Release Notes
System Software
Release 6.2.5
BRICK Generation

May 2003

System Software Release 6.2.5

This document describes new features, changes, bugfixes and known bugs in System Software Release 6.2.5 for BRICK Generation Routers.

1 Important Information

Note that configurations you create with System Software Release 6.2.5 are not downward compatible! Before updating to System Software Release 6.2.5, you should save your old configuration so that you can load Release 6.1 again in case a "roll-back" is necessary.

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

If you implement IPSec configurations with System Software Release 6.2.5, note that the remote peer to which you want to set up a tunnel must also run with System Software Release 6.2.5, if it is a BinTec device.

Note that among the **BIANCA/BRICK XM** routers only the version with 2 MB of Flash memory and 8 MB of RAM is supported. If you are using a **BRICK XM** with only 4 MB of RAM, you can purchase additional RAM modules from BinTec.

1.1 Updating the System Software

Proceed as follows in order 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 your router manual.

1 Important Information

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.

2 New Features

The following new features have been implemented in System Software Release 6.2.5:

- Easy Licensing (chapter 2.1, page 10)
- New RADIUS Features (chapter 2.2, page 13)
- Multiuser WAN Partner (chapter 2.3, page 16)
- Mutual PPP Authentication (chapter 2.4, page 19)
- PPPoE Server Mode (chapter 2.5, page 19)
- Silent Deny in NAT (chapter 2.6, page 19)
- Keepalive for Multi-Protocol HDLC Framing (chapter 2.7, page 20)
- New Restart Delay Timer in X.25 (chapter 2.8, page 21)
- DHCP Client (chapter 2.9, page 21)
- BAP/BACP: Channel Bundling with Group Numbers (chapter 2.10, page 23)
- V.120 (chapter 2.11, page 26)
- Multi-NAT (chapter 2.12, page 27)
- Configurable ICMP Behavior (chapter 2.13, page 32)
- Disabling RIP and OSPF (chapter 2.14, page 33)
- Weekly Schedule (chapter 2.15, page 34)
- CAPI Supplementary Services (chapter 2.16, page 35)

2.1 Easy Licensing

Beginning with System Software Release 6.2.5, BinTec introduces a new system of licensing your hardware and software products. The basic licenses your router comes with are no longer found in form of a license key, mask and serial number, but all of them are enabled by default. Only when you purchase additional hardware or software licenses do you have to go through the following procedure to enable them.

If you happen to delete licenses of the ex works state, proceed as follows to reactivate them:

- Go to ***LICENSES*** ➧ **ADD**.
- Enter **Mask** 65535.
- Leave all other fields blank.
- Confirm with **Enter**.

The licenses of the ex works state are reactivated.

License Data

The data you need comprise the serial number of your router or your expansion card respectively, a PIN and a license serial number. Both, the PIN and the license serial number you receive together with the license you purchase. When licensing online at www.bintec.net, you must enter all of the data, and you will then receive a key. In the Setup Tool, you enter this key together with the license serial number to enable the license you have purchased.

Please note that with System Software Release 6.2.5 you must obtain your license data in the described way. You will no longer be able to enter license data of the kind you have previously found on the license data sheet.

Note, also, that additional hardware like expansion cards and resource modules now require a license. This was not necessary with older versions of the system software.

Valid licenses that have been entered before updating to System Software Release 6.2.5, however, will be recognized and you need not reenter them.

Entering a License

To enter your license proceed as follows:

- Log in on your router as `admin` as described in your **User's Guide**.
- Enter `setup` in the command prompt to enter the Setup Tool.
- Go to ***LICENSES***.

The licenses, which are already enabled on your router, are listed under **Available Licenses**. The field **Software License ID** displays the serial number of your router which you need to enter to enable any software licenses.

The relevant menu in the Setup Tool looks like this:

```
BinTec Router Setup Tool                          BinTec Access Networks
GmbH
[LICENSE]: Licenses                                              MyRouter

Available Licenses:

IP (builtin), STAC, CAPI, BRIDGE

Software License ID: X4A2001IWAN0020

Serialnumber     Mask     Key             Description      State
999999           55       88PNUPZ         composite        ok


ADD                       DELETE                        EXIT

Press<Ctrl-n>,<Ctrl-p>to scroll,<Space>tag/untagDELETE,<Return>to edit
```

To enter your license, proceed as follows:

- Create a new entry with **ADD**.

  Another menu window opens.

- Enter **Serial Number** (the license serial number you have received upon purchasing the license), and **Key** (the one you have received upon licensing online).

- Confirm with **SAVE.**

  You have returned to the ***LICENSES*** menu. The subsystems activated by your license data are now listed. The license entered is displayed with the state *ok*.

If *not ok* is shown as the state, you have probably made a typing error.

- Try again.

If the license state is shown as *not_supported*, you have entered a license for a subsystem your router does not support. You will not be able to make use of the functionality associated with the license

Disabling a License

Proceed as follows to disable a license on your router:

➤ Go to ***LICENSES***.

➤ Mark the license you want to disable by putting the cursor on it and hit **Space**.

➤ Confirm with **DELETE**.

