Corporate Access

BIANCA/BRICK XL2/XMP

Workgroup Access

BIANCA/BRICK XS2/XM2

Personal Access

BINGO!

Release Notes

System Software Release 5.2 Revision 1

September, 2000

New System Software

Release 5. 2 Revision 1

These release notes describe the new features, changes, bugfixes and known issues contained in system software Release 5. 2 Revision 1 for the following products: BIANCA/BRICK-XL, BIANCA/BRICK-XL 2, BIANCA/BRICK-XMP, BIANCA/BRICK-XS2, BIANCA/BRICK-XM2, BINGO!).

1 Upgrading System Software

- Retrieve the current system software image from BinTec's WWW server at http://www.bintec.de (Section: Download).
- With this image you can upgrade the BIANCA/BRICK with the `update` command from the SNMP shell via a remote host (i.e. using telnet, minipad, or isdnlogin) or by using the BOOTmonitor, if you are logged in directly on the console.
  Information on using the BOOTmonitor can be found in the BIANCA/BRICK User's Guides under Firmware Upgrades.

Caution!

- Do not update your Logic or BOOTmonitor images unless expressly instructed to do so.
  Normally, it is not necessary to upgrade these images. Only in exceptional cases is an upgrade explicitly recommended.
- If you are unsure whether to upgrade or not, read the BOOTmonitor and Firmware Logic Release Notes (available below the images on the FTP server, section: Download) where you will find tables that specify the appropriate Logic and BOOTmonitor versions available for your BinTec product, and if an update is recommended or not.

Please note that there is an update procedure in case there is not enough memory available to perform a software update via the `update` command from the SNMP shell. The incremental update loads the new software image in blocks of 64 KB via TFTP and writes it to the Flash ROM immediately.

Because this procedure offers no possibility to check the integrity of the image:

- first use the option "-v" that verifies the image file.

When upgrading system software, it is also recommended that you use the most current versions of BRICKware for Windows and UNIX Tools. Both can be retrieved from BinTec's WWW server.

If you are updating from a software release equal to or older than 4.7.x to the current version, 5..2.1 or later, it is necessary to firstly upgrade to 4.9.3, save the configuration, then upgrade to 5.2.1. If you update directly from 4.7.x to 5.2.x, the old IP access lists can not be automatically converted and are lost.

2 Features

2.1 ADSL Connection via PPPoE

2.1.1 Introduction

BinTec Communications AG offers the PPP-over-Ethernet protocol to enable networked terminals access to the Internet over the T-DSL connection of the Deutsche Telekom AG.

Why use a BinTec router for T-DSL access?

The use of a Bintec router on a T-DSL connection is of particular benefit when you have one or more of the following requirements:

- LAN / WAN:
  - You want to connect an entire LAN via T-DSL to the Internet and not just one workstation.
  - In addition to T-DSL Internet access, you also need other WAN connections (e.g. Modem dial-in, ISDN-Intranet connection etc.).
- Security:

This point relates only to BinTec routers that have two Ethernet interfaces. The security advantages listed below that can be enjoyed by users of products with two Ethernet interfaces can not be shared by users of products with just one Ethernet interface. Indeed, the use of PPPoE over one Ethernet interface presents several disadvantages you should be aware of, see "Two Ethernet interfaces or one?", page 13.

  - The customer´s network should be protected from unauthorised access from the Internet.

  - The Internet should be made strictly inaccessable to unauthorised individuals from the customer´s network.

- Accounting:
  - Online time: the number of connections and transmission volumes for IP traffic should be recorded in detail.
  - Superfluous load connections (such as broadcasts) should be prevented.

This last point relates only to BinTec routers that have two Ethernet interfaces. The use of PPPoE over one Ethernet interface presents several disadvantages you should be aware of, see chapter 2.1.3, page 25.

- Platforms:
  - Workstations running operating systems for which the PPPoE protocol is not available should be connected (e.g. OS/2, Linux, Windows 3.x etc.)
- Backup:
  - A high degree of availability should be guaranteed; should the T-DSL access fail, an alternative path should be activated.
- Services:
  - In addition to T-DSL Internet access, other communications services are required network-wide (e.g. Fax, Eurofiletransfer etc.).
- Configuration:
  - Access should be configured and administrated from a central site or by an external service provider.

Furthermore, you would like to continue to benefit from the full range of functions available with your BinTec multiprotocol router.

A brief introduction to T-DSL

With T-DSL Deutsche Telekom AG is offering high-speed Internet access. The underlying technology is ADSL. Large amounts of data can be asymetrically

transmitted over conventional, copper telephone lines by ADSL (Asymmetric Digital Subscriber Line). The T-DSL packet consists of an ISDN connection and a data line with a bandwidth of up to 768 kbps from the Internet Service Provider to the customer (downstream) and 128 kbps in the opposite direction (upstream). This bandwidth capacity provides downstream Internet services availability at speeds of up to twelve times faster than with ISDN.

The T-DSL connection (without a BinTec router) looks like this:

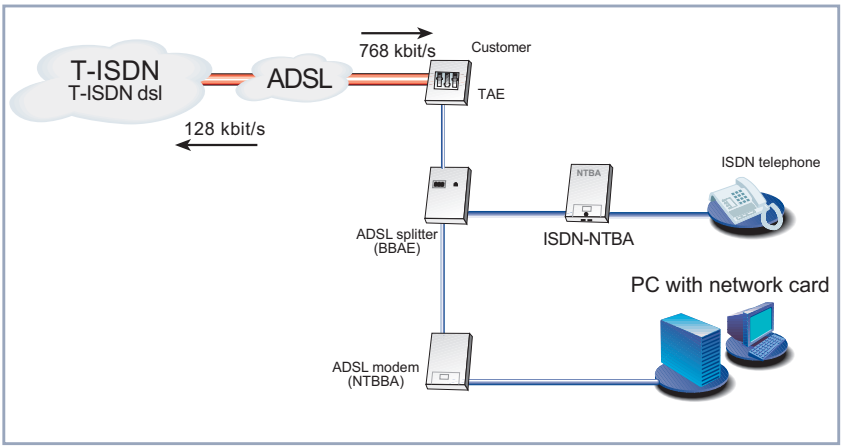

Figure 2-1: T-DSL connection (without BinTec router)

Two Ethernet interfaces or one?

To be able to use ADSL (Asymmetric Digital Subscriber Line) with a BinTec router, you must configure a PPP-over-Ethernet interface over the LAN interface. This is done by connecting your BinTec router to T-DSL, which is the ADSL connection of Deutsche Telekom AG. It is possible to avail of the services of ADSL by connecting a BinTec router to two Ethernet interfaces or to just one, depending on how your router is equipped.

The use of PPPoE over one Ethernet interface presents several disadvantages you should be aware of, see chapter 2.1.3, page 25.

At the time of writing, BinTec Communications AG has three routers fitted or with the potential to be fitted with two Ethernet interfaces: XM-PPPoE, XM2 and XL2 (this list will be quickly outdated as new modular devices supplement the product range). All other BinTec routers addressed in this release (BinGO!, XS2, XS-Office, XMP) are only capable of connecting to the ADSL modem and to the LAN using just the one Ethernet interface.

