Release Notes
System-Software
Release 6.2.2
X-Generation

July 2002

System-Software Release 6.2.2

This document describes new features, changes, bugfixes and known bugs in System-Software Release 6.2.2.

1 Important Information

Note that configurations you create with System-Software Release 6.2.2 are not downward compatible! Before updating to System-Software Release 6.2.2, you should save your old configuration so that you can load Release 6.1 again in case a "rollback" is necessary.

Instructions on saving and reloading a configuration with the Setup Tool can be found in the chapter "Configuration Management" in your router manual.

If you implement IPSec configurations with System-Software Release 6.2.2, note that the remote station to which you want to set up a tunnel must also run with System-Software Release 6.2.2, if this is a BinTec device.

2 Updating the System Software

- ➤ Download System-Software Release 6.2.2 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 6.2.2, you must update the BOOT-monitor and logic of your device:

You can initially 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 6.2.2 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.

3 New Features

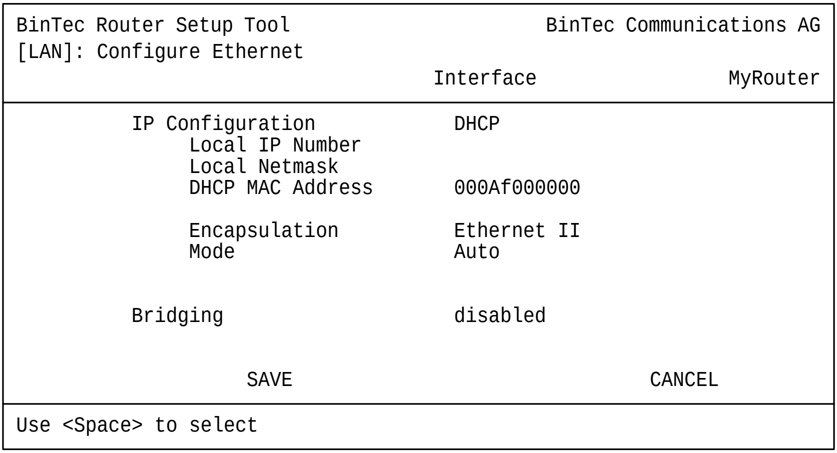
BinTec has extended the scope of features for X-Generation routers by adding the following features since Software Release 6.1:

- DHCP Client (chapter 3.1, page 10)
- H.323 (chapter 3.2, page 11)
- New BinTec IPSec Version (chapter 3.3, page 11)
- XoT – X.25 over TCP/IP (chapter 3.4, page 12)
- Dynamic DNS (chapter 3.5, page 15)
- Dynamic VPN (PPPT) (chapter 3.6, page 20)
- Dynamic IPSec (chapter 3.7, page 23)
- MPPC and STAC Hardware Compression (chapter 3.8, page 24)
- BAP/BACP: Channel Bundling with Group Numbers (chapter 3.9, page 25)
- V.120 (chapter 3.10, page 28)
- Multi-NAT (chapter 3.11, page 28)
- Configurable ICMP Behavior (chapter 3.12, page 34)
- Disabling RIP and OSPF (chapter 3.13, page 35)
- Automatic Cable Detection at X.21 Interfaces (chapter 3.14, page 36)
- Weekly Schedule (chapter 3.15, page 41)
- CAPI Supplementary Services (chapter 3.16, page 42)

3.1 DHCP Client

From System-Software Release 6.2.2 onwards, the IP configuration of an Ethernet interface can also be obtained dynamically from a DHCP server and not just set up manually.

This setting can be made for any Ethernet interface. If you select the value *DHCP* in the ***IP CONFIGURATION*** field of a menu for configuration of an Ethernet interface, the menu changes e.g. as follows:



```
BinTec Router Setup Tool                       BinTec Communications AG
[LAN]: Configure Ethernet
                                    Interface                  MyRouter

           IP Configuration            DHCP
                Local IP Number
                Local Netmask
                DHCP MAC Address       000Af000000

                Encapsulation          Ethernet II
                Mode                   Auto


           Bridging                    disabled


                     SAVE                                CANCEL

Use <Space> to select
```

Although the fields for the local IP address and netmask are still visible, you cannot make any more changes here.

DHCP MAC Address appears as a new field. Here you enter the MAC address of the Ethernet interface you are currently configuring. Your router can be uniquely identified in the LAN using the MAC address, even if it has not yet been assigned an IP address. You do not generally need to make an entry here, the router uses the MAC address "burnt into" the hardware.

Some providers use hardware-independent MAC addresses to assign their clients IP addresses dynamically. If your provider has assigned you a MAC address, enter this in the relevant field. A description of the configuration for connecting to the Internet in this case (e.g. use of Ethernet or IPoA) can be found in the **Basic Configuration** manual.

Depending on the router type or the expansion cards equipped in the router, this option can be relevant in different menus, e.g. in the ***ATM*** ➧ ***IPoA*** or ***Ethernet (PPPoE,...)*** ➧ ***IP*** menu of **X2300i**, the ***CM-10BT*** menu of **X1200** or the ***X4E-100BT, Fast Ethernet*** menu of an Ethernet expansion card for **X4000**.

3.2 H.323

System-Software Release 6.2.2 for the first time offers implementation of the H.323 protocol, thus allowing a large number of "Voice over IP" (VoIP) applications. The software implemented is currently divided into an H.323 proxy and a gatekeeper. These permit support such as for IP telephones or complete VoIP systems.

A detailed description of the H.323 functions can be found in chapter "H.323" of the Software Reference, which you can download from our Web server (www.bintec.net).

3.3 New BinTec IPSec Version

The BinTec IPSec solution is now available in version 2.1.1. This implementation involves extensive changes. The changes and additions made can be obtained from chapter "IPSec" in the Software Reference, which you can download from our Web server (www.bintec.net). An advance version of this chapter is available there at the same time as the IPSec software; the new documentation will be complete by the end of July.

The major new features are:

- Simple basic configuration with the help of a wizard

- Dynamic IPSec – IPSec with dynamic IP addresses (see chapter 3.7, page 23)
- Integration of new encryption algorithms (Twofish and Rijndael/AES) and new hash algorithms (RipeMD 160 and Tiger 192)
- Peer-specific configuration of IKE and IPSec

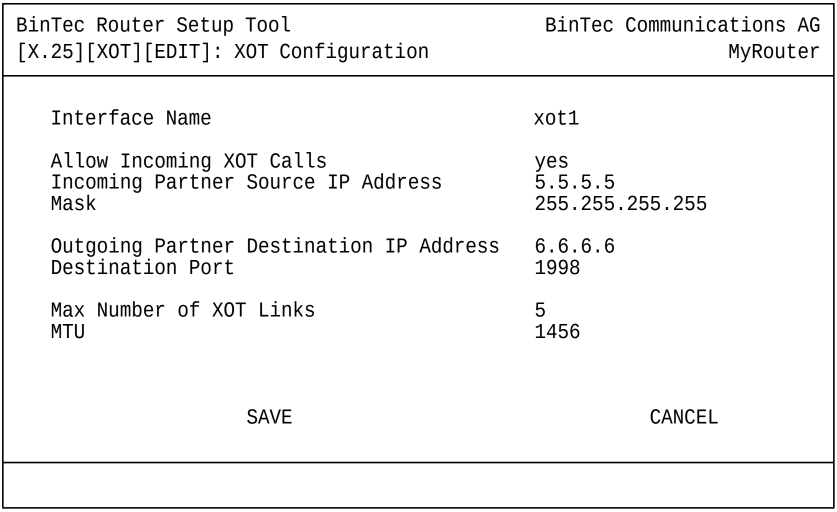
3.4 XoT – X.25 over TCP/IP

XoT makes it possible to send X.25 packets over an IP network. This is done by "wrapping" X.25 packets in TCP packets and then sending them over an IP network.

> XoT is not available on the following routers:
>
> - **X1000**
> - **X1200**
> - **X3200**

The port at which the router accepts XoT connections must be defined first in the configuration. The default port for this is 1998, but the BinTec implementation allows a free choice of port to support individual configurations. The port is defined in the **XOT TCP Port** field of ***X.25*** ➧ ***STATIC SETTINGS***. All packets arriving at this port are forwarded to the XoT service which processes them according to the configuration of the interfaces.