The license is now disabled. You can reactivate this license any time by entering the valid key and license serial number for this license.

2.2 New RADIUS Features

2.2.1 Login Authentication via RADIUS

With System Software Release 6.2.5 user authentication on the login shell is performed through a RADIUS authentication request. The router proceeds as follows:

- When a login name and a password are entered in a login-shell (of e.g. ISDN Login, Telnet, Console or Minipad), the router checks if a RADIUS server is configured for login authentication.
- If a RADIUS server is configured on the router, an alive check is performed, and, if successful, an authentication request is sent. If the RADIUS server is unreachable, the router continues with local authentication as described below. If the RADIUS servers responds, it checks the login-data, if it does not respond, the router again proceeds with local authentication. If the RADIUS server performs the authentication and the login data are valid, access to the shell prompt is granted. If the data are invalid, the user is presented with a new login prompt.
- If no RADIUS server is configured, it checks the login name and which access level is assigned to it. Next, it checks the entered password and whether it matches the password configured for the access level. If authen-

tication is successful, access to the shell prompt is granted. If authentication, however, fails the user is presented with a new login prompt.

The following figure illustrates this procedure:

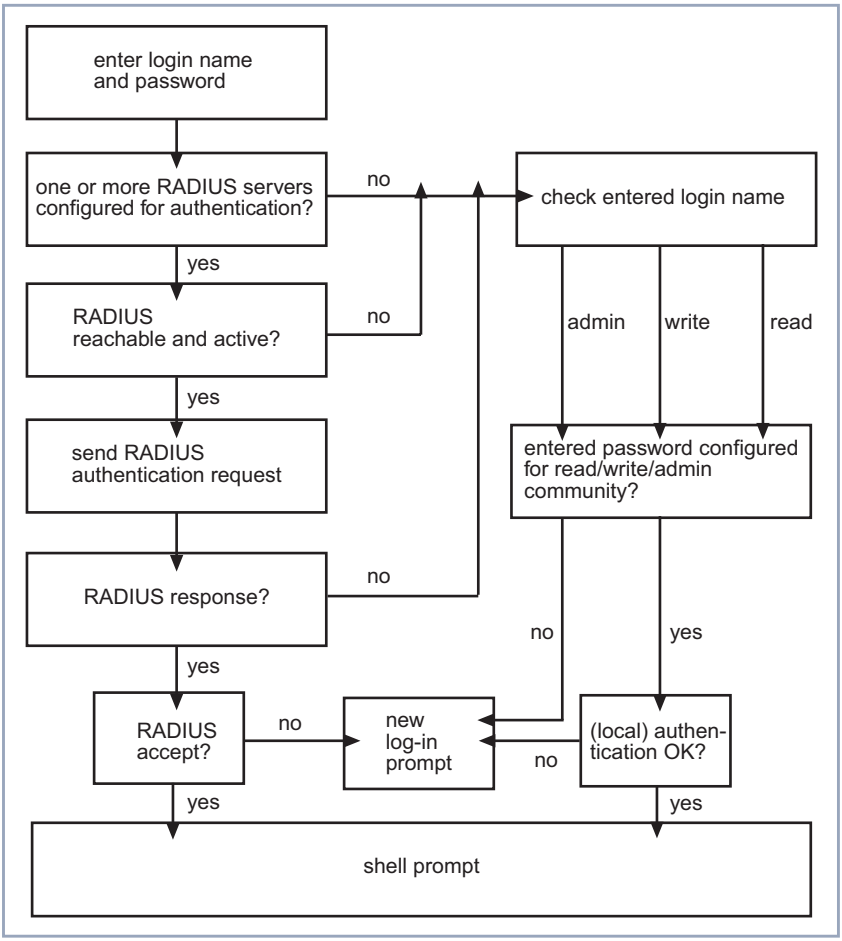

Figure 2-1: RADIUS login authentication

There are certain mandatory settings for this configuration. Since currently not all of the variables necessary can be configured in the Setup Tool, the configuration should be carried out in the SNMP shell.

These are the mandatory settings in the **radiusServerTable**:

- The **radiusServerProtocol** variable has to be set to *login*.
- The **radiusServerAddress** variable has to specify the IP address of the RADIUS server.
- The **radiusServerPort** variable has to be specify the port number used for transmission of the RADIUS packets. This usually is *1645* for Steel-Belted, Merit, Cistron, or *1812* for several other RADIUS servers.
- The **radiusServerSecret** has to specify the NAS-secret configured on the RADIUS server.
- The **radiusServerPriority** has to specify the priority of the RADIUS server specified by the IP address in the **radiusServerAddress** variable. Use *0* for the highest priority or a value higher than *0* for backup servers.

An example entry in the **radiusServerTable** will thus look like this:

```
inx Protocol(*rw)            Address(rw)          Port(rw)
    Secret(rw)               Priority(rw)         Timeout(rw)
    Retries(rw)              State(-rw)           Policy(rw)
    Validate(rw)             Dialout(rw)          DefaultPW(rw)
    ReloadInterval(rw)

00 login                     172.16.96.93         1645
   "my_nas_secret4rad_93"    0                    1000
   1                         active               authoritative
   enabled                   disabled             "lola"
   0
```

More than one entries can be created in the table to configure backup servers if RADIUS authentication is highly preferable over local authentication.