2.1.2 Using T-DSL with BinTec routers with two Ethernet Interfaces

BinTec Communications AG recommends using a BinTec router with 2 Ethernet interfaces for your ADSL connection: one back to the LAN, the other to the ADSL connection. When using 2 Ethernet interfaces, all the advantages mentioned in chapter 2.1.3, page 25 can be enjoyed without exception or restriction.

Scenario: Internet access for several PCs

In order to give your Local Area Network cheap and fast access to the Internet, your BinTec router is connected to the Ethernet between the PCs and the ADSL modem:

If you receive a special cable from Deutsche Telekom AG for connecting the ADSL modem, please use only this cable.

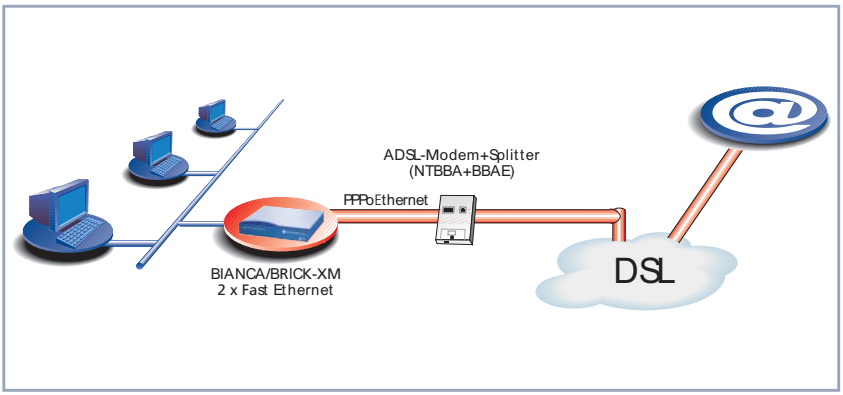

Figure 2-2: Scenario 1: Internet access for several PCs

Scenario: Connecting to a second location

In order to give your Local Area Network cheap and fast access to the Internet, as well as to a second remote location, your BinTec router is connected to the Ethernet between the PCs and the NTBBA (ADSL network termination):

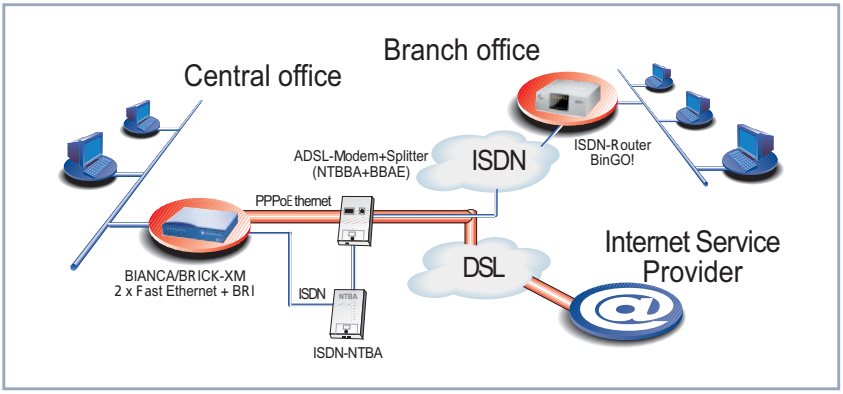

Figure 2-3: T-DSL connection and ISDN LAN-LAN connection

Scenario: Connecting with fax servers

In order to give your Local Area Network cheap and fast access to the Internet, as well as simultaneous use of the ISDN connection for professional fax services, the BinTec router is fitted with two Fast Ethernet modules and a 2XBRI-module:

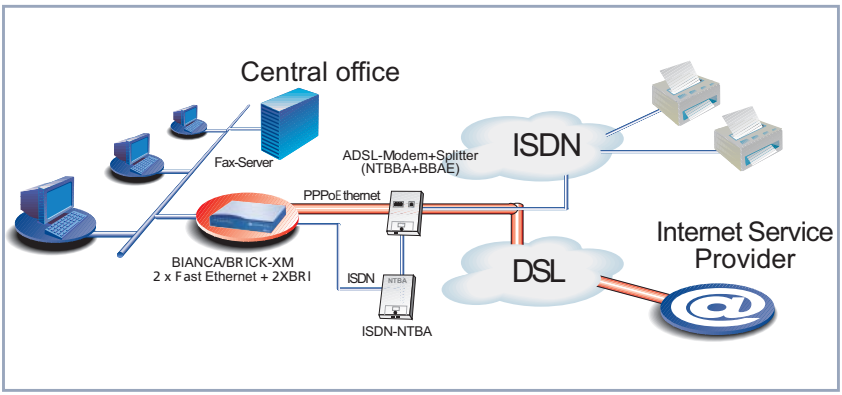

Figure 2-4: Connecting with fax servers

Hardware connections on the XM-PPPoE to T-DSL

When connecting a LAN, WAN or ADSL connection to the XM-PPPoE for example, the following slot assignments should be observed:

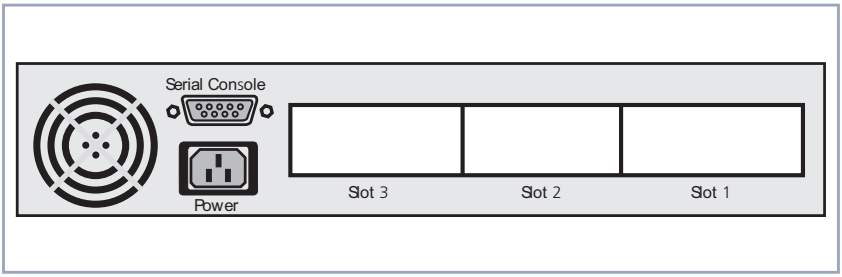

Figure 2-5: Slot assignments to the XM-PPPoE

Slot	Module/Function
Slot 1	Ethernet (to the LAN)
Slot 2	Ethernet (to the ADSL)
Slot 3	S_0 or another module (optional)

Table 2-A-1: Slot assignments to the Xm-PPPoE

Configuration

After entering `setup` from the shell prompt, Setup Tool's main menu is displayed as below. Depending on your hardware setup and software configuration, your router's menu may differ slightly.

```
BRICK Setup Tool                                BinTec Communications AG
                                                                MyBrick


Licences                  System

Slot1:                    CM-BNC/TP, Ethernet
Slot2:                    CM-BNC/TP, Ethernet

Slot3:                    CM-1BRI, ISDN S0

WAN Partner
IP  PPP IPX     X.25      VPN

Configuration Management
Monitoring and Debugging
Exit


Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to
enter
```

Configuring IP Addresses

➤ Go to ***SLOT 1*** (Ethernet)

.

```
BRICK Setup Tool                              BinTec Communications AG
[SLOT 1 ETHERNET]: Configure Ethernet Interface                MyBrick


            IP-Configuration
                local IP-Number      192.168.1.254
                local Netmask        255.255.255.0
                Encapsulation        Ethernet II

            IPX-Configuration
                local IPX-NetNumber  0
                Encapsulation        none

            Bridging                 disabled

            Advanced Settings>

                SAVE                 CANCEL

Enter IP address (a.b.c.d or resolvable hostname)
```

Field	Meaning
local IP-Number	Enter the LAN IP address of your BinTec router here. This address should be the default gateway for the hosts in your LAN.
local Netmask	Enter the netmask for your LAN here.

