Release Notes System Software Release 7.1.1

March 2004

Version 1.0

System Software Release 7.1.1

This document describes the new features, changes, bugfixes and known bugs in System Software Release 7.1.1.

1 Important Information

1.1 Downgrade Restrictions

It is not possible to downgrade directly from System Software Release 7.1.1 to a previous version of the system software.

Configurations created with System Software Release 7.1.1 are not compatible with older versions of our system software.

Save a backup copy of your router configuration on a PC before carrying out an upgrade.

It is possible to downgrade in stages:

- Save a backup copy of your router configuration on a PC before you carry out an upgrade to System Software Release 7.1.1. Information on saving an external copy of your configuration can be found in the chapter "Configuration Management" in your router manual.
- Now you can carry out the upgrade and still fall back on your old system software version if necessary. After a downgrade you must restore a configuration that matches the system software installed. Information about the necessary steps can be found in your router manual.

- Note that certain features will no longer be available after a downgrade.

Further information about upgrade or downgrade restrictions and the documentation for your router can be found at www.bintec.net.

1.2 Scope of Features

System Software Release 7.1.1 introduces many new features and optimizations. Please note the following special points:

1.2.1 Restrictions

- For **X1000** and **X1200** there is no IPSec Release available for System Software Release 7.1.1.
- **BinGO! DSL II** like **BinGO! DSL** is not IPSec-capable.
- Moreover the following features which are new in System Software Release 7.1.1 are not available for **X1000**, **X1200**, **BinGO! DSL** and **X3200**:
  - SSH Login
  - Content Filtering
  - IP Load Balancing.
- **X8500** does not support Content Filtering at this time.

1.2.2 Extended Features

X1000 II IPSec and **X1200 II IPSec** restore a number of functions that had to be removed from older IPSec Releases for **X1000** and **X1200**:

- Bridging
- X.25
- XoT
- AoDI
- H.323
- Encrypted ISDN Login

- RIP

In addition, the following features are available for the first time for **X1000 II** and **X1200 II**:

- PPPoE server (also for **BinGO! DSL II**)
- OSPF
- RADIUS PPP authentication
- BRRP
- Frame Relay (with relevant license)
- IPSec peers over RADIUS

1.3 Software Image Names

The names of the software images have changed and the device code is now placed before the actual release code. If your routers are configured using the configuration tool XAdmin, you must initially still use the old image names. This is done by just deleting the device code from the name: "X1x00II-b7101.x2x" then becomes "b7101.x2x".

1.4 BRICKware Wizard

Starting with version 7.1.1, our system software does not longer support the **BRICKware** Configuration wizard. A new HTML-based Configuration Wizard offering extended configuration options will be introduced with System Software Release 7.1.3 which will be available shortly after System Software Release 7.1.1.

2 New Features

System Software Release 7.1.1 contains the following new features:

- 2.1: "Support for new 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 Support for new X8500 Boards

Starting with version 7.1.1 our system software supports the newly introduced boards of **X8500**: The **X8E-1/2E3** board for one or two E3 connections and the new system board **X8A-SYS-VPN**. Information on configuration and installation can be found in the download section of **X8500** atwww.bintec.net.

2.2 IPSec Interface Concept

The configuration of IPSec peers was previously only possible via traffic lists. This meant it was not possible to use all the configuration options available for WAN partners. System Software Release 7.1.1 IPSec introduces a fundamentally new type of IPSec configuration that eliminates this disadvantage. The usual type of peer configuration via traffic lists is still available.

In the new configuration concept, an IPSec peer corresponds to a virtual interface. This provides the following features for handling IPSec connections:

- NAT and IPSec
- routing protocols like RIP
- rerouting
- other security features like SIF and TAF, filter lists
- IP Accounting for IPSec peers
- other features available for WAN partner configuration.

The configuration of an IPSec peer based on traffic lists has only changed slightly (see "Changes in the Configuration of Traffic Lists", page 16). Information on the configuration of traffic lists can be found in the IPSec manual or the relevant Release Notes.

2.2.1 IKE and IPSec Profiles

In System Software Release 7.1.1 the settings that determine how phase 1 and phase 2 of tunnel establishment are carried out are contained in **Profiles**. These profiles are available in all configuration contexts in which settings previously had to be made in isolation. That is, a profile created in a certain context (e.g. when modifying a peer) is also available in other contexts (e.g. for definition of the default settings for phase 1 and phase 2 in the IPSec main menu).

The menu for profile configuration can be found at three places in the Setup Tool:

- ***IPSec*** ➧ ***IKE (Phase 1)/IPSec (Phase 2) Defaults: edit*** in the context of defining the default profile that applies to each peer, if no peer-specific settings are made.
- ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT** ➧ ***Peer specific Settings*** ➧ ***IKE (Phase 1)/IPSec (Phase 2) Profile edit*** in the context of the peer-specific settings.
- ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT** ➧ ***Traffic List Settings*** ➧ **APPEND/EDIT** in the context of traffic list configuration (only for phase 2 profiles).

The menus are identical in all contexts; a profile created in one context is also available in all the other contexts.

As a profile must be available for IPSec configuration (even if this is not to be used later), the IPSec Wizard should be used to create the first peer. This ensures that a functioning profile exists.

When you create a new profile in the Setup Tool, most of the parameters in the relevant menu are set to the value *default*. This means the values of the profile selected as default profile in the IPSec main menu are used for the corresponding parameter.

As in previous versions of the IPSec software, it is still necessary to run through the non-interactive part of the IPSec Wizard once, as this provides the IKE and IPSec proposals and corresponding profiles.

2.2.2 Peer Configuration

The menu for creating a peer (of any type) in System Software Release 7.1.1 is shown below:

```
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
```

It contains the following fields:

Field	Meaning
Description	Here you enter the desired description of the peer. The maximum length of the entry is 255 characters.

Field	Meaning
Admin Status	Here you select the status to which you wish to set the peer after saving the configuration. Possible settings: ■ *up* - The peer is available for setting up a tunnel immediately after saving the configuration. ■ *down* - The peer is initially not available after saving the configuration. ■ *dialup* - A tunnel is set up once immediately after saving. All the possible types of connection (including callback) are covered. ■ *callback* - A tunnel is set up after saving. The router proceeds as if an initial callback call had already been received.
Oper Status	Shows the present status of the peer. This field cannot be edited.
Peer Address	Here you enter the official IP address of the peer or the peer's resolvable host name. This entry is not necessary in certain configurations. Further information can be found in the IPSec manual.
Peer IDs	Here you enter the ID of the peer. This entry is not necessary in certain configurations. This ID corresponds to the **Local ID** (***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** ➧ ***IKE (PHASE 1) DEFAULTS: EDIT*** ➧ **ADD/EDIT**) of the peer's router. Further information can be found in the IPSec manual.

Field	Meaning
Pre Shared Key	Only for authentication via preshared keys. Here you enter the pass phrase agreed on with the peer. The **Authentication Method** can be modified for the peer in the ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** ➧ ***IKE (PHASE 1) DEFAULTS: EDIT*** menu.
Virtual Interface	Here you decide if the peer is included with a traffic list or as a virtual interface. Possible settings: ■ *no* - Connections to the peer are controlled via a traffic list. ■ *yes* - The peer is created as a virtual interface. The data traffic routed over this interface is fully encrypted. The default setting is *no*.

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

The peer is modified in the following menus:

- ***IPSEC CALLBACK*** (information on the configuration of IPSec callback can be found in the Release Notes for System Software Release 6.2.5.)
- ***PEER SPECIFIC SETTINGS*** (see chapter 2.2.3, page 17)
- ***TRAFFIC LIST SETTINGS*** (for **Virtual Interface** = *no*, information on the configuration of traffic lists can be found in the IPSec manual)
- ***INTERFACE IP SETTINGS*** (for **Virtual Interface** = *yes*, see chapter 2.2.4, page 24).