The main benefit of this kind of login authentication is enhanced remote administration possibilities: A centralized data base for administrative router access is available on the RADIUS server, making it possible to define more than one administrative account per router. Likewise, only one administrative account is

necessary to access any number of routers on which RADIUS authentication is performed.

On the RADIUS server itself, merely a user needs to be added to the users file, specifying the access level in the **Service Type** attribute. If set to administrative, the user has "admin" rights, if set to login, the user has "read" rights only. Thus, it is equally easy to block administrative access to routers: you only need to delete the respective user entry.

2.2.2 Client Authentication during Callback

Prior to System Software Release 6.2.5 it was mandatory for PPP authentication during a callback that BinTec specific RADIUS attributes were used to transmit the necessary protocol/ID/password triple. These settings were then sent back to the remote access server. This procedure had some drawbacks, since there were compatibility issues with certain user data bases a RADIUS server may have to interact with (especially Windows NT), as well as with the Microsoft IAS RADIUS server. Moreover, with this configuration sensitive data were sent unencrypted from the RADIUS servers to the remote access server.

All of these drawbacks have been removed. During the callback a second RADIUS request is sent to the RADIUS server to perform the remote authentication. Thus the temporary account data created by the initial authentication need not be handled with the BinTec specific RADIUS attributes.

2.3 Multiuser WAN Partner

With the concept of a Multiuser WAN Partner, BinTec offers a convenient way for Internet Service Providers to offer Internet by Call services where multiple users can dial in using the same ID and password. It is available for PPP connections as well as for PPPoE and PPTP connections; and similarly to a RADIUS procedure it is realized by creating a temporary WAN partner once authentication has been successful.

Creating a Multiuser WAN Partner

To make use of this concept it is sufficient to define just one static WAN partner as a kind of template with certain configuration specifications. All settings necessary for the creation of the temporary WAN partner are copied from the MIB tables once authentication has been successful.

On how to create a WAN partner, please refer to the **User's Guide** of your router.

You can either create a generic WAN partner, called e.g. *MultiUser*, and then make the necessary adjustments, or you can make sure to choose the right settings directly upon WAN partner creation.

The following table shows which values are entered in the **biboPPPTable** while creating a WAN partner:

inx	IfIndex(ro)	Type(*rw)	Encapsulation(-rw)
	Keepalive(rw)	Timeout(rw)	Compression(rw)
	Authentication(rw)	AuthIdent(rw)	AuthSecret(rw)
	IpAddress(rw)	RetryTime(rw)	BlockTime(rw)
	MaxRetries(rw)	ShortHold(rw)	InitConn(rw)
	MaxConn(rw)	MinConn(rw)	Callback(rw)
	Layer1Protocol(rw)	LoginString(rw)	VJHeaderComp(rw)
	Layer2Mode(rw)	DynShortHold(rw)	LocalIdent(rw)
	DNSNegotiation(rw)	Encryption(rw)	LQMonitoring(rw)
	IpPoolId(rw)	SessionTimeout(rw)	
02	10001	multiuser	ppp
	off	3000	none
	chap	"user"	"geheim"
	dynamic_server	4	300
	5	20	1
	2	1	disabled
	data_64k		disabled
	auto	0	
	enabled	none	off
	0	0	

Most of these values serve as examples only, but some are essential for the configuration of a multiuser WAN partner:

- The variable **biboPPPType** has to be set to *multiuser*.
  In the Setup Tool you can set this value in the ***WAN PARTNER*** ➧ **EDIT** ➧ ***ADVANCED SETTINGS*** menu: Set the value for the **Special Interface Types** field to *Call-by-Call (dialin only)*.

- The **biboPPPIpAddress** variable has to be set to *dynamic_server*.
  In the Setup Tool, you can set this value in the ***WAN PARTNER*** ➧ **EDIT** ➧ ***IP CONFIGURATION*** menu: Set the value for the **IP Transit Network** field to *dynamic server*.

- There has to be an IP pool specified by the **biboPPPIpPoolId** variable, since you must assign an address pool to your multiuser WAN partner.
  In the Setup Tool, you can do this in the ***WAN PARTNER*** ➧ **EDIT** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** menu: Specify the IP address pool you want to assign to the multiuser WAN partner in the **IP Address Pool** field.

On how to create an IP address pool, please refer to the **User's Guide**.

Channel Bundling and Callback

If you want to allow channel bundling on a multiuser interface, you can specify the maximum number of B-channels that can be opened through the **biboPPPMaxConn** variable. Alternatively you can configure channel bundling in the ***WAN PARTNER*** ➧ **EDIT** ➧ ***ADVANCED SETTINGS*** menu of the Setup Tool: Choose dynamic channel bundling and enter the maximum number of opened channels in the **Total Number of Channels** field.

Likewise you can allow a callback. It is specified by the **biboPPPCallback** variable. Presently only the value *ppp_offered* is supported. It equals setting the **Callback** field in the ***WAN PARTNER*** ➧ **EDIT** ➧ ***ADVANCED SETTINGS*** menu to *yes (PPP negotiated)*.