Table 2-A-2: Slot 1 Ethernet

General PPP Settings

Here you must configure an interface over which PPP-over-Ethernet should run. All other settings can be left as they are.

➤ From the main menu, go to ***PPP***.

```
BRICK Setup Tool                                BinTec Communications AG
[PPP]: PPP Profile Configuration                                MyBrick



Authentication Protocol                 CHAP + PAP + MS-CHAP
Radius Server Authentication            inband

PPP Link Quality Monitoring             no

PPPoE Ethernet Interface                en2


                  SAVE                        CANCEL

Use <Space> to select
```

The following field is relevant:

Field	Meaning
PPPoE Ethernet Interface	This field defines the interface over which PPP-over-Ethernet runs.

Table 2-A-3: ***PPP***

WAN Partner Settings

The configuration of a PPP-over-Ethernet partner is exactly the same as the configuration of any other WAN partner.

➤ Go to ***WAN PARTNER*** ➧ ***ADD***.

```
BRICK Setup Tool                                BinTec Communications AG
[WAN][ADD]: Configure WAN Partner                                MyBrick

Partner Name                          t-online

Encapsulation                         PPP
Compression                           none
Encryption                            none
Calling Line Identification           no

PPP>
Advanced Settings>
WAN Numbers>

IP>
IPX>
Bridge>

                SAVE                        CANCEL

Enter string, max length = 25 chars
```

These are the relevant fields:

Field	Meaning
Partner Name	The name assigned to this PPP-over-Ethernet partner.
Encapsulation	Defines how data packets are encapsulated for transmission to the WAN partner. For the purpose of PPP-over-Ethernet, only *PPP* should be selected.

Table 2-A-4: ***WAN PARTNER*** ➧ ***ADD***

PPP Submenu Settings

➤ Go to ***PPP***.

```
BRICK Setup Tool                                BinTec Communications AG
[WAN][ADD][PPP]: PPP Settings (t-online)                          MyBrick


Authentication                PAP
Partner PPP ID
Local PPP ID                  000460004256091169386#0001@t-online.de
PPP Password                  1234567

Keepalives                    on
Link Quality Monitoring       off


                     OK                          CANCEL

Use <Space> to select
```

These are the relevant fields:

Field	Meaning
Authentication	PAP. The default value CHAP + PAP must be changed.
Partner PPP ID	WAN-Partners ID. Leave blank.
Local PPP ID	Your T-Online User-ID. This is how the ID is constructed: <Code><T-Online-Nr.>#<Other user-Nr.>@t-online.de. Code = a 12-digit connection code (e.g.: ***000460004256***) T-Online-Nr. = Telephone number (e.g.: ***091169386***) Other user-Nr. = a four-digit other user number (e.g.: ***0001***)
PPP Password	Your T-Online password.
Keepalives	Activates keepalive packets.

Table 2-A-5: ***WAN*** ➧ ***ADD*** ➧ ***PPP***

➤ Set **Keepalives** to *on*.
When the keepalive function is active, the status of the interface is checked. If the connection to the Provider fails, this feature quickly recognises and signals the altered status of the interface.

Advanced Settings

➤ Return to ***ADVANCED SETTINGS***.
You can define the Layer 1 Protocol of the ISDN B channel the BinTec router should use for connections to the WAN partner. The protocol for ISDN data connections, standard value for the B-channel, is preconfigured. For PPP-over-Ethernet, this setting must be changed.

```
BRICK Setup Tool                                BinTec Communications AG
[WAN][ADD][ADVANCED]: Advanced Settings (t-online)             MyBrick


Callback                                    no
Static Short Hold (sec)                     20
Idle for Dynamic Short Hold (%)             0
Delay after Connection Failure (sec)        300

Extended Interface Settings (optional)<

Channel-Bundling                            no

Layer 1 Protocol                            PPP over Ethernet (PPPoE)



                     OK                     CANCEL

Use <Space> to select
```

➤ In the field **Layer 1 Protocol**, select *PPP over Ethernet (PPPoE)*.

IP Settings

➤ Return to ***IP***.

```
BRICK Setup Tool                              BinTec Communications AG
[WAN][ADD][IP]: IP Confuguration (t-online)                    MyBrick

IP Transit Network               dynamic client

local IP Address


Advanced Settings>
                SAVE                CANCEL
```

The following field is relevant here:

Field	Meaning
IP Transit Network	Defines whether the BinTec router is to establish a Transit Network to the WAN partner. IP address is dynamically assigned if *dynamic client* is selected.

Table 2-A-6: ***WAN*** ➧ ***ADD*** ➧ ***IP***

- Set **IP Transit Network** to *dynamic client*.
- The **local IP Address** field remains blank.

General IP Settings

Configuring the default route

- Go to ***IP*** ➧ ***ROUTING*** ➧ ***ADD***.

```
BRICK Setup Tool                                BinTec Communications AG
[IP][ROUTING][ADD]: IP Routing                                    MyBrick


Route Type                    Default route
Network                       WAN without transit network

Partner / Interface           t-online

Metric                        1

                SAVE                CANCEL

Use <Space> to select
```

The following field is relevant here:

Field	Meaning
Partner / Interface	Ihr PPPoE Partner.

Table 2-A-7: ***IP*** ➧ ***ROUTING*** ➧ ***ADD***

- In the **Route Type** field, select *Default route*.
- In the field **Partner / Interface**, select *PPPoEPartner*, e. g. ***t-online***.

Activate Network Address Translation (NAT)

This results in the following:

- your network can not be accessed from the Internet (as long as no session profiles are configured),
- The source address of connections to the Internet only appears as the one dynamically assigned IP address.

- Go to ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.
- Select the WAN interface you want to activate NAT for, e. g. ***t-online***.

```
BRICK Setup Tool                                BinTec Communications AG
[IP][NAT][CONFIG]: NAT Configuration (t-online)                 MyBrick

Network Address Translation                on

Configuration for sessions requested from outside
Service      Destination      Source Dep.  Dest. Dep.   Port Remap


    ADD          DELETE       SAVE         CANCEL
```

The following field is relevant here:

Field	Meaning
Network Address Translation	Here you can activate Network Address Translation (NAT) for your WAN partner. Thereby, you conceal your entire LAN behind the one official IP address.

Table 2-A-8: ***IP*** ➧ ***NAT***

➤ Set **Network Address Translation** to *on*.

2.1.3 Using T-DSL with BinTec routers with one Ethernet Interface

To be able to use ADSL (Asymmetric Digital Subscriber Line) with a BinTec router, you must configure a PPP-over-Ethernet interface over the LAN interface. This is done by connecting your BinTec router to T-DSL, which is the ADSL connection of Deutsche Telekom AG. It is possible to avail of the services of ADSL by connecting a BinTec router to two Ethernet interfaces or to just one, depending on how your router is equipped.