The major parameters are configured in the ***X.25*** ➧ ***XoT*** ➧ **ADD/EDIT** menu:



```
BinTec Router Setup Tool                            BinTec Communications AG
[X.25][XOT][EDIT]: XOT Configuration                                MyRouter

   Interface Name                              xot1

   Allow Incoming XOT Calls                    yes
   Incoming Partner Source IP Address          5.5.5.5
   Mask                                        255.255.255.255

   Outgoing Partner Destination IP Address     6.6.6.6
   Destination Port                            1998

   Max Number of XOT Links                     5
   MTU                                         1456


                    SAVE                                   CANCEL
```

The menu contains the following fields:

Field	Meaning
Interface Name	Here you enter any desired name (max. 25 characters) for the XoT interface.
Allow Incoming XOT Calls	Defines whether or not incoming XoT connections are permitted. Possible values: ■ *yes*: Incoming XoT packets are accepted at this interface. ■ *no*: Incoming XoT connections are not accepted at this interface (but outgoing connections can be set up).

Field	Meaning
Incoming Partner Source IP Address	Defines the IP address of the XoT partner that is sending XoT packets. This field is only visible if you have allowed incoming XoT connections at this interface. If you enter *0.0.0.0* as IP address, connections are accepted from any IP addresses.
Mask	The netmask belonging to the IP address (**Incoming Partner Source IP Address**). This field is only visible if you have allowed incoming XoT connections at this interface. You have the option of entering no IP address, but defining a netmask. Connections are then accepted from all IP addresses fitting this netmask.
Outgoing Partner Destination IP Address	Here you enter the IP address of the XoT partner to whom XoT packets are to be sent.
Destination Port	Defines the port to which the XoT packets are sent. Make sure the recipient of the packet actually accepts XoT packets at this port.
Max Number of XOT Links	Defines the maximum number of incoming and outgoing XoT connections to this XoT partner.
MTU	The Maximum Transfer Unit defines the maximum size of the packets to be sent (in bits). Possible values: *576* to *8180*.

Table 3-1: ***X.25*** ➧ ***XOT*** ➧ **ADD/EDIT**

To ensure that incoming and outgoing XoT packets can be forwarded, a suitable route must be created in the ***X.25*** ➧ ***ROUTING*** menu. Configuration of the X.25-specific parameters of the XoT interface in the ***X.25*** ➧ ***LINK CONFIGURATION*** menu is also recommended.

Information about configuration of an X.25 route and settings in the ***LINK CONFIGURATION*** menu can be found in chapter "X.25" in the Software Reference. You can download the Software Reference at www.bintec.net.

3.5 Dynamic DNS

The disadvantage of using dynamic IP addresses is that a host in the network can no longer be found once its IP address has changed. Dynamic DNS ensures that your router can still be reached after changing the IP address.

DynDNS is intended exclusively for use at interfaces that are assigned a dynamic IP address. Static IP addresses are not propagated.

The following configuration steps are necessary:

- Registration of a host name at a DynDNS provider
- Configuration of the router

Registration

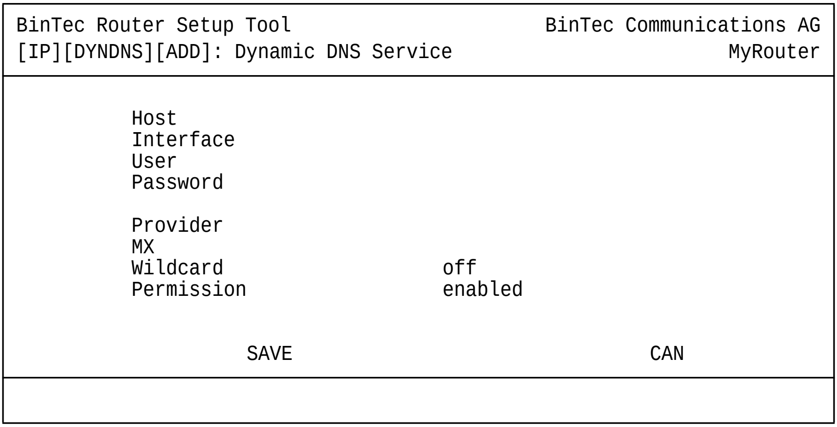
The registration of a host name means that you define an individual user name for the DynDNS service, e.g. ***dyn_client***. The service providers offer various domain names for this, so that a unique host name results for your router, e.g. ***dyn_client.provider.com***. The DynDNS provider relieves you of the task of answering DNS requests concerning the host ***dyn_client. provider.com*** with the dynamic IP address of your router.

To ensure that the provider always knows the current IP address of your router, the router contacts the provider as soon as a new connection is established and propagates its present IP address. System-Software Release 6.2.2 enables you to use this service.

Configuration of the Router

The configuration is set up in ***IP*** ➧ ***DynDNS***. The first menu window contains a list of the DynDNS services already configured. This window also offers you access to the submenus ***IP*** ➧ ***DynDNS*** ➧ **ADD/EDIT** and ***IP*** ➧ ***DynDNS*** ➧ ***DynDNS Provider List***.

The **ADD/EDIT** menu is shown below:



```
BinTec Router Setup Tool                       BinTec Communications AG
[IP][DYNDNS][ADD]: Dynamic DNS Service                         MyRouter


          Host
          Interface
          User
          Password

          Provider
          MX
          Wildcard                   off
          Permission                 enabled


                    SAVE                                CAN

```

This menu is for configuring a DynDNS service. The fields have the following meaning:

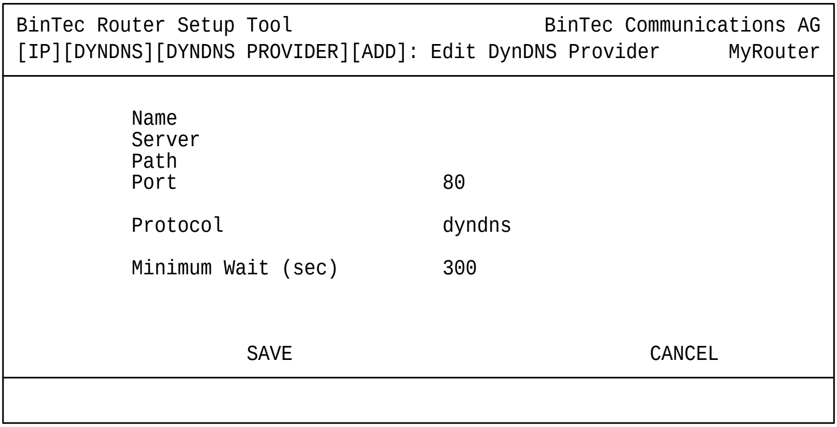
Field	Meaning
Host	Here you enter your full host name for this service, e.g. ***dyn_client.provider.com***.
Interface	Defines the WAN interface whose IP address is to be propagated over the DynDNS service (generally the interface of the Internet Service Provider).
User	Defines the user name with which you log in to your DynDNS provider.

Field	Meaning
Password	Here you enter the password you use for authentication with your DynDNS provider.
Provider	Defines one of the preconfigured providers. Six services are already available in the unconfigured state and their protocols are supported. You can enter and configure more providers in the ***IP*** ➔ ***DynDNS*** ➔ ***Edit DynDNS Provider*** menu.
MX	Defines another host name to which e-mails are forwarded if the host currently configured is not to receive mail. Ask your provider about this service and make sure that the host you have entered is able to receive e-mails.
Wildcard	Here you can enable additional DNS name resolution within your network, but this requires a DNS server in your network. Possible values are: ■ *on*: Additional name resolution is enabled. ■ *off*: Additional name resolution is disabled.
Permission	Here you can enable or disable the DynDNS service just configured. Possible values are: ■ *enabled* ■ *disabled*

Table 3-2: ***IP*** ➔ ***DynDNS*** ➔ **ADD/EDIT**

You can configure and edit more DynDNS providers in the ***IP*** ➔ ***DynDNS*** ➔ ***DynDNS Provider List*** menu. You cannot edit or delete the default providers (*dyndns*, *stat dyndns*, *ods*, *hn*, *dyns* and *orgdns*).

The menu for adding and editing entries is shown below:



```
BinTec Router Setup Tool                      BinTec Communications AG
[IP][DYNDNS][DYNDNS PROVIDER][ADD]: Edit DynDNS Provider      MyRouter

          Name
          Server
          Path
          Port                        80

          Protocol                    dyndns

          Minimum Wait (sec)          300


                    SAVE                                CANCEL

```

In principle, you can enter any DynDNS provider, but as many providers have developed proprietary protocols for handling the service, you must ensure that the provider you have selected uses one of the protocols supported by BinTec (see table 3-3, page 19).