2.4 Mutual PPP Authentication

Prior to System Software Release 6.2.5, authentication was only required from the calling party, but not from the called party (with the exception of negotiated callback). Mutual authentication must be enabled through the newly created MIB variable **pppExtIfAuthMutual**, the default value is *1*=disabled (*2*=enabled). During the LCP (Link Control Protocol) negotiation, the router tries to negotiate and use the same authentication protocol for both authentications.

Mutual Authentication is an integral feature of MS CHAP V2. Therefore, if MS CHAP V2 is chosen, the **pppExtIfAuthMutual** variable need not be set.

2.5 PPPoE Server Mode

Just as BinTec routers can be used as PPP dial-in servers, they can now be used as servers for PPPoE connections, too. This function can be enabled in the ***PPP*** menu by setting the value of the **PPP Profile Configuration** field. It offers support of static and dynamic WAN partners, RADIUS Accounting, encryption and PPP authentication for PPPoE dial-in interfaces.

2.6 Silent Deny in NAT (Network Address Translation)

When an incoming packet is discarded because of the NAT configuration of the router, a message is usually sent back to the packet originator (either a TCP RST message or an ICMP Host Unreachable message), informing the originator that the packet has been discarded.

If Silent Deny in NAT is enabled, however, neither message is sent. This option has been common in the configuration of IP Access Rules, and is now made

available for NAT. It is useful when much unsolicited incoming traffic has to be handled, and the originators of the packets need or should not be informed that the traffic has been blocked. Not informing a packet originator of discarded packets can be a vital security function if the ports of inactive services are supposed to be in stealth mode.

To enable Silent Deny in NAT, go to ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.

- Choose the interface on which you want to configure silent deny.
- In ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **EDIT**, set **Network Address Translation**: *on*, and **Silent Deny**: *yes*.
- Confirm with **SAVE**, and in the following menu windows with **EXIT**.
- You have returned to the main menu.

2.7 Keepalive for Multi-Protocol HDLC Framing

With System Software Release 6.2.5, there now is a keepalive for encapsulation *Multi-Protocol HDLC Framing*. Thus the keepalive of Cisco routers operating on the remote side is supported. It is configured through the **biboPPPKeepalive** variable in the **biboPPPTable**. The default value *1* (off) means that the keepalive is in passive mode. In this mode all received keepalive packets are answered with a keepalive request, and no checks are performed upon outstanding remote keepalive requests.

In active mode (**biboPPPKeepalive** set to *2*=on), keepalive requests are sent by the BinTec router periodically. To avoid flooding the connection, no received keepalive packets is answered. Outstanding remote keepalive requests are checked upon, and the interface can be set into the *down* state, if there are no remote keepalive requests.

2.8 New Restart Delay Timer in X.25

There is now a Restart Delay Timer that can be configured individually for all X.25 interfaces. It specifies the time (in milliseconds) to pass between establishment of layer 2 of the X.25 connection and the sending of the restart packet that initiates establishment of layer 3. Should the router receive a restart packet before it sends one itself, the timer is halted and a restart confirm packet is sent.

The timer is configured through the **x25LinkPresetRestDelayTimer** variable in the **x25LinkPresetTable**. The default value is *0* (a restart packet is sent immediately after layer 2 has been established, the maximum value is *15000*).

2.9 DHCP Client

From System Software Release 6.2.5 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 Access Networks
GmbH
[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.

2.10 BAP/BACP: Channel Bundling with Group Numbers

From System Software Release 6.2.5 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 2-1: **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**.

2.11 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.

2.12 Multi-NAT (Network Address Translation)

System Software Release 6.2.5 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 6.2.5 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 Access Networks GmbH
[IP][NAT][EDIT][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 2-2: ***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.

2.13 Configurable ICMP Behavior

From System Software Release 6.2.5 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.

2.14 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 **BIANCA/BRICK XL**, 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*.

2.15 Weekly Schedule (Dialup)

System Software Release 6.2.5 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 Access Networks
GmbH
[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 in-

terval 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.

2.16 CAPI Supplementary Services

BinTec Access Networks GmbH provides the following supplementary services with System Software Release 6.2.5:

- 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.

3 Changes

To enhance the functionality of our system software, several changes have been made to previously available functions:

- Bridging and X.25 Availability (chapter 3.1, page 37)
- PPTP Improvements (chapter 3.2, page 37)
- HP OpenView Compatibility (chapter 3.3, page 38)
- Changes in RADIUS Implementation (chapter 3.4, page 38)
- CAPI 1.1 Development Discontinued (chapter 3.5, page 39)
- Configurable MTU and MRU Values (chapter 3.6, page 39)
- Interface Blocked with Inconsistent Encryption Configurations (chapter 3.7, page 39)
- Interdependent Configuration of PPP Encapsulation, Encryption and Compression (chapter 3.8, page 44)
- New Activity Monitor Password (chapter 3.9, page 44)
- Discarding Link Level Broadcast Packets (chapter 3.10, page 44)
- X.25 PAD (chapter 3.11, page 45)
- Improved Compatibility with SNMP Managers (chapter 3.12, page 45)
- Time Display for `ps` Command (chapter 3.13, page 46)
- New Option `-r` for `rtlookup` (chapter 3.14, page 46)
- Solution to ADSL Modem Problem (chapter 3.15, page 46)

3.1 Bridging and X.25 Availability

With System Software Release 6.2.5, Bridging of IP protocols is available on all X-Generation routers without a software license.