Security risks and restrictions

BinTec Communications AG recommends using a BinTec router with 2 Ethernet interfaces for your ADSL connection. Due to customer demand, however, PPP over Ethernet is also being made available with this release for BinTec routers with just one Ethernet interface.

When using PPP over Ethernet with one Ethernet interface, you should be aware of the following security risks and other disadvantages.

The following restrictions and security risks exist when the BinTec router connection to T-DSL is only over one Ethernet interface:

- If PPP-over-Ethernet is operated with only one Ethernet interface, there is a risk of unauthorized accesses from the Internet to the local BinTec router LAN. Such unauthorized accesses can originate from the first node of the Internet.
- Users of the local network can configure a PPP-over-Ethernet client on their PC and use the Internet unnoticed by the BinTec router.
- Broadcasts in the local LAN are always forwarded by the ADSL modem (NTBBA) to the PTT exchange and are not rejected until the exchange. This means that the maximum bandwidth of 128 kbps upstream to the PTT may not be fully available.

Scenario: ADSL with BinTec routers with one Ethernet Interface

The following scenario (see figure 2-6, page 27) is used to describe the necessary configuration steps: The LAN interface of the BinTec router is connected to your hub, and to the ADSL modem (NTBBA) of Deutsche Telekom AG.

If you receive a special cable from Deutsche Telekom AG for connecting the ADSL modem, please use only this cable.

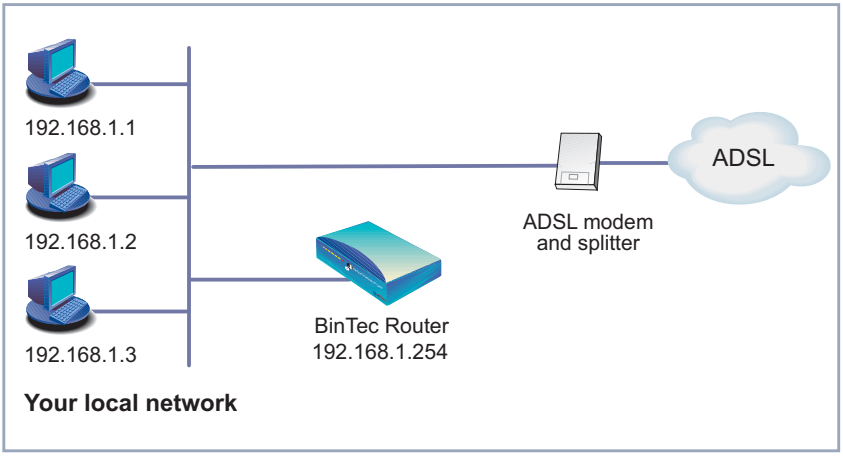

Figure 2-6: Example scenario (with BinTec router)

The following settings are necessary (the Setup Tool menus concerned are described elsewhere):

- Go to ***PPP***.
- Select **PPPoE Ethernet Interface**: *en1*.
- Press **SAVE**.
- Go to ***WAN PARTNER*** ➧ **ADD**.
- Enter your **Partner Name**: e.g. *t-online.*
- Select **Encapsulation**: *PPP.*
- Go to ***WAN PARTNER*** ➧ **ADD** ➧ ***PPP***.
- Enter **Local PPP ID** (= your user name):
  e.g. *00046000425609116938 6#0001@t-online.de.*

The T-Online user name comprises the following elements:

<user account><T-Online number>#<co-user number>@t-online.de

The user account is a 12-digit number, in this case: *000460004256.*

The T-Online number is the extension number, in this case: *091169386.*

The co-user number is a 4-digit number, in this case: *0001.*

The T-Online number and the co-user number must be separated by # if the T-Online number has less than 12 digits.

- Enter **PPP Password** (= your T-Online password).
- Select **Keepalives**: *on.*
- Confirm with **OK**.
- Go to ***WAN Partner*** ➧ **ADD** ➧ ***Advanced Settings***.
- Select **Layer 1 Protocol**: *PPP over Ethernet (PPPoE).*
- Confirm with **OK**.
- Go to ***WAN Partner*** ➧ **ADD** ➧ ***IP***.
- Select **IP Transit Network**: *dynamic client.*
- Press **SAVE**.
- Go to ***IP*** ➧ ***Routing*** ➧ **ADD**
- Select **Route Type**: *Default route.*
- Select **Network**: *WAN without transit network.*
- Select **Partner / Interface**: e.g. *t-online.*
- Enter **Metric**: e.g. *1*.
- Press **SAVE**.
- Go to ***IP*** ➧ ***Network Address Translation***
- Select the PPPoE interface, e.g. **t-online**, and confirm with **Return**.

- Select **Network Address Translation**: *on.*
- Press **SAVE**.

2.1.4 Additional information

If you want to find out more about xDSL and the technologies involved, here are some links you may find useful:

- http://www.heise.de/ct/99/16/120/ is an article in German about T-DSL "Volles Rohr - T-DSL in Theorie und Praxis" by Johannes Endres, Frank Fremerey.
- http://www.adsl.com is the ADSL forum home page.
- http://tdsl.sda.t-online.de is the T-Online Speed home page of Deutsche Telekom AG.

2.2 MS-CHAP Version 2 now Supported

The new Microsoft authentication procedure MS-CHAP V2 included in Windows NT 4.0 Service Pack 4, the post-SP3 hotfix, and Windows 95 Dial-Up Networking 1.3 Upgrade is now supported by Bintec. MS-CHAP V2, the successor to MS-CHAP, is the Microsoft version of CHAP and can be used for PPP authentication between a Windows environment and a BinTec router.

Like MS-CHAP V1, MS-CHAP V2 is not compatible with the standard CHAP protocol.

Authentication via MS-CHAP can now be done over a RADIUS server. Provided the RADIUS server supports the authentication protocol, the addition of new RADIUS attributes allows RADIUS authentication via MS-CHAP V1/V2.

The following Microsoft-specific RADIUS attributes are now supported:

```
- MS_CHAP_RESPONSE (authenticate request)
- MS_CHAP2_RESPONSE (authenticate request)
- MS_CHAP_CHALLENGE (authenticate request)
- MS_CHAP2_SUCCESS (authenticate response)
- MS_CHAP_MPPE_KEYS (authenticate response)
```

2.2.1 Configuration over Setup Tool

The following range of authentication protocols is now available: PAP, CHAP, MS-CHAP V1 and MS-CHAP V2. All of these protocols can be configured singularly or in different combinations in Setup Tool in either of these two menues: **PPP ➧ PPP Profile Configuration** or **WAN ➧ ADD ➧ PPP ➧ PPPSettings**.

```
BinTec router Setup Tool                        BinTec Communications AG
[WAN][ADD][PPP]: PPP Settings (ISP)                              MyBrick


Authentication                  MS-CHAP V2
Partner PPP ID                  myisp
Local PPP ID                    mybintec
PPP Password                    *******

Keepalives                      on
Link Quality Monitoring         off


            OK              CANCEL

Use <Space> to select
```

Table 2-1: PPP Settings

2.2.2 Configuration over the MIB

For all partners identifiable by CLID, MS-CHAP V2 can be configured over the **biboPPPAuthentication** variable in the **biboPPPTable**. And for inband identification and authentication over the **pppProfileAuthProtocol** variable in the **pppProfileTable**.