Changes in the Configuration of Traffic Lists

Although the configuration of traffic lists has remained largely the same, IPSec profiles are also used for setting the *protect* mode of the traffic lists:

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

    Description:

     Protocol:      any

     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
```

The use of the profiles is described in chapter 2.2.3, page 17.

In addition, the IKE and IPSec settings of peers based on traffic lists can be modified generally for the peer in the ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** menu.

2.2.3 IKE and IPSec Settings

The ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** menu contains the options for modifying the IKE and IPSec settings for the 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
```

This menu allows the selection of previously defined profiles for phase 1 and phase 2. The value *default* represents the profile set in the **IKE (Phase 1)/IPSec (Phase 2) Defaults** field of the IPSec main menu.

The ***SELECT DIFFERENT TRAFFIC LIST*** menu is only accessible if a peer with traffic lists is configured.

Phase 1 Profile

The menu for configuration of a phase 1 profile is accessible for peer configuration via the ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** ➧ ***IKE (PHASE 1) PROFILE: EDIT*** ➧ **ADD/EDIT** menu:

```
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
```

The menu contains the following fields:

Field	Meaning
Description	Information on these parameters can be found in chapter 3.4.3 of the IPSec manual.
Proposal	
Lifetime	
Group	
Authentication Method	
Mode	

Field	Meaning
Heartbeats	Here you select whether and in what way IPSec heartbeats are used. In order to monitor if a Security Association (SA) is still valid, BinTec has introduced an IPSec-Heartbeat. Depending on its configuration, this Heartbeat sends and/or receives signals. If these signals fail, the SA is considered invalid. Possible settings: ■ *default* - The router uses the settings made for the default profile. ■ *none* - The router sends and expects no heartbeat. ■ *expect* - The router expects a heartbeat from the peer, but does not send one itself. ■ *send* - The router expects no heartbeat from the peer, but sends one itself. ■ *both* - The router expects a heartbeat from the peer and sends one itself. Heartbeats for phase 1 and phase 2 are configured separately with effect from System Software Release 7.1.1. If interoperability with older software is to be assured, the same values must be configured for phase 1 and phase 2.

Field	Meaning
Block Time	Here you define how long a peer is blocked for tunnel setups after a phase 1 tunnel setup has failed. This affects only locally initiated setup attempts. Possible values are *-1* to *86400* (seconds); *-1* (default) means the value in the default profile is used and *0* means that the peer is never blocked.
Local ID	Information on these parameters can be found in chapter 3.4.3 of the IPSec manual.
Local Certificate	
CA Certificates	

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

The ***View Proposals*** and ***Edit Lifetimes*** menus do not differ from those of IPSec software version 6.3.4 (information can be found in chapter 3.4.3 of the IPSec manual).

Phase 2 Profile

You can define profiles for phase 2 of the tunnel setup just as for phase 1. The configuration is set in the ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** ➧ ***PEER SPECIFIC SETTINGS*** ➧ ***IPSEC (PHASE 2) PROFILE EDIT*** ➧ **ADD/EDIT** menu:

```
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
```

The menu contains the following fields:

Field	Meaning
Proposal	Information on these parameters can be found in chapter 3.4.3 of the IPSec manual.
Lifetime	
Use PFS	

Field	Meaning
Heartbeats	Here you select whether and in what way IPSec heartbeats are used. In order to monitor if a Security Association (SA) is still valid, BinTec has introduced an IPSec-Heartbeat. Depending on its configuration, this Heartbeat sends and/or receives signals. If these signals fail, the SA is considered invalid. Possible settings: ■ *default* - The router uses the settings made for the default profile. ■ *none* - The router sends and expects no heartbeat. ■ *expect* - The router expects a heartbeat from the peer, but does not send one itself. ■ *send* - The router expects no heartbeat from the peer, but sends one itself. ■ *both* - The router expects a heartbeat from the peer and sends one itself. Heartbeats for phase 1 and phase 2 are configured separately with effect from System Software Release 7.1.1. If interoperability with older software is to be assured, the same values must be configured for phase 1 and phase 2.

Field	Meaning
Propagate PMTU	Here you select whether or not the PMTU (Path Maximum Transfer Unit) is to be propagated during phase 2. Possible settings: ■ *default* - The router uses the settings made for the default profile. ■ *no* - The Path Maximum Transfer Unit is not transferred. ■ *yes* - The Path Maximum Transfer Unit is transferred.

Table 2-3: ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT** ➧ ***Peer specific Settings*** ➧ ***IPSec (Phase 2) Profile: edit*** ➧ **ADD/EDIT**

The ***View Proposals*** and ***Edit Lifetimes*** menus do not differ from those of IPSec software version 6.3.4 (information can be found in chapter 3.4.3 of the IPSec manual).

2.2.4 Peer IP Configuration

The IP configuration of an interface peer is set in the ***Configure Peers*** ➧ **APPEND/EDIT** ➧ ***Interface IP Settings*** menu. The menu is identical to the menu for IP configuration of a WAN partner. It has been redesigned in the course of the IPSec changes. The changes are described in chapter 3 "Changes".

2.3 Content Filtering

BinTec introduces URL-based content filtering in System Software Release 7.1.1. This service behaves like a local HTTP proxy. It accesses the

Cobion Orange Filter (http://www.cobion.de) during operation and checks how a requested Internet page has been categorized by the Cobion filter. The action resulting from the categorization is configured on the router.

A license must be purchased from Cobion to operate the Cobion Orange Filter. A 30-day test license can be generated via a certain status in the Admin Status (see table 2-4, page 27). This is linked to the serial number of your router and can only be activated once.

Basically the attempt to call a URL or IP address can cause the following reactions in Content Filtering:

- The call for the requested page is blocked.
- The call is allowed, but logged.
- The call is allowed, but not logged.

2.3.1 Basic Parameters

The configuration is set up in the ***SECURITY*** ➧ ***COBION ORANGE FILTER*** menu:

```
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
```

This menu permits the configuration of basic parameters and access to the other configuration menus. It contains the following fields:

Field	Meaning
Admin Status	Here you can activate the filter. Possible settings: ■ *disable* - (Default value) Content filtering is deactivated. ■ *enable* - Content filtering is activated. ■ *enable 30 day demo ticket* - The router requests a demo license from Cobion.
Orange Filter Ticket	Here you enter the number of the license purchased from Cobion. The preset code designates the device type.

Field	Meaning
Expiring Date	This field is only shown if a license has been entered and checked. It shows the date the license expires and cannot be edited.
Ticket Status	Shows the result of the last validity check of the license. The validity of the license is checked every 23 hours.
Filtered Interface	Here you select for which of the existing Ethernet interfaces content filtering is activated. Only one interface can be specified. All calls to URLs or IP addresses arriving at this interface will be monitored. The default value is *none*.
History Entries	Here you define the number of entries to be saved in the content filtering history. Possible settings are whole numbers between *1* and *512*; the default value is *64*.

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

Apart from configuration of the basic parameters, the ***SECURITY*** ➧ ***COBION ORANGE FILTER*** menu permits access to the following menus:

- ***CONFIGURE WHITE LIST*** for the configuration of URLs that can be called independently of the Cobion categorization.
- ***CONFIGURE FILTERS*** for the configuration of the actions to be carried out as a result of the Cobion categorization.
- ***VIEW HISTORY*** for viewing the saved URL calls.

2.3.2 Configuring White List

The ***Security*** ➧ ***Cobion Orange Filter*** ➧ ***Configure White List*** menu contains a list of all URLs and IP addresses that can still be called even if they would be blocked as a result of the filter configuration and the categorization in the Cobion filter (the example contains arbitrary values; the default configuration contains no entries):

```
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
```

You can add other URLs or IP addresses to the list using the **ADD** button. The length of an entry is limited to 60 characters. Addresses listed in the White List are allowed automatically. It is not necessary to configure a corresponding filter.

2.3.3 Configuring Filters

The ***Security*** ➧ ***Cobion Orange Filter*** ➧ ***Configure Filters*** menu is for configuring which URLs and IP addresses are to be handled and how. There are basically different approaches for this: First a filter list can be created that only contains entries for those addresses that are to be blocked or logged. In this case it is necessary to make an entry at the end of the filter list that permits all accesses that do not match a filter. If you only create entries for those addresses that are to be allowed, it is not necessary to change the default behavior.

If you have configured filters, these will be run through in accordance with your priority, i.e. if more than one category matches for an address, the first matching filter is used.