Bridging is one of the easiest ways to connect network segments. A bridge is attached to two or more networks and simply forwards frames between them. The contents of these frames are of no concern to the bridge; frames are forwarded unchanged.

In bridging each bridge makes its own routing decisions and is therefore transparent to the communicating hosts on the end networks. Additionally, a transparent bridge configures itself (in terms of routing information) after coming into service. Because a bridge forwards complete frames between connected networks many different protocols can coexist on either network, the messages are forwarded unchanged (protocol information is passed as raw data in the Ethernet frames). Bridges are used when multiple-protocol packets need to be shared among networks.

For detailed information on Bridging and its configuration, please refer to the **Software Reference**, available from our webserver.

3.2 PPTP Improvements

BinTec's PPTP implementation has been improved to be fully RFC 2637 compliant. This also solves a number of problems that have been verified with earlier versions of our System Software.

3.3 HP OpenView Compatibility

To enhance the compatibility of the BinTec SNMP implementation with HP OpenView, the SNMP behavior of System Software Release 6.2.5 has been changed so as to allow all basic HP OpenView functions. Moreover, the **SysObjectID** has bee changed so that HP OpenView can now correctly identify the different types of BinTec routers.

3.4 Changes in RADIUS Implementation

3.4.1 RIP Update of RADIUS Dial-out Routes

Prior to System Software Release 6.2.5, any change of a RADIUS dial-out IP route was immediately propagated by the RIP (Routing Information Protocol). Since all routes, and not only those that had actually changed were updated up to several thousands of routes were propagated each time, leading to an unnecessary increase in traffic. Now only such routes that have actually changed are updated, and the update of RADIUS dial-out routes takes place together with the cyclical RIP updates which takes place every 30 seconds.

3.4.2 Configurable RADIUS Keepalive

For each RADIUS server in an inactive state, a periodical alive check was conducted. When a server was down for a longer time, this may have caused undesirable costs, if the server was reachable through a dial-up connection only.

A new variable (**radiusServerKeepalive** has been created in the **radiusServerTable**). If switched to enabled (*1*=the default value), the keepalive ping will be sent every 20 seconds, if disabled (*2*), the RADIUS server state will not be set to inactive, and accordingly no keepalive packets will be sent. The keepalive can also be configured through the **Alive Check (if inactive)** field the ***IP*** ➧ ***RADIUS SERVER*** ➧ **EDIT** menu.

3.5 CAPI 1.1 Development Discontinued

For a considerable time, CAPI 2 has now been the CAPI standard most commonly used. Only few applications remain that use – or are able to use – CAPI 1.1. BinTec will, therefore, not continue to develop, maintain or update the CAPI 1.1 implementation of our system software.

3.6 Configurable MTU and MRU Values

If the variable **pppExtIfMtu** in the **pppExtIfTable** is set to any integer other than *0*, the value for the Maximum Transmit Unit (MTU) size negotiated during connection establishment is overwritten once the connection is established. Otherwise the size of the MTU depends on the information the remote partner sends on its MRU (Maximum Receive Unit) size. Where this information is unavailable the MTU is set to a default size of *1500*.

Likewise, a value for the MRU can be configured through the variable **pppExtIfMru**.

Since entries in the **pppExtIfTable** are entirely optional for WAN partner configuration, configuration of the MTU and MRU values may be unavailable for some or even for all interfaces. In these cases LCP negotiation starts with a default MRU value of *1524*.

3.7 Interface Blocked with Inconsistent Encryption Configurations

If encryption is required, but inconsistencies can be found in the configurations of the local and the remote partner, the relevant interface is now set into a blocked state and no connection is established. This is done to prevent outgoing calls over unencrypted connections or continuous dial-up attempts.

The conditions under which an interfaced is blocked are:

- There is no encryption configured by the local partner, but the remote partner requires encryption during connection establishment. As there is no RFC-conform way to terminate the connection in this case, both routers must be BinTec routers for the interface to be blocked.
- Encryption is configured by the local partner, but is rejected by the remote partner during connection establishment. This can be due to inconsistent configurations on both sides.
- There are inconsistencies in the local configuration, i.e. encryption is set to DES or Blowfish even though there is no valid VPN license, or the encryption chosen is incompatible with the PPP authentication methods configured. Again, both routers have to be BinTec routers for the reasons described above.

The following tables show which combinations of authentication and encryption methods, encryption method and VPN license availability, and encryption methods are possible and which lead to a blocking of the interface.