2.3 New Encryption Protocols Supported

MPPE V2

MPPE V2, the successor to MPPE, is an encryption method designed by Microsoft.

The authentication protocol MPPE Version 2 is now supported by BinTec Communications AG. MPPE V2 can use 40-bit or 56-bit encryption keys.

If the server requires a higher key strength than is supported by a dial-in client, the connection attempt fails. If one side has MPPE V1 configured, MPPE V2 will be accepted in the course of the connection process, providing the key strength is identical.

DES and Blowfish

The encryption protocols DES and blowfish are now supported by BinTec routers. 56-bit key versions of both protocols are licensed features and can be activated only in conjunction with the VPN license.

2.3.1 Configuration over Setup Tool

The following range of encryption methods can now be set over Setup Tool.

Value	Meaning
MPPE 40	MPPE V1 with 40-bit key
MPPE 56	MPPE V1with 56-bit key
MPPE V2 40	MPPE V2 with 40-bit key
MPPE V2 56	MPPE V2 with 56-bit key
Blowfish 56	Blowfish with 56-bit key
DES 56	DES with 56-bit key

Table 2-2: Encryption values in Setup Tool

When using DES or Blowfish, the key can be automatically generated or statically defined. For this purpose, the following menu has been extended:

Field	Meaning
Encryption Key Negotiation	Defines whether an encryption key is to be automatically generated or statically defined. Possible values: ■ *authentication* (default value): the key is automatically generated. ■ *static*: the key is statically defined and entered under **Encryption Key (TX)** or **Encryption Key (RX)**.
Encryption Key (TX)	(only when **Encryption Key Negotiation** = *static*) The key (in hexadecimal format) for the encryption of outgoing data (must match the partner´s **Encryption Key (RX)** entry).
Encryption Key (RX)	(only when **Encryption Key Negotiation** = *static*) The key (in hexadecimal format) for the encryption of incoming data (must match the partner´s **Encryption Key (TX)** entry).

Table 2-3: ***WAN Partner*** ➧ ***ADD*** ➧ ***Advanced Settings*** ➧ ***Extended Interface Settings (optional)***

2.4 Passwords in Setup Tool

From this software release on, passwords will no longer be visible in Setup Tool. Instead, each character of the password will appear as an asterisk. The following password fields are affected.

- **admin Login Password/SNMP Community**
- **read Login Password/SNMP Community**

- **write Login Password/SNMP Community**
- **Radius Server Password**
- **HTTP Server Password**
- **PPP Password**
- **Provider Password**
- **CAPI User Password**
- **PABX User Password**
- **PABX User PIN**
- **TAPIadmin Password**

2.4.1 Changing and Confirming a Password

When a password is changed, each changed character is represented by an asterisk. Once a password has been altered, Setup Tool switches over to change mode. "Change Password" is displayed in the status line, and the first attempt to leave that field fails and initiates confirmation mode. "Confirm Password" is then displayed in the menu line. Once the password has been sucessfuly confirmed, the password is changed. If confirmation fails, the following message is reported: "Password doesn´t match. Try again." and the old password is redisplayed (as asterisks).

2.4.2 Relevant Commands

- Before confirming a changed password, the process can be interrupted by pressing ESC ESC.
- The BACKSPACE key always deletes the entire entry and not just the previous character.
- The SPACEBAR can also be used at the end of the password.

- If Setup Tool is opened with the command `setup -p`, the characters of all passwords are not displayed as asterisks, but as legible entries.

2.5 Filtering of Services in IPX Networks (SAP Filters)

With Release 5.2 Revision 1, one can filter services in IPX networks with SAP filters.

If the number of services in an IPX network is very high, this can lead to various performance problems with WAN links or routers because of the periodic sending of SAP packets. Workstations rarely need to see all the services in a network. So the administrator can now solve these performance problems by configuring SAP filters to reduce the number of services to be learned by the BRICK and to be forwarded to other interfaces.

Filtering of services can be done by:

- interface index
- direction (incoming / outgoing / both)
- service type
- service's network number
- service's network node
- service's socket
- service´s name

It is up to you to decide which criteria to employ by setting the value of the above variables to either *verify* or *dont_verify* (see below). The procedure is similiar to configuring IPX packet filters (described in Software Reference).

2.5.1 The Variables, Values and their Meanings

The following are tabular depictions of the variables, values and meanings of the two new MIB tables **SapDenyTable** and **SapAllowTable**.

Variable	Meaning
sapDenyIfIndexMode	The interface index to be verified or not. Possible values: *verify, dont_verify, delete* Default: *dont_verify*
sapDenyIfIndex	This rule is applied to services originating from or (see **sapDenyDirection**) destined for the interface with this index number. If, in the case of a service known to the BRICK and where the service name is entered, the **IfIndex** is set to *0* and a direction is set to either *incoming* or *outgoing*, all interfaces are affected by the rule. If, however, the service name is used and the **IfIndex** is set to *0*, but NO direction is given, the entry will assume the interface over which that service was learned and direction will be set to *incoming*.
sapDenyDirection	The direction that is to be subject to the rule. Possible values: *incoming, outgoing, both, dont_verify.*
sapDenyTypeMode	The SAP service type to be checked or not. Possible values: *verify, dont_verify.*
sapDenyType	The various SAP service types to be checked. For example: 4: file server 7: print server.
sapDenyNetMode	The network number to be checked or not. Possible values: *verify, dont_verify.*
sapDenyNet	The service´s network number to be checked.
sapDenyNodeMode	The node number to be checked or not. Possible values: *verify, dont_verify.*

Variable	Meaning
sapDenyNode	The service´s node number to be checked.
sapDenySockMode	The socket number to be checked or not. Possible values: *verify, dont_verify.*
sapDenySock	The service´s socket number to be checked.
sapDenyName	Instead of entering Type/Net/Node/Socket directly, you need only fill in the service name here, provided the service has been learned by the BRICK IPX. The values of the Type/Net/ Node/Socket fields contained in the **ipxDestServTable** will then be copied to the **sapDenyTable**.

Table 2-4: **SapDenyTable**

Variable	Meaning
sapAllowIfIndexMode	The interface index to be verified or not. Possible values: *verify, dont_verify, delete* Default: *dont_verify*
sapAllowIfIndex	This rule is applied to services originating and/ or (see **sapDenyDirection**) destined for the interface with this index number. If, in the case of a service known to the BRICK and where the service name is entered, the **IfIndex** is set to *0* and a direction is set to either *incoming* or *outgoing*, all interfaces are affected by the rule. If, however, the service name is used and the **IfIndex** is set to *0*, but NO direction is given, the entry will assume the interface over which that service was learned and direction will be set to *incoming*.
sapAllowDirection	The direction that is to be subject to the rule. Possible values: *incoming, outgoing, both, dont_verify.*
sapAllowTypeMode	The SAP service type to be checked or not. Possible values: *verify, dont_verify.*
sapAllowType	The various SAP service types to be checked. For example: 4: file server 7: print server.
sapAllowNetMode	The network number to be checked or not. Possible values: *verify, dont_verify.*
sapAllowNet	The service´s network number to be checked.
sapAllowNodeMode	The node number to be checked or not. Possible values: *verify, dont_verify.*

Variable	Meaning
sapAllowNode	The service´s node number to be checked.
sapAllowSockMode	The socket number to be checked or not. Possible values: *verify, dont_verify.*
sapAllowSock	The service´s socket number to be checked.
sapAllowName	Instead of entering Type/Net/Node/Socket directly, you need only fill in the service name here, provided the service has been learned by the BRICK IPX. The values of the Type/Net/Node/Socket fields contained in the **ipxDestServTable** will then be copied to the **sapAllowTable**.

