Release Notes System Software Release 6.2.5 X-Generation

October 2002

System Software Release 6.2.5

This document describes the new features, changes, bugfixes and known bugs in System Software Release 6.2.5.

This is a draft version of the Release Notes 6.2.5. While we have made every effort to provide the most accurate information, it is still possible that information contained in this document is inaccurate.

Table of Contents

Table of Contents

1 Introduction

BinTec's System Software Release 6.2.5 presents a new element of the BinTec security concept: the Stateful Inspection Firewall (SIF). This release also contains more new features and a number of bugfixes.

1.1 Updating System Software

Proceed as follows to update your router to System Software Release 6.2.5:

- Download System Software Release 6.2.5 from our Web server (www.bintec.net).
- Update the software on your router. You will find instructions on this in the chapter "Updating Software" in your router manual.

When you update the system software of your router, you should also consider installing the latest version of BRICKware for Windows on your PC. You can also download this from our Web server.

If you want to update **X4000** from an earlier software version than 6.1.2 (i.e. 5.1.6 or earlier) to System Software Release 6.2.5, you must first update the BOOTmonitor and logic of your device:

- Update your software with the 6.1.2 BLUP (BinTec Large Update). This contains all the necessary files.
- When you have installed the BLUP, you can update to System Software Release 6.2.5 as described in your router manual.

Only a single updating operation is necessary when updating with the BLUP. You can download the necessary files and the instructions for updating the software at www.bintec.net.

1.1.1 Updating Modem Logic

If you want to use modem modules in a router of the **X4000 Family** or in **X8500** with System Software Release 6.2.5, you need to update the logic of the modem modules. You can download the necessary files for this from our Web server (www.bintec.de). How to update the modem logic is described in chapter 2.5, page 28.

2 New Features

2.1 Stateful Inspection Firewall

BinTec's Stateful Inspection Firewall (SIF) is a new security feature for System Software Release 6.2.5.

The SIF with dynamic packet filtering has a decisive advantage over static packet filtering: The decision to send a packet is not just based on the source and destination addresses or ports. In dynamic packet filtering, the *state* of the connection to a partner is checked. Packets are only forwarded if they belong to an active connection. The result of the check of the source and destination address, the service (protocol and port numbers) and the state of the connection must also be positive before packets are forwarded. Packets that cannot be assigned to an existing connection, e.g. Echo Requests (Pings), are therefore ignored.

The SIF also forwards packets that belong to an active "affiliated connection": The negotiation of an FTP connection takes place, for example, over port 21, but the actual data exchange can take place via a completely different port.

2.1.1 SIF and other Security Features

BinTec's Stateful Inspection Firewall fits into the existing security architecture of BinTec routers very well due to its simple configuration. Systems like Network Address Translation (NAT) and IP Access Lists (IPAL) require more configuration effort than the SIF.

As SIF, NAT and IPAL are active in the system simultaneously, attention must be given to possible interaction: If any packet is discarded by one of the security instances, this takes place immediately. This means it is irrelevant if this packet would be allowed by another instance. For this reason, you should accurately analyze your need for security features and then implement them in the most direct way.

The essential difference between SIF and NAT/IPAL is that the rules for the SIF are always applied globally, i.e. not restricted to one interface. Although interfaces can also be used similarly to the source and destination address as filter criteria in the configuration of the SIF, it is then no longer possible to differentiate further on the basis of the source and destination address of the packet as with NAT and IPAL.

In principle, however, the same filter criteria are applied to the data traffic:

- Source and destination address of the packet (if applicable, with associated netmask), plus filtering according to interfaces when using the SIF
- Service (preconfigured, e.g. ICMP, FTP, HTTP)
- Protocol
- Port number(s)

To illustrate the differences in packet filtering, a list of the individual security instances and their method of operation is given in the order in which they are carried out by the router. This order is based on an incoming packet at the router from outside.

NAT

One of the basic functions of NAT is the translation of the local IP addresses of your LAN into the global IP addresses you are assigned by your ISP and vice versa. All connections initiated externally are first blocked, i.e. every packet the router cannot assign to an existing connection is discarded. This means that a connection can only be set up from inside to outside. Without explicit permissions, NAT rejects every access from the WAN to the LAN.