The **ADD/EDIT** menu has the following fields:

Field	Meaning
Name	Here you can give the provider any name you like.
Server	Here you enter the IP address or the (resolvable) host name of the server on which the provider's DynDNS service is running.
Path	Here you enter the path on the provider's server that contains the script for updating the IP address of your router. Ask your provider about the path to be used.

Field	Meaning
Port	Here you enter the port at which your router is to reach your provider's server. Ask your provider for the relevant port.
Protocol	Here you select one of the protocols implemented. The following are available: – *dyndns* (www.dyndns.org) – *static dyndns* (www.dyndns.org) – *ods* (http://www.ods.org) – *hn* (http://hn.org) – *dyns* (http://dyns.cx) – *GnuDIP HTML* (http://gnudip2.sourceforge.net) – *GnuDIP TCP* (http://gnudip2.sourceforge.net)
Minimum Wait	Here you enter the minimum time (in seconds) that the router must wait before it is allowed to propagate its current IP address to the DynDNS provider again. The default value is set to 300 seconds.

Table 3-3: ***IP*** ➧ ***DynDNS*** ➧ ***Edit DynDNS provider*** ➧ **ADD/EDIT**

GnuDIP is a protocol that supports the GnuDIP server, which is available as freeware. This protocol enables a separate DynDNS service to be offered.

Note that you should set a relatively long short hold (approx. 120 seconds) for the interface over which the DynDNS connections are to be implemented, as updating the IP address at the DynDNS provider may take a relatively long time. If the short hold acts and the connection is ended before the IP address could be successfully updated at the provider, the DynDNS service on your router may not work.

If you set up connections to the Internet over a flat-rate connection, you have other options for adapting the short hold to your needs. You will find information about this in your router manual under the keyword "short hold".

DynDNS therefore enables hosts with dynamic IP addresses to set up a peer-to-peer connection, e.g. over the Internet. This is vitally important in PPTP/VPN scenarios in which the responder or both peers only have dynamic IP addresses. It has not yet been possible to set up the VPN tunnel under these circumstances, because the address of one of the tunnel endpoints was not known.

Now it is no longer just possible for a branch office with a dynamic IP address to log in to the head office, but the head office can also reach the branch office (also by callback). Branch offices can also set up PPTP tunnels to the head office or to each other and safely exchange sensitive data.

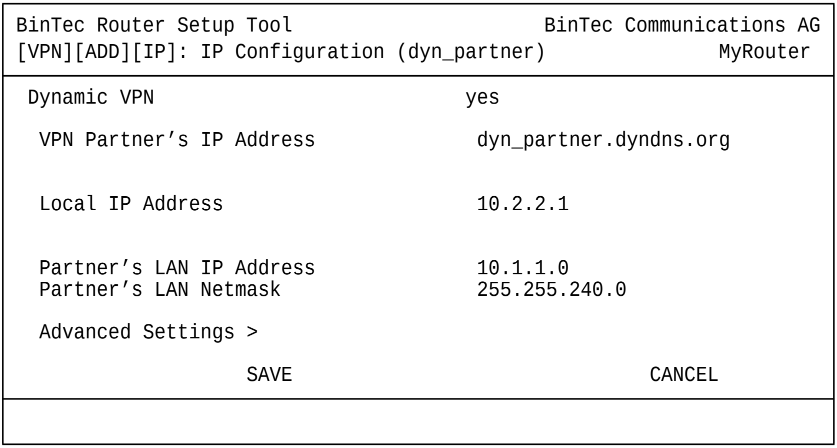
3.6 DynVPN (PPTP)

DynVPN makes it possible to implement PPTP VPNs even if the two participants only have dynamic IP addresses or the role of the initiator is not defined. If only one of the two partners has a dynamic IP address, this partner always had to initiate setting up the VPN tunnel. If permanent "role casting" is not possible, a way must be found how the two partners can "find" each other in the network without in advance knowing the IP address of the other partner (if both partners have dynamic IP addresses, this is absolutely essential).

DynDNS offers the possibility of propagating a one’s own dynamic IP address e.g. in the Internet and so being identifiable via a certain host name. It is important here that each participant that may have to be reachable by another participant has already configured DynDNS.

The configuration of a VPN partner to be reached via a DynDNS host name does not differ fundamentally from the configuration of a VPN partner with a fixed IP address. A number of options to enable dynamic VPNs have been added to the ***VPN*** ➧ ***IP*** menu.

The menu for an already configured VPN partner is shown below:



```
BinTec Router Setup Tool                      BinTec Communications AG
[VPN][ADD][IP]: IP Configuration (dyn_partner)                MyRouter

 Dynamic VPN                            yes

  VPN Partner’s IP Address               dyn_partner.dyndns.org


  Local IP Address                       10.2.2.1


  Partner’s LAN IP Address               10.1.1.0
  Partner’s LAN Netmask                  255.255.240.0

  Advanced Settings >

                  SAVE                                  CANCEL
```

Field	Meaning
Dynamic VPN	Here you enable or disable the DynDNS service for this VPN partner.

Field	Meaning
VPN Partner’s IP Address	Defines the host name of the VPN partner under which this partner is registered at his DynDNS provider in the case of a dynamic VPN.
Local IP Address	Defines the local IP address of the virtual VPN interface you are currently configuring. This is a freely selectable IP address of the private address range.
Partner’s LAN IP Address	Defines the local IP address of the LAN beyond the VPN tunnel.
Partner’s LAN Netmask	Defines the netmask belonging to the **Partner’s LAN IP Address**.

Table 3-4: ***VPN*** ➧ **ADD/EDIT** ➧ ***IP***

If your router displays a warning that the host name cannot be resolved when you enter the host name in the **VPN Partner’s IP Address** field, you have either not yet configured the DynDNS host name of the partner or your router cannot access the Internet to resolve the host name at the DynDNS provider.

Configure the DynDNS service before you set up a dynamic VPN.

If you want to configure a scenario in which two partners who are not permanently online can reach each other, you can also activate the option *yes (callback via VPN)* for the **Callback** field in the ***VPN*** ➧ **ADD/EDIT** ➧ ***ADVANCED SETTINGS*** menu. One partner can then initiate the setup of a VPN tunnel over the Internet by making an ISDN call to the other partner, even if this partner is momentarily not online. The router recognizes the waiting partner from his telephone number and (depending on the configuration of the routing, but generally over the Internet) sets up a VPN tunnel to the IP address propagated by the DynDNS service. The authentication of the VPN partner is the same as for a static VPN and uses the PPP authentication configured in ***VPN*** ➧ **ADD/EDIT** ➧ ***PPP***.

Enter the WAN numbers, which the router must know for callback purposes, in the ***VPN*** ➧ ***WAN NUMBERS*** menu (this menu only appears if callback is activated). This corresponds to the ***WAN PARTNER*** ➧ **ADD/EDIT** ➧ ***WAN NUMBERS*** menu. Further information about the WAN numbers can be found in your router manual.

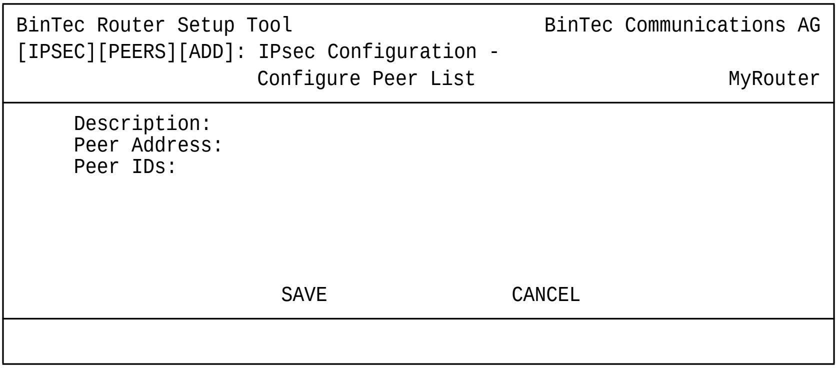
Note that for a callback you must activate the relevant option on the routers of both partners.

3.7 Dynamic IPSec

The security of IPSec data traffic has been subject to the same limitations as for PPTP VPNs until now: If only one of the peers had a dynamic IP address, this peer had to initiate setting up the IPSec tunnel. IPSec was not possible at all with dynamic IP addresses at both ends.