Table 2-5: **SapAllowTable**

2.5.2 Examples

In order to create SAP filters for the services of a file server, entries must be made in the **sapDenyTable** and/or in the **sapAllowTable**: in the first, to specify the services to be prevented from being learned or propagated; and in the second, to specify those to be allowed to be learned or propagated.

To block or allow a single service the administrator has to look up type, net, node and socket in the **IpxDestServTable** or at the server's console. Then these values can be used to create an entry in the **sapDenyTable** or **sapAllowTable**.

A service *x* is allowed to enter or leave the BRICK if:

1. it matches an entry in the **sapAllowTable** and there is no matching entry in the **sapDenyTable**,
2. there is no entry in the **sapAllowTable** and no matching entry in the **sapDenyTable**,
3. there is no entry in either table.

A service *y* is denied entry to or exit from the BRICK if:

1. it matches an entry in the **sapDenyTable**,
2. there is no entry in the **sapDenyTable** and no matching entry in the **sapAllowTable**..

Let´s have a look at some of the various configuration scenarios:

- You could specify only those services you wish to allow the BRICK to propagate over one particular interface; all other services are prevented from being propagated over that interface. This would be done by making outgoing entries in the **sapAllowTable** over the interface 10001, for example:

```
brick:sapAllowTable
inx   IfIndexMode(-rw)  IfIndex(*rw)   Direction(rw)TypeMode(rw
      Type(rw)          NetMode(rw)    Net(rw)      NodeMode(rw)
      Node(rw)          SockMode(rw)   Sock(rw)     Name(rw)

brick:sapAllowTable>  IfIndexMode=verify  ifindex=10001  direc-
tion=outgoing     typemode=verify     type=0:4     netmode=verify
net=172:36:10:62
00: sapAllowIfIndex.0(rw):       10001
00: sapAllowDirection.0(rw):     outgoing
00: sapAllowTypeMode.0(rw):      verify
00: sapAllowType.0(rw):          0:4
00: sapAllowNetMode.0(rw):       verify
00: sapAllowNet.0(rw):           172:36:10:62

brick:sapAllowTable> sapAllowTable
inx   IfIndexMode(-rw)  IfIndex(*rw)   Direction(rw)TypeMode(rw
      Type(rw)          NetMode(rw)    Net(rw)      NodeMode(rw)
      Node(rw)          SockMode(rw)   Sock(rw)     Name(rw)

      verify            10001          outgoing     verify
      0:4               verify         172:36:10:62dont_verify
                        dont_verify
brick:sapAllowTable
```

- You could, of course, specify only those services you wish to prohibit the BRICK to propagate; all others are propagated. This would be done by making outgoing entries in the **sapDenyTable**. In this case, as the service

is known to the BRICK, it is sufficient to merely enter the name of the service, the direction and the interface, the rest (Type/Net/Node/Socket) will be read from the **ipxDestServTable**. In the following example where the BRICK has already learned the service and the service name is being used and index=0 and direction=outgoing, all interfaces are affected:

```
brick:sapDenyTable
inx   IfIndexMode(-rw)  IfIndex(*rw)   Direction(rw)TypeMode(rw
      Type(rw)          NetMode(rw)    Net(rw)     NodeMode(rw)
      Node(rw)          SockMode(rw)   Sock(rw)    Name(rw)

brick:sapDenyTable> ifindex=0 direction=outgoing name=FILESERVER
00: sapDenyIfIndex.0(rw):        0
00: sapDenyDirection.0(rw):      outgoing
00: sapAllowTypeMode.0(rw):      FILESERVER
brick:sapDenyTable> sapDenyTable>
inx   IfIndexMode(-rw)  IfIndex(*rw)   Direction(rw)TypeMode(rw
      Type(rw)          NetMode(rw)    Net(rw)     NodeMode(rw)
      Node(rw)          SockMode(rw)   Sock(rw)    Name(rw)

      dont_verify       0              outgoing    verify
      0:4               verify         aa:bb:cc:dd verify
      0:0:0:0:0:1       verify         40:00       FILESERVER
```

Now the service known as FILESERVER will not be propagated over any interface.

- Alternatively, you could specify those services you wish to prohibit from being learned by the BRICK; all other services are learned and propagated. This would be done by making incoming entries in the **sapDenyTable**.
- You could specify only those services you wish to allow the BRICK to learn; all others are denied access. This would be done by making incoming entries in the **sapAllowTable**.
- Finally, it is possible to make entries in both tables. In this case, you would explicitly specify which services are to be denied and which are to be allowed. This would involve either incoming or outgoing entries in both tables.

2.6 Name Resolution with DNS Proxy

2.6.1 Why Name Resolution?

IP address = ?

Name resolution is necessary for converting host names in a LAN or on the Internet into IP addresses. For example, if you would like to reach the host "Goofy" in your LAN or enter the URL "http://www.bintec.de" in your Internet browser, you need the associated IP address before you can set up the required connection. The following options are available:

- DNS (Domain Name Server):
  A DNS stores the relevant IP addresses for host names in the form of DNS records and resolves the names if a relevant request is received, i.e. the name server sends a DNS record with the IP address associated with the name to the source of the request. Name servers form a hierarchical tree structure. If a name server cannot resolve a name, it therefore asks a higher-order name server, etc.
- HOSTS files:
  HOSTS files are located on the PCs in the LAN. You can use these files to create a table of host names with associated addresses. This means connections to DNS are no longer needed to resolve these names. As the HOSTS files must be updated on each PC, this method of name resolution is not very practicable.

In practice, the DNS of the Internet Service Provider is often used for name resolution.

2.6.2 Advantages of Name Resolution

With your BinTec router, the following functions and facilities for name resolution (port 53) are available:

- DNS Proxy, for passing DNS requests to the right DNS.
- DNS cache, for saving the results of DNS requests.
- Static name entries, for defining assignments of names to IP addresses.
- Filter function, to prevent the resolution of certain names.
- Monitoring via Setup Tool, to provide an overview of DNS requests.

This is how it works:

DNS Proxy

DNS Proxy makes the tedious updating of HOSTS files on PCs in the LAN unnecessary, as you can enter your BinTec router as DNS on the relevant PCs. DNS requests are passed by the PC to the BinTec router for processing. The configuration of the PCs in the LAN is then easy and can also be left when changing providers. This also works if the PCs in the LAN do not have any static DNS entries, but are assigned these dynamically by your BinTec router as DHCP server.