SIF

NAT filtering is followed by filtering by the Stateful Inspection Firewall. As NAT prevents every access to the LAN from outside, permissions configured in the SIF are transferred to the NAT configuration. That is, you need not consider the connections desired from outside in the NAT configuration if you are planning an SIF configuration. The SIF sorts out all packets that are not explicitly permit-

ted. The result can be a "deny", in which case no error message is sent to the sender of the discarded packet, or a "reject", where the sender is informed of the rejection of the packet.

Incoming packets are processed as follows:

- The SIF first checks if an incoming packet can be assigned to an existing connection. If so, it is forwarded. If the packet cannot be assigned to an existing connection, a check is made to see if a suitable connection is expected (e.g. as affiliated connection of an existing connection). If so, the packet is also accepted.
- If the packet cannot be assigned to any existing or expected connection, the SIF filter rules are applied: If a deny rule matches the packet, the packet is discarded without sending an error message to the sender of the packet; if a reject rule matches, the packet is discarded and an ICMP Host Unreachable message sent to the sender of the packet. The packet is only forwarded if a pass rule matches.
- All packets without matching rules are discarded without sending an error message to the sender once all the existing rules have been checked.

IP Access Lists

Here packets are allowed or discarded on the basis of the criteria listed above, i.e. the state of the connection is usually not considered.

2.1.2 Configuration

An example of a basic configuration that nevertheless offers a high level of security is shown below:

- NAT is activated without further configuration on all interfaces with access to the WAN. This prevents all connections from the WAN to the LAN that have not been requested. NAT is also required for address translation.

- The SIF is configured so that all traffic to be allowed from outside is permitted by suitable rules. Undesired traffic from inside to outside can be prevented at the same time.
- Configuration of the IP Access Lists is not necessary in this case.

The menus in which you configure the SIF are described in the following chapters. Further information about NAT and IP Access Lists can be found in your router manual.

BinTec has equipped the SIF with user-friendly configuration, in which the rules can be clearly displayed and defined using definable aliases. Configuration is carried out in ***IP*** ➧ ***STATEFUL INSPECTION***.

The first menu window is shown below:

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

Stateful Inspection Filter List

Pos.     Source     Destination     Service     Action

  1      LAN_EN1    WAN_ISP         http        accept
  2      WAN_ISP    LAN_EN1         ftp         deny



           ADD          DELETE          SAVE          EXIT

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

All the filter rules configured are shown in the list in this menu window. The sequence of filter rules in the list is relevant: The rules are applied to each packet in succession until a rule matches. If overlapping occurs, i.e. more than one rule matches a packet, only the first rule is executed. This means that if the first rule denies a packet, whereas a later rule allows it, the packet is discarded. A deny rule also has no effect if the relevant packet has previously been allowed by another rule.

Adding Filter Rules

If you want to add a filter rule for the SIF or edit an existing rule, you can do this in the ***IP*** ➧ ***STATEFUL INSPECTION FIREWALL*** ➧ **ADD/EDIT** menu:

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

Source                      ANY
Destination                 ANY
Edit Addresses>

Service                     any
Edit Service>

Action                      accept

                SAVE                        CANCEL
```

The menu fields have the following meaning:

Field	Meaning
Source	Here you can select one of the preconfigured aliases for the source address of the packet. The router reads the list of existing WAN and LAN interfaces and offers these as default setting. You can create a new alias in ***IP*** ➧ ***STATEFUL INSPECTION FIREWALL*** ➧ **ADD/EDIT** ➧ ***EDIT ADDRESSES***.
Destination	Here you can select one of the preconfigured aliases for the destination address of the packet. The router reads the list of existing WAN and LAN interfaces and offers these as default setting. You can also create a new alias in ***IP*** ➧ ***STATEFUL INSPECTION FIREWALL*** ➧ **ADD/EDIT** ➧ ***EDIT ADDRESSES***.

Field	Meaning
Service	Here you can select one of the preconfigured services, to which the packet to be filtered must be assigned. The extensive range of services configured ex works includes the following: ■ *ftp* ■ *telnet* ■ *smtp* ■ *domain/udp* ■ *domain/tcp* ■ *http* ■ *nntp* ■ *netmeeting* You can configure further services in the ***IP*** ➧ ***STATEFUL INSPECTION FIREWALL*** ➧ **ADD/EDIT** ➧ ***EDIT SERVICES*** menu.
Action	Here you select the action to be applied to a filtered packet. Possible values are: ■ *accept* ■ *deny* ■ *reject* The packet is discarded for both *reject* and *deny*, but in the case of *deny* without sending an error message to the sender of the packet.

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

The preconfigured services under **Service** already cover the major applications. Three more complex default settings are also available:

- *any*
  A rule with this setting matches each packet that belongs to a connection with a certain address alias.
- *internet*
  This alias covers the following services: *dns*, *http*, *http (SSL)*, *smtp*, *pop3*, *pop3 (SSL)*, *nntp*,*nntp (SSL)* and *echo*. It is used mainly for simple protection of the usual Internet data traffic.
- *netmeeting*
  This alias covers all the settings necessary for using Microsoft NetMeeting.

Adding an Address Alias

If you want to configure another address alias or edit an existing one, you can do this in the ***IP*** ➧ ***STATEFUL INSPECTION FIREWALL*** ➧ **ADD/EDIT** ➧ ***EDIT ADDRESSES*** menu. The interfaces configured on the router are displayed:

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

Alias Address List

  Alias            IP Address         IP Mask             Interface

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

          ADD             DELETE            EXIT
```

All the configured aliases are listed in this window. Select **ADD** or an existing entry to enter the ***IP*** ➧ ***STATEFUL INSPECTION FIREWALL*** ➧ **ADD/EDIT** ➧ ***EDIT ADDRESSES*** ➧ **ADD/EDIT** menu.

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

Alias

Mode                interface

Interface           en1

                          SAVE                CANCEL
```

The **Interface** field is visible if you have selected *interface* for **Mode**.

If you have selected *address* under **Mode**, the **IP Address** and **IP Mask** fields are visible

The menu fields have the following meaning:

Field	Meaning
Alias	Here you enter a name for the alias you want to configure.
Mode	Here you indicate whether you want to designate an IP address (*address*) or an interface (*interface*) with the alias.
IP-Address	Only if you have selected *address* for **Mode**. Here you enter the IP address of the host to which the alias is to apply.
IP-Mask	Only if you have selected *address* for **Mode**. Here you enter the netmask belonging to the IP address of the host.

Field	Meaning
Interface	Only if you have selected *interface* for **Mode**. Here you select the interface over which the host's packets are to be received and sent. You can select from all configured WAN partners.

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

If an IP address is used for configuration of the address alias, **Interface** is set to *any* automatically; if an interface is entered, **IP-Address** and **IP-Mask** are shown as not used.

Adding a Service Alias

If you want to configure another service alias or edit an existing one, you can do this in the ***IP*** ➧ ***STATEFUL INSPECTION FIREWALL*** ➧ **ADD/EDIT** ➧ ***EDIT SERVICES*** menu.

A list of over 60 preconfigured service aliases is displayed:

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

Alias Service List

 Alias          Protocol      Port/Range     ICMP Type

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

     ADD               DELETE             EXIT
```

Select **ADD** or an existing entry to enter the ***IP*** ➧ ***STATEFUL INSPECTION FIREWALL*** ➧ **ADD/EDIT** ➧ ***EDIT SERVICES*** ➧ **ADD/EDIT** menu:

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

Alias

Protocol          icmp
ICMP Type         echo


                    SAVE                  CANCEL
```

The **ICMP Type** field is visible if you have selected *icmp* under **Protocol**.

If you have selected *tcp*, *udp* or *udp/tcp* under **Protocol**, the **Port** and **Range** fields are visible.

The menu fields have the following meaning:

Field	Meaning
Alias	Here you enter an alias for the service you want to configure.
Protocol	Here you select the protocol on which the service is based. You can select from 28 protocols.
ICMP Type	Only if you have selected *icmp* for **Mode**. This field is set to *echo* ex works. This setting covers the so-called pings.

Field	Meaning
Port	Only if you have selected *tcp*, *udp/tcp* or *udp* for **Protocol**. Here you enter the port over which the service runs, if applicable. Not all protocols are port-specific, in which case you do not need to enter a port.
Port Range	Only if you have selected *tcp*, *udp/tcp* or *udp* for **Protocol**. Here you enter the number of ports the service uses. Possible values are *1* to *65535*. If you do not enter a value, the router assumes the value *1* as default.

Table 2-3: ***IP*** ➧ ***STATEFUL INSPECTION FIREWALL*** ➧ **ADD/EDIT** ➧ ***EDIT SERVICES*** ➧ **ADD/EDIT**

Syslog Messages

A syslog entry is generated if one of the configured rules matches a packet and the action then executed is either *deny* or *reject*. There are two levels of detail for the entries, *info* and *debug*.

The logged details differ as follows:

- *info*
  Only the source and destination alias and the service alias of the discarded packet are indicated at this level.
- *debug*
  The source and destination IP address and the port of the discarded packet are indicated at this level.

The syslog messages are generated as configured in the ***SYSTEM*** menu.

SIF Reject Table

An entry is created in the **ipSifAliasRejectTable** for each connection rejected by the SIF. This is not accessible via the Setup Tool. The entries can be used as the basis for analysis of possible attacks.

The **ipSifAliasRejectTable** contains the following variables:

Variable	Meaning
Index	The index number of the entry, which is issued automatically.
Source	The source IP address of the discarded packet.
Destination	The destination IP address of the discarded packet.
Rejects	Number of discarded packets for this connection.
Silence	Time in seconds during which no packets are discarded.
PortLo	Lowest port to which discarded packets have been sent.
PortHigh	Highest port to which discarded packets have been sent.

Table 2-4: **ipSifAliasRejectTable**

The entries in the **ipSifAliasRejectTable** are not static: If no packet is discarded for 3,600 seconds, the entries are generated as syslog message and then deleted from the table.

2.2 IPSec Callback

To enable hosts without fixed IP addresses to obtain a secure connection over the Internet, BinTec has supported the DynDNS service since Release 6.2.2. This service enables a peer to be identified using a host name. It is not necessary to configure the IP address of the peer.

The DynDNS service does not signal that the peer is actually online and cannot cause a peer to set up an Internet connection to enable an IPSec tunnel over the Internet. This possibility is created with the IPSec Callback: Using a direct ISDN call to a peer, you can signal that you are online and waiting for the peer to set up an IPSec tunnel over the Internet. If the called peer currently has no connection to the Internet, the ISDN call causes a connection to be set up. This ISDN call is free of charge, as it does not have to be accepted by the router. The identification of the caller from his ISDN number is sufficient information to initiate setting up an ISDN tunnel.

Before you can configure this service, you must first configure a number for the IPSec Callback service in the ***WAN*** ➧ ***INCOMING CALL ANSWERING*** menu. The new value *IPSec* is available for this purpose in the **Item** field. This entry ensures that incoming calls for this number are routed to the IPSec service.

The rest of the configuration is carried out in the ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** menu. This menu contains the new **ISDN Callback** field. This field can have the following values:

Possible Values	Meaning
disabled	ISDN Callback is deactivated. The router neither reacts to incoming ISDN calls from this peer nor initiates ISDN calls to this peer.
passive	The router reacts only to incoming ISDN calls and, if necessary, initiates setting up an IPSec tunnel to the peer. No ISDN calls are sent to the peer to cause the peer to set up an IPSec tunnel.

Possible Values	Meaning
active	The router sends an ISDN call to the peer to cause the peer to set up an IPSec tunnel. The router does not react to incoming ISDN calls.
both	The router reacts to incoming ISDN calls and sends ISDN calls to the peer. The setting up of an IPSec tunnel is executed (after an incoming ISDN call) and initiated (by an outgoing ISDN call).

Table 2-5: **ISDN Callback**

Depending on the value you enter, the menu changes again and allows you to enter the ISDN numbers for incoming and outgoing ISDN calls for the **IN** and **OUT** fields. If you have selected *both* for **ISDN Callback**, you must enter a number for incoming ISDN calls and a number for the router to dial to cause the peer to set up an IPSec tunnel.

Note that the number of the distant router is always entered here, i.e. the number entered for the IN field is the number from which the peer calls your router (calling party number), and the number entered for the OUT field is the number under which your router calls the peer (called party number).

In general, the two numbers will be identical. It may be necessary under certain circumstances to enter different numbers. Ask the system administrator for the numbers to be configured.

The following ***IPSec*** ➧ ***Configure Peers*** ➧ **ADD/EDIT** menu appears if you activate callback in both directions:

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

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



                            SAVE              CANCEL
```