System-Software Release 6.2.2 makes it possible to also use the DynDNS service described above for IPSec. It is necessary to configure a corresponding DynDNS service for this (see chapter 3.5, page 15) and enter the host name under which the peer is registered with the DynDNS service instead of an IP address for the peer configuration. As soon as the peer's router has propagated its current IP address, your own router can resolve this host name and thus also initiate a connection to a peer with a dynamic IP address.

Entering the host name instead of an IP address in the peer configuration is carried out in the ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT** menu:



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

     Description:
     Peer Address:
     Peer IDs:




                        SAVE                    CANCEL

```

You can now enter the DynDNS host name instead of an IP address in the **Peer Address** field.

Note that phase 1 authentication with *preshared_keys* in *id_protect* mode is also not possible when using the DynDNS service in IPSec.

No more configuration steps are necessary in the ***IPSec*** menu.

3.8 MPPC and STAC Hardware Compression

BinTec's System-Software Release 6.2.2 supports MPPC, MS-STAC and STAC compression on all resource modules that are equipped with an appropriate HiFn chip (XTR-Enc and XTR-VPN).

3.9 BAP/BACP: Channel Bundling with Group Numbers

From System-Software Release 6.2.2 onwards, channel bundling can be provided by an ISP even if this provider distributes the incoming calls to several routers: A certain ISDN number is conveyed to the client when he dials in and requests another B-channel. This is assigned individually for each router at the central site, so that the calls of several channels over this number are actually terminated on the same router. The additional B-channel is set up by a type of callback: The client requests another B-channel. The central site then requests a call to the individual number of the router to which the client is already connected at this moment.

> The client is the active subscriber in this scenario, i.e. he is in control and responsible for the channel bundling costs. The central site accepts all requests from the client, as long as these agree with the WAN partner configuration of the router.

The following new parameters have been introduced:

- the MIB table **pppDialProfile**
- the values *bap_client* and *bap_server* for the variable **BodMode** in **pppExtIfTable**

Configuration of pppDialProfileTable

The configuration of the parameters contained in this table is only necessary on the server side and is not integrated in the Setup Tool. Configuration must be carried out in the SNMP shell.

The **pppDialProfileTable** contains the following variables:

Variable	Bedeutung
Index	The value is automatically created and used to designate the dialout profile you are about to configure.
Descr	Here you enter a description for the dialout profile.
BapNumber	Here you enter the phone number the client must use for the required callback.
BapSubAddress	Here you define the BAP subaddress to be used for a BAP call response or a BAP call request.
BapLkType	Here you define the link type to be used for a BAP call response or a BAP call request.
StkMask	Here you define the ISDN stack mask. A value of *0* disables dialup completely, a value of *-1* allows dialup over any available ISDN stack.
CallbackL1Prot	Here you define the layer 1 protocol to be used for the callback. *Initial (1)* means that the layer 1 protocol of the initial call is used.

Table 3-5: **pppDialProfileTable**

The following settings are necessary for configuration of this service on the central site:

- Settings in the **pppDialProfileTable**:
  Certain values must be assigned to the two variables **BapNumber** and **BapLkType** in this table:
  - For **BapNumber**, you must enter a number that is assigned to this router only. This is conveyed to the client for "callback" purposes.
  - The value for **BapLkType** must be set to *isdn*.

- The values of the other variables depend on the environment at the central site.

Configuration of **pppExtIfTable**

The variable **pppExtIfBodMode** must be configured on both, the server and client. This can be done in the Setup Tool. The variable **pppExtIfDialProfileIndex** must be configured on the server.

- Server settings:
  - The variable **pppExtIfBodMode** in the **pppExtIfTable** must be set to *bap_server*. You can set the value for the corresponding WAN partner in the Setup Tool. This is done in the menu ***WAN Partner*** ➡ **ADD/EDIT** ➡ ***Advanced Settings*** ➡ ***Extended Interface Settings (optional)*** using the setting **Mode** = *BAP, Dialup Server Mode*. Alternatively, you can set the value via the SNMP shell.
  - The value of the variable **pppExtIfDialProfileIndex** must be the index number of the entry in the **pppDialProfileTable** whose settings are to be used. You cannot set this value in the Setup Tool.
- Client settings:
  The variable **pppExtIfBodMode** in the **pppExtIfTable** must be set to *bap_client*.
  This is done in the ***WAN Partner*** ➡ **ADD/EDIT** ➡ ***Advanced Settings*** ➡ ***Extended InterFace Settings (optional)*** menu by setting the value of the **Mode** field to *BAP, Dialup Client Mode*.

Channel bundling must be activated at both ends as described in your router manual (***WAN Partner*** ➡ **ADD/EDIT** ➡ ***Advanced Settings***, **Channel Bundling** = *dynamic* or *static*, **Total Number of Channels** *>1*).

If dialin authentication is via a RADIUS server, the BinTec-specific attributes must be used for RADIUS server configuration. There must be an entry in the Users file which creates the necessary entries in the **pppExtIfTable**.

3.10 V.120

V.120 is used for dialing in to a router with a mobile phone. HSCSD is used for connecting the mobile phone to the telephone provider's switch and V.120 for the ISDN connection from the telephone provider to the router. V.120 thus fulfills largely the same purposes as V.110, but permits higher transfer speeds.

No specific configuration is necessary for using V.120 for incoming calls: The router detects the protocol automatically and handles the packets accordingly. However, the router cannot use V.120 to call a mobile phone, which is possible with V.110.

If you operate you router with a private branch exchange, it may happen that the exchange falsifies the service used for an incoming call. To obviate this problem, a MSN (Multiple Subscriber Number) can be dedicated to the V.120 service in the menu ***WAN*** ➧ ***INCOMING CALL ANSWERING***. All calls arriving at this MSN are treated as V.120 calls.

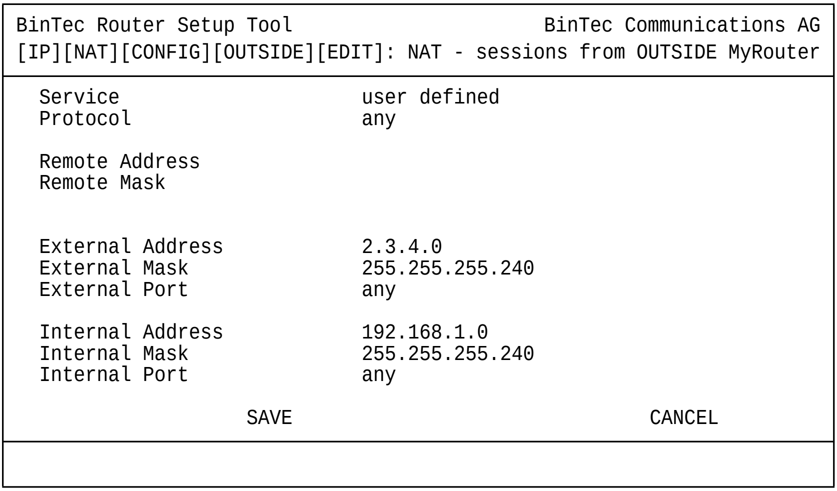
If you want to configure a WAN partner on your router that responds exclusively to V.120 calls, you can set this appropriately during the configuration of this WAN partner in ***WAN PARTNER*** ➧ **ADD**: Set the value for the **Encapsulation** field to *Async PPP over V.120 (HSCSD)*. Bear in mind that only V.120 connections are then possible over this interface.

3.11 Multi-NAT (Network Address Translation)

System-Software Release 6.2.2 offers an extension of BinTec's NAT implementation, which simplifies NAT configuration for networks with more than one external IP address. Previously only single IP addresses could be translated and the translation of several IP addresses involved increased configuration effort. System-Software Release 6.2.2 introduces two new variables, **ExtMask** in the **ipNat Out Table** and **IntMask** in the **IP NatPresetTable**. These make it possible to translate entire IP networks. This is relevant if you are assigned more than one IP address from your provider. Using the new variables, the IP addresses of a global IP address pool, e.g., can be translated to the local addresses of the LAN. It is necessary to ensure that the IP addresses calculated by the router from the netmask entered actually are within the address range of the LAN.

The configuration can be made in the Setup Tool using the menus ***IP*** ➧***NETWORK ADDRESS TRANSLATION*** ➧ **EDIT** ➧***REQUESTED FROM OUTSIDE*** ➧**ADD/EDIT** and ***REQUESTED FROM INSIDE*** ➧**ADD/EDIT**.

The menu for incoming connections is shown below:



```
BinTec Router Setup Tool                      BinTec Communications AG
[IP][NAT][CONFIG][OUTSIDE][EDIT]: NAT - sessions from OUTSIDE MyRouter

  Service                       user defined
  Protocol                      any

  Remote Address
  Remote Mask


  External Address              2.3.4.0
  External Mask                 255.255.255.240
  External Port                 any

  Internal Address              192.168.1.0
  Internal Mask                 255.255.255.240
  Internal Port                 any

                    SAVE                              CANCEL
```

The Setup Tool menus permit very accurate configuration. The following settings can be made:

Field	Meaning
Service	Service defined for connections to a defined host or a group of hosts in a LAN in the ***REQUESTED FROM OUTSIDE*** ➧ **EDIT/ADD** menu. Service for which the IP address mapping defined in the ***REQUESTED FROM INSIDE*** ➧ **EDIT/ADD** menu is carried out. Possible values: ■ *ftp* ■ *telnet* ■ *smtp* ■ *domain/udp* ■ *domain/tcp* ■ *http* ■ *nntp* ■ *user defined* (if you do not use any of the predefined services)

Field	Meaning
Protocol	Only for **Service** = *user defined*. Defines the protocol. Possible values: - *icmp* - *tcp* - *udp* - *gre* - *esp* - *ah* - *l2tp* - *any*
Remote Address	Optional. IP address of the host or group of hosts in the remote network. Only packets from this host/group are accepted for incoming connections.
Remote Mask	Netmask of **Remote Address** in the remote network. Entering the netmask ensures that incoming connections are allowed from the entire remote network.

Field	Meaning
Remote Port	Only in the ***REQUESTED FROM INSIDE*** ➜ **EDIT/ADD** menu. Only for **Service** = *user defined*. Defines the port number of the service on the host or group of hosts in the remote network. Possible values: ■ *any* ■ *specify* ■ *specify range*
Remote Port: Port	Only if **Remote Port** is set to *specify*. Port number of the service on the remote host(s).
Remote Port: Port to Port	Only if **Remote Port** is set to *specify range*. Port number range of the services on the remote host(s).
External Address	External IP address of the BinTec router for this interface. You must enter the corresponding external netmask for an external IP network address.
External Mask	Netmask of **External Address**. If you use external and internal IP network addresses, the values for **External Mask** and **Internal Mask** must be identical.

Field	Meaning
External Port	Only for **Service** = *user defined*. Defines the port number of the service of the BinTec router for this interface. Possible values: ■ *any* ■ *specify* ■ *specify range* (only in ***REQUESTED FROM OUTSIDE*** ➡ **EDIT/ADD** menu)
External Port: Port	Only if **External Port** is set to *specify*. Port number of the service of the BinTec router for this interface.
External Port: Port to Port	Only in the ***REQUESTED FROM OUTSIDE*** ➡ **EDIT/ADD** menu. Only if **External Port** is set to *specify range*. Port number range of the services on the BinTec router for this interface.
Internal Address	IP address of the internal host or group of hosts in a subnetwork. You must enter the corresponding internal netmask for an internal IP network address.
Internal Mask	Netmask of **Internal Address**. If you use external and internal IP network addresses, the values for **External Mask** and **Internal Mask** must be identical.

Field	Meaning
Internal Port	Defines the port number of the service on the internal host or group of hosts in a subnetwork. Possible values: ■ *any* ■ *specify*
Internal Port: Port	Only if **Internal Port** is set to *specify*. Port number of the service at **Internal Address**.

Table 3-6: ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **EDIT** ➧ ***REQUESTED FROM OUTSIDE*** and ***REQUESTED FROM INSIDE*** ➧ **ADD/EDIT**.

The menu for outgoing (***REQUESTED FROM INSIDE***) connections corresponds to the menu for incoming connections (***REQUESTED FROM OUTSIDE***). The **Remote Port** can also be determined in addition to **Remote Address** and **Remote Mask** (only if you have selected *user defined* for **Service**). Make sure the WAN partner also accepts packets with the appropriate protocol at this port.

3.12 Configurable ICMP Behavior

From System-Software Release 6.2.2 onwards, the ICMP messages sent by the router can be configured in the **ipIcmpTable**. The default behavior has not been changed over previous versions. You should only change the default settings if you have problems with the ICMP behavior of your router.

The following ICMP messages can be enabled or disabled in the **ipIcmpTable** (the example shows the default configuration):

```
ipIcmpSourceQuench( rw):              enabled
ipIcmpTimeExceededTrans( rw):         enabled
ipIcmpTimeExceededFrag( rw):          enabled
ipIcmpDestUnreachFrag( rw):           enabled
ipIcmpDestUnreachHost( rw):           enabled
ipIcmpDestUnreachHostTcp( rw):        tcp_rst
ipIcmpDestUnreachProto( rw):          enabled
ipIcmpEchoReply( rw):                 enabled
ipIcmpMaskReply( rw):                 enabled
MyRouter:ipIcmp>
```

The variable **ipIcmpDestUnreachHostTcp** has a special function: It modifies an "ICMP Destination Unreachable" message in such a way that the TCP connection is ended by a suitable packet. **ipIcmpDestUnreachHostTcp** must be set to *tcp_rst* for this purpose. If the variable is set to *icmp*, only an "ICMP Destination Unreachable" message is sent. If **ipIcmpDestUnreachHost** is set to *disabled*, this option is ignored.

3.13 Disabling IP and OSPF

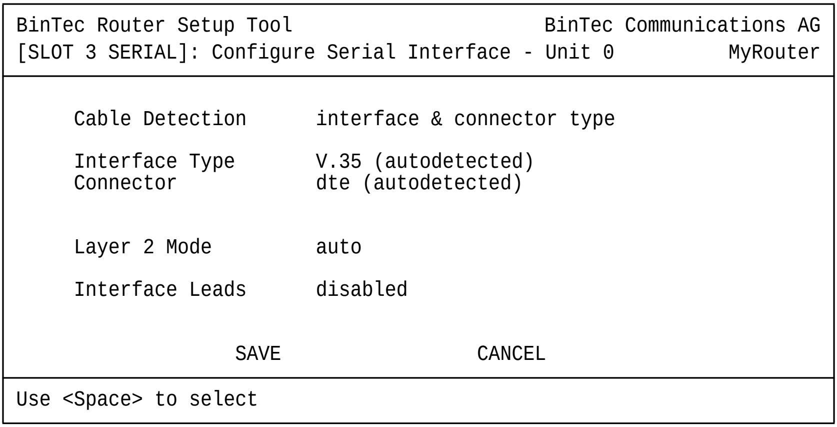
BinTec routers can calculate routes using both RIP (Routing Information Protocol) and OSPF (Open Shortest Path First; with the exception of **X8500**, this requires a valid license). You can free resources by disabling the RIP/OSPF process. This is advisable if neither RIP nor OSPF are used and if synchronization of the RIP/OSPF process to the interface or routing tables is not necessary.

The process could previously only be disabled via the configuration of several variables either protocol-specific or interface-specific. The new variable

biboExtAdmProcRouted now also makes this possible globally by setting its value to *disabled*.

3.14 Automatic Cable Detection at X.21 Interfaces

From System-Software Release 6.2.2 onwards, the cable types at X.21 interfaces can be detected automatically, provided suitable cables are used. The interface configuration menu has therefore changed accordingly. The example shows the menu for a serial port of an **X4300** (***SERIAL WAN: CM-SERIAL, SERIAL*** ➡ ***UNIT 0: SERIAL***):



```
BinTec Router Setup Tool                          BinTec Communications AG
[SLOT 3 SERIAL]: Configure Serial Interface - Unit 0              MyRouter

     Cable Detection      interface & connector type

     Interface Type       V.35 (autodetected)
     Connector            dte (autodetected)


     Layer 2 Mode         auto

     Interface Leads      disabled


                   SAVE                    CANCEL

Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
Cable Detection	Defines whether the interface and connector types used are to be detected automatically (*autodetected*) or set manually. Possible values: ■ *interface & connector type*: The interface and connector types are detected automatically. ■ *interface type*: Only the interface type is detected automatically. The connector type must be set manually. ■ *connector type*: Only the connector type is detected automatically. The interface type must be set manually. ■ *manual*: Both the interface and connector type must be set manually.
Interface Type	Defines the interface type of the port used. If you select *interface type* or *interface & connector type* for the **Cable Detection** field, the interface type is detected automatically. The detected value is displayed, e.g. ***V.35 (autodetected)***. If you select *connector type* or *manual* for the **Cable Detection** field, you must set the **Interface Type** field manually. For possible values, see table 3-8, page 40.