If filters are configured and an address matches none of the filters, this address is blocked. A filter of the "Default behaviour" category is necessary for changing this behaviour. This filter allows such addresses if applicable.

The filters are configured in the ***Security*** ➧ ***Cobion Orange Filter*** ➧ ***Configure Filters*** menu. Initially a list of the filters already configured is shown (the example contains arbitrary values; the default configuration contains no filters).

```
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
```

The filter configuration menu is opened by pressing the **ADD** button:

```
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
```

It contains the following fields:

Field	Meaning
Category	Here you select which category of addresses/URLs the filter is to be used on. The standard categories of the Cobion Orange Filter are all available. Additionally, actions can be defined for the following special cases: ■ *Default behaviour* - If an address matches none of the filters it is blocked by default. This behavior can be changed with this category. ■ *No valid license ticket* - If the Cobion license is invalid, all calls are blocked if content filtering is active. This behavior can be changed with this category without having to change the *Default behaviour*. ■ *Orange Server not reachable* - If the Cobion server is not reachable, the action associated with this category is used. ■ *Other Category* - Some addresses are already known to the Cobion filter, but not yet categorized. The action associated with this category is used for such addresses. ■ *Unknown URL* - If an address is not known to the Cobion filter, the action associated with this category is used.

Field	Meaning
Day	Here you select the days on which the filter is to be active. Possible settings: ■ *Everyday* - The filter is used every day of the week. ■ *<Workday>* - The filter is used on a certain day of the week. Only one day can be selected per filter; several filters must be configured if several individual days are to be covered. ■ *Monday-Friday* - The filter is used from Mondays to Fridays. The default setting is *Everyday.*
From	Here you enter the time at which the filter is to be activated. The time is entered in the form *hh:mm*. The default setting is *0:0*.
To	Here you enter the time at which the filter is to be deactivated. The time is entered in the form *hh:mm*. The default setting is *23:59*.

Field	Meaning
Action	Here you select the action to be executed if the filter matches a call. Possible settings: ■ *block* - The call for the requested page is blocked. ■ *logging* - The call is allowed, but logged. You can access the logfile in the ***SECURITY*** ➧ ***COBION ORANGE FILTER*** ➧ ***VIEW HISTORY*** menu. ■ *allow* - The call is allowed, but not logged. The default setting is *block*.
Priority	Here you assign the filter a priority. The filters are used in accordance with this priority. Possible settings are all (whole number) values from *1* to *999*. A value of *1* denotes the highest priority.

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

Information on the standard categories of the Cobion Orange Filter can be found here: http://www.cobion.de/support/techsupport/dbcategories/). The English terms are used in the Setup Tool. These can be found on the relevant English pages.

2.3.4 View History

You can view the recorded history of the content filter in the ***SECURITY*** ➧ ***COBION ORANGE FILTER*** ➧ ***VIEW HISTORY*** menu:

```
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 16:09.52 192.168.0.1 www.droge.de/    Drugs              block

                                            EXIT
```

All calls marked for logging by a relevant filter are logged in the history (action = *logging*), likewise all rejected calls.

2.4 IP Load Balancing

The increasing amount of data traffic over the Internet necessitates the possibility of being able to send data over different links or interfaces in order to increase the total bandwidth available. Few ISPs, however, offer the possibility to combine several different interfaces to form one logical connection. IP Load Balancing enables the distribution of the data traffic of one logical connection to several links or interfaces.

The configuration is set in the IP ➧ ***BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)*** ➧ ***IP LOAD BALANCING OVER MULTIPLE INTERFACES*** menu.

All interfaces that are combined into one interface group using load balancing must have routes with the same metric. For load balancing over Internet connections, for example, a default route with the same metric is necessary for each interface of the group.

IP Load Balancing only shapes outgoing data traffic.Incoming traffic is handled according to the routing decisions made by the remote partner.

First a list of the interface groups already configured for load balancing is displayed. Press **ADD/EDIT** to access the menu for configuring the groups:

```
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
```

The menu contains the following fields:

Field	Meaning
Description	Here you enter the desired description of the interface group.
Interface Group ID	The ID of the interface group. This is assigned by the system automatically, but can also be edited. It is used only for internal assignment of the group.

Field	Meaning
Distribution Policy	Here you select how the data traffic is distributed to the interfaces configured for the group. Possible settings: ■ *session round-robin* - A newly set up session is assigned to one of the group interfaces according to the percentage allocation of sessions to the interface. The number of sessions assigned to an interface is measured. ■ *bandwidth load-dependent* - A newly set up session is assigned to one of the group interfaces according to the percentage utilization of the interfaces. The utilization of the interface is measured for data traffic in both the send and receive direction. ■ *bandwidth download-dependent* - A newly set up session is assigned to one of the group interfaces according to the percentage utilization of the interfaces. The utilization of the interface is measured for the data traffic in the receive direction only. ■ *bandwidth upload-dependent* - A newly set up session is assigned to one of the group interfaces according to the percentage utilization of the interfaces. The utilization of the interface is measured for the data traffic in the send direction only.

Field	Meaning
Distribution Policy (cont.)	■ *service/source-based routing* - A new session is assigned to one of the group interfaces according to the configuration of the static routing in the ***IP Load Balancing over Multiple Interfaces*** ➧ **ADD/EDIT** ➧ ***IP Routing List*** menu. This menu is only accessible if you have selected *service/source-based routing*.
Distribution Mode	Here you select the permissible **ifOperStatus** of an interface if it is to be included in load balancing. Possible settings: ■ *always (use operational up and dormant interfaces)* - Interfaces that are either *up* or *dormant* are included. ■ *up-only (operational up interfaces only)* - Only interfaces that are *up* are included.
Distribution Ratio	Not for **Distribution Policy** = *service/source-based routing.* Here you select whether the share of the sessions to be set up is to be the same for all interfaces of the group or configured individually for each interface. Possible settings: ■ *equal for all interfaces of the group* - All interfaces are automatically assigned the same share. ■ *individual for all interfaces of the group* - Each interface can be individually assigned a share of the sessions.

Field	Meaning
Interface <1 - 3>	Here you select the interfaces that are to belong to the group from the available interfaces.
Distribution Fraction (in percent)	Not for **Distribution Policy** = *service/source-based routing.* Here you enter the percentage of the sessions occurring that is to be assigned to an interface. The meaning differs according to the **Distribution Policy** used: ■ *session round robin* is based on the number of sessions to be distributed, for example, *60%* means that 60 % of all sessions can be assigned to the interface. ■ *bandwidth upload/download dependent* is based on the percentage utilization of the interface, for example, 60% means that the interface can be assigned 60 % of the total load.

Table 2-6: ***IP*** ➧ ***BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)*** ➧ ***IP LOAD BALANCING OVER MULTIPLE INTERFACES*** ➧ **ADD/EDIT**

Only one other submenu is relevant for the configuration of load balancing: ***IP LOAD BALANCING OVER MULTIPLE INTERFACES*** ➧ **ADD/EDIT** ➧ ***IP ROUTING LIST*** ➧ **ADD/EDIT**. Here the parameters are configured that determine how

new sessions are distributed to the interfaces if *service/source-based routing* has been selected as distribution policy:

```
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
```

The menu contains the following fields:

Field	Meaning
Interface	In these fields the menu corresponds to the menu for creating an extended routing configuration in the ***IP*** ➧ ***ROUTING*** ➧ **ADDEXT** menu. Information on this can be found in the manual of **X4100/200/300**, chapter "Advanced Configuration".
Type	
Network	
Destination IP Address	
Destination Mask	
Gateway IP Address	
Source IP Address	
Source Mask	
Protocol	

Field	Meaning
Service	Here you select a predefined service whose data traffic is to be affected by the entry. The value *unnamed service* is shown when accessing the menu. This is only a placeholder. The data traffic is not filtered by this entry as long as the default value *-1* is left in the **Port** field.
Port	Here you select the destination port of the data traffic, which is to be assigned to the interface. Possible values are *-1* to *65535*. The default value *-1* means that the destination port is not evaluated and can have any value.