If you have configured callback for a peer, this will always be executed. If callback is active, the peer is therefore caused to initiate setting up an IPSec tunnel by an ISDN call as soon as this tunnel is required. If callback is set to passive, setting up a tunnel to the peer is always initiated if an ISDN call is received on the relevant number. This ensures that both peers are reachable and that the connection can be set up over the Internet. The only case in which callback is not executed is if SAs (Security Associations) already exist, i.e. the tunnel to the peer already exists.

2.2.1 IPSec Heartbeat

BinTec has implemented an IPSec Heartbeat to be able to determine whether or not an SA is still valid. This function sends and receives signals according to the configuration. If these signals are not received, the SA is discarded as invalid. The packets the router sends and receives due to this signaling are not counted as IPSec packets, i.e. an SA does not remain active solely because a heartbeat is sent or received.

The heartbeat is configured in two of the IPSec menus:

- The default parameters are set in ***IPSec*** ➧ ***Advanced Settings*** ➧ ***Heartbeat***.
- Certain default parameters for individual peers can be modified in ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT**.

The ***IPSec*** ➧ ***Advanced Settings*** ➧ ***Heartbeat*** menu contains the following fields:

Field	Meaning
Heartbeat	Here you determine how the router handles heartbeats. Possible values: ■ *none*: The router sends and expects no heartbeat; the heartbeat function is not available. ■ *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.
Interval	Here you enter the intervals at which the router sends and expects heartbeats. This value is given in seconds.
Tolerance	Here you enter how many heartbeats are allowed to be missing before an SA is discarded.

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

The type of heartbeat for the respective peer can be modified in the ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT** menu. This menu contains only the

Heartbeat field with the values described above, plus the *default* value. In this setting, the router uses the settings for the peer that have been configured in the ***IPSec*** ➧ ***Advanced Settings*** ➧ ***Heartbeat*** menu.

2.3 PPTP Passthrough

The operation of the advanced GRE protocol (Generic Routing Encapsulation) used for PPTP connections is not port-specific, i.e the PPTP connections of different hosts initially cannot be separated from each other in NAT (Network Address Translation). Packets received as answer to a request from the LAN therefore cannot be assigned to a certain destination host.

To allow several PPTP endpoints (hosts) a connection to a VPN server over one router, BinTec has implemented a PPTP Passthrough in addition to NAT. GRE context numbers are assigned here in a similar way to NAT port mapping: The router assigns an external GRE context number to the internal GRE context number of a packet coming from the LAN, which enables it to assign GRE packets coming from the WAN to a certain PPTP connection. The assigned GRE context number is released again when the GRE connection is cleared.

This procedure is functional only for outgoing connections, i.e. it is still only possible to set up a single PPTP connection from outside to inside. The assignment to a host in the LAN is made via the NAT configuration, as the router still cannot assign the external GRE context number to an internal number for incoming PPTP packets. Only the external IP address is translated to an internal address.

Note that NAT must be appropriately configured to accept incoming connections. This also applies to incoming PPTP connections.

PPTP Passthrough is enabled or disabled in the ***IP*** ➧ ***Network Address Translation*** ➧ **EDIT** menu: You can select either *yes* or *no* for the **PPTP Passthrough** field. Like NAT itself, the use of PPTP Passthrough is interface-specific.

2.4 Bundling of PRI Hyperchannels

Previously the channels of an S_{2M} connection could only be bundled with PPP Multilink on Layer 2. BinTec has added a facility for bundling channels on the Physical Layer. In addition, PPP Multilink channel bundles can now be freely configured, i.e. the available timeslots can be combined into several PPP Multilink channel bundles. Previously only one channel bundle was possible with all timeslots.

For channel bundle configuration, it is necessary in the PRI interface menu to set **ISDN Switch Type** to*leased line, chan. B1..B31*. This provides access to the new submenu ***BUNDLE CONFIGURATION***. The first window shows a list of the channel bundles already configured.