Field	Meaning
Connector	Defines the connector type of the port used. If you select *connector type* or *interface & connector type* for the **Cable Detection** field, the connector type is detected automatically. The detected value is displayed, e.g. ***dte (autodetected)***. If you select *interface type* or *manual* for the **Cable Detection** field, you must set the **Connector Type** field manually. For possible values, see table 3-9, page 41.
Speed	Only if the **Connector** field is set to *dce*. Transmission rate of connection. Possible values: ■ *2400 bps, 9600 bps, 14400 bps, 19200 bps, 38400 bps, 64000 bps* ■ *128 kbps, 256 kbps, 512 kbps* ■ *1 Mbps, 2 Mbps, 4 Mbps, 8 Mbps* ■ *custom*: The field **Speed: value (bps)** appears. Scalable from *2400 bps* to *8 Mbps*. The value to be set depends on the quality and length of the cable, the connector type and the min./max. speed accepted at the opposite end (DTE). Up to 8 Mbps are possible over a short distance of up to 5 m if shielded twisted-pair cables are used. Default value: *64000 bps*

Field	Meaning
Layer 2 Mode	Defines the value of the HDLC address field in the transmitted command frames (Layer 2). Possible values: - *auto* (default value): The selection made for **Connector** is assumed. You can usually accept this setting, e.g. for access to a public data network such as Datex-P in Germany. - *dte:* The address field has the value for DTE. - *dce:* The address field has the value for DCE.
Interface Leads	Defines whether the router checks the status of the interface line. The same value should be set for both connection partners. Possible values: - *enabled:* The Layer 1 signaling of the opposite station if checked on the signal line (I for X.21, CTS at V.35). The check correspondingly affects the variable **L1State**. - *disabled* (default value): The Layer 1 signaling of the opposite station is not checked, the physical line is always "up". In this setting, you should monitor the interface line in some other way, e.g. with PPP Keepalive.

Table 3-7: ***X21[x]***

The **Interface Type** field contains the following selection options:

Possible Values	Meaning
unknown (autodetected)	No cable is connected to the port or the cable connected does not support autodetection.
none	The port is not used.
X.21 (term)	V.11 on all lines, 120-ohm terminating resistor on critical lines.
V.35	V.35 on critical lines, V.28 on uncritical lines.
V.36	V.11 on critical lines, V.10 on uncritical lines.
X.21bis	V.28 on all lines.
X.21 (not term)	Unterminated V.11 on all lines.
RS-449	V.11 on critical lines, V.10 on uncritical lines.
RS-530	V.11 on critical lines, V.10 on uncritical lines.

Table 3-8: **Interface Type**

If you use an X.21 cable that supports autodetection, the value *X.21 (term)* is selected automatically. If you do not want termination, you must disable autodetection and make the configuration manually.

The **Connector** field contains the following selection options:

Possible Values	Meaning
unknown (autodetected)	No cable is connected to the port or the cable connected does not support autodetection.
dte	The pins are assigned as DTE interface. This setting is necessary, for example, if the router is connected to a public data network like Datex-P in Germany.

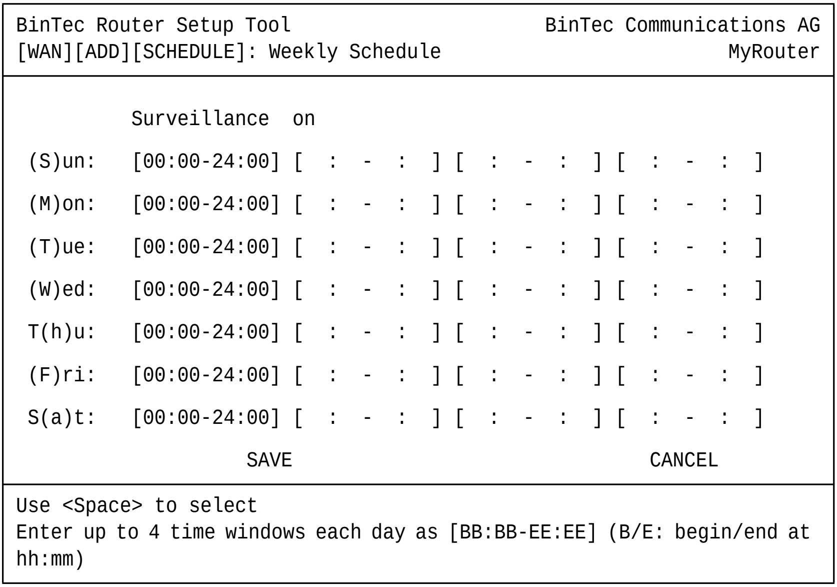
Possible Values	Meaning
dce	The pins are assigned as DCE interface.

Table 3-9: **Connector**

3.15 Weekly Schedule (Dialup)

System-Software Release 6.2.2 offers the facility for creating an access schedule (weekly schedule) for each dialup WAN partner to control when and for how long connections can be set up over this interface. This schedule is created in the ***WAN PARTNER*** ➧ **ADD/EDIT** ➧***WEEKLY SCHEDULE*** menu. Here you can activate or deactivate the surveillance.

If you activate the surveillance (**Surveillance** *on*), the following menu appears:



```
BinTec Router Setup Tool                     BinTec Communications AG
[WAN][ADD][SCHEDULE]: Weekly Schedule                        MyRouter

          Surveillance  on

 (S)un:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]

 (M)on:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]

 (T)ue:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]

 (W)ed:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]

 T(h)u:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]

 (F)ri:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]

 S(a)t:   [00:00-24:00] [  :  -  :  ] [  :  -  :  ] [  :  -  :  ]

                    SAVE                               CANCEL

Use <Space> to select
Enter up to 4 time windows each day as [BB:BB-EE:EE] (B/E: begin/end at
hh:mm)
```

For each day of the week, you can define four time windows in which a connection can be set up to this WAN partner. When the end of the configured time interval is reached for an existing connection, the connection is ended. Setting up again is not permitted until the next time window is reached.

When the surveillance is activated for the first time (default value is *off*), the period from 00:00 to 24:00 h is enabled for each day of the period to ensure unrestricted connections.

The letters shown in brackets in the abbreviations for the days of the week can be used to pass directly to the desired day. Just press the corresponding key on the keyboard.

If you want to define the access options more precisely, you can also configure more than four time windows in the **isdnScheduleTable**. Note the following in this case: Even though more than four time windows have been defined in the MIB tables, only the first four are shown in the Setup Tool. A warning message appears: If you press **SAVE**, the entries in the MIB will be deleted and replaced by the four visible in the Setup Tool.

3.16 CAPI Supplementary Services

BinTec Communications AG provides the following supplementary services with System-Software Release 6.2.2:

- Hold/Retrieve
- ECT (Explicit Call Transfer)
- Call Forwarding
- Call Deflection

The supplementary services are executed in the exchange of the telephone network operator or in an intermediate telephone system.

4 Changes

- Scope of Features for **X1000**/**X1200** and **X3200** with IPSec (chapter 4.1, page 43)
- S_2M Configuration (chapter 4.2, page 44)
- X.25 PAD (chapter 4.3, page 47)
- Improved Compatibility with SNMP Managers (chapter 4.4, page 48)
- Configuration of Serial Interfaces (chapter 4.5, page 48)
- Time Display for `ps` Command (chapter 4.6, page 48)
- New Option `-r` for `rtlookup` (chapter 4.7, page 49)
- Solution to ADSL Modem Problem (chapter 4.8, page 49)

4.1 Scope of Features for X1000/X1200 and X3200 with IPSec

As the considerably extended scope of features makes the new IPSec software very extensive, some changes had to be made to other features for the IPSec versions of System-Software Release 6.2.2 for **X1000**, **X1200** and **X3200**. The following features are therefore no longer available in the IPSec version of System-Software Release 6.2.2:

- Encrypted ISDN Login (`dhkeyd`, `icrypt`, `dhkey`)
- RIP (Routing Information Protocol) demon (`routed`)
- Web-based monitoring (`httpd`)
- Bridging (`bridged`, `bridgemux`)

The command line interface `cli.cmd`, the debug feature `profile` and the ISDN approval feature `zul` are no longer available either.

