten Interface-Gruppen angezeigt. Über **ADD/EDIT** gelangen Sie in das Menü zur Konfiguration der Gruppen (der Screenshot enthält beliebige Beispielwerte):

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[IP][IP LOAD BALANCING][ADD]                                  MyRouter


Description
Interface Group ID    1

Distribution Policy session round-robin
Distribution Mode   always (use operational up and dormant interfaces)
Distribution Ratio  equal for all interfaces of the group

Interface 1                              en1-0
Distribution Fraction (in percent)       50

Interface 2                              ethoa50-0
Distribution Fraction (in percent)       50

Interface 3                              none


               SAVE                                  CANCEL
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Description** | Hier geben Sie eine beliebige Beschreibung der Interface-Gruppe ein. |
| **Interface Group ID** | Die ID der Interface-Gruppe. Sie wird vom System automatisch vergeben, kann aber auch editiert werden. Sie dient lediglich der internen Zuordnung der Gruppe. |
| **Distribution Policy** | Hier wählen Sie aus, auf welche Art der Datenverkehr auf die für die Gruppe konfigurierten Interfaces verteilt wird.<br>Zur Verfügung stehen:<br>■ *session round-robin* - Eine neu aufgebaute Session wird je nach prozentualer Belegung der Interfaces mit Sessions einem der Gruppen-Interfaces zugewiesen. Gemessen wird die Anzahl der einem Interface zugewiesenen Sessions.<br>■ *bandwidth load-dependent* - Eine neu aufgebaute Session wird je nach prozentualer Auslastung der Interfaces einem der Gruppen-Interfaces zugewiesen. Gemessen wird die aktuelle Datenrate des Interfaces, wobei der Datenverkehr sowohl in Sende- als auch in Empfangsrichtung berücksichtigt wird. |

| Feld | Bedeutung |
|---|---|
| **Distribution Policy (Forts.)** | ■ *bandwidth download-dependent* - Eine neu aufgebaute Session wird je nach prozentualer Auslastung der Interfaces einem der Gruppen-Interfaces zugewiesen. Gemessen wird die aktuelle Datenrate des Interfaces, wobei nur der Datenverkehr in Empfangsrichtung berücksichtigt wird.<br>■ *bandwidth upload-dependent* - Eine neu aufgebaute Session wird je nach prozentualer Auslastung der Interfaces einem der Gruppen-Interfaces zugewiesen. Gemessen wird die aktuelle Datenrate des Interfaces, wobei nur der Datenverkehr in Senderichtung berücksichtigt wird.<br>■ *service/source-based routing* - Eine neue Session wird einem der Gruppen-Interfaces gemäß der Konfiguration des statischen Routings im Menü ***IP LOAD BALANCING OVER MULTIPLE INTERFACES*** ➧ **ADD/EDIT** ➧ ***IP ROUTING LIST*** zugewiesen.<br>Das Menü ist nur zugänglich, wenn Sie *service/source-based routing* ausgewählt haben. |

| Feld | Bedeutung |
|---|---|
| **Distribution Mode** | Hier wählen Sie aus, in welchem **ifOperStatus** sich ein Interface der Gruppe befinden darf, damit es ins Load Balancing einbezogen wird.<br>Zur Verfügung stehen:<br>■ *always (use operational up and dormant interfaces)* - Interfaces, die entweder *up* oder *dormant* sind, werden einbezogen.<br>■ *up-only (operational up interfaces only)* - Nur Interfaces, die *up* sind, werden einbezogen. |
| **Distribution Ratio** | Nicht bei **Distribution Policy** = *service/source-based routing.*<br>Hier wählen Sie aus, ob der Anteil an den aufzubauenden Sessions für alle Interfaces der Gruppe der gleiche sein oder ob er für jedes Interface individuell konfiguriert werden soll. Zur Verfügung stehen:<br>■ *equal for all interfaces of the group* - Allen Interfaces wird automatisch der gleiche Anteil zugewiesen.<br>■ *individual for all interfaces of the group* - Jedem Interface kann individuell ein Anteil an Sessions zugewiesen werden. |
| **Interface <1 - 3>** | Hier wählen Sie unter den zur Verfügung stehenden Interfaces diejenigen aus, die der Gruppe angehören sollen. |

| Feld | Bedeutung |
|---|---|
| **Distribution Fraction (in percent)** | Nicht bei **Distribution Policy** = *service/source-based routing.*<br>Hier geben Sie an, welchen Prozentsatz der anfallenden Sessions ein Interface übernehmen soll.<br>Die Bedeutung unterscheidet sich je nach verwendeter **Distribution Policy**:<br>■ für *session round robin* wird die Anzahl der zu verteilenden Sessions zugrunde gelegt - z. B. bedeutet. *60%*, dass 60% aller Sessions dem Interface zugewiesen werden können.<br>■ für *bandwidth load/upload/download dependent* wird die prozentuale Auslastung des Interfaces zugrunde gelegt - z. B. bedeutet 60%, dass dem Interface 60% Prozent der Gesamtlast zugewiesen werden können. |

Tabelle 2-6: ***IP*** ➧ ***Bandwidth Management (Load Balancing / BOD)*** ➧ ***IP Load Balancing over Multiple Interfaces*** ➧ **ADD/EDIT**

Für die Konfiguration des Load Balancing kann je Interface ein weiteres Untermenü relevant sein: ***IP Load Balancing over Multiple Interfaces*** ➧ **ADD/EDIT** ➧ ***IP Routing List*** ➧ **ADD/EDIT**. Hier werden die Parameter kon-

figuriert, nach denen neue Sessions auf die Interfaces verteilt werden, wenn als Distribution Policy *service/source-based routing* ausgewählt worden ist:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[IP][ROUTING][ADD]: Configure Service/Source-Based Routing    MyRouter

    Interface                    en1-0

    Type                         Host route
    Network                      LAN

    Destination IP-Address

    Gateway IP-Address

    Source IP-Address
    Source Mask

    Protocol                    tcp
    Service                      unlisted service            Port   -1


                                SAVE                CANCEL
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Interface** | In diesen Feldern entspricht das Menü dem Menü zum Erstellen einer Extended-Routing-Konfiguration im Menü ***IP*** ➧ ***ROUTING*** ➧ **ADDEXT**. Informationen dazu finden Sie im Handbuch von **X4100/200/300** im Abschnitt "Weiterführende Konfiguration". |
| **Type** | |
| **Network** | |
| **Destination IP-Address** | |
| **Destination Mask** | |
| **Gateway IP-Address** | |
| **Source IP-Address** | |
| **Source Mask** | |
| **Protocol** | |

| Feld | Bedeutung |
|---|---|
| **Service** | Hier wählen Sie einen vordefinierten Service, für dessen Datenverkehr der Eintrag gelten soll.<br>Beim Zugriff auf das Menü wird der Wert *unnamed service* angezeigt. Dies ist lediglich ein Platzhalter. Der Datenverkehr wird durch diesen Eintrag solange nicht gefiltert, wie man den Defaultwert *-1* im Feld **Port** belässt. |
| **Port** | Hier wählen Sie den Zielport des Datenverkehrs aus, der dem Interface zugewiesen werden soll.<br>Zur Verfügung stehen die Werte von *-1* bis *65535*. Der Defaultwert *-1* bedeutet, dass der Zielport nicht ausgewertet wird und einen beliebigen Wert annehmen kann. |

Tabelle 2-7: ***IP*** ➧ ***Bandwidth Management (Load Balancing / BOD)*** ➧ ***IP Load Balancing over Multiple Interfaces*** ➧ **ADD/EDIT** ➧ ***IP Routing List*** ➧ **ADD/EDIT**

## 2.5 ATM-Redesign

BinTecs ATM-Implementierung ist in wesentlichen Teilen überarbeitet worden und bietet neben neuen Funktionen (OAM F4, ATM QoS) in Vorbereitung auf künftige Anforderungen wie Multiple VC und neue xDSL-Technologien deutlich verbesserte Leistung und Operabilität. Die Konfiguration eines ATM-Profils für einen Permanent Virtual Circuit (PVC, die Verbindung zwischen zwei Partnern via ATM) hat sich aufgrund der Änderungen in der Funktionsweise ebenfalls geändert, dies allerdings weniger in funktionaler Hinsicht, als vielmehr in Hinblick auf die Darstellung im Setup Tool und in den MIB-Tabellen.

Das ATM-Root-Menü enthält folgende Untermenüs:

- Protokollkonfigurationen (***Ethernet over ATM***, ***PPP over ATM***, ***Routed Protocols over ATM***)
- Operations-and-Maintenance-Konfiguration (***OAM***)
- Quality of Service für ATM-Verbindungen (***ATM QoS***).

Je nachdem, welches Protokoll Sie für das ATM-Interface verwenden, legen Sie das ATM-Profil in einem der Protokoll-Menüs an.