The first table displays which encryption and which authentication methods can be combined. If a combination is not possible, this means that it cannot be chosen in the Setup Tool:

	PAP	CHAP	MS-CHAP V1	MS-CHAP V2
MPPE V1/V2 40	x	x	x	x
MPPE V1/V2 56	x	x	x	x
MPPE V1/V2 128	-	-	x	x
DES 56	-	x	x	x
Blowfish 56	-	x	x	x
3DES 168	-	x	x	x
Blowfish 168	-	x	x	x

Table 3-1: Combinations of authentication and encryption methods ("x"=possible, "-"=not possible)

Note that PAP authentication is compatible only with MPPE (either version 1 or 2) and key length of 40 and 56 bit, and that CHAP is incompatible with MPPE (either version 1 or 2) and a key length of 128 bit.

The next table displays possible and impossible combinations of encryption methods and the availability of a valid VPN license. Again, impossible combinations cannot be configured in the Setup Tool:

	no VPN (PPTP) License	valid VPN (PPTP) License
MPPE V1/V2 40	x	x
MPPE V1/V2 56	x	x
MPPE V1/V2 128	x	x
DES 56	-	x
Blowfish 56	-	x
3DES 168	-	x
Blowfish 168	-	x

Table 3-2: Combinations of VPN license availability and encryption ("x"=possible, "-"=not possible)

The next set of tables displays the conditions under which a connection is either established or blocked.

The first table displays the combinations of MPPE V1 and other encryption methods:

	MPPE V1 40	MPPE V1 56	MPPE V1 128
MPPE V1 40	x	b	b

	MPPE V1 40	MPPE V1 56	MPPE V1 128
MPPE V1 56	b	x	b
MPPE V1 128	b	b	x
MPPE V2 40	MPPE V2 40	b	b
MPPE V2 56	b	MPPE V2 56	b
MPPE V2 128	b	b	MPPE V2128
DES 56	b	b	b
3DES 168	b	b	b
Blowfish 56	b	b	b
Blowfish 168	b	b	b

Table 3-3: Combinations of MPPE V1 encryption and all other encryption methods ("x"=ok, "b"=interface blocked)

In general, the same encryption method should be chosen on both sides. Almost any inconsistency leads to the interface being blocked – with the only exception that if MPPE version 1 is configured on one side and MPPE version 2 on the other, MPPE version 2 is chosen during negotiation and the connection is established.

The next table displays the combinations of MPPE V2 and other encryption methods:

	MPPE V2 40	MPPE V2 56	MPPE V2 128
MPPE V1 40	MPPE V2 40	b	b
MPPE V1 56	b	MPPE V2 56	b
MPPE V1 128	b	b	MPPE V2 128
MPPE V2 40	x	b	b
MPPE V2 56	b	x	b

	MPPE V2 40	MPPE V2 56	MPPE V2 128
MPPE V2 128	b	b	x
DES 56	b	b	b
3DES 168	b	b	b
Blowfish 56	b	b	b
Blowfish 168	b	b	b

Table 3-4: Combinations of MPPE V2 Encryption and all other encryption methods ("x"=ok, "b"=interface blocked)

The last table displays the combinations of encryption methods other than MPPE:

	DES 56	3DES 168	Blowfish 56	Blowfish 168
MPPE V1 40	b	b	b	b
MPPE V1 56	b	b	b	b
MPPE V1 128	b	b	b	b
MPPE V2 40	b	b	b	b
MPPE V2 56	b	b	b	b
MPPE V2 128	b	b	b	b
DES 56	x	b	b	b
3DES 168	b	x	b	b
Blowfish 56	b	b	x	b
Blowfish 168	b	b	b	x

Table 3-5: Combinations of non-MPPE encryption and all other encryption methods ("x"=ok, "b"=blocked)

3.8 Interdependent Configuration of PPP Encapsulation, Encryption and Compression

To avoid inconsistent configurations when using the Setup Tool, the choices available for encryption and compression in the ***WAN PARTNER*** ➧ **EDIT** menu are now reduced according to previous choices. Combinations that would not be available are no longer shown in the Setup Tool.

3.9 New Activity Monitor Password

With System Software Release 6.2.5, a password for the **Activity Monitor** has been introduced. It is needed to set any interface of a monitored router into an up or down state respectively. As long as no Activity Monitor password is configured on your router, you need the admin password to do so.

The Activity Monitor password is configured in ***SYSTEM*** ➧ ***PASSWORD SETTINGS***. Enter a password of your choice in the **Activity Montor Password** field, then confirm with **SAVE** twice to return to the main menu.

3.10 Discarding Link Level Broadcast Packets

According to RFC 1812 link level broadcast packets must be discarded if they are not directed towards an IP multicast address. With System Software Release 6.2.5, BinTec routers follow this recommendation. This also fixes a problem that occurred when IP routing was configured on two Ethernet interfaces and bridging was then enabled on these interfaces. The router rebooted at the arrival of the first IP broadcast packet. Since link level broadcast packets are now discarded, this will no longer happen.

3.11 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.

3.12 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 6.2.5 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*.

3.13 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.

3.14 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.

3.15 Solution to ADSL Modem Problem

Alcatel's implementation of PPTP/GRE (Point-to-Point Tunnelling Protocol/Generic Routing Encapsulation) can lead to incorrect "acknowledgment 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 time-out. Otherwise attempts to restore the connection to the opposite Alcatel station could fail.