Forwarding entries enable the BinTec router to decide which DNS is to be used for the resolution of certain names. If you have configured two WAN partners on your router, your head office and your Internet Service Provider, it is advisable to have Internet names resolved by the DNS of your ISP, but names of the corporate network by the DNS of the head office. A DNS request for resolution of an internal company address usually cannot be answered by the DNS of the ISP and is thus superfluous, causes unnecessary costs and resolution takes longer than necessary. A forwarding entry, which passes DNS requests for names such as "*.intranet.de" to the WAN partner "head office", is therefore advisable.

DNS cache

If a DNS request is passed by a BinTec router to a DNS and this DNS answers with a DNS record, the resolved name is saved with the associated IP address as a positive dynamic entry in the DNS cache of the BinTec router. This means that once a name has been resolved and is required again, the BinTec router can answer the request from the cache and a new request to an external name server is not necessary. These requests can therefore be answered more quickly, bandwidth is reduced on the WAN connections and the costs of unnecessary connections are saved.

If a DNS request cannot be answered by any of the DNS asked, this is saved in the cache as a negative dynamic entry. As failed DNS requests (requests that cannot be answered) are not usually saved by applications or IP stacks, these negative dynamic entries in the cache prevent frequent unsuccessful connection setups to external DNS.

The validity of the positive dynamic entries in the cache is given by the TTL (Time To Live), which is contained in the DNS record. Negative entries are assigned the value **Maximum TTL for Neg Cache Entries**. A dynamic entry is deleted from the cache when the TTL expires.

Static name entries

You use positive static entries to enter names with the associated IP addresses on the BinTec router. If you save frequently needed IP addresses in this way, the BinTec router can answer relevant DNS requests itself and the connection to an external name server is not necessary. This speeds up access to these addresses. For a small network, such a name server can be configured on the BinTec router. The installation of a separate DNS and the tedious updating of HOSTS files on the PCs in the LAN is not necessary.

With negative static entries, a name is not assigned an IP address, a corresponding DNS request is answered negatively and not passed to any other name server either.

You can easily change a dynamic entry to a static entry "at the press of a button" in ***IP*** ➧ ***DNS*** ➧ ***DYNAMIC CACHE*** (see table 2-10, page 57).

Filter function

By using negative static entries, you can limit name resolution on the BinTec router using a filter function. This makes access to certain domains much more difficult for users in the LAN, as it prevents the corresponding names being resolved. You can use wildcards (*) when entering the name.

When you enter a static entry, you define how long this assignment of name and IP address is valid by setting the TTL. This TTL is entered in each DNS record with which the BinTec router answers a relevant DNS request.

Make sure your static entries are always up to date. Names or IP addresses can change at any time!

Monitor function

Which IP addresses are requested by hosts in the LAN and how often?

The Setup Tool permits rapid access to this and other statistical information. You can also use the `nslookup` command in the command line (SNMP shell) to check how a name or an IP address is resolved by your BinTec router or another name server. To obtain help information for the command, enter `nslookup -?`.

2.6.3 Other Options

Global name server

In ***IP*** ➧ ***STATIC SETTINGS***, you can also enter the IP address of preferred global name servers that are to be asked if the BinTec router cannot answer requests itself or with forwarding entries.

For local applications, the IP address of BinTec router or the loopback address (127.0.0.1) can be entered as global name server.

If necessary, the BinTec router can send or receive the addresses of name servers to and from WAN partners:

Default interface

In **Default Interface**, you can also select a WAN partner to whom a connection is set up as standard for name server negotiation if name resolution was not successful using the methods already stated.

2.6.4 Exchanging DNS Addresses with LAN Partners

DHCP

If the BinTec router is configured as DHCP server, DHCP clients in the LAN can be sent IP addresses from name servers. In this case, the addresses of the global name servers entered on the BinTec router can be sent or the address of BinTec router itself. In the latter case, DNS requests from the DHCP clients are sent to the BinTec router, which either answers these itself or passes them on if necessary (proxy function).

2.6.5 Exchanging DNS Addresses with WAN Partners

IPCP

The same applies if the dynamic negotiation of name servers is activated for the IP configuration of a WAN partner and the BinTec router is operating in Server Mode (**Dynamic Name Server Negotiation** = *server (send)*). In this case, the addresses of the global name servers or the address of the BinTec router itself can also be sent for name server negotiations via IPCP to the WAN partner, who is the IP address client.

If the BinTec router is operating in Client Mode (**Dynamic Name Server Negotiation** = *client (receive)*), name server addresses can if necessary be negotiated with the WAN partner, who is the IP address server, and sent to the BinTec router. These can be entered as global name servers on your BinTec router and are thus available for future name resolutions.

2.6.6 Strategy for Name Resolution

A DNS request is handled by the the BinTec router as follows:

1. Can the request be answered directly from the static or dynamic cache (IP address or negative answer)?
   - If yes, the information is forwarded.
   - If no, see 2.
2. Is a matching forwarding entry available?
   In this case, the relevant DNS are asked. If the connection to the WAN partner is not active, an attempt is made to set it up.
   - If a DNS can resolve the name, the information is forwarded and a dynamic entry created in the cache.
   - If none of the DNS asked can resolve the name or no matching forwarding entry is available, see 3.

3. Are global name servers entered?
   In this case, the relevant DNS are asked. If the IP address of the BinTec router or the loopback address is entered for local applications, these are ignored here.
   – If a DNS can resolve the name, the information is forwarded and a dynamic entry created in the cache.
   – If none of the DNS asked can resolve the name or no static name servers are entered, see 4.
4. Is a WAN partner selected as default interface?
   In this case, the associated DNS are asked. If the connection to the WAN partner is not active, an attempt is made to set it up.
   – If a DNS can resolve the name, the information is forwarded and a dynamic entry created in the cache.
   – If none of the DNS asked can resolve the name or no default interface has been selected, see 5.
5. Is overwriting the global name server addresses admissible (**Overwrite Global Nameserver** = *yes*)?
   In this case, a connection is set up to the first WAN partner, which is configured so that addresses of DNS can be sent – provided this has not previously been attempted. If name server negotiation is successful, these are entered as global name servers and are therefore available for further requests.
6. Request is answered with server error.

If one of the DNS answers with "non-existent domain", this answer is forwarded to the source of the request immediately and included in the cache as negative entry.

2.6.7 Overview of Configuration with the Setup Tool

The configuration and monitoring of name resolution on the BinTec router is set in:

- ***IP*** ➧ ***STATIC SETTINGS***:
- ***IP*** ➧ ***DNS***
- ***IP*** ➧ ***DNS*** ➧ ***STATIC HOSTS***
- ***IP*** ➧ ***DNS*** ➧ ***FORWARDED DOMAINS***
- ***IP*** ➧ ***DNS*** ➧ ***DYNAMIC CACHE***
- ***IP*** ➧ ***DNS*** ➧ ***ADVANCED SETTINGS...***
- ***IP*** ➧ ***DNS*** ➧ ***GLOBAL STATISTICS...***
- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

IP ➧ ***STATIC SETTINGS*** contains the following fields:

Field	Meaning
Domain Name	Defines BinTec router's Domain Name.
Primary Domain Name Server	IP address of BinTec router's first global Domain Name Server (DNS).
Secondary Domain Name Server	IP address of another global Domain Name Server.
Primary WINS	IP address of BinTec router's first global WINS (Windows Internet Name Server) or NBNS (NetBIOS Name Server).
Secondary WINS	IP address of another global WINS or NBNS.

Table 2-6: ***IP*** ➧ ***STATIC SETTINGS***

IP ➧ ***DNS*** contains the following fields:

Field	Meaning
Positive Cache	Enables positive dynamic entries in the cache. Possible values: ■ *enabled* (default value): Successfully resolved names and IP addresses are saved in the cache. ■ *flush*: All positive dynamic entries in the cache are deleted. ■ *disabled*: Successfully resolved names and IP addresses are not saved in the cache and existing dynamic positive entries are deleted (static entries are not deleted).
Negative Cache	Enables negative dynamic entries in the cache. Possible values: ■ *enabled* (default value): Names that could not be resolved are saved in the cache as negative entries. ■ *flush*: All negative dynamic entries in the cache are deleted. ■ *disabled*: Names that could not be resolved are not saved in the cache and existing dynamic negative entries are deleted (static entries are not deleted).

Field	Meaning
Overwrite Global Nameservers	Defines whether the addresses of global name servers on the BinTec router (in ***IP*** ➧ ***STATIC SETTINGS***) may be overwritten with name server addresses sent by WAN partners. Possible values: ■ *yes* (default value) ■ *no*
Default Interface	Defines the WAN partner to which a connection is normally set up for name server negotiation if other name resolution attempts were not successful.
DHCP Assignment	Defines which name server addresses are sent to the DHCP client if the BinTec router is configured as DHCP server. Possible values: ■ *none*: No name server address is sent. ■ *self* (default value): The address of BinTec router is sent as name server address. ■ *global*: The addresses of the global name servers entered on the BinTec router are sent.

Field	Meaning
IPCP Assignment	Defines which name server addresses are sent by the BinTec router to a WAN partner for dynamic name server negotiation. Possible values: ■ *none*: No name server address is sent. ■ *self*: The address of the BinTec router is sent as name server address. ■ *global* (default value): The addresses of the global name servers entered on the BinTec router are sent.
Static Hosts	The number of static entries is displayed in brackets.
Forwarded Domains	The number of forwarding entries is displayed in brackets.
Dynamic Cache	The number of positive and negative dynamic entries in the DNS cache is displayed in brackets.

Table 2-7: ***IP*** ➧ ***DNS***

IP ➧ ***DNS*** ➧ ***STATIC HOSTS*** ➧ ***ADD*** contains the following fields:

Field	Meaning
Default Domain:	The Domain Name of the BinTec router entered in ***IP*** ➧ ***STATIC SETTINGS*** is displayed.
Name	Host name, which is assigned the **Address** with this static entry. May also contain wildcards (*) (only at the start of **Name**, e.g. *.bintec.de). If an incomplete name is entered without a dot, this is completed with ".**Default Domain**" after confirming with **SAVE**.
Response	Defines the type of static entry. Possible values: ■ *positive* (default value): A DNS request for **Name** is answered with a DNS record, which contains the associated **Address**. ■ *ignore*: A DNS request is ignored; no answer is given (not even a negative answer). ■ *negative*: A DNS request for **Name** is answered with a negative answer.
Address	(Only for **Response** = *positive*) IP address, which is assigned to **Name**.
TTL	Period of validity in s for the assignment of **Name** to **Address** (only relevant for **Response** = *positive*). This value is displayed in the TTL field (Time To Live) if the BinTec router sends a corresponding DNS record. Default value: *86400* (= 24 h)

Table 2-8: ***IP*** ➧ ***DNS*** ➧ ***STATIC HOSTS*** ➧ ***ADD***

IP ➧ ***DNS*** ➧ ***FORWARDED DOMAINS*** ➧ ***ADD*** contains the following fields:

Field	Meaning
Global Nameservers:	The global name servers entered in ***IP*** ➧ ***STATIC SETTINGS*** are displayed.
Default Domain:	The Domain Name of the BinTec router entered in ***IP*** ➧ ***STATIC SETTINGS*** is displayed.
Name	Host name that is to be resolved with this forwarding entry. May also contain wildcards (only at the start of **Name**, e.g. *.bintec.de). If an incomplete name is entered without a dot, this is completed with ".**Default Domain**" after confirming with **SAVE**.
Interface	Defines the WAN partner to which a connection is set up for the resolution of **Name**.
TTL	Period of validity in s for the assignment of **Name** to **Address**. Default value: *86400* (= 24 h) If the request of the BinTec router for **Name** is answered with a DNS record, this contains a TTL field (= Time To Live in s), whose value is not normally changed by the BinTec router on forwarding the DNS record. If the TTL field received has the value 0 or exceeds **Maximum TTL for Pos Cache Entries**, then **TTL** is also sent with the DNS record forwarded.

Table 2-9: ***IP*** ➧ ***DNS*** ➧ ***FORWARDED DOMAINS*** ➧ ***ADD***

IP ➧ ***DNS*** ➧ ***DYNAMIC CACHE*** contains the following fields:

Field	Meaning
Name	Host name, which is assigned the **Address** with this dynamic entry in the cache.
Address	IP address, which is assigned to **Name**.
Resp	Defines the type of dynamic entry. Possible values: ■ *positive*: A DNS request for **Name** is answered with the associated IP address from the cache. ■ *negative*: A DNS request for **Name** is answered with a negative answer from the cache.
TTL	Indicates how many seconds the dynamic entry remains in the cache. The entry is deleted on expiry of **TTL**. When a positive dynamic entry is saved in the cache, the value of the TTL field (= Time To Live in s) contained in the DNS record is used. If the TTL field in the DNS record is set to 0 or exceeds **Maximum TTL for Pos Cache Entries**, the value **Maximum TTL for Pos Cache Entries** is used when saving the entry. When a negative dynamic entry is saved in the cache, **Maximum TTL for Neg Cache Entries** is always assigned as this value.
Ref	Indicates how often the entry has been referenced, i.e. how often a DNS request has been answered with the entry from the cache.

Field	Meaning
STATIC	A dynamic entry can be converted to a static entry by tagging the entry with the **Space** bar and confirming with STATIC. The relevant entry then disappears from ***IP*** ➧ ***DNS*** ➧ ***DYNAMIC CACHE*** and is listed in ***IP*** ➧ ***DNS*** ➧ ***STATIC HOSTS***. **TTL** is transferred in this operation.

Table 2-10: ***IP*** ➧ ***DNS*** ➧ ***DYNAMIC CACHE***

IP ➧ ***DNS*** ➧ ***ADVANCED SETTINGS...*** contains the following fields:

Field	Meaning
Maximum Number of DNS Records	Defines the maximum number of static and dynamic entries. Once this value is reached, an older dynamic entry is deleted from the cache when a new entry is added. The entry deleted is always the dynamic entry that has not been requested for the longest period of time. If **Maximum Number of DNS Records** is reduced by the user, dynamic entries are also deleted, if necessary. Static entries are not deleted; **Maximum Number of DNS Records** cannot be set lower than the current number of existing static entries. If **Maximum Number of DNS Records** corresponds to the