### 2.5.1 Ethernet over ATM

Im ersten Menüfenster werden alle bereits konfigurierten Verbindungen (PVCs) angezeigt, die Ethernet over ATM (ETHoA) verwenden. Mit **ADD/EDIT** gelangen Sie in das Menü zur Konfiguration einer entsprechenden Verbindung:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[ATM][ETHOA][ADD]                                              MyRouter


     Description

     ATM Interface                          atm860-3

     Virtual path identifier (VPI)          1
     Virtual channel identifier (VCI)       32

     Encapsulation                          bridged-no-fcs

     IP and Bridging >

                    SAVE                                  CANCEL
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Description** | Hier geben Sie eine beliebige Beschreibung für die Verbindung ein. |
| **ATM Interface** | Das ATM-Interface wird lediglich angezeigt und kann nicht ausgewählt werden. Derzeit verfügen BinTec-Router nur über ein ATM-Interface. |
| **Virtual path identifier (VPI)** | Hier geben Sie den VPI-Wert der ATM-Verbindung ein. Bei ATM unterscheidet man zwischen VP (Virtual Path) und VC (Virtual Channel). Jeder VP umfasst dabei bis zu 65503 VCs. Der VPI ist die Identifikationsnummer des zu verwendenden virtuellen Pfades im ATM-Netz.<br>Zur Verfügung stehen Werte von *0* bis *255*, Defaultwert ist *8*. |
| **Virtual channel identifier (VCI)** | Hier geben Sie den VCI-Wert der ATM-Verbindung ein. Der VCI ist die Identifikationsnummer des virtuellen Kanals im ATM-Netz. Ein virtueller Kanal ist die logische Verbindung für den Transport von ATM-Zellen zwischen zwei oder mehreren Punkten.<br>Zur Verfügung stehen Werte von *32* bis *65535*, Defaultwert ist *32.* |

| Feld | Bedeutung |
|---|---|
| **Encapsulation** | Hier wählen Sie die zu verwendende Enkapsulierung aus.<br>Zur Verfügung stehen:<br>■ *bridged-no-fcs* - Defaultwert. Bridged Ethernet ohne Frame Check Sequence (Prüfsummenfeld)<br>■ *bridged-fcs* - Bridged Ethernet mit Frame Check Sequence (Prüfsummenfeld)<br>■ *VC Multiplexing* - erlaubt die Anwendung von Multiplexverfahren auf den virtuellen Kanal. |

Tabelle 2-8: ***ATM*** ➧ ***ETHERNET OVER ATM*** ➧ **ADD/EDIT**

Die ATM-Enkapsulierungen sind in den RFCs 1483 und 2684 beschrieben.

Sie finden die RFCs auf den entsprechenden Seiten der IETF (www.ietf.org/rfc.html).

Für eine ETHoA-Verbindung werden Interfaces im Indexbereich zwischen *50.000* und *79.999* generiert.

Darüber hinaus erlaubt das Menü den Zugang zum Menü ***IP AND BRIDGING***. Hier konfigurieren Sie das lokale Ethernet-Interface für die ATM-Verbindung. Die zur Verfügung stehenden Parameter sind identisch mit denen im Menü zur Konfiguration physikalischer Ethernet-Interfaces (***LAN***). Informationen zur Konfiguration finden Sie im Handbuch Ihres Routers.

## 2.5.2 PPP over ATM

Das Menü zur Konfiguration eines PVC mit PPP over ATM (PPPoA) unterscheidet sich nur geringfügig von dem zur Konfiguration eines ETHoA-PVC:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[ATM][PPPOA][ADD]                                              MyRouter


    Description

    ATM Interface                          atm860-3

    Virtual path identifier (VPI)          8
    Virtual channel identifier (VCI)       32

    Encapsulation                          VC Multiplexing

    Client Type                            Permanent (Leased Line)


                  SAVE                                    CANCEL
```

Folgende Felder sind in diesem Menü neu bzw. bieten abweichende Optionen:

| Feld | Bedeutung |
|---|---|
| **Encapsulation** | Hier wählen Sie die zu verwendende Enkapsulierung aus.<br>Zur Verfügung stehen:<br>■ *VC Multiplexing* - erlaubt die Anwendung von Multiplexverfahren auf den virtuellen Kanal.<br>■ *llc* - Das LLC-Protokoll (Logical Link Control Protocol) wird für die Verbindung verwendet. |

| Feld | Bedeutung |
|---|---|
| **Client Type** | Hier wählen Sie aus, ob die PPPoA-Verbindung permanent oder bei Bedarf aufgebaut wird.<br>Zur Verfügung stehen:<br>■ *Permanent (Leased Line)* - Defaultwert. Es werden Interfaces im Indexbereich *80.000* bis *89.999* generiert.<br>■ *On Demand (Dialup)*. |

Tabelle 2-9: ***ATM*** ➧ ***PPP OVER ATM*** ➧ **ADD/EDIT**

Für den **Client Type** *On Demand (Dialup)* wird kein automatischer Eintrag in der **pppTable** erzeugt. D. h. Sie müssen ggf. einen entsprechenden WAN-Partner mit dem Layer-1-Protokoll PPPoA erstellen.

Für permanente Verbindungen wird ein entsprechender WAN-Partner automatisch erzeugt.

### 2.5.3 Routed Protocols over ATM

Das Menü zur Konfiguration einer Verbindung über Routed Protocols over ATM (RPoA) (***ATM*** ➧ ***ROUTED PROTOCOLS OVER ATM*** ➧ **ADD/EDIT**) unterscheidet sich ebenfalls nur in Teilen vom ETHoA-Menü:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[ATM][RPOA][ADD]                                              MyRouter

    Description

     ATM Interface                          atm860-3

     Virtual path identifier (VPI)          8
     Virtual channel identifier (VCI)       32

     Encapsulation                          non-ISO

     IP >


                    SAVE                                    CANCEL
```

Die Unterschiede finden sich in folgenden Feldern:

| Feld | Bedeutung |
|---|---|
| **Encapsulation** | Hier wählen Sie die zu verwendende Enkapsulierung aus.<br>Zur Verfügung stehen:<br>■ *non-ISO* - Defaultwert. Enkapsulation nach IEEE 802.1a LLC / RFC 2684.<br>■ *ISO (not allowed for IP)* - Enkapsulation nach IEEE 802.2 LLC / RFC 2684.<br>■ *VC Multiplexing* - erlaubt die Anwendung von Multiplexverfahren auf den virtuellen Kanal. |

| Feld | Bedeutung |
|---|---|
| **IP** | Nicht sichtbar für **Encapsulation** = *ISO*.<br>Zur IP-Konfiguration stehen bei RPoA-Verbindungen lediglich die folgenden Parameter zur Verfügung:<br>■ **local IP-Number**<br>■ **local Netmask** .<br>Informationen zur IP-Konfiguration finden Sie im Handbuch Ihres Routers. |

Tabelle 2-10: ***ATM*** ➧ ***ROUTED PROTOCOLS OVER ATM*** ➧ **ADD/EDIT**

Für RPoA werden Interfaces im Indexbereich *90.000* bis *99.999* erstellt.

## 2.5.4 Operations and Maintenance (OAM)

OAM ist ein Dienst zur Überwachung von ATM-Verbindungen. Für OAM sind insgesamt fünf Hierarchien (F1 bis F5) für den Informationsfluss definiert. Für eine ATM-Verbindung sind die wichtigsten Informationsflüsse F4 und F5. Der F4-Informationsfluss betrifft den virtuellen Pfad (VP), der F5-Informationsfluss den virtuellen Kanal (VC).

Im Allgemeinen geht die Überwachung nicht vom Endgerät aus, sondern wird vom ISP initiiert. Der Router muss dann lediglich korrekt auf die empfangenen Signale reagieren. Dies ist auch ohne eine spezifische OAM-Konfiguration sowohl auf dem Flow Level 4 als auch auf dem Flow Level 5 gegeben.

Zur Überwachung der ATM-Verbindung stehen zwei Mechanismen zur Verfügung: Loopback Tests und OAM CC (OAM Continuity Check). Sie können un-

abhängig voneinander konfiguriert werden. Die Konfiguration kann zum einen für eine bereits definierte Virtual Channel Connection (VCC, definiert durch die Festlegung von VPI und VCI in einem der Menüs zur Konfiguration der ATM-Verbindungen) erfolgen. Zum anderen kann man ebenfalls neue Kombinationen von VPI und VCI definieren und die OAM-Einstellungen vornehmen.

Das Menü zur OAM-Konfiguration sieht folgendermaßen aus (Der Screenshot enthält beliebige Beispielwerte):

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[ATM][OAM][ADD]                                                MyRouter

  ATM Interface           atm860-3

  OAM flow level          virtual channel (VC) level (F5)

  Virtual channel connection (VCC)      specify VPI/VCI
  VPI   0           VCI   32

  Loopback
      Loopback End-to-End  enabled    Loopback Segment     enabled
      Send Interval (sec)     5        Send Interval (sec)     5
      Pending Requests (max)  5        Pending Requests (max)  5



  CC activation
      CC End-to-End passive                CC Segment    passive
      Direction     both                   Direction     both

                    SAVE                             CANCEL
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **ATM Interface** | Das ATM-Interface wird lediglich angezeigt und kann nicht ausgewählt werden. Derzeit verfügen BinTec-Router nur über ein ATM-Interface. |

| Feld | Bedeutung |
|---|---|
| **OAM flow level** | Hier wählen Sie den OAM Flow Level.<br>Zur Verfügung stehen:<br>■ *virtual channel (VC) level (F5)* - Die OAM-Einstellungen werden auf den virtuellen Kanal angewendet (Defaultwert).<br>■ *virtual path (VP) level (F4)* - Die OAM-Einstellungen werden auf den virtuellen Pfad angewendet. |
| **Virtual channel connection (VCC)** | Sichtbar für **OAM flow level** = *virtual channel (VC) level (F5)*.<br>Hier wählen Sie aus, ob Sie eine bereits voreingestellte Kombination von VPI und VCI verwenden oder eine neue Kombination anlegen wollen.<br>Im Menü **ADD** stehen zur Verfügung:<br>■ *specify VPI/VCI* - Eine neue Kombination wird angelegt.<br>■ *Vpi: <"Vpi-Wert"> Vci <"Vci-Wert">* - Sie wählen die Kombination einer bereits konfigurierten ATM-Verbindung.<br>Im Menü **EDIT** stehen zur Verfügung:<br>■ *no VCC defined* - Die in den Feldern **VPI** und **VCI** angezeigte Kombination kann keiner bestehenden ATM-Verbindung (PVC) zugeordnet werden.<br>■ *Vpi: <"Vpi-Wert"> Vci <"Vci-Wert">* - Sie wählen die Kombination einer bereits konfigurierten ATM-Verbindung. |