4 Bugfixes

Since System Software Release 6.2.5 is a release for all routers of the BRICK-Generation, the problems and their solution described here do not relate to a single router type or to a certain system software release only.

The following problems have been solved:

- RADIUS Issues Solved (chapter 4.1, page 48)
- PPTP: Memory Leakage Removed (chapter 4.2, page 50)
- PPPoE: Memory Leakage Removed (chapter 4.3, page 50)
- PPPoE Credits (chapter 4.4, page 50)
- Multilink PPP with Cisco 4500 (chapter 4.5, page 51)
- Calculation of MRU Size for PPP Interfaces (chapter 4.6, page 51)
- Data Transfer with DES or Blowfish Encryption (chapter 4.7, page 52)
- MPP Encryption with Windows NT/2000 (chapter 4.8, page 52)
- Portscan on Port 1723 (chapter 4.9, page 52)
- ICMP Fragment Unreachable Messages (chapter 4.10, page 53)
- RFC Compliance with CHAP Reauthentication (chapter 4.11, page 53)
- DDI Called Party Numbers (chapter 4.12, page 54)
- Second Logical Channel with X.25 and CAPI (chapter 4.13, page 54)
- Removed Memory Leakage with DNS Requests (chapter 4.14, page 54)
- DHCP: Stacktrace after Reboot (chapter 4.15, page 55)
- Error "dl_look: len 0" (chapter 4.16, page 55)
- Full RIP V2 Multicast Support on Ethernet Interfaces (chapter 4.17, page 55)
- Bridging Fully Functional (chapter 4.18, page 56)

4.1 Radius Issues Solved

Several problems of the RADIUS implementation have been solved in System Software Release 6.2.5.

4.1.1 Temporary Entries in pppExtIfTable Become Static

If a configuration was saved while there were active (temporary) RADIUS interfaces, these were saved as static entries. Upon a reboot these entries were handled as presets and several problems could occur. Thus false numbers may have been dialed with enabled callback, or the false information was requested from the RADIUS server.

This problem has been solved. Now the following tables are checked for interface numbers that are associated with temporary RADIUS interfaces:

- **ifEntryTable**
- **ipExtIfEntryTable**

- **ipRouteEntryTable**
- **ipExtRtEntryTable**
- **ipExtRtEntryTable**
- **ospfIfEntryTable**
- **pppExtIfEntryTable**
- **biboPPPEntryTable**
- **biboDialEntryTable**
- **pppExtIfEntryTable**
- **ipNatPresetEntryTable**
- **ipQoSEntryTable**
- **qosIfEntryTable**
- **qosPolicyEntryTable**

No data found in these tables will be saved for interfaces with index numbers associated with RADIUS.

4.1.2 Missing RADIUS Attribute Now Transmitted

With a BinTec router used for RADIUS accounting, the *Framed-IP-Address* attribute was missing in the Accounting Start Packet if the IP address was assigned from a local IP address pool by the router. Some service providers, however, need this information for accurate accounting.

This problem has been solved, the *Framed-IP-Address* attribute is now transmitted.

4.1.3 Wrong Calculation of RADIUS Dial-out Reload Interval

The **radiusServerReloadInterval** variable was defined as a duration in minutes, but was handled as a value for seconds.

This problem has been solved, the value of the variable is now interpreted as being in minutes.

4.2 PPTP: Memory Leakage Removed

If an ADSL connection attempt via PPTP failed permanently, and if the interface was configured as a flatrate interface (i.e. with **Short Hold** *-1*), 88 bytes of memory were lost with each failure.

This problem has been solved.

4.3 PPPoE: Memory Leakage Removed

If an ADSL-over-PPPoE connection failed and if the interface was configured as a flatrate interface (i.e. with **Short Hold** *-1*), 88 bytes of memory were lost with each failure.

This problem has been solved.

4.4 PPPoE Credits

If no PPPoE service name was specified in the ***WAN PARTNER*** ➧ **EDIT** ➧ ***ADVANCED SETTINGS*** ➧ ***EXTENDED INTERFACE SETTINGS (OPTIONAL)*** menu, the PPPoE credits did not work. The values for the **pppoeCreditTotalOutCon** and

the **pppoeTotalOutDuration** variables in the **pppoeCreditsTable** were not updated. Therefore, the credits control did not work.

This problem has been solved, the credit counters are now updated correctly.

4.5 Multilink PPP with Cisco 4500

No channel bundling was possible when using a Cisco 4500 for dial-in to a BinTec router with inband authentication. This was due to a faulty implementation of the LCP (Link Control Protocol) negotiation routine. It lead to configuration rejects concerning the Multilink Endpoint Discriminator (used for Always On/Dynamic ISDN). The same option was sent again with the next LCP configure request, so that the LCP layer was never established.

This problem has been solved, the Multilink Endpoint Discriminator is sent only if requested by the remote partner.

4.6 Calculation of MRU Size for PPP Interfaces

The MTU size of PPP dial-up interfaces was miscalculated when encapsulation was set to *PPP*, *Async PPP over X.75* or *Async PPP over X.75/T.70/BTX*, as well as for all layer 1 protocols except *PPPoE*, *PPTP PNS* and *PPP over PPTP.* This was due to a erroneous calculation of the received remote MRU/MRRU to the value of *-4.* This may have caused unnecessary fragmentation of packets.