Timeslots divide the available 2-Mbps bandwidth of an S_{2M} connection into logical channels. No distinction is made below between timeslots and channels, as the difference is immaterial for configuration purposes.

The following menu appears if, for example, you have not defined any physical channel bundles, but have combined all channels in PPP Multilink bundles (example shows the menu of an X4E-2PRI expansion card):

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

 Type   Name       Timeslots                                     Channels
 PPP    bundle4    01 - 31                                       31




                    DELETE              EXIT
```

The overview window contains the following fields:

Field	Meaning
Type	Shows the type of channel bundle. Possible values are: ■ *PPP*: The channels are bundled as PPP Multilink channels. ■ *Physical*: The channels are bundled as physical hyperchannels.
Name	Shows the name assigned to this channel bundle.
Timeslots	Shows the logical channels (timeslots) combined to form this channel bundle.
Channels	Shows the number of bundled channels.

Table 2-7: ***BUNDLE CONFIGURATION***

Select an existing entry or **ADD** to pass to the ***BUNDLE CONFIGURATION*** ➧ **ADD/EDIT** submenu. Here you can figure the desired channel bundle.

The following menu appears if you have defined no physical channel bundles, but have combined all channels into one PPP Multilink bundle:

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


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

  Used 31 Timeslots:

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

  X.75 Layer 2 Mode       DTE
  Bundle Id               1

                 SAVE                              CANCEL
```

The menu contains the following fields:

Field	Meaning
Bundle Type	Here you define the type of channel bundle. Possible values are: ■ *PPP Multilink* ■ *Physical (Hyperchannel)*
Interface Name	Shows the name of the interface that is created in the ***WAN PARTNER*** menu due to the channel bundle. This value is set automatically.

Field	Meaning
From Timeslot	Shows the first of the channels used for this channel bundle. If you select a configuration that uses unconnected channels, the first channel used is shown together with the comment *customized*, e.g. ***6 customized***. If you wish to select a certain "start channel", you can do this here.
To Timeslot	Shows the last of the channels used for this channel bundle. If you select a configuration that uses unconnected channels, the last channel used is shown together with the comment *customized*, e.g. ***31 customized***. If you wish to select a certain "stop channel", you can do this here.
Used x Timeslots	Shows the total number of channels used and a list of the individual channels that have been used. If you do not wish to use all the channels between a certain start and stop channel for a channel bundle, you can make a selective assignment here.
X.75 Layer 2 Mode	Here you define how the interface created by this channel bundle is to behave during connection setup. Possible values: ■ *dte* ■ *dce*

Field	Meaning
Bundle Id	Here you assign the channel bundle a unique ID number. Possible values are *1* to *255*. The number of the first channel used is taken as the default value.

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

In principle, there are no limitations on the configuration of the channel bundle (whether PPP Multilink or physical bundle) as far as the breakdown of the channels is concerned: It is possible to configure many small channel bundles as well as different types (PPP Multilink or physical bundle).

2.5 Modem Update

With System Software Release 6.2.5 it is possible to update the firmware of the modem resource modules (XTR-S, XTR-M, XTR-2M, XTR-L) of **X4000 Family** and **X8500** devices.

You can download the latest logic files from the download section of your router at www.bintec.net. You need the following files:

- For **X4000 Family**
  - (The names of the files are not yet fixed)
- For **X8500**
  - (The names of the files are not yet fixed)

To update firmware, log in to your router. The update procedure is explained in the chapter "Updating Software" in your manual. The following syntax is to be used:

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

The new modem logic is ready for operation as soon as you have installed it. It is not necessary to restart the router.

3 Changes

Under preparation.

4 Bugfixes

Under preparation.

5 Known Issues

The following problems are known to exist under System Software Release 6.2.5:

- H.323 and Stateful Inspection Firewall
- TFTP Operations with Configuration Files

5.1 H.323 and Stateful Inspection Firewall

As of now it is not possible to operate the H.323 implementation and the Stateful Inspection Firewall (SIF) simultaneously.

5.2 TFTP Operations with Configuration Files

System Software Release 6.2.5 allows integrating banners longer than one line into the setup tool. This, however, leads to the problem that configuration files containing such banners cannot be reloaded into the router via TFTP.