| Feld | Bedeutung |
|---|---|
| **Virtual path connection (VPC)** | Sichtbar für **OAM flow level** = *virtual path (VP) level (F4)*.<br>Hier wählen Sie aus, ob Sie eine bereits voreingestellten VPI-Wert verwenden oder einen neuen Wert angeben wollen.<br>Im Menü **ADD** stehen zur Verfügung:<br>■ *specify VPI* -Sie spezifizieren einen neuen Wert.<br>■ *Vpi: <"Vpi-Wert">* - Sie wählen den Wert einer bereits konfigurierten ATM-Verbindung.<br>Im Menü **EDIT** stehen zur Verfügung:<br>■ *no VPC defined* - Der im Feld **VPI** angezeigte Wert kann keiner bestehenden ATM-Verbindung (PVC) zugeordnet werden.<br>■ *Vpi: <"Vpi-Wert">* - Sie wählen den Wert einer bereits konfigurierten ATM-Verbindung. |
| **VPI** | Nur sichtbar, wenn **Virtual channel connection (VCC)** = *specify VPI/VCI* oder **Virtual path connection (VPC)** = *specify VPI.*<br>Hier geben Sie einen VPI-Wert für diese VCC ein (*0* bis *255*). Der Defaultwert ist *0*. |
| **VCI** | Nur sichtbar, wenn **Virtual channel connection (VCC)** = *specify VPI/VCI* und **OAM flow level** = *virtual channel (VC) level (F5)*.<br>Hier geben Sie einen VCI Wert für diese VCC ein (*32* bis *65535*).<br>Der Defaultwert ist *32*. |

| Feld | Bedeutung |
|---|---|
| **Loopback End-to-End** | Hier wählen Sie aus, ob Sie den Loopback-Test für die Verbindung zwischen den Endpunkten der VCC aktivieren wollen.<br>Zur Verfügung stehen:<br>■ *disabled* - Defaultwert<br>■ *enabled* |
| **Send Interval (sec)** | Nur sichtbar, wenn **Loopback End-to-End** = *enabled*.<br>Hier geben Sie das Zeitintervall in Sekunden an, nachdem jeweils ein Loopback-Test ausgeführt wird.<br>Zur Verfügung stehen Werte von *0* bis *999*. Defaultwert ist *5*. |
| **Pending Requests (max)** | Nur sichtbar, wenn **Loopback End-to-End** = *enabled*.<br>Hier geben Sie ein, wieviele Loopback-Tests ohne Antwort bleiben können, bevor die Verbindung als nicht nutzbar angesehen wird.<br>Zur Verfügung stehen Werte von *1* bis *99*. Defaultwert ist *5*. |
| **Loopback Segment enable** | Hier wählen Sie aus, ob Sie den Loopback-Test für die Segment-Verbindung der VCC aktivieren wollen.<br>Zur Verfügung stehen:<br>■ *disabled* - Defaultwert<br>■ *enabled* |

| Feld | Bedeutung |
|---|---|
| **Send Interval (sec)** | Nur sichtbar, wenn **Loopback Segment** = *enabled*.<br>Hier geben Sie das Zeitintervall in Sekunden an, nach dem jeweils ein Loopback-Test ausgeführt wird.<br>Zur Verfügung stehen Werte von *0* bis *999*. Defaultwert ist *5*. |
| **Pending Requests (max)** | Nur sichtbar, wenn **Loopback Segment** = *enabled*.<br>Hier geben Sie ein, wieviele Loopback-Tests ohne Antwort bleiben können, bevor die Verbindung als nicht nutzbar angesehen wird.<br>Zur Verfügung stehen Werte von *1* bis *99*. Defaultwert ist *5*. |

| Feld | Bedeutung |
|---|---|
| **CC End-to-End** | Hier wählen Sie aus, ob Sie den OAM-CC-Test (CC = Continuity Check) für die Verbindung zwischen den Endpunkten der VCC aktivieren wollen.<br>Zur Verfügung stehen:<br>■ *passive* - OAM CC Requests werden nach der Aushandlung (CC activation negotiation) beantwortet (Defaultwert).<br>■ *active* - OAM CC Requests werden nach der Aushandlung (CC activation negotiation) gesendet.<br>■ *both* - OAM CC requests werden nach der Aushandlung (CC activation negotiation) gesendet und beantwortet.<br>■ *without negotiation* - Je nach Einstellung im Feld **Direction** werden OAM CC Requests entweder gesendet und/oder beantwortet. Es findet keine Aushandlung statt.<br>■ *disabled*. |

| Feld | Bedeutung |
|---|---|
| **Direction** | Nur wenn **CC End-to-End** nicht *disabled* ist.<br>Hier wählen Sie, wie die Testmuster des OAM CC gesendet bzw. empfangen werden.<br>Zur Verfügung stehen:<br>■ *both* - CC-Daten werden sowohl empfangen als auch generiert (Defaultwert).<br>■ *sink* - CC-Daten werden lediglich empfangen.<br>■ *source* - CC-Daten werden lediglich generiert. |
| **CC Segment** | Hier wählen Sie aus, ob Sie den OAM-CC-Test für die Segment-Verbindung der VCC aktivieren wollen.<br>Zur Verfügung stehen:<br>■ *passive* - OAM CC Requests werden nach der Aushandlung (CC activation negotiation) beantwortet (Defaultwert)<br>■ *active* - OAM CC Requests werden nach der Aushandlung (CC activation negotiation) gesendet.<br>■ *both* - OAM CC Requests werden nach der Aushandlung (CC activation negotiation) gesendet und beantwortet.<br>■ *without negotiation* - Je nach Einstellung im feld Direction werden OAM CC Requests entweder gesendet und/oder beantwortet. es findet keine Aushandlung statt.<br>■ *disabled.* |

| Feld | Bedeutung |
|---|---|
| **Direction** | Nur wenn **CC Segment** nicht *disabled* ist.<br>Hier wählen Sie, wie die Testmuster des OAM CC gesendet bzw. empfangen werden.<br>Zur Verfügung stehen:<br>■ *both* - CC-Daten werden sowohl empfangen als auch generiert (Defaultwert).<br>■ *sink* - CC-Daten werden lediglich empfangen.<br>■ *source* - CC-Daten werden lediglich generiert. |

Tabelle 2-11: ***ATM*** ➧ ***OAM*** ➧ **ADD/EDIT**

## 2.5.5 QoS-Kategorien für ATM

Systemsoftware-Release 7.1.1 unterstützt QoS (Quality of Service) für ATM-Interfaces. Die Konfiguration erfolgt im Menü ***ATM*** ➧ ***ATM QoS*** ➧ **ADD/EDIT**:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[ATM][QOS][ADD]                                              MyRouter

  ATM Interface           atm860-3


  Virtual channel connection (VCC)      specify VPI/VCI
  VPI   0           VCI   32

  ATM Service Category        Unspecified Bit Rate (UBR)