This problem has been solved, and the MRU/MRRU size value received from the remote partner will be interpreted correctly, so that the MTU size can be determined adequately.

4.7 Data Transfer with DES or Blowfish Encryption

After a packet had been lost, the resynchronisation of interfaces configured to use either DES or Blowfish encryption failed if the next packet received had a sequence number greater than 4095. Accordingly, no date could be transferred.

This problem has been solved, the sequence number of the next packet will now be calculated correctly.

4.8 MPP Encryption with Windows NT/2000

When encryption was set to MPPE (any key length) and authentication to MS-CHAP version 2, a PC running Windows NT or Windows 2000 was unable to access the LAN. This behavior was created by a faulty implementation (due to the CBCP protocol provided by Microsoft) which caused a wrong calculation of the initial encryption keys on connections between a BinTec router and a Windows PC.

This problem has been solved, the implementation was corrected and keys are calculated correctly now.

4.9 Portscan on Port 1723

If there was a port scan on port 1723 which is used for tunneling connections (VPN), the router froze if no valid VPN license is available.

This problem has been solved, and the router now ignores scans on port 1723 if no VPN license is enabled.

In general you should consider configuring filters and access rules so as to discard all packets that belong to services which are not used in your network, like e.g. filtering and discarding any VPN packets (or packets directed at the VPN port) when you do not use VPNs.

4.10 ICMP Fragment Unreachable Messages

With a fragment size greater than the MTU value of the destination interface, and the "Don't Fragment Bit" set in the IP header, the packet fragments cannot be delivered and an ICMP Fragment Unreachable message is sent back to the packet originator.

If, however NAT is configured on the destination interface, the NAT procedure is performed before the MTU check, and thus the original source IP address was lost. Accordingly, the ICMP message could not be sent to the fragment originator, which had the effect that the path MTU discovery was impossible.

This problem has been solved, and the original source IP address is now retained.

4.11 RFC Compliance with CHAP Reauthentication

Established PPP connections were terminated by the BinTec router if the remote partner required an additional CHAP (including MS-CHAP) authentication. Since RFC 1994 recommends that CHAP challenges should be sent while a connection is active, this behavior was undesirable.

The problem has been solved, and the PPP authentication routine now works in accordance with RFC 1994.

4.12 DDI Called Party Numbers

Some CAPI applications did not receive the DDI (Direct Dial In) called party number information, making it impossible to assign incoming calls to specific CAPI users. This problem was due to an unwanted reaction to a Listen request sent by the application.

This problem has been solved, the DDI information is now transmitted properly.

4.13 Second Logical Channel with X.25 and CAPI

When a CAPI application using the X.25 protocol tried to open more than one logical channel, the connection was refused.

The problem has been solved, it is now possible for CAPI applications to open more than one logical channel.

4.14 Removed Memory Leakage with DNS Requests

Each time a DNS request was successfully answered (either positively or negatively), the reference number of the relevant MIB was increased, consuming memory.

This problem has been solved.

4.15 DHCP: Stacktrace After Reboot

With a BinTec router acting as DHCP server certain actions or situations could cause either a stacktrace or a freeze.

These problems have been solved, and IP address requests are now handled properly after a reboot.

4.16 Error `dl_look: len 0`

Under certain conditions the router froze, printing the error message `dl_look len:0` to the serial console. This behavior was due to incorrect handling of receive-buffer-too-small conditions.

The problem has been solved, the mentioned conditions will now be handled properly.

4.17 Full RIP V2 Multicast Support on Ethernet Interfaces

The **ipExtIfRipSend** variable could not be set to *ripV2mcast* with the Setup Tool. With System Software Release 6.2.5 it is possible to set the **RIP Send** field in the ***Ethernet*** ➧ ***Advanced Settings*** menu to *RIP V2 multicast*.

Moreover, RIP V2 messages were sent to the IP address 224.0.0.9 in compliance with RFCs 1388 and 1723 when RIP V2 Multicast was enabled, but they were sent as MAC broadcast instead of Link Level multicast packets. System Software Release 6.2.5 now complies with RFC 1812 and forwards IP multicast packets as Link Level multicasts.

4.18 Bridging Fully Functional

On some routers bridging was not possible, even if covered by the available licenses.

This problem has been solved, and bridging is now fully functional.

4.19 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.

4.20 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.

4.21 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.

4.22 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.

4.23 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.

4.24 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.

4.25 Compatibility between System Software Release 6.2.5 and Older Software

It was not possible to change back to an older release after carrying out an update to System Software Release 6.2.5.

This problem was caused by the write protection of System Software Release 6.2.5. 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.

4.26 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.

5 Known Issues

A number of errors still persists in System Software Release 6.2.5. 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:

- PAP Authentication with an ACE RADIUS Server (chapter 5.1, page 59)
- Windows 2000 128 Bit MPPE (chapter 5.2, page 59)

5.1 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.

5.2 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.

5 Known Issues