Table 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

BinTec's ATM implementation has been largely revised, and in addition to new features (OAM F4, ATM QoS) it offers distinctly improved performance and operability preparing the router for upcoming requirements such as Multiple VC and new xDSL technology. Parts of the configuration of an ATM profile for a Permanent Virtual Circuit (PVC, the connection between two partners via ATM) have also changed due to the changes in the method of operation. This above all applies to the representation in our Setup Tool and in the MIB tables.

The first ATM root menu provides access to the following configuration menus:

- Protocol Configurations (***Ethernet over ATM***, ***PPP over ATM***, ***Routed Protocols over ATM***)
- Operation and Maintenance Configuration (***OAM***)

- Quality of Service for ATM Connections (***ATM QoS***).

The ATM profile is configured in the protocol menu corresponding to the protocol you use for the ATM interface.

2.5.1 Ethernet over ATM

The first menu window shows all the connections (PVCs) already configured that use Ethernet over ATM (ETHoA). Press **ADD/EDIT** to access the menu for configuring an ETHoA connection:

```
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
```

The menu contains the following fields:

Field	Meaning
Description	Here you enter the desired description for the connection.
ATM Interface	The ATM interface is only shown and cannot be selected. BinTec routers are currently equipped with only one ATM interface.

Field	Meaning
Virtual path identifier (VPI)	Here you enter the VPI value of the ATM connection. ATM distinguishes VP (Virtual Path) and VC (Virtual Channel). Each VP can envelop up to 65503 VCs. The VPI is the identification number of the virtual path to be used in the ATM network. Possible values are *0* to *255* and the default value is *1*.
Virtual channel identifier (VCI)	Here you enter the VCI value of the ATM connection. The VCI is the identification number of the virtual channel to be used in the ATM network. A virtual channel is the logical connection for the transport of ATM cells between two or more points. Possible values are *32* to *65535* and the default value is *32*.
Encapsulation	Here you select the encapsulation to be used. Possible settings: ■ *bridged-no-fcs* - Default value. Bridged Ethernet without frame check sequence (checksum field) ■ *bridged-fcs* - Bridged Ethernet with frame check sequence (checksum field) ■ *VC Multiplexing* - Allows the use of multiplexing on the virtual channel.

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

The ATM encapsulations are described in RFC 1483 and 2684.

You will find the RFC on the relevant pages of the IETF (www.ietf.org/rfc.html).

For ETHoA connections interfaces within the index range of *50.000* and *79.999* are created.

The menu also allows access to the ***IP AND BRIDGING*** menu. Here you configure the local Ethernet interface for the ATM connection. The available parameters are identical with those of the menu for the configuration of physical Ethernet interfaces (***LAN***). Information on configuration can be found in your router manual.

2.5.2 PPP over ATM

The menu for the configuration of a PVC with PPP over ATM (PPPoA) differs only slightly from the menu for the configuration of an 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
```

The following fields in this menu are new or provide other options:

Field	Meaning
Encapsulation	Here you select the encapsulation to be used. Possible settings: ■ *VC Multiplexing* - Default value. Allows the use of multiplexing on the virtual channel. ■ *llc* - The LLC protocol (Logical Link Control Protocol) is used for the connection.
Client Type	Here you select whether the PPPoA connection is set up permanently or on demand. Possible settings: ■ *Permanent (Leased Line)* - Default value. This setting creates interfaces within the index range of *80.000* and *89.999*. ■ *On Demand (Dialup)*.

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

Choosing **Client Type** *On Demand (Dialup)* does not automatically create an entry in the **pppTable**. This means that you may need to create an appropriate WAN-Partner using the Layer 1 Protocol PPPoA.

A respective WAN-Partner is automatically created for permanent connections.

2.5.3 Routed Protocols over ATM

The menu for the configuration of a connection via Routed Protocols over ATM (RPoA) (***ATM*** ➧ ***ROUTED PROTOCOLS OVER ATM*** ➧ **ADD/EDIT**) also differs only in parts from the ETHoA menu:

```
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
```

The differences are to be found in the following fields:

Field	Meaning
Encapsulation	Here you select the encapsulation to be used. Possible settings: ■ *non-ISO* - Default value. Encapsulation according to IEEE 802.1a LLC / RFC 2684. ■ *ISO (not allowed for IP)* - Encapsulation according to IEEE 802.2 LLC / RFC 2684. ■ *VC Multiplexing* - Allows the use of multiplexing on the virtual channel.

Field	Meaning
IP	Only the following parameters are available for IP configuration with RPoA connections: ■ **local IP Number** ■ **local Netmask**. Information on IP configuration can be found in your router manual.

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

For RPoA connections interfaces within the index range of *90.000* and *99.999* are created.

2.5.4 Operation and Maintenance (OAM)

OAM is a service for monitoring ATM connections. A total of five hierarchies (F1 to F5) are defined for OAM information flow. The most important information flows for an ATM connection are F4 and F5. The F4 information flow concerns the virtual path (VP) and the F5 information flow the virtual channel (VC).

In general monitoring is not initiated by your router but is initiated by the ISP. The router only has to respond correctly to the signals received. This is the case for both Flow levels (4 and 5) even without a specific OAM configuration.

Two mechanisms are available for monitoring the ATM connection: Loopback Tests and OAM CC (OAM Continuity Check). These can be configured independently of each other. First the configuration can be specified for an already defined Virtual Channel Connection (VCC, specified by the definition of VPI and VCI in one of the menus for configuration of ATM connections). Second

you can also define new combinations of VPI and VCI and then make the OAM settings.

The menu for OAM configuration is shown below (the screenshot contains random values):

```
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
```

The menu contains the following fields:

Field	Meaning
ATM Interface	The ATM interface is only shown and cannot be selected. BinTec routers are currently equipped with only one ATM interface.

Field	Meaning
OAM flow level	Here you select the OAM flow level. Possible settings: ■ *virtual channel (VC) level (F5)* - The OAM settings are used for the virtual channel (default value). ■ *virtual path (VP) level (F4)* - The OAM settings are used for the virtual path.
Virtual channel connection (VCC)	Here you select whether you use a previously set combination of VPI and VCI or configure a new combination. Possible settings in the **ADD** menu: ■ *specify VPI/VCI* - For configuring a new combination. ■ *Vpi: <"Vpi value"> Vci <"Vci value">* - You select a combination already configured in one of the existing ATM connections. Possible settings in the **EDIT** menu: ■ *no VPC defined* - The combination shown in the **VPI** and **VCI** fields cannot be linked to an existing ATM-connection (PVC). ■ *specify VPI/VCI* - For configuring a new combination.

Field	Meaning
Virtual path connection (VPC)	Visible only if **OAM flow level** = *virtual path (VP) level (F4)*. Here you select whether you use a previously set value for *VPI* or specify a new one. Possible settings in the **ADD** menu: ■ *specify VPI* - For configuring a new value. ■ *Vpi: <"Vpi value">* - You select a value already configured in one of the existing ATM connections. Possible settings in the **EDIT** menu: ■ *no VPC defined* - The value shown in the **VPI** field cannot be linked to an existing ATM-connection (PVC). ■ *Vpi: <"Vpi value">* - You select a value already configured in one of the existing ATM connections.
VPI	Only visible if **Virtual channel connection (VCC)** = *specify VPI/VCI* or **Virtual path connection (VPC)** = *specify VPI*. Here you enter a VPI value for this VCC (*0* to *255*). The default value is *0*.
VCI	Only visible if **Virtual channel connection (VCC)** = *specify VPI/VCI* and **OAM flow level** = *virtual channel (VC) level (F5)*. Here you enter a VCI value for this VCC (*32* to *65535*). The default value is *32*.

Field	Meaning
Loopback End-to-End	Here you select whether you activate the loopback test for the connection between the endpoints of the VCC. Possible settings: ■ *disabled* - Default value ■ *enabled.*
Send Interval (sec)	Only visible if **Loopback End-to-End** = *enabled*. Here you enter the intervals at which the loopback tests are performed. Possible values are *0* to *999*. The default value is *5*.
Pending Requests (max)	Only visible if **Loopback End-to-End** = *enabled*. Here you enter how many loopback tests can remain unanswered before the connection is regarded as “down”. Possible values are *1* to *99*. The default value is *5*.
Loopback Segment enable	Here you select whether you activate the loopback test for the segment connection of the VCC. Possible settings: ■ *disabled* - Default value ■ *enabled.*

Field	Meaning
Send Interval (sec)	Only visible if **Loopback Segment** = *enabled*. Here you enter the intervals at which the loopback tests are sent. Possible values are *0* to *999*. The default value is *5*.
Pending Requests (max)	Only visible if **Loopback Segment** = *enabled*. Here you enter how many loopback tests can remain unanswered before the connection is regarded as “down”. Possible values are *1* to *99*. The default value is *5*.
CC End-to-End	Here you select whether you activate the OAM CC (continuity check) test for the connection between the endpoints of the VCC. Possible settings: ■ *passive* - OAM CC requests are answered after negotiation (CC activation negotiation) (default value). ■ *active* - OAM CC requests are sent after negotiation (CC activation negotiation) (default value). ■ *both* - OAM CC requests are sent and answered after negotiation (CC activation negotiation) (default value). ■ *without negotiation* - Depending on the setting in the Direction field, OAM CC requests are either sent and/or answered. There is no negotiation. ■ *disabled*

Field	Meaning
Direction	Not visible if **CC End-to-End** = *disabled*. Here you select how the OAM CC test signals are sent or received. Possible settings: ■ *both* - CC data are received and generated (default value). ■ *sink* - CC data are only received. ■ *source* - CC data are only generated.
CC Segment	Here you select whether you activate the OAM CC test for the segment connection of the VCC. Possible settings: ■ *passive* - OAM CC requests are answered after negotiation (CC activation negotiation) (default value). ■ *active* - OAM CC requests are sent after negotiation (CC activation negotiation) (default value). ■ *both* - OAM CC requests are sent and answered after negotiation (CC activation negotiation). ■ *without negotiation* - Depending on the setting in the Direction field, OAM CC requests are either sent and/or answered. There is no negotiation. ■ *disabled*

Field	Meaning
Direction	Not visible if **CC Segment** = *disabled*. Here you select how the OAM CC test signals are sent or received. Possible settings: ■ *both* - CC data are received and generated (default value). ■ *sink* - CC data are only received. ■ *source* - CC data are only generated.

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

2.5.5 QoS Categories for ATM

System Software Release 7.1.1 supports QoS (Quality of Service) for ATM interfaces. Configuration is carried out in the ***ATM*** ➧ ***ATM QoS*** ➧ **ADD/EDIT** menu:

```
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
```

It contains the following fields:

Field	Meaning
ATM Interface	The ATM interface is only shown and cannot be selected. BinTec routers are currently equipped with only one ATM interface.
Virtual channel connection (VCC)	Here you select whether you use a combination of VPI and VCI already specified by an ATM connection or configure a new combination. Possible settings: ■ *specify VPI/VCI* - Default value. Used for configuring a new combination. ■ *Vpi: <"Vpi value"> Vci <"Vci value">* - You select a combination specified by one of the existing ATM connections.
VPI	Only visible if **Virtual channel connection (VCC)** = *specify VPI/VCI.* Here you enter a VPI value for this VCC (*0* to *255*). The default value is *0*.
VCI	Only visible if **Virtual channel connection (VCC)** = *specify VPI/VCI*. Here you enter a VCI value for this VCC (*32* to *65535*). The default value is *32*.

Field	Meaning
ATM Service Category	Here you select the service category for the data traffic of an ATM connection. The choice implies a specific way of how ATM traffic is handled. Possible settings: ■ *Unspecified Bit Rate (UBR)* - (Default value). The connection is not guaranteed any specific bandwidth. The **Peak Cell Rate** (PCR) defines the limit above which data (bursts) are discarded. This category is suitable for non-critical applications. ■ *Constant Bit Rate (CBR)* - The connection is assigned a guaranteed bandwidth. The maximum available bandwidth is determined by the **Peak Cell Rate**. This category is suitable for real-time applications that require a guaranteed bandwidth. ■ *Variable Bit Rate (VBR.1)* - The connection is assigned a (low) guaranteed bandwidth (**Sustained Cell Rate**). The data transfer is also limited by the **Peak Cell Rate** and the **Maximum Burst Size** (MBS). The PCR may be temporarily exceeded if necessary, but only for the number of bytes indicated by the MBS. Bursts after this are discarded. This category is suitable for non-critical applications with burst data traffic.

Field	Meaning
Peak Cell Rate (PCR) in bits per second	Here you enter a value for the maximum bandwidth used. Possible values are *0* to *10000000* and the default value is *0*. A value of *0* means that the PCR is not used to shape data traffic.
Sustained Cell Rate (SCR) in bits per second	Only for **ATM Service Category** = *Variable Bit Rate (VBR.1)*. Here you enter a value for the guaranteed minimum bandwidth. Possible values are *0* to *10000000* and the default value is *0*. A value of *0* means that the SCR is not used to shape data traffic.
Maximum Burst Size (MBS) in bytes	Only for **ATM Service Category** = *Variable Bit Rate (VBR.1)*. Here you enter a value for the maximum number of bytes which the PCR can be temporarily exceeded by. Possible values are *0* to *100000* and the default value is *0*. A value of *0* means that the MBS is not used to shape data traffic.

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

2.6 Analog/GSM Interface

Analog connections and GSM modems have not been supported by BinTec until now. With an analog/GSM interface it is also possible to use these types of connections with effect from System Software Release 7.1.1 (e.g. as backup). You can use any Hayes or GSM07.07-compatible modem with a serial interface for this purpose.

You need a special cable to connect the modem to a BinTec router. The specification of this cable is given in the appendix to this document.

Note that you can only use the single connector cable (see appendix) for routers of the **X2000 Family**.

The configuration is set in the ***AUX*** menu:

```
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
```

The menu contains the following fields:

Field	Meaning
Serial Port	Here you select which serial interface you want to use for connection to the modem. Possible settings: ■ *second* - You use the second, previously unused serial interface. Routers of the **X2000 Family** are not equipped with a second serial interface. ■ *console* - You use the console interface. The serial console is no longer available.
Line speed	Here you select the speed at which the router addresses the modem (in bps). Possible settings: ■ *default* - The speed is not modified. All other values mean that the modem is addressed at the corresponding speed in bps. ■ *9600* ■ *19200* - Default value; recommended for communication with a GSM modem ■ *38400* ■ *57600* ■ *115200* - recommended for communication with an analog modem.
Active Profile	Here you select the profile whose settings are used for communication with the modem.

Field	Meaning
Profile <1 to 4>	Use these buttons to access the menus for configuration of the relevant profile.

Table 2-13: ***AUX***

You can define different presets for router modem communication via profile configuration:

```
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
```

The menu contains the following fields:

Field	Meaning
Dispatch Item	Here you select the subsystem of the router to which a call coming in via the modem is to be assigned. Possible settings: ■ *none* - Calls are not accepted. ■ *PPP dialin* - The call is assigned to the PPP subsystem. ■ *isdnlogin* - The call is assigned to the ISDN Login subsystem. Default setting is *PPP dialin*.

Field	Meaning
GSM SIM PIN	Here you enter the PIN of your GSM modem, if your modem asks for it. Entering a wrong PIN blocks communication with the modem until the entry in the profile is corrected. Default value is *0000*.
Escape Char	The value for this field is set by default to "+". It should only be changed if the escape character of the modem is different.
Init Sequence	Here you can enter an init sequence for your modem. The command *ATX3* is the default setting (the modem does not wait for a free signal before dialing). You can add other AT commands by separating them with semicolons. The entry is limited to 50 characters. Make sure you enter the command for activating the XON/XOFF software flow control. This depends on the manufacturer and cannot be set automatically. The command sequence can be found in the manual of your modem or can be obtained from the manufacturer.

Table 2-14: ***AUX*** ➧ **Profile <1 to 4>**

If you want to create a WAN partner who uses the AUX interface for PPP Dial-In/Dial-Out, you must activate the **Slot 0 Auxiliary** control box in the ***WAN PARTNER*** ➧ **ADD/EDIT** ➧ ***WAN NUMBERS*** menu. This is done by tagging the box with the cursor and changing the setting with the space bar.

The AUX interface is supported by the BinTec trace. To activate the trace, enter, e.g., `trace -h 0 9 0` in the shell.

AUX Syslog messages are generated at the *debug* and *err* levels. Active calls are shown in the **isdnCallTable** and terminated calls in the **isdnCallHistoryTable**.

2.7 Email Alert

It was already possible to send syslog messages from the router to any syslog host. System Software Release 7.1.1 now adds the Email Alert feature: Depending on the configuration, e-mails are sent to the administrator as soon as relevant syslog messages occur.

The configuration is set in the ***Monitoring and Debugging*** ➧ ***Email Alert*** menu:

```
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
```

The menu contains the following fields:

Field	Meaning
Adminstatus	Here you activate or deactivate the feature. Possible settings: ■ *enable* (default value) ■ *disable*

Field	Meaning
SMTP Server	Here you enter the address (IP address or valid DNS name) of the mail server to be used for sending the mail. The entry is limited to 40 characters.
Originator	Here you enter the mail address to be entered in the sender field of the email. The entry is limited to 40 characters.
max. Mails/min	Here you can limit the number of outgoing mails per minute. Possible values are *1* to *30*; the default value is *6*.

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

The Notification Rules already configured are shown in the bottom part of the menu window. You can configure a new rule or edit an existing one with **ADD/EDIT**:

```
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
```

The menu contains the following fields:

Field	Meaning
Receiver	Here you enter the email address of the receiver. The entry is limited to 40 characters.
Contents	Here you must enter a regular expression. Its occurrence in a syslog message triggers an email alert. The entry is limited to 55 characters. Note that without the use of wildcards (e.g. "*") only such strings meet the conditions for an email alert which exactly match the entry. The entry will therefore usually contain wildcards. To be informed about all syslog messages on principle, you only need to enter "*".
Level	Here you select the syslog level at which the string entered for **Contents** must occur to trigger an email alert. Possible settings are all the values available in the **Message level for the syslog table** field of the ***SYSTEM*** menu; the default value is *emergency*.
Timeout	Here you specify the maximum wait time before an alert email is forced to be sent after an alert event. Possible values are *0* to *86400*. A value of *0* deactivates the timeout and the default value is *60*.

Field	Meaning
Messages	Here you enter the number of syslog messages that must be reached before an alert email can be sent for this case. If a **Timeout** is configured, the alert is sent when this expires, even if the number of messages is not yet reached. Possible values are *1* to *99*; the default value is *1*.
Compress	Here you can select whether the email alert text is to be abstracted. The email sent only contains a notice which kind of alert has occurred and the number of relevant occurrences. Possible settings: ■ *disable* - default value ■ *enable*
Select subsystems	Here you select the subsystems to be monitored. Tag the subsystem with the cursor and activate or deactivate it with the space bar.

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

2.8 SSH Login

System Software Release 7.1.1 provides encrypted access to the shell of your router. You can activate and configure this access in the ***SECURITY*** ➧ ***SSH DAEMON*** menu:

```
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
```

Here you can deactivate or reactivate the SSH Daemon activated in the default setting and access the menus for configuration of the SSH Login.

After configuration you should check that the SSH Daemon has started: Enter `ps -e` in the shell and verify that `sshd` is executed.

If not, you must restart the router to start the SSH Daemon.

Please note that if you intend to use SSH Login with the PuTTY client, you need to observe some configuration specifics. We have created a FAQ telling you how exactly to configure the router and PuTTY to work together. You can find the FAQ in the Service/Support section off www.bintec.de. As of now it is available only in German.

Static Settings

Here you determine the basic parameters of the SSH Login:

```
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
```

The menu contains the following fields:

Field	Meaning
Max. # of Clients	Here you enter how many concurrent connections are allowed to the SSH Daemon. Further connections are rejected until a connection is cleared. Possible values are *1* to *100* and the default value is *1*. Only one SSH connection is currently possible due to technical reasons.
Port # used for Connections	Here you enter the port at which a client can connect to the SSH Daemon. The default value is *22*.

Field	Meaning
Compression	Here you can activate (*enabled*) or deactivate (*disabled*) the use of data compression. The default value is *disabled*.
Verify Reverse Mapping	Here you select whether the SSH Daemon executes a Reverse Lookup of the client IP address. This makes sure that the host name and the IP address match and the IP address has not been faked. Possible settings: ■ *disabled* - Default value ■ *enabled*.
Print Motd	Here you select whether the SSH Daemon sends a Message of the Day (MotD) as soon as a client has logged in. Possible settings: ■ *disabled* ■ *enabled* - Default value.
Print LastLog	Here you select whether the SSH Daemon prints the date and time of the last login when a client logs in. Possible settings: ■ *disabled* - Default value ■ *enabled*.

Field	Meaning
Logging Level	Here you can select the syslog level for the syslog messages generated by the SSH Daemon. Possible settings: ■ *quiet* ■ *fatal* ■ *error* ■ *info* - Default value ■ *verbose* ■ *debug.*

Table 2-17: ***SECURITY*** ➧ ***SSH DAEMON*** ➧ ***STATIC SETTINGS***

Timer

You can configure the timing behavior of the SSH Daemon in the ***SECURITY*** ➧ ***SSH DAEMON*** ➧ ***TIMER*** menu:

```
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
```

The menu contains the following fields:

Field	Meaning
Login Grace Time	Here you enter the time interval within which a client must authenticate before the connection is cleared. Possible values are *0* to *3600* (seconds). A value of *0* means no limit and the default value is *600*.
TCP Keepalives	Here you select whether the router is to send keepalive packets. Possible settings: ■ *disabled* ■ *enabled* - Default value. The same value should be configured for both client and server.
ClientAliveCountMax	Here you enter the number of Client Alive Messages that can be sent by the router and remain unanswered before the SSH Daemon clears the connection. Possible values are *0* to *10* and the default value is *3*.
ClientAliveInterval	Here you enter the interval after which the SSH Daemon sends a Keepalive Request to the client if no more data are received from the client. Possible values are *1* to *3600* (seconds) and the default value is *10*.

Table 2-18: ***SECURITY ➧ SSH DAEMON ➧ TIMER***

Authentication Algorithms

In this menu you can make the settings for the authentication mechanisms used:

```
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
```

The menu contains the following fields:

Field	Meaning
Protocol Version	This shows which SSH version the SSH Daemon uses. This field cannot be edited, as only version 2 is currently supported.
Public Key	Here you select whether or not public key authentication of the client is allowed. Possible settings: ■ *disabled* ■ *enabled* - Default value. This authentication mechanism is still in the experimental stage.

Field	Meaning
Password	Here you select whether or not password authentication of the client is allowed. Possible settings: ■ *disabled* ■ *enabled* - Default value.
Challenge Response	Here you select whether or not challenge response authentication of the client is allowed. Possible settings: ■ *disabled* ■ *enabled* - Default value. This authentication mechanism is still in the experimental stage.

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

Supported Ciphers

In this menu you can make the settings for the encryption algorithms used:

```
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
```

You can choose between *enabled* (default value) and *disabled* for each of the algorithms listed in the menu.

Message Authentication Codes

In this menu you can make the settings for the message authentication algorithms used:

```
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
```

You can choose between *enabled* and *disabled* for each of the algorithms listed in the menu.

Certification Management

This menu is for creating the keys necessary for authentication. You can select a DSA key and an RSA key. We recommend you create both keys. The keys will be internally stored on the router.

Creating the keys needs several minutes and cannot be interrupted or aborted.

Monitoring

This menu shows you the connections set up. The implementation of this feature is not yet completed at present.

2.9 GRE (Generic Routing Encapsulation)

The specification of the GRE protocol is available in two versions: GRE V.1 for use in PPTP connections (RFC 2637) and GRE V.0 (RFC 2784). GRE V.1 is already available for BinTec routers and with effect from System Software Release 7.1.1 you can also use GRE V.0 outside this context.

The ***GRE*** menu is for configuring a virtual interface. Data traffic routed over this interface is then encapsulated using GRE and sent to the specified recipient. The first menu window shows a list of the GRE interfaces already configured. Press **ADD/EDIT** to access the menu for configuring such an interface:

```
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
```

The menu contains the following fields:

Field	Meaning
Name	Here you enter the desired named for the virtual interface.
GRE Partner's IP Address	Here you enter the IP address of the GRE partner.

Field	Meaning
GRE Local IP Address	Here you enter the IP address to be used as source address for GRE packets. If you choose a value of *0.0.0.0*, the IP address necessary for sending packets to the IP address of the GRE partner is selected automatically.
Partner's LAN IP Address	Here you enter the IP address of the network in which the **GRE Partner's IP Address** is located.
Partner's LAN IP Mask	Here you enter the netmask of the network in which the GRE partner is located.
Mtu	Here you enter the MTU (Maximum Transfer Unit) to be used for a GRE connection between the partners. Possible values are *1* to *8192* (bytes). The default value is *1500*.
Key Used	Here you select whether different connections to the same GRE partner are to be tagged as such using a key. Possible settings: ■ *no* - Default value ■ *yes.*
Value	Only for **Key Used** = *yes*. Here you enter a value for the key. Possible values are *0* to *2147483647* (32-bit).

Table 2-20: ***GRE*** ➧ **ADD/EDIT**

3 Changes

3.1 Structure of Setup Tool

To provide easy access to the increasing number of security features in the Set-up Tool, the relevant menus are now arranged in the ***SECURITY*** menu. This is located directly in the main menu and contains the following submenus:

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

- ***LOCAL SERVICES ACCESS CONTROL.***

With the exception of the newly added menus ***COBION ORANGE FILTER*** and ***SSH DAEMON***, these menus have been moved from the ***IP*** menu to the ***SECURITY*** menu. Unless otherwise described, the structure of the menus themselves is unchanged.

3.2 Changes in WAN Partner Configuration

Changes have been made to the ***WAN PARTNER*** ➧ **ADD/EDIT** ➧ ***IP*** menu for the configuration of a WAN partner. These changes also affect the IP configuration of IPSec peers. They make it possible to make routing settings specifically for a WAN partner that could previously only be configured globally.

In System Software Release 7.1.1 the first menu window offers access to the other configuration menus:

```
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*

The ***BASIC IP SETTINGS*** menu corresponds to the ***WAN PARTNER*** ➧ **ADD/EDIT** ➧***IP*** menu of older system software. Only the access to the ***ADVANCED SETTINGS*** menu has been shifted.

3.2.2 *MORE ROUTING*

The ***MORE ROUTING*** menu is for configuring more routes for the WAN partner specifically. These routes are not shown in the ***IP*** ➧***ROUTING*** menu and apply exclusively to the respective WAN partner. The menu corresponds to the ***IP*** ➧ ***ROUTING*** menu.

3.2.3 *ADVANCED SETTINGS*

This menu does not differ from the ***WAN PARTNER*** ➧ **ADD/EDIT** ➧***IP*** ➧ ***ADVANCED SETTINGS*** menu of older system software.

3.3 Stateful Inspection Firewall Stage 2

The Stateful Inspection Firewall (SIF) has been extended over earlier releases. Additional parameters are available in the newly designed SIF main menu and there is also a new mode for address alias definition.

3.3.1 New SIF Main Menu

The ***SECURITY*** ➧ ***STATEFUL INSPECTION*** menu in System Software Release 7.1.1 no longer shows a list of filters already configured, but a menu with global parameters:

```
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
```

The menu contains the following fields:

Field	Meaning
Adminstatus	Here you can basically activate and deactivate the service. Possible settings: ■ *enable* - default value ■ *disable*

Field	Meaning
Local Filter	Here you define whether locally initiated connections are also to be filtered by the SIF. Possible settings: ■ *enable* - Locally generated sessions are also filtered. ■ *disable* - Locally generated sessions are generally allowed (default value).
Full Filtering	Here you define whether packets are only to be filtered if they are sent to an interface other than the interface that created the connection. Possible settings: ■ *enable* - All packets are filtered (default value). ■ *disable* - Packets are only filtered if their destination interface differs from the output interface of the connection.
Logging level	Here you can select the syslog level. Possible settings: ■ *all* - All SIF activity is shown (default value). ■ *deny only* - Only reject and ignore events are shown. ■ *accept only* - Only accept events are shown. ■ *none* - Syslog messages are not generated.

Table 3-1: ***Security*** ➧ ***Stateful Inspection Firewall***

Access for configuration of the filters and the services and addresses for the filters is via the ***Security*** ➧ ***Stateful Inspection Firewall*** menu. It also pro-

vides access to the ***SECURITY*** ➧ ***STATEFUL INSPECTION*** ➧ ***ADVANCED SETTINGS*** menu:

```
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
```

It contains the following fields:

Field	Meaning
UDP inactivity Timeout	Here you can enter the inactivity time after which a UDP session is regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *180*.
TCP inactivity Timeout	Here you can enter the inactivity time after which a TCP session is regarded as expired (in seconds). Possible values are *30* to *86400*; the default value is *3600*.
PPTP inactivity Timeout	Here you can enter the inactivity time after which a PPTP session is regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *86400*.

Field	Meaning
Other inactivity Timeout	Here you can enter the inactivity time after which another type of session is regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *30*.

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

3.3.2 Address Alias Definition

An option for the **Mode** field has been added to the menu for creating or changing an address alias (***STATEFUL INSPECTION*** ➧ ***EDIT ADDRESSES*** ➧ **ADD/EDIT**): *Address/Range*. If this is selected, an entry is possible in the **IP Address** (default: empty) and **IP Range** fields (default: *1*).

This mode makes it possible to provide a string of IP addresses for SIF filtering, without having to specify a whole subnetwork.

3.4 IPSec - New Phase 1 Mode

System Software Release 7.1.1 introduces two new IPSec Phase 1 modes:

- *aggressive_only*: During IKE negotiation only aggressive mode proposals are accepted.
- *id_protect_only*: During IKE negotiation only ID protect mode (main mode) proposals are accepted.

The new values are available in all menus for IPSec Phase 1 configuration: See chapter 2.2.1, page 11 for information on Phase 1 profiles.

3.5 NAT - NAT Session Timeout

NAT sessions could previously not be maintained for longer than 18 hours if no data were sent or received over the relevant interface. The maximum timeout of a NAT session has been increased to 5184000 seconds (60 days). To avoid insecure configurations, not only can interface-specific timeouts be configured (**ipExtIfNatTcpTimeout** and **ipExtIfNatOtherTimeout**), but also a global timeout (**ipNatOutTimeout** and **ipNatPrTimeout**). The default value of both global parameters is *0*, i.e. the interface-specific values are used. If a value is set for the global parameters, this is used if no specific values are configured for the interface. Using these parameters, it is possible without time-consuming configuration to assign certain interfaces a long timeout, but all others a shorter and therefore more secure timeout.

3.6 Second BOOTP Relay Server

To avoid problems with the accessibility of a BOOTP relay server, it is now possible to enter a second server. This is done in the ***IP*** ➧ ***STATIC SETTINGS*** field: **Secondary BOOTP Relay Server**.

3.7 Telnet - New Option

The Telnet application now supports the `-s` option for entering a source address for the Telnet connection. The syntax is:

```
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 Calculation Changed

Prior to System Software Release 7.1.1 the ping Daemon waited until the end of the ping timeout before the next ICMP Echo Request was sent, even if an ICMP Echo Reply was received before the timout.

The behavior has been changed so that the Next Ping Time is not longer than one second, if the preceding ping was successful.

3.9 BootP - TTL Value

For interoperability reasons the value of the BootP Time to Live has been set to a default value of *0* (previously *16*). It thus corresponds to the value of the IP TTL (**ipDefaultTTL**).

3.10 Trace - IfIndex Usable

It was not previously possible to enter the interface index for the trace of an interface. The name of the interface had to be entered. The use of both entries is possible with effect from System Software Release 7.1.1.

3.11 Setup Tool - Leased Line Menus

If an ISDN leased line connection was previously configured with "leased line D+B1+B2 (TS02)", it was still possible to make an X.31 configuration in the corresponding ***ADVANCED SETTINGS*** menu. This menu is now not accessible in this configuration.

3.12 Temperature Alarm

In the **biboAdmCardTable**, the default value for the variable **TempAlarmThreshold** has been increased to 60 degrees Celsius.

4 Bugfixes

The following bugs have been fixed in System Software Release 7.1.1:

- 4.1: "RADIUS - Multiuser Accounting"
- 4.2: "Trace - Malfunction"
- 4.3: "Configuration Not Deleted"
- 4.4: "ISDN Login Fails"
- 4.5: "Command ifconfig - Route Changed"
- 4.6: "QoS - Classified Data Corrupt"
- 4.7: "HTML Setup Error in URL"
- 4.8: "HTML Setup - Pop-Up Window after Ending a Session"
- 4.9: "SIF - Fragmented Packets"
- 4.10: "Setup Tool - DHCP Configuration Fails"
- 4.11: "PPPoE - LCP Echo Mechanism Unreliable"
- 4.12: "HTTP Daemon - Daemon Freezes if TCP Session is Interrupted"
- 4.13: "Alive Daemon - Redundant ICMP Packets"
- 4.14: "QoS - Delay"
- 4.15: "Multilink PPP - Compression"
- 4.16: "NetBIOS - Unnecessary Data Traffic"
- 4.17: "Counter - Excessively High Values"
- 4.18: "IPSec - Packet Loss"

The IDs below the headings refer to the error IDs of our bugtracking system. If you have questions about any of the bugfixes, this ID helps our support team to identify the error.

In addition, you will find further information like restrictions to certain devices or releases, if applicable.

4.1 RADIUS - Multiuser Accounting

(ID 1705)

If multiuser accounts (Internet by Call) are controlled via RADIUS, problems were possible with the identification of the correct RADIUS context, because all users with the same login were assigned the same interface description.

This problem has been solved: Individual names are used for the temporary interfaces.

4.2 Trace - Malfunction

(ID 1858)

For a trace of a PPP connection over ISDN channel 0 only hex code was shown and not the PPP interpretation.

This problem has been solved.

4.3 Configuration Not Deleted

(ID 1903)

If a configuration file was loaded using the `cmd=get` command, tables that were empty in the configuration to be loaded were not deleted in an possibly exiting configuration file with the same name in the flash ROM.

This problem has been solved: The complete old configuration is now deleted or overwritten.

4.4 ISDN Login Fails

(ID 2209)

For devices with several BRI interfaces it was possible on an outgoing ISDN Login that an ISDN stack was selected that was not connected to an ISDN line. The ISDN Login failed.

This problem has been solved: Stacks without a connection to the ISDN are treated with reduced priority and are therefore no longer selected.

4.5 Command `ifconfig` - Route Changed

(ID 2507)

If the `ifconfig` command is used, the route of an interface is also changed if the command has been entered with the wrong syntax.

This problem has been solved: If the syntax is wrong, reference is made to the correct use.

4.6 QoS - Classified Data Corrupt

(ID 2684)

Prior to System Software Release 7.1.1 it was possible after the configuration of a QoS classification for a certain service that the data of this service were corrupt and the service was not reachable.

This problem has been solved.

4.7 HTML Setup Error in URL

(ID 2743)

On activating an HTML setup session via the HTML status page, the following URL was shown in the address field of the Internet Explorer: "http://your.router:/setup"; this contained a meaningless colon.

This was only a display problem and did not affect the operation of your router. The problem has been solved.

4.8 HTML Setup - Pop-Up Window after Ending a Session

(ID 2744)

If an HTML setup session was closed using the "x" button of the browser window, a small pop-up window appeared briefly with a control message. In Internet Explorer this window was too small and the time too short to be able to read the message.

This problem has been solved.

4.9 SIF - Fragmented Packets

(ID 2775)

Fragmented data packets could only be correctly assembled by the Stateful Inspection Firewall if the first fragment was actually received first. If the packets were not received in the original order, the packets were assembled incorrectly.

This problem has been solved with SIF stage 2.

4.10 Setup Tool - DHCP Configuration Fails

(ID 2776)

In the configuration of an Ethernet interface for the use of DHCP the MAC address was not saved in the **ipDhcpClientTable**. The DHCP Client Request then failed. It was possible to enter the relevant MAC address via the SNMP shell, after which the DHCP Request was successful.

This problem has been solved: The MAC address is saved correctly.

4.11 PPPoE - LCP Echo Mechanism Unreliable

(ID 2864)

If a PPPoE connection was set up to a BinTec router operating as RAS server, this sent an LCP Echo Request. This request contained an error and was therefore not answered. The connection was not set up.

This problem has been solved.

4.12 HTTP Daemon - Daemon Freezes if TCP Session is Interrupted

(ID 2875)

If a TCP session could not be ended correctly, the HTTP Daemon froze. This possibly occurred, for example, if the IP address of the router was changed using the HTML user interface.

This problem has been solved.

4.13 Alive Daemon - Redundant ICMP Packets

(ID 2898)

After `cmd=load` or changing the host configuration, the Alive Daemon sent redundant ICMP messages and did not correctly detect the host status.

This problem has been solved: The host status is detected correctly and no redundant packets are sent.

4.14 QoS - Delay

(ID n/a)

If an interface was controlled using the QoS algorithms *weighted round-robin (WRR)* or *weighted fair queueing (WFQ)* (configuration using ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***QoS Scheduling and Shaping***: **Queueing and Scheduling Algorithm**), individual packets were delayed (e.g. each second packet for a ping).

This problem has been solved.

4.15 Multilink PPP - Compression

(ID n/a)

Although no compression was negotiated during negotiation of the connection parameters, the PPP Protocol field was compressed by the router. This possibly caused incompatibilities with routers of other manufacturers.

This problem has been solved.

4.16 NetBIOS - Unnecessary Data Traffic

(ID n/a)

With several virtual interfaces bound to an Ethernet interface of the router, redundant NetBIOS traffic occurred: As the address of the WINS server on the router is specified globally, WINS requests had to be forwarded internally, whereupon the source address of the request was ignored. The request was therefore passed back to the source address and was sent again.

This problem has been solved.

4.17 Counter - Excessively High Values

(ID n/a)

In the **biboPPPStatTable**, the values shown by the variables **biboPPPConnTransmitOctets** and **biboPPPTotalTransmitOctets** were much too high.

This problem has been solved: The values are shown correctly.

4.18 IPSec - Packet Loss

(ID n/a / **X2100** with serial connection)

Packet losses were possible if a large TCP window size was used (e.g. *33580* for FTP transfers) in combination with heavy encryption (e.g. *3DES*).

This problem has been solved: Improved data handling prevents packet loss.

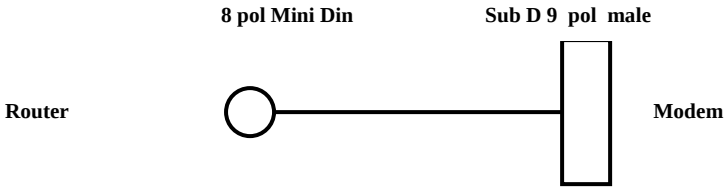
5 Known Issues

As problems can still occur in everyday operation with our system software in spite of extensive tests, BinTec has created a mailing list (**release info**), which keeps you up to date on problems, solutions and workarounds that have been verified in our laboratories. Please see our Internet site if you would like to subscribe to this mailing list: You will find an appropriate link in the download section of www.bintec.net.

5 Known Issues

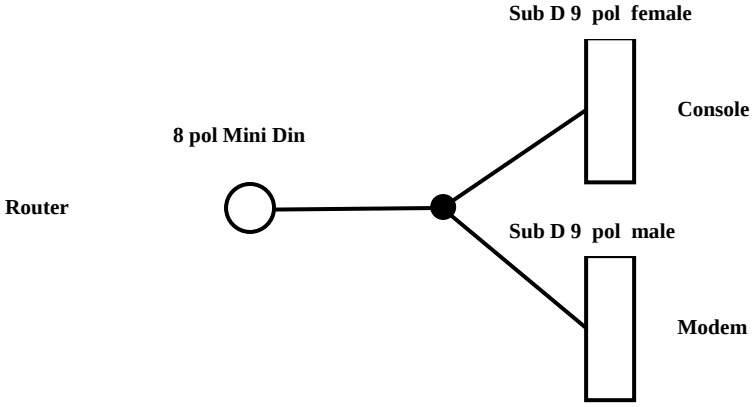
Pin assignment to connect serial modems to X-Generation devices

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