  Peak Cell Rate (PCR) in bits per second         0


                   SAVE                                  CANCEL
```

Es enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **ATM Interface** | Das ATM-Interface wird lediglich angezeigt und kann nicht ausgewählt werden. Derzeit verfügen BinTec-Router nur über ein ATM-Interface. |
| **Virtual channel connection (VCC)** | Hier wählen Sie aus, ob Sie eine bereits in einer ATM-Verbindung angelegte Kombination von VPI und VCI verwenden oder eine neue Kombination eingeben wollen.<br>Zur Verfügung stehen:<br>■ *specify VPI/VCI* - Sie geben eine neue Kombination ein.<br>■ *Vpi: <"Vpi-Wert"> Vci <"Vci-Wert">* - Sie wählen den Wert einer bereits konfigurierten ATM-Verbindung. |
| **VPI** | Nur sichtbar, wenn **Virtual channel connection (VCC)** = *specify VPI/VCI.*<br>Hier geben Sie einen VPI-Wert für diese VCC ein (*0* bis *255*). Der Defaultwert ist *0*. |
| **VCI** | Nur sichtbar, wenn **Virtual channel connection (VCC)** = *specify VPI/VCI*.<br>Hier geben Sie einen VCI Wert für diese VCC ein (*32* bis *65535*).<br>Der Defaultwert ist *32*. |

| Feld | Bedeutung |
|---|---|
| **ATM Service Category** | Hier wählen Sie aus, auf welche Art der Datenverkehr eines ATM-Verbindung beeinflusst werden soll.<br>Zur Verfügung stehen:<br>■ *Unspecified Bit Rate (UBR)* - (Defaultwert) Der Verbindung wird keine bestimmte Bandbreite garantiert. Die **Peak Cell Rate** (PCR) legt die Grenze fest, bei deren Überschrteiten (Bursts) Daten verworfen werden. Diese Kategorie eignet sich für nicht-kritische Anwendungen.<br>■ *Constant Bit Rate (CBR)* - Der Verbindung wird eine garantierte Bandbreite zugewiesen. Diese maximal zur Verfügung stehende Bandbreite wird von der **Peak Cell Rate** bestimmt. Diese Kategorie eignet sich für Real-Time-Anwendungen, die eine garantierte Bandbreite voraussetzen.<br>■ *Variable Bit Rate (VBR.1)* - Der Verbindung wird eine (geringe) garantierte Bandbreite zugewiesen (**Sustained Cell Rate**). Darüber hinaus wird der Datentransfer von der **Peak Cell Rate** und der **Maximum Burst Size** (MBS) beschränkt. Die PCR darf kurzzeitig überschritten werden, aber nur für die mit der MBS angegebenen Anzahl an Bytes. Darüber hinausgehende Bursts werden verworfen. Die Kategorie eignet sich für nicht-kritische Anwendungen mit stoßweisem Datenaufkommen. |

| Feld | Bedeutung |
|---|---|
| **Peak Cell Rate (PCR) in bits per second** | Hier geben Sie einen Wert für die maximale Bandbreite ein.<br>Zur Verfügung stehen Werte von *0* bis *10000000*, der Defaultwert ist *0*. Bei einem Wert von *0* wird die PCR nicht für QoS verwendet. |
| **Sustained Cell Rate (SCR) in bits per second** | Nur für **ATM Service Category** = *Variable Bit Rate (VBR.1)*.<br>Hier geben Sie einen Wert für die garantierte minimale Bandbreite ein.<br>Zur Verfügung stehen Werte von *0* bis *10000000*, der Defaultwert ist *0*. Bei einem Wert von *0* wird die SCR nicht für QoS verwendet |
| **Maximum Burst Size (MBS) in bytes** | Nur für **ATM Service Category** = *Variable Bit Rate (VBR.1)*.<br>Hier geben Sie einen Wert für die maximale Anzahl an Bytes ein, um die die PCR kurzzeitig überschritten werden darf.<br>Zur Verfügung stehen Werte von *0* bis *100000*, der Defaultwert ist *0*. Bei einem Wert von *0* wird die MBS nicht für QoS verwendet |

Tabelle 2-12: ***ATM*** ➧ ***ATM QoS*** ➧ **ADD/EDIT**

## 2.6 Analog-/GSM-Interface

Analoge Anschlüsse und GSM-Modems wurden bisher nicht von BinTec unterstützt. Mit einem Analog-/GSM-Interface ist es ab Systemsoftware-Release 7.1.1 möglich, auch diese Anschlussarten (z. B. als Backup) zu verwenden.

Dazu können Sie grundsätzlich jedes Hayes- bzw. GSM07.07-kompatible Modem mit serieller Schnittstelle verwenden. Folgende Modems sind von BinTec erfolgreich getestet worden:

- US Robotics Sportster Flash (Analogmodem)
- US Robotics 56K Faxmodem (Analogmodem)
- Siemens TC35i (GSM-Modem).

Um das Modem an einen BinTec-Router anzuschließen, benötigen Sie ein spezielles Kabel zum Anschluss des Modems an den Konsolen-Port Ihres Routers. Die Spezifikation des Kabels finden Sie im Anhang dieses Dokuments.

Für die Geräte der **X2000-Familie** können Sie lediglich das Kabel mit einem einzelnen Anschluss verwenden (siehe Anhang).

Die Konfiguration erfolgt im Menü ***AUX***:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[AUXILIARY]: Settings                                          MyRouter


          Serial Port      : second

          Line speed       : 19200
          Active Profile   : Profile 1

             Available Profiles:

                  Profile 1
                  Profile 2
                  Profile 3
                  Profile 4


          SAVE                                              CANCEL
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Serial Port** | Hier wählen Sie aus, welche serielle Schnittstelle Sie für den Anschluss an das Modem nutzen wollen.<br>Zur Verfügung stehen:<br>■ *second* - Sie verwenden die zweite, bisher unbelegte serielle Schnittstelle. Die Geräte der **X2000-Familie** verfügen nicht über eine solche zweite serielle Schnittstelle.<br>■ *console* - Sie verwenden die Konsolenschnittstelle. Die serielle Konsole steht nicht mehr zur Verfügung. |
| **Line speed** | Hier wählen Sie die Geschwindigkeit, mit der das Modem vom Router angesprochen wird (in bit/s).<br>Zur Verfügung stehen:<br>■ *default* - Die Geschwindigkeit wird nicht geändert.<br>Alle anderen Werte bedeuten, dass das Modem mit der entsprechenden Geschwindigkeit in bit/s angesprochen wird.<br>■ *9600* |

| Feld | Bedeutung |
|---|---|
| **Line speed (Forts.)** | ■ *19200* - Defaultwert; für die Kommunikation mit einem GSM-Modem empfohlen.<br>■ *38400*<br>■ *57600*<br>■ *115200* - Für die Kommunikation mit einem analogen Modem empfohlen. |
| **Active Profile** | Hier wählen Sie das Profil aus, dessen Vorgaben für die Kommunikation mit dem Modem verwendet werden. |
| **Profile <1 bis 4>** | Über diese Schaltflächen gelangen Sie in die Menüs zur Konfiguration des entsprechenden Profils. |

Tabelle 2-13: ***AUX***

Über die Konfiguration der Profile können Sie unterschiedliche Vorgaben für die Kommunikation zwischen Router und Modem definieren:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[AUXILIARY][SETUP]: Modem Configuration                        MyRouter

   Profile Configuration


         Dispatch Item :    PPP dialin
         GSM SIM PIN   :    ****
         Escape Char   :    +
         Init Sequence :    ATX3

         SAVE                                              CANCEL
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Dispatch Item** | Hier wählen Sie aus, welchem Subsystem des Routers ein über das Modem eingehender Ruf zugewiesen werden soll.<br>Zur Verfügung stehen:<br>■ *none* - Es erfolgt keine Rufannahme.<br>■ *PPP dialin* - Der Ruf wird dem PPP-Subsystem zugewiesen.<br>■ *isdnlogin* - Der Ruf wird dem ISDNLogin-Subsystem zugewiesen.<br>Defaultwert ist *PPP dialin*. |
| **GSM SIM PIN** | Hier geben Sie die PIN Ihres GSM-Modems ein, sofern Ihr Modem dies erfordert.<br>Die Eingabe einer falschen PIN unterbindet die Kommunikation mit dem Modem, bis der Eintrag im Profil korrigiert wird.<br>Der Defaultwert ist *0000*. |
| **Escape Char** | Der Wert für dieses Feld ist per Default auf "*+*" gesetzt. Er sollte nur dann verändert werden, wenn der Escape Character des Modems ein anderer ist. |

| Feld | Bedeutung |
|---|---|
| **Init Sequence** | Hier können Sie einen Initialisierungsstring für Ihr Modem eingeben. Per Default ist der Befehl *ATX3* (das Modem wartet vor dem Wählen nicht auf ein Freizeichen) eingestellt. Sie können weitere AT-Befehle durch Semikola getrennt anhängen. Die Eingabe ist auf 50 Zeichen begrenzt.<br>Stellen Sie sicher, dass Sie den Befehl zur Aktivierung der XON/XOFF Software Flow Control eingeben. Dieser ist herstellerabhängig und kann nicht automatisch eingestellt werden. Die Befehlssequenz erfahren Sie ggf. im Handbuch Ihres Modems oder beim Hersteller. |

Tabelle 2-14: ***AUX*** ➧ **Profile <1 bis 4>**

Wenn Sie einen WAN-Partner für PPP Dial-In/Dial-Out anlegen, der das AUX-Interface verwendet, so müssen Sie im Menü ***WAN-PARTNER*** ➧ **ADD/EDIT** ➧ ***WAN NUMBERS*** das Kontrollkästchen **Slot 0 Auxiliary** aktivieren. Markieren Sie es dazu mit dem Cursor und schalten Sie die Einstellung mit der Leertaste um.

Das AUX-Interface wird vom BinTec-Trace unterstützt. Geben Sie zur Aktivierung des Traces z. B. `trace -h 0 9 0` auf der Shell ein.

Syslog-Messages werden auf den Levels *debug* und *err* erzeugt. Aktive Rufe werden in der **isdnCallTable**, beendete in der **isdnCallHistoryTable** angezeigt.

## 2.7 Email Alert

Schon bisher war es möglich Syslog Messages vom Router an einen beliebigen Syslog-Host übertragen zu lassen. Dem fügt Systemsoftware-Release 7.1.1

einenEmail Alert hinzu: Je nach Konfiguration werden dem Administrator Emails gesendet, sobald relevante Syslog Messages auftreten.

Die Konfiguration erfolgt im Menü ***Monitoring and Debugging*** ➧ ***Email Alert***.

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[ALERT NOTIFICATION]: Settings                                  MyRouter

 Global notification settings:

       Adminstatus    :   enable
       SMTP Server    :
       Originator     :
       max. Mails/min :   6


 Current notification list:
 Receiver           Expression            Time  Count  compress  Level


   ADD                DELETE              CANCEL              SAVE
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Adminstatus** | Hier aktivieren bzw. deaktivieren Sie die Funktion.<br>Zur Verfügung stehen:<br>■ *enable* (Defaultwert)<br>■ *disable* |
| **SMTP Server** | Hier geben Sie die Adresse (IP-Adresse oder gültiger DNS-Name) des Mailservers ein, der zum Versenden der Mails verwendet werden soll.<br>Die Eingabe ist auf 40 Zeichen begrenzt. |

| Feld | Bedeutung |
|---|---|
| **Originator** | Hier geben Sie die Mailadresse ein, die in das Absenderfeld der Email eingetragen werden soll. |
| **max. Mails/min** | Hier können Sie die Anzahl der ausgehenden Mails pro Minute begrenzen.<br>Zur Verfügung stehen Werte von *1* bis *30*, der Defaultwert ist *6*. |

Tabelle 2-15: ***MONITORING AND DEBUGGING*** ➧ ***EMAIL ALERT***

Im unteren Teil des Menüfensters werden die bereits konfigurierten Notification Rules dargestellt. Mit **ADD/EDIT** können Sie eine neue Regel konfigurieren bzw. einen bestehenden editieren:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[ALERT NOTIFICATION][ADD]                                       MyRouter

   Notification rule configuration:

          Receiver     :
          Contents     :
          Level        : emergency
          Timeout      : 60
          Messages     : 1
          Compress     : disable

    Select subsystems:

<X> ACCOUNT <X> ISDN    <X> INET    <X> X25     <X> CAPI    <X> PPP
<X> CONFIG  <X> SNMP    <X> X21     <X> ETHER   <X> RADIUS  <X> OSPF
<X> MODEM   <X> RIP     <X> ATM     <X> IPSEC   <X> AUX


          SAVE                                          CANCEL
```