Note that the H.323 proxy and H.323 gatekeeper cannot be included in the IPSec version of System-Software Release 6.2.2.

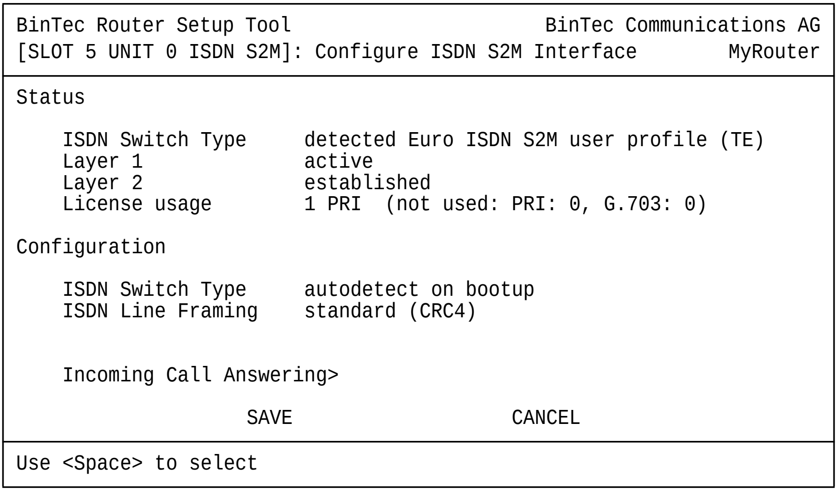
4.2 S_2M Configuration

The configuration of an S_2M (PRI) connection has been extended by two items. This simplifies handling several PRI expansion cards (e.g. in an **X8500**) and ensures compatibility with specific service providers.

4.2.1 Status Display

The menu for configuration of an S_2M connection contains a status display in addition to the fields and submenus for the configuration.

The following example shows the menu for the first PRI in slot 5 (`SLOT 5 UNIT 0 ISDN S2M`) of an **X8500**:



```
BinTec Router Setup Tool                           BinTec Communications AG
[SLOT 5 UNIT 0 ISDN S2M]: Configure ISDN S2M Interface             MyRouter

Status

    ISDN Switch Type     detected Euro ISDN S2M user profile (TE)
    Layer 1              active
    Layer 2              established
    License usage        1 PRI  (not used: PRI: 0, G.703: 0)

Configuration

    ISDN Switch Type     autodetect on bootup
    ISDN Line Framing    standard (CRC4)


    Incoming Call Answering>

                    SAVE                       CANCEL

Use <Space> to select
```

The top part of the menu provides status information on the ISDN protocol and layer activity of the PRI port and on license usage of the expansion card. The **License usage** field indicates which license is used for the current configuration and how many of the licenses activated by you on this expansion card are still available (*not used)*. In our example, all four PRIs are licensed and configured (*not used: PRI: 0, G.703: 0*). A PRI expansion card with two PRI licenses and only one PRI already configured would be displayed as follows: *not used: PRI: 1, G.703: 0*. You can obtain further details on status information in table 4-1, page 46.

The fields under **Status** cannot be modified. They show the current status of the PRI. The fields have the following meaning:

Field	Meaning
Status: ISDN Switch Type	Shows the currently valid protocol for this port and the status of ISDN autoconfiguration. Possible values: - *autodetection is waiting to run*: The router waits until Layer 1 becomes active. Autoconfiguration is then started. - *autodetection is running*: ISDN autoconfiguration is in progress. - *detected <any switch type name>*: The given protocol has been detected by ISDN autoconfiguration and is active. - *<any switch type name>*: Shows the ISDN protocol currently configured.

Field	Meaning
Status: Layer 1	Shows the physical status of the PRI port. Possible values: - *active*: Layer 1 is OK. - *no signal*: Possibly no cable or no license available. - other information: Defective cable or wrong value for **ISDN Line Framing**.
Status: Layer 2	Shows the status of the Layer 2 protocol LAPD of the D-channel. Possible values: - *connecting*: Layer 2 is not connected. - *established*: Layer 2 is connected.
Status: License usage	Shows which license is currently assigned to this port. Possible values: - *license missing*: The license needed for the ISDN protocol configured is not available. All available licenses are currently being used by other ports of the expansion card. - *not used*: A license is not required for the current configuration (or a license available for this expansion card is not being used). - *1 PRI*: One PRI license is used for this interface. - *1 G.703*: One G.703 license is used for this interface.

Table 4-1: ***PRI[x]***: Status information

4.2.2 Channel Selection

To ensure compatibility with special service providers, a further option is provided for the **ISDN Switch Type** *Euro ISDN S2M user profile (TE)*: If you set the switch type appropriately, you can select a value for the new variable **Channel Selection**. This defines how the B-channel is selected for an outgoing call. Possible values are:

- *standard (any channel)*: (default setting) The (PABX) network selects the channel to be used.
- *no channel identification*: System-Software Release 6.2.2 sends no IE (Information Element) for channel identification. The (PABX) network selects the channel to be used.
- *submit preferred channel*: System-Software Release 6.2.2 selects the channel to be used and signals this to the (PABX) network.

You can usually keep the default setting. It is only necessary to change the setting in a few special cases. Ask your provider if a special setting is necessary.

4.3 X.25 PAD

The X.25-PAD functionality is only available if the connection is set up over an asynchronous Layer 1 protocol (*V.110* or *Modem*). It was previously necessary to configure a separate WAN partner with the relevant protocol. An MSN also had to be reserved for the X.25 PAD service. The simultaneous use of X.25 and X.25 PAD on one interface was therefore not possible.

The detection of the Layer 1 protocol is now automatic. If the Layer 1 protocol actually used for a connection to an X.25 WAN partner is asynchronous, X.25 PAD is activated automatically. Otherwise X.25 native is used. It is no longer necessary to tie an MSN exclusively to the X.25 PAD service.

4.4 Improved Compatibility with SNMP Managers

Three new values have been created for the variable **biboAdmSnmpVersion**, *version1p1*, *version1p1_compat* and *version1p1_auto*. Version 1p1 strongly improves the compatibility of the BinTec SNMP implementation with SNMP managers like HP OpenView.

Note that the default setting is *version1p1_auto* from System-Software Release 6.2.2 onwards. Version 1p1 is used in this setting if possible. Otherwise version 1p1 is used in Compatibility Mode (*version1p1_compat*).

If you use SNMP managers like HP OpenView, you should change the value of **biboAdmSnmpVersion** in existing configurations and set to *version1p1_auto*.

4.5 Configuration of Serial Interfaces

Changes have been made to the MIB tables in System-Software Release 6.2.2 that affect the configuration of serial WAN interfaces. It is therefore possible that unwanted changes occur in the configuration of the interfaces when updating to System-Software Release 6.2.2.

After updating to System-Software Release 6.2.2, you should check the configuration of the relevant interfaces and restore as necessary.

4.6 Time Display for `ps` Command

If the `ps` command is used in the SNMP shell, all time information (`time`, `ktime`, `utime`) is now given down to one hundredth of a second.

4.7 New Option `-r` for `rtlookup`

If the default interface for a packet to be routed was inactive (`dormant`, `down` or `blocked`), but a backup interface existed for this packet, it was previously not possible to show this backup interface with the `rtlookup` command. This is now shown with the `-r` option when it is used.

4.8 Solution to ADSL Modem Problem

Alcatel’s implementation of PPTP/GRE (Point-to-Point Tunnelling Protocol/Generic Routing Encapsulation) can lead to incorrect "acknowledgement numbers" and thus PPTP interfaces may be blocked.

The following workaround has been implemented: There is now a configurable timer (**pptpProfileMaxBlockTime**, the value is entered in milliseconds up to *10000*): A blocked PPTP connection as well as the associated control connection over TCP port 1723 are terminated after timeout. Otherwise attempts to restore the connection to the opposite Alcatel station could fail.