| Feld | Bedeutung |
|---|---|
| **Receiver** | Hier geben Sie die Emailadresse des Empfängers ein.<br>Die Eingabe ist auf 40 Zeichen begrenzt. |
| **Contents** | Hier müssen Sie eine "Regular Expression" eingeben. Ihr Vorkommen in einer Syslog Message ist die notwendige Bedingung für das Auslösen eines Alerts.<br>Die Eingabe ist auf 55 Zeichen begrenzt.<br>Bedenken Sie, dass ohne die Verwendung von Wildcards (z. B. "*") nur diejenigen Strings die Bedingung erfüllen, die exakt der Eingabe entsprechen. In der Regel wird die eingegebene Regular Expression also Wildcards enthalten. Um grundsätzlich über alle Syslog-Messages des gewählten Levels informiert zu werden, geben Sie lediglich "*" ein. |
| **Level** | Hier wählen Sie den Syslog-Level aus, auf dem der im Feld **Contents** konfigurierte String vorkommen muss, damit ein Email Alert ausgelöst wird.<br>Zur Verfügung stehen alle im Menü ***SYSTEM***, Feld **Message level for the syslog table**, verfügbaren Werte, Defaultwert ist *emergency*. |
| **Timeout** | Hier geben Sie ein, wie lange der Router nach einem entsrechenden Ereignis maximal warten darf, bevor das Versenden der Alert Mail erzwungen wird.<br>Zur Verfügung stehen Werte von *0* bis *86400*. Ein Wert von *0* deaktiviert dem Timeout, Defaultwert ist *60*. |

| Feld | Bedeutung |
|---|---|
| **Messages** | Hier geben Sie die Anzahl an Syslog Messages ein, die erreicht sein muss, ehe eine Alert Email für diesen Fall gesendet werden kann. Wenn **Timeout** konfiguriert ist, wird die Mail bei dessen Ablauf gesendet, auch wenn die Anzahl an Meldungen noch nicht erreicht ist.<br>Zur Verfügung stehen Werte von *1* bis *99*, Defaultwert ist *1*. |
| **Compress** | Hier können Sie auswählen, ob der Text des Email Alerts verkürzt werden soll. Die Mail enthält dann die Syslog-Message nur einmal und zusätzlich die Anzahl der entsprechenden Ereignisse.<br>Zur Verfügung stehen:<br>■ *disable* - Defaultwert<br>■ *enable* |
| **Select subsystems** | Hier wählen Sie die Subsysteme aus, die überwacht werden sollen. Markieren Sie ein Subsystem mit dem Cursor und aktivieren oder deaktivieren Sie ihn mit der Leertaste. |

Tabelle 2-16: ***MONITORING AND DEBUGGING*** ➧ ***EMAIL ALERT*** ➧ **ADD/EDIT**

## 2.8 SSH Login

Systemsoftware-Release 7.1.1 ermöglicht Ihnen einen verschlüsselten Zugang zur Shell Ihres Routers. Diesen Zugang können Sie im Menü ***SECURITY*** ➧ ***SSH DAEMON*** aktivieren und konfigurieren:

```
BinTec Router Setup Tool                  BinTec Access Networks GmbH
[SECURITY][SSHD]: SSH Daemon Configuration                    MyRouter


          SSH Daemon                                  running

          Static Settings >
          Timer >

          Authentication Algorithms >
          Supported Ciphers >
          Message Authentication Codes >


          Certification Management >

          Monitoring >

               SAVE                                   EXIT
```

Hier können Sie den per Default aktivierten SSH-Daemon deaktivieren bzw. reaktivieren und haben Zugriff auf die Menüs zur Konfiguration des SSH Login.

Nach der Konfiguration sollten Sie kontrollieren, dass der SSH-Daemon gestartet ist: Geben Sie in der Shell `ps -e` ein und verifizieren Sie, dass der `sshd` aufgeführt ist.

Sollte dies nicht der Fall sein, müssen Sie den Router neu starten, um den SSH-Daemon zu starten.

Wenn SIe SSH Login zusammen mit dem PuTTY-Client verwenden wollen, müssen Sie einige Besonderheiten bei der Konfiguration beachten. Wir haben diesbezüglich eine FAQ erstellt. Sie finden diese im Bereich Service/Support auf www.bintec.de finden.

### Static Settings

Hier bestimmen Sie grundlegende Parameter des SSH Logins:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[SECURITY][SSHD][STATIC]: SSHD Static Options                   MyRouter


          Max. # of Clients                 1
          Port # used for Connections       22
          Compression                       disabled

          Verify Reverse Mapping            disabled



          Print Motd                        enabled
          Print LastLog                     disabled

          Logging Level                     info

               SAVE                         CANCEL
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Max. # of Clients** | Hier geben Sie an, wie viele gleichzeitige Verbindungen zum SSH-Daemon gestattet sind. Weitere Verbindungen werden abgewiesen, bis eine Verbindung beendet ist.<br>Zur Verfügung stehen Werte von *1* bis *100*, der Defaultwert ist *1*.<br>Derzeit ist aus technischen Gründen lediglich eine einzelne SSH-Verbindung möglich. |
| **Port # used for Connections** | Hier geben Sie an, auf welchem Port sich ein Client mit dem SSH-Daemon verbinden kann. Der Defaultwert ist *22*. |
| **Compression** | Hier können Sie die Verwendung von Datenkompression aktivieren (*enabled*) bzw. deaktivieren (*disabled*). Der Defaultwert ist *disabled*. |
| **Verify Reverse Mapping** | Hier wählen Sie aus, ob der SSH-Daemon einen "Reverse Lookup" der Client-IP-Adresse durchführt. Dabei wird verifiziert, dass der zur IP-Adresse gehörende Host-Name korrekt ist, die IP-Adresse also nicht gefälscht wurde.<br>Zur Verfügung stehen:<br>■ *disabled* - Defaultwert<br>■ *enabled*. |
| **Print Motd** | Hier wählen Sie aus, ob der SSH-Daemon eine "Message of the Day (MotD)" ausgibt, sobald sich ein Client angemeldet hat.<br>Zur Verfügung stehen:<br>■ *disabled*<br>■ *enabled* - Defaultwert. |

| Feld | Bedeutung |
|---|---|
| **Print LastLog** | Hier wählen Sie aus, ob der SSH-Daemon beim Login eines Clients Datum und Uhrzeit des letzten Logins ausgeben soll.<br>Zur Verfügung stehen:<br>■ *disabled* - Defaultwert<br>■ *enabled*. |
| **Logging Level** | Hier können Sie den Syslog-Level für die vom SSH-Daemon generierten Syslog Messages auswählen.<br>Zur Verfügung stehen:<br>■ *quiet*<br>■ *fatal*<br>■ *error*<br>■ *info* - Defaultwert<br>■ *verbose*<br>■ *debug*. |

Tabelle 2-17: ***SECURITY*** ➧ ***SSH DAEMON*** ➧ ***STATIS SETTINGS***

### Timer

Im Menü ***Security*** ➧ ***SSH Daemon*** ➧ ***Timer*** können Sie zeitabhängiges Verhalten des SSH-Daemon konfigurieren:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[SECURITY][SSHD][TIMER]: SSHD Timer Options                    MyRouter

          Login Grace Time                  600

          TCP Keepalives                    enabled

          ClientAliveCountMax               3

          ClientAliveInterval               10


               SAVE                         CANCEL
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Login Grace Time** | Hier geben Sie den Zeitraum ein, innerhalb dessen sich ein Client authentisieren muss bevor die Verbindung abgebrochen wird.<br>Zur Verfügung stehen Werte von *0* bis *3600* (Sekunden). Ein Wert von *0* bedeutet keine Begrenzung, der Defaultwert ist *600*. |
| **TCP Keepalives** | Hier wählen Sie aus, ob der Router Keepalive-Pakete senden soll.<br>Zur Verfügung stehen:<br>■ *disabled*<br>■ *enabled* - Defaultwert.<br>Der Wert sollte für Client und Server gleich konfiguriert werden. |

| Feld | Bedeutung |
|---|---|
| **ClientAliveCountMax** | Hier geben Sie die Anzahl der vom Router gesendeten Keepalive-Pakete an, die unbeantwortet bleiben dürfen, bevor der SSH-Daemon die Verbindung unterbricht.<br>Zur Verfügung stehen Werte von *0* bis *10*, der Defaultwert ist *3*. |
| **ClientAliveInterval** | Hier geben Sie das Intervall an, nach dessen Ablauf der SSH-Daemon einen Keepalive Request an den Client sendet, wenn keine Daten mehr vom Client empfangen werden.<br>Zur Verfügung stehen Werte von *1* bis *3600* (Sekunden), der Defaultwert ist *10*. |

Tabelle 2-18: ***Security*** ➧ ***SSH Daemon*** ➧ ***Timer***

### Authentication Algorithms

In diesem Menü können Sie die Mechanismen der Authentisierung konfigurieren:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[SECURITY][SSHD][AUTH]: SSHD Authentication Options              MyRouter

          Protocol Version                  2


          Public Key                        enabled
          Password                          enabled
          Challenge Response                enabled


              SAVE                          CANCEL
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Protocol Version** | Hier wird angezeigt, welche SSH-Version der SSH-Daemon verwendet. Das Feld ist nicht editierbar, da derzeit lediglich Version 2 unterstützt wird. |
| **Public Key** | Hier wählen Sie aus, ob eine Public - Key-Authentisierung des Clients zulässig ist oder nicht.<br>Zur Verfügung stehen:<br>■ *disabled*<br>■ *enabled* - Defaultwert.<br>Dieser Authentisierungsmechanismus befindet sich noch in einem experimentellen Stadium. |
| **Password** | Hier wählen Sie aus, ob eine Passwort-Authentisierung des Clients zulässig ist oder nicht.<br>Zur Verfügung stehen:<br>■ *disabled*<br>■ *enabled* - Defaultwert. |
| **Challenge Response** | Hier wählen Sie aus, ob eine Challenge - Response-Authentisierung des Clients zulässig ist oder nicht.<br>Zur Verfügung stehen:<br>■ *disabled*<br>■ *enabled* - Defaultwert.<br>Dieser Authentisierungsmechanismus befindet sich noch in einem experimentellen Stadium. |

Tabelle 2-19: ***SECURITY*** ➧ ***SSH DAEMON*** ➧ ***AUTHENTICATION ALGORITHMS***

### Supported Ciphers

In diesem Menü können Sie die zur Verschlüsselung verwendeten Algorithmen aktivieren bzw. deaktivieren:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[SECURITY][SSHD][AUTH]: SSHD Cipher Options                    MyRouter

          aes128                              enabled
          3des                                enabled
          blowfish                            enabled
          cast128                             enabled
          arc4                                enabled
          aes192                              enabled
          aes256                              enabled

               SAVE                           CANCEL
```

Für jeden der im Menü aufgelisteten Algorithmen können Sie zwischen *enabled* (Defaultwert) und *disabled* wählen.

### Message Authentication Codes

In diesem Menü können Sie die zur Message-Authentisierung verwendeten Algorithmen aktivieren bzw. deaktivieren:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[SECURITY][SSHD][MACS]: SSHD Message Authentication Codes     MyRouter

          md5                                 disabled
          sha1                                disabled
          ripemd160                           disabled
          sha1-96                             enabled
          md5-96                              disabled

               SAVE                           CANCEL
```

Für jeden der im Menü aufgelisteten Algorithmen können Sie zwischen *enabled* und *disabled* wählen.

### Certification Management

In diesem Menü können Sie die zur Authentisierung notwendigen Schlüssel erstellen. Sie können einen DSA- und einen RSA-Schlüssel wählen, wir empfehlen, beide Schlüssel zu erstellen. Die Schlüssel werden systemintern abgespeichert.

Das Erstellen der Schlüssel nimmt mehrere Minuten in Anspruch und kann nicht abgebrochen werden.

### Monitoring

In diesem Menü können Sie die aufgebauten Verbindungen einsehen. Die Implementierung dieser Funktion ist derzeit noch nicht abgeschlossen.

## 2.9 GRE (Generic Routing Encapsulation)

Die Spezifikation des GRE-Protokolls liegt in zwei Versionen vor: GRE V.1 zur Verwendung in PPTP-Verbindungen (RFC 2637) und GRE V.0 (RFC 2784) zur allgemeinen Enkapsulierung mittels GRE. Für PPTP-Verbindungen steht GRE V.1 bereits für BinTec-Router zur Verfügung, ab Systemsoftware-Release 7.1.1 können Sie GRE V.0 auch außerhalb dieses Kontextes nutzen.

Im Menü ***GRE*** können Sie ein virtuelles Interface konfigurieren. Der Datenverkehr, der über dieses Interface geroutet wird, wird dann mittels GRE enkapsuliert und an den spezifizierten Empfänger gesendet. Im ersten Menüfenster wir eine Liste der bereits konfigurierten GRE-Interfaces angezeigt. Über **ADD/EDIT** gelangen Sie in das Menü zur Konfiguration eines solchen Interfaces.

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[GRE]: Configure GRE tunnels                                  MyRouter


          Name
          GRE Partner's IP Address
          GRE Local IP Address
          Partner's LAN IP Address
          Partner's LAN IP Mask
          Mtu                          1500
          Key Used                     no


                    SAVE                                CANCEL
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Name** | Hier geben Sie eine beliebige Beschreibung des virtuellen Interfaces ein. |
| **GRE Partner's IP Address** | Hier geben Sie die IP-Adresse des GRE-Partners ein. |
| **GRE Local IP Address** | Hier geben Sie die IP-Adresse ein, die als Quelladresse für GRE-Pakete verwendet werden soll.<br>Ist der Wert = *0.0.0.0* wird die IP-Adresse automatisch ausgewählt, die notwendig ist, um Pakete an die IP-Adresse des GRE-Partners zu senden. |
| **Partner's LAN IP Address** | Hier geben Sie die IP-Adresse des Netzes an, in dem sich die **GRE Partner's IP Address** befindet. |
| **Partner's LAN IP Mask** | Hier geben Sie die Netzmaske des Netzes an, in dem sich der GRE-Partner befindet. |
| **Mtu** | Hier geben Sie die MTU (Maximum Transfer Unit) ein, das für eine GRE-Verbindung zwischen den Partnern verwendet werden soll.<br>Zur Verfügung stehen Werte von *1* bis *8192* (in Bytes). Der Defaultwert ist *1500*. |
| **Key Used** | Hier wählen Sie aus, ob unterschiedliche Verbindungen zum selben GRE-Partner mittels eines Schlüssels als solche markiert werden sollen.<br>Zur Verfügung stehen:<br>■ *no* - Defaultwert<br>■ *yes*. |

| Feld | Bedeutung |
|---|---|
| **Value** | Nur für **Key Used** = *yes*.<br>Hier geben Sie einen Wert für den Schlüssel ein.<br>Zur Verfügung stehen Werte von *0* bis *2147483647* (32 bit). |

Tabelle 2-20: ***GRE*** ➧ **ADD/EDIT**

# 3 Änderungen



## 3.1 Setup-Tool-Aufbau

Um die zunehmende Anzahl an Sicherheitsfunktionen im Setup Tool leicht zugänglich zu machen, sind die entsprechenden Menüs im Menü ***SECURITY*** eingeordnet worden. Dieses befindet sich direkt im Hauptmenü und enthält die folgenden Untermenüs:

- ***COBION ORANGE FILTER***
- ***ACCESS LISTS***
- ***STATEFUL INSPECTION***
- ***TOKEN AUTHENTICATION FIREWALL*** (optional)

- ***SSH DAEMON***
- ***LOCAL SERVICES ACCESS CONTROL.***

Bis auf die neu hinzugekommenen Menüs ***COBION ORANGE FILTER*** und ***SSH DAEMON*** sind diese Menüs aus dem Menü ***IP*** in das Menü ***SECURITY*** verschoben worden. Die Struktur der Menüs selbst ist, sofern nicht anders beschrieben, unverändert.

## 3.2 Änderungen der WAN-Partner-Konfiguration

Bei der Konfiguration eines WAN-Partners haben sich Änderungen im Menü ***WAN-PARTNER*** ➧ **ADD/EDIT** ➧ ***IP*** ergeben. Diese Änderungen betreffen auch die IP-Konfiguration von IPSec-Peers. Sie ermöglichen es, Routing-Einstellungen spezifisch für einen WAN Partner vorzunehmen, die bislang lediglich global konfiguriert werden konnten.

Das erste Menüfenster bietet unter Systemsoftware-Release 7.1.1Zugang zu den weiteren Konfigurationsmenüs:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[WAN][ADD][IP]: IP Settings                                    MyRouter


                    Basic IP-Settings >

                    More Routing >

                    Advanced Settings >


                           EXIT
```

### 3.2.1 *BASIC IP-SETTINGS*

Das Menü ***BASIC IP-SETTINGS*** entspricht dem Menü ***WAN PARTNER*** ➧ **ADD/EDIT** ➧***IP*** älterer Systemsoftware. Lediglich der Zugang zum Menü ***ADVANCED SETTINGS*** ist verschoben worden.

### 3.2.2 *MORE ROUTING*

Im Menü ***MORE ROUTING*** können weitere Routen für den betreffenden WAN-Partner konfiguriert werden. Das Menü entspricht dem Menü ***IP*** ➧ ***ROUTING***.

### 3.2.3 *ADVANCED SETTINGS*

Das Menü unterscheidet sich nicht vom Menü ***WAN-PARTNER*** ➧ **ADD/EDIT** ➧***IP*** ➧ ***ADVANCES SETTINGS*** älterer Software Releases.

## 3.3 Stateful Inspection Firewall Stufe 2

Die Stateful Inspection Firewall (SIF) ist gegenüber früheren Releases erweitert worden. Es stehen zusätzliche Parameter im neu gestalteten SIF-Hauptmenü zur Verfügung, ebenso ein neuer Modus der Adressalias-Definition.

### 3.3.1 Neues SIF-Hauptmenü

Das Menü ***SECURITY*** ➧ ***STATEFUL INSPECTION*** zeigt unter Systemsoftware-Release 7.1.1 nicht mehr eine Liste bereits konfigurierter Filter, sondern ein Menü mit globalen Parametern an:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION]: Static settings              MyRouter

 Stateful Inspection Firewall global settings:

          Adminstatus     :  enable
          Local Filter    :  disable
          Full Filtering  :  enable
          Logging level   :  all


          Edit Filters >
          Edit Services >
          Edit Addresses >

          Advanced settings >


                    SAVE                                  CANCEL
```