5 Bugfixes

System-Software Release 6.2.2 fixes a number of bugs that occurred in Release 6.1.2:

- SNMP Bug (chapter 5.1, page 50)
- SNMP Shell (chapter 5.2, page 51)
- Crash due to Syslog Level Debug (chapter 5.3, page 51)
- IPSec and Back Route Verification (chapter 5.4, page 51)
- Closed User Group (chapter 5.5, page 52)
- Path MTU Discovery and IP Accounting (chapter 5.6, page 52)
- Corrupted Data in Flash ROM (chapter 5.7, page 53)
- LEDs on X4E-3BRI Expansion Card (chapter 5.8, page 53)
- Logic Update (chapter 5.9, page 53)
- IP and Bridge Menus in Frame Relay (chapter 5.10, page 53)
- Compatibility between System-Software Release 6.2.2 and Older Software (chapter 5.11, page 54)
- RADIUS Accounting (chapter 5.12, page 54)

5.1 SNMP Implementation Bug

With System Software 6.1.2, BinTec routers were susceptible to a bug in the SNMP protocol in connection with processing SNMP requests. Under certain circumstances, this bug could be utilized to cause our routers to crash or reboot.

Further information and a description for working around the bug can be found at:

http://www.cert.org/advisories/CA-2002-03.html.

The problem has been solved.

5.2 SNMP Shell

An infinite table of zeroes was shown when logging in with an unscheduled name for an SNMP community in the SNMP shell (`admin`, `read` and `write` are scheduled values).

The problem has been solved. An error message is now generated saying that the community entered does not exist.

5.3 Crash due to Syslog Level Debug

When the syslog level of the router was set to the value *debug*, the system crashed as soon as all-zero packets arrived. This problem was caused by an error in the syslog messages.

The problem has been solved.

5.4 IPSec and Back Route Verification

It was possible for IPSec packets to be rejected by the "back route verification" function.

This problem was caused by assuming that the interface from which the original packet came was the source interface of an IPSec packet. If the IPSec packet was then routed over a different interface to the source interface (IPSec packets are routed over all available interfaces), a collision occurred with "back route verification".

The problem has been solved. IPSec packets can therefore certainly be routed over any interfaces.

5.5 Closed User Group

If a closed user group was entered at a service provider to control ISDN calls, it was possible that the calls were not allowed. This happened when the information about the members of the user group was still to be transferred by the service provider, but evaluated in the router. The router evaluated information incorrectly, so that calls from the user group were no longer detected and therefore rejected.

The problem has been solved. The information on the user group is processed correctly.

5.6 Path MTU Discovery and IP Accounting

PMTU (Path Maximum Transfer Unit) Discovery was not operational if IP accounting was activated on a router at the same time.

This problem was caused by the PMTU Discovery mechanism not assuming that fragmented packets are assembled on the path (e.g. due to NAT or Access Control). Problems are therefore caused with the Don’t Fragment Bit, which is used to mark smaller units than the calculated PMTU.

The problem has been solved: The Don’t Fragment Bit is now deleted on assembling the packet fragments.

5.7 Corrupted Data in Flash ROM

The data in the flash memory could be corrupted when disconnecting or connecting the power supply of **X8500** and **X4000**.

The problem has been solved. Valid data are protected by Sector Lock Bits.

5.8 LEDs on X4E-3BRI Expansion Card

The red and green LED on the X4E-3BRI expansion card were reversed in hardware version 1.2, so that the LEDs did not indicate in accordance with the description in the documentation.

The problem has been solved. The driver of the LEDs causes the LEDs to indicate appropriately.

5.9 Logic Update

It was possible that the MAC address of the Ethernet interface, the serial number of the router and part of the configuration were deleted in a logic update.

This problem has been solved. The stated sectors now remain untouched and no data are overwritten.

5.10 IP and Bridge Menus in Frame Relay

The submenus ***IP*** and ***BRIDGE*** could not be accessed from the ***FR*** ➧ ***MULTIPROTOCOL OVER FRAME RELAY*** ➧ **ADD/EDIT** menu.

The problem has been solved. The menus can now be accessed again and their settings configured.

5.11 Compatibility between System-Software Release 6.2.2 and Older Software

It was not possible to change back to an older release after carrying out an update to System-Software Release 6.2.2.

This problem was caused by the write protection of System-Software Release 6.2.2. Older software versions are no longer able to modify data created by the newer software.

The problem has been solved. The BOOTmonitor and update shell check the software version and only version 6.2.x software is protected.

5.12 RADIUS Attribute NAS Port

It was possible that an Accounting Start Request referred to a different port of a network access server than the Accounting Stop Request. This meant that the connection could not be ended for accounting.

The problem has been solved. The Accounting Stop Requests reliably refers to the same port. The accounting is accordingly stopped.

6 Known Issues

A number of errors still persists in System-Software Release 6.2.2. We try hard to resolve any remaining issues as fast as possible. As soon as any improvements have been made to the software, they will be made available on our webserver. Please watch www.bintec.net for software updates.

The following issues are known to us:

- DSL LED (chapter 6.1, page 55)
- Termination of a DSL Connection (chapter 6.2, page 56)
- PAP Authentication with an ACE Radius Server (chapter 6.3, page 56)
- Wrong Netmask in NAT Entries (chapter 6.4, page 56)
- Configuration of MPPC (chapter 6.5, page 57)
- Compression and Encryption (chapter 6.6, page 57)
- V.90 Dialup with Acer Modems (chapter 6.7, page 57)
- Windows 2000 128 Bit MPPE (chapter 6.8, page 57)
- IPSec (chapter 6.9, page 58)

6.1 DSL LED

The Deutsche Telekom AG in general interrupts a DSL connection every 24 hours. On reconnecting it may occur that the DSL LED of a BinTec router does not light up. Establishing yet another connection fixes this problem.

6.2 Termination of a DSL Connection

When rebooting a BinTec router by typing `cmd=reboot` at the SNMP shell prompt, it may occur that an active DSL connection is not terminated. We recommend to manually deactivate and then reactivate the respective interface. You can do so in the menu ***MONITORING AND DEBUGGING*** ➧ ***INTERFACES***.

6.3 PAP Authentication with an ACE Radius Server

When a Windows PC sends a PAP authentication request to an ACE Radius Server, the router forwards the request to the server. After a short time (less than two seconds), the PC sends another request. The router forwards the second request, too, but in the process deletes the first one. If the Radius Server approves of the first request, the router cannot assign the approval to any request and authentication fails.

6.4 Wrong Netmask in NAT Entries

When creating a new entry in the **ipNatPresetTable** (menu ***IP*** ➧ ***NETWOORK ADDRESS TRANSLATION*** ➧ **EDIT** ➧ ***REQUESTED FROM OUTSIDE*** ➧ **ADD**), the default values for **External Mask** and **Internal Mask** are exchanged for one another.

If these values are not changed, the configuration may not be functional. If a values is entered for both variables during configuration, the wrong default values are overwritten and there will be no problems.

6.5 Configuration of MPPC

MPPC cannot be activated in the Setup Tool. It can be activated, however, by setting the variable **Compression** in the **biboPPPTable** to *MPPC*.

By saving a WAN partner in the Setup Tool all values of the MIB tables are overwritten. If you have activated MPPC for a WAN partner in the way described above, make sure you do not save the same WAN partner again in the Setup Tool.

6.6 Compression and Encryption

When employing HiFn-equipped resource modules (XTR-ENC or XTR-VPN), the combination of MPPC (data compression) and MPPE (data encryption) is not functional.

6.7 V.90 Dialup with Acer Modems

Using V.90, Acer modems cannot dial in to BinTec routers that have been configured to exclusively accept V.90 calls.

6.8 Windows 2000 128 Bit MPPE

128-bit-MPPE-encrypted connections of a BinTec router and a Windows 2000 PC cannot be authenticated with MS-CHAP V1. Please use MS-CHAP V2 for authentication.

6.9 IPSec

There is a small number of problems in the context of BinTec's IPSec solution. They do not, however, affect basic IPSec functionality.

6.9.1 Traffic List Entries not Deleted

When deleting an IPSec peer in the Setup Tool, the traffic list entries for this peer are not deleted. This may lead to problems when configuring a new peer, since the "orphaned" entries may be assigned to the new peer.

If you delete a peer, you should manually delete the respective traffic list entries.

6.9.2 IPSec Daemon

If the IPSec configuration of a BinTec router is changed, the IPSec daemon is reset in order to allow the changes to become effective. This happens, too, if a new peer is added to an existing configuration. Consequently all IPSec tunnels are reset, and Phase-2 Lifetimes may have to time out before all tunnels are up again.