Das Menü enthält folgende Felder:

| Feld | Bedeutung |
|---|---|
| **Adminstatus** | Hier können Sie die Funktion grundsätzlich aktivieren und deaktivieren.<br>Zur Verfügung stehen:<br>■ *enable* - Defaultwert<br>■ *disable* |

| Feld | Bedeutung |
|---|---|
| **Local Filter** | Hier legen Sie fest, ob lokal initiierte Verbindungen ebenfalls von der SIF gefiltert werden sollen.<br>Zur Verfügung stehen:<br>■ *enable* - Lokal erzeugte Sessions werden ebenfalls gefiltert.<br>■ *disable* - Lokal erzeugte Sessions werden generell zugelassen (Defaultwert). |
| **Full Filtering** | Hier legen Sie fest, ob nur Pakete gefiltert werden sollen, bei denen sich Ein- und Ausgangsinterface unterscheiden.<br>Zur Verfügung stehen:<br>■ *enable* - Alle Pakete werden gefiltert (Defaultwert).<br>■ *disable* - Nur Pakete, bei denen sich Ein- und Ausgangsinterface unterscheiden, werden gefiltert. |
| **Logging level** | Hier können Sie den Syslog-Level auswählen.<br>Zur Verfügung stehen:<br>■ *all* - Alle SIF-Aktivitäten werden angezeigt (Defaultwert).<br>■ *deny only* - Nur Reject- und Ignore-Ereignisse werden angezeigt.<br>■ *accept only* - Nur Accept-Ereignisse werden angezeigt.<br>■ *none* - Syslog Messages werden nicht erzeugt. |

Tabelle 3-1: ***SECURITY*** ➧ ***STATEFUL INSPECTION FIREWALL***

Vom Menü ***SECURITY*** ➧ ***STATEFUL INSPECTION*** gelangt man zur Konfiguration der Filter sowie der Services und der Adressen für die Filter. Darüber hinaus gelangt man in das Menü ***SECURITY*** ➧ ***STATEFUL INSPECTION*** ➧ ***ADVANCED SETTINGS***:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][ADVANCED]: Settings            MyRouter

 Stateful Inspection session expiration:

          UDP   inactivity Timeout : 180
          TCP   inactivity Timeout : 3600
          PPTP  inactivity Timeout : 86400
          Other inactivity Timeout : 30


                     SAVE                                  CANCEL
```

Es enthält die folgenden Felder:

| Feld | Bedeutung |
|---|---|
| **UDP inactivity Timeout** | Hier können Sie eingeben, nach welcher Zeit der Inaktivität eine UDP-Session als abgelaufen betrachtet wird (in Sekunden).<br>Zur Verfügung stehen Werte von *30* bis *86400*. Der Defaultwert ist *180*. |
| **TCP inactivity Timeout** | Hier können Sie eingeben, nach welcher Zeit der Inaktivität eine TCP-Session als abgelaufen betrachtet wird (in Sekunden).<br>Zur Verfügung stehen Werte von *30* bis *86400*. Der Defaultwert ist *3600*. |

| Feld | Bedeutung |
|---|---|
| **PPTP inactivity Timeout** | Hier können Sie eingeben, nach welcher Zeit der Inaktivität eine PPTP-Session als abgelaufen betrachtet wird (in Sekunden).<br>Zur Verfügung stehen Werte von *30* bis *86400*. Der Defaultwert ist *86400*. |
| **Other inactivity Timeout** | Hier können Sie eingeben, nach welcher Zeit der Inaktivität eine Session eines anderen Typs als abgelaufen betrachtet wird (in Sekunden).<br>Zur Verfügung stehen Werte von *30* bis *86400*. Der Defaultwert ist *30*. |

Tabelle 3-2: ***SECURITY*** ➧ ***STATEFUL INSPECTION*** ➧ ***ADVANCED SETTINGS***

### 3.3.2 Adressalias-Definition

Im Menü zur Erstellung oder Änderung eines Adressalias (***STATEFUL INSPECTION*** ➧ ***EDIT ADDRESSES*** ➧ **ADD/EDIT**) ist eine Option für das Feld **Mode** hinzugekommen: *Adress/Range*. Wird dies gewählt, ist eine Eingabe in die Felder **IP-Address** (Default: leer) und **IP-Range** möglich (Default: *1*).

Mittels dieses Modus kann eine Folge von IP-Adressen für die SIF-Filterung vorgesehen werden, ohne dass ein ganzes Subnetz spezifiziert werden muss.

## 3.4 IPSec - New Phase 1 Mode

Systemsoftware-Release 7.1.1 bietet zwei neue IPSec Phase 1 Modi:

- *aggressive_only* - Während der IKE-Aushandlung werden nur Proposals mit dem Aggressive Mode akzeptiert.
- *id_protect_only* - Während der IKE-Aushandlung werden nur Proposals mit dem ID Protect Mode (Main Mode) akzeptiert.

Die neuen Werte stehen in allen Menüs zur Konfiguration der IPSec-Phase-1 zur Verfügung. Siehe Kapitel 2.2.1, Seite 11 zu den Pahse-1-Profilen.

## 3.5 NAT - NAT-Session Timeout

NAT-Sessions konnten bisher nicht länger als 18 Stunden aufrechterhalten werden, wenn keinerlei Datenverkehr über das entsprechende Interface gesendet oder empfangen wurde. Der maximale Timeout einer NAT-Session ist auf 5184000 Sekunden (60 Tage) erhöht worden. Um unsichere Konfigurationen zu vermeiden, können nicht nur interface-spezifische Timeouts konfiguriert werden (**ipExtIfNatTcpTimeout** und **ipExtIfNatOtherTimeout**), sondern auch ein globaler Timeout (**ipNatOutTimeout** und **ipNatPrTimeout**). Der Defaultwert beider globalen Parameter ist *0*, d. h. es werden die interface-spezifischen Werte verwendet. Wird ein Wert für die globalen Parameter gesetzt, wird dieser verwendet, sofern für das Interface keine spezifischen Werte konfiguriert sind. Es ist mittels dieser Parameter möglich, bestimmten Interfaces ohne aufwendige Konfiguration einen langen Timeout zuzuweisen, allen anderen aber einen kürzeren und damit sichereren.

## 3.6 Zweiter BOOTP Relay Server

Um mögliche Probleme mit der Erreichbarkeit eines BOOTP Relay Servers zu umgehen, ist es nun möglich, einen weiteren Server anzugeben. Dies erfolgt mittels des Feldes ***IP*** ➧ ***STATIC SETTINGS***: **Secondary BOOTP Relay Server**.

## 3.7 Telnet - Neue Option

Die Telnet-Applikation unterstützt nun die Option -s zur Angabe einer Quelladresse für die Telnet-Verbindung. Die Syntax ist:

```
Usage: telnet [-frb] [-s <src>] host [port]
Options:
      -f       forward data forth and back transparently
      -r       use console raw mode (allows XMODEM transfers)
      -b       negotiate telnet binary mode (allows XMODEM transfers)
```

## 3.8 Ping - Next Ping Time Berechnung korrigiert

Vor Systemsoftware-Release 7.1.1 wartete der Ping-Daemon bis zum Ende des Ping Timeouts, bevor die nächste ICMP Echo Request gesendet wurde, selbst wenn vor dem Ping Timeout eine ICMP Echo Reply empfangen wurde.

Das Verhalten ist dahingehend verändert worden, dass die Next Ping Time nicht mehr als eine Sekunde beträgt, sofern der vorhergehende Ping erfolgreich war.

## 3.9 BootP - TTL-Wert

Aus Gründen der Interoperabilität ist der Wert der BootP-Time-to-Live auf eine Defaultwert von *0* (bisher *16*) gesetzt worden. Damit entpricht er dem Defaultwert der IP-TTL (**ipDefaultTTL**).

## 3.10 Trace - IfIndex verwendbar

Bisher war es nicht möglich, für den Trace eines Interfaces den Interface-Index anzugeben. Es musste der Name des Interfaces angegeben werden. Ab Systemsoftware-Release 7.1.1 ist die Verwendung beider Angaben möglich.

## 3.11 Setup Tool - Leased Line Menüs

Wurde eine ISDN-Festverbindung mit "leased line D+B1+B2 (TS02)" angelegt, so konnte im entsprechenden Menü ***ADVANCED SETTINGS*** immer noch eine X.31-Konfiguration vorgenommen werden. Dieses Menü ist bei dieser Konfiguration nun unzugänglich.

## 3.12 Temperaturalarm

Der Defaultwert für die Variable **TempAlarmThreshold** in der **biboAdmCardTable** ist auf 60 Grad Celsius erhöht worden.

# 4 Beseitigte Fehler

Folgende Fehler sind in Systemsoftware-Release 7.1.1 beseitigt worden:

- 4.1: "RADIUS - Multiuser Accounting"
- 4.2: "Trace - Fehlfunktion"
- 4.3: "Konfiguration nicht gelöscht"
- 4.4: "ISDN-Login schlägt fehl"
- 4.5: "Befehl ifconfig - Route geändert"
- 4.6: "QoS - Klassifizierte Daten korrupt"
- 4.7: "HTML Setup - Fehler in URL"
- 4.8: "HTML Setup - Pop-Up-Window nach Beendigung einer Session"
- 4.9: "SIF - Fragmentierte Pakete"
- 4.10: "Setup Tool - DHCP-Konfiguration schlägt fehl"
- 4.11: "PPPoE - LCP-Echo-Mechanismus unzuverlässig"
- 4.12: "HTTP Daemon - Daemon friert bei unterbrochener TCP-Session ein"
- 4.13: "Alive-Daemon - Redundante ICMP-Pakete"
- 4.14: "QoS - Verzögerung"
- 4.15: "Multilink PPP - Kompression"
- 4.16: "NetBIOS - Unnötiger Datenverkehr"
- 4.17: "Counter - Zu hohe Werte"
- 4.18: "IPSec - Paketverlust"

Die IDs unter der Überschriften beziehen sich auf die Fehler-IDs unseres Bugtracking-Systems. Wenn Sie Fragen zu einem der beseitigten Fehler haben, hilft diese ID unserem Support-Team bei der Identifikation des Fehlers.

Darüber hinaus finden Sie ggf. weitere Informationen wie Beschränkungen auf bestimmte Geräte oder Releases.

## 4.1 RADIUS - Multiuser Accounting

(ID 1705)

Werden Multiuser-Accounts (Internet by Call) über RADIUS gesteuert, so konnte es zu Problemen mit der Identifikation des korrekten RADIUS-Kontextes kommen, weil allen Benutzern mit identischem Login die gleiche Interface-Description zugeteilt wurde.

Das Problem ist gelöst worden: Es werden individuelle Namen für die temporären Interfaces verwendet.

## 4.2 Trace - Fehlfunktion

(ID 1858)

Bei einem Trace einer PPP-Verbindung über den ISDN Kanal 0 wurde nur Hex-Code und nicht die PPP-Interpretation angezeigt.

Dieses Problem ist gelöst worden.

## 4.3 Konfiguration nicht gelöscht

(ID 1903)

Wenn eine Konfigurationsdatei mittels des Befehls `cmd=get` eingespielt wurde, wurden solche Tabellen, die in der einzuspielenden Konfiguration leer waren, in einer ggf. vorhandenen Konfigurationsdatei gleichen Namens im Flash-ROM nicht gelöscht.

Dieses Problem ist gelöst worden: Es ist sichergestellt, dass die gesamte alte Konfiguration gelöscht bzw. überschrieben wird.

## 4.4 ISDN-Login schlägt fehl

(ID 2209)

Bei Geräten mit mehreren BRI-Interfaces konnte es vorkommen, dass bei einem ausgehenden ISDN-Login ein ISDN-Stack ausgewählt wurde, der nicht mit einer ISDN-Leitung verbunden war. Der ISDN-Login schlug fehl.

Dieses Problem ist gelöst worden: Stacks ohne Verbindung zum ISDN werden mit reduzierter Priorität behandelt und daher nicht mehr ausgewählt.

## 4.5 Befehl `ifconfig` - Route geändert

(ID 2507)

Bei der Verwendung des Befehls `ifconfig` wurde die Route eines Interfaces auch dann geändert, wenn der Befehl mit falscher Syntax eingegeben wurde.

Dieses Problem ist gelöst worden: Bei falscher Syntax wird auf die korrekte Verwendung hingewiesen.

## 4.6 QoS - Klassifizierte Daten korrupt

(ID 2684)

Vor Systemsoftware-Release 7.1.1 konnte es vorkommen, dass nach der Konfiguration einer QoS-Klassifikation für einen bestimmten Dienst die Daten dieses Dienstes korrupt waren und der Dienst nicht erreichbar war.

Dieses Problem ist gelöst worden.

## 4.7 HTML Setup - Fehler in URL

(ID 2743)

Wenn Sie eine HTML-Setup-Session über die HTML-Statusseite aufriefen, wurde die folgende URL im Adressfeld des Internet Explorers angezeigt: "http://your.router:/setup"; diese enthielt einen sinnlosen Doppelpunkt.

Es handelte sich lediglich um ein Anzeigeproblem, die Funktionsfähigkeit Ihres Routers war nicht betroffen. Das Problem ist gelöst worden.

## 4.8 HTML Setup - Pop-Up-Window nach Beendigung einer Session

(ID 2744)

Wenn eine HTML-Setup-Session mittels des "x"-Buttons des Browser-Fensters geschlossen wurde, erschien kurzfristig ein kleines Pop-Up-Fenster mit einer Kontrollmitteilung. Beim Internet Explorer war dieses Fenster zu klein und die Zeit zu kurz, um die Nachricht lesen zu können.

Dieses Problem ist gelöst worden.

## 4.9 SIF - Fragmentierte Pakete

(ID 2775)

Fragmentierte Datenpakete konnten von der Stateful Inspection Firewall nur dann korrekt zusammengefügt werden, wenn das erste Fragment auch als erstes empfangen wurde. Wurden die Pakete nicht in der originalen Reihenfolge empfangen, wurden die Pakete falsch zusammengesetzt.

Dieses Problem ist mit der SIF Stufe 2 gelöst worden.

## 4.10 Setup Tool - DHCP-Konfiguration schlägt fehl

(ID 2776)

Bei der Konfiguration eines Ethernet-Interfaces für die Verwendung von DHCP wurde die MAC-Adresse nicht in der **ipDhcpClientTable** gespeichert. Der DHCP-Client-Request schlug dann fehl. Die Eingabe der relevanten MAC-Adresse über die SNMP-Shell war möglich, der DHCP-Request war dann erfolgreich.

Dieses Problem ist gelöst worden: Die MAC-Adresse wird korrekt gespeichert.

## 4.11 PPPoE - LCP-Echo-Mechanismus unzuverlässig

(ID 2864)

Wurde eine PPPoE-Verbindung zu einem als RAS-Server arbeitenden BinTec-Router aufgebaut, so sendete dieser einen LCP Echo Request. Dieser enthielt einen Fehler und wurde daher nicht beantwortet. Die Verbindung kam nicht zustande.

Dieses Problem ist gelöst worden.

## 4.12 HTTP Daemon - Daemon friert bei unterbrochener TCP-Session ein

(ID 2875)

Wenn eine TCP-Session nicht korrekt beendet werden konnte, fror der HTTP Daemon ein. Das konnte z. B. dann vorkommen, wenn man die IP-Adresse des Routers mittels des HTML User Interfaces änderte.

Dieses Problem ist gelöst worden.

## 4.13 Alive-Daemon - Redundante ICMP-Pakete

(ID 2898)

Nach einem `cmd=load` oder aber der Änderung der Host-Konfiguration, sendete der Alive-Daemon redundante ICMP Messages und erkannte den Host Status nicht korrekt.

Dieses Problem ist gelöst worden: Der Host-Status wird korrekt erkannt und es werden keine redundante Pakete versendet.

## 4.14 QoS - Verzögerung

(ID n/a)

Wurde ein Interface mittels der QoS-Algorithmen *weighted round-robin (WRR)* oder *weighted fair queueing (WFQ)* gesteuert (Konfiguration mittels ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***QoS Scheduling and Shaping***:

**Queueing and Scheduling Algorithm**), so kam es zu Verzögerungen einzelner Pakete (z. B. jedes zweiten Pakets bei einem Ping).

Dieses Problem ist gelöst worden.

## 4.15 Multilink PPP - Kompression

(ID n/a)

Auch wenn während der Aushandlung der Verbindungsparameter keine Kompression ausgehandelt wurde, wurde das PPP Protocol Field vom Router komprimiert. Dazu konnte es zu Inkompatibilitäten mit Routern anderer Hersteller kommen.

Dieses Problem ist gelöst worden.

## 4.16 NetBIOS - Unnötiger Datenverkehr

(ID n/a)

Bei mehreren virtuellen Interfaces auf einem Ethernet-Interface des Routers, kam es zu redundantem NetBIOS-Verkehr.

Dieses Problem ist gelöst worden.

## 4.17 Counter - Zu hohe Werte

(ID n/a)

In der **biboPPPStatTable** waren die Variablen **biboPPPConnTransmitOctets** und **biboPPPTotalTransmitOctets** wiedergegebenen Werte erheblich zu hoch.

Dieses Problem ist gelöst worden: Die Werte werden korrekt angezeigt.

## 4.18 IPSec - Paketverlust

(ID n/a / **X2100** mit serieller Verbindung)

Bei der Verwendung einer großen TCP Windowsize (z. B. *33580* bei FTP-Transfers) und starker Verschlüsselung (z. B. *3DES*) konnte es zu Paketverlusten kommen.

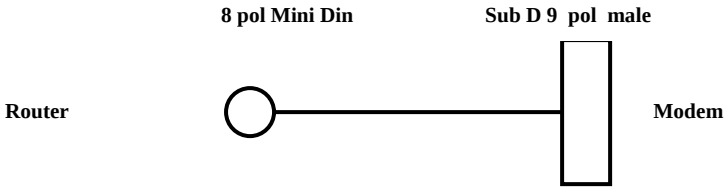
Dieses Problem ist gelöst worden: Eine verbesserte Datenbehandlung verhindert den Paketverlust.

# 5 Bekannte Fehler

Da es im alltäglichen Betrieb trotz umfangreicher Tests zu Problemen mit unserer Systemsoftware 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.

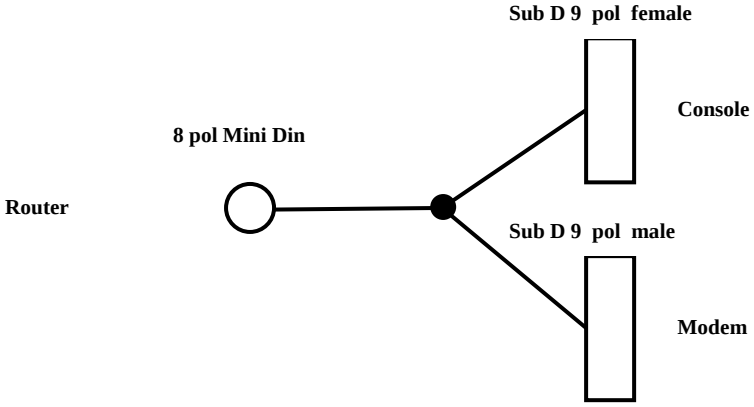
# Pin assignment to connect serial modems to X-Generation devices

## 1. Single mode modem connector




| Stecker 8pol Mini DIN | Sub-D 9polig male | |
|---|---|---|
| 5 | 2 | RXD |
| 4 | 5 | GND |
| 3 | 3 | TXD |
| | 4 | DSR |
| | 6 | DTR |
| | 7 | CTS |
| | 8 | RTS |

## 2. Dual Mode modem connector (Y-cable)




| Stecker 8pol Mini DIN | Sub-D 9polig female | |
|---|---|---|
| 3 | 3 | TXD |
| 4 | 5 | GND |
| 5 | 2 | RXD |
| | Sub-D 9polig male | |
| 1 | 2 | TXD |
| 2 | 3 | RXD |
| | 5 | GND |
| | 4 | DSR |
| | 6 | DTR |
| | 7 | CTS |
| | 8 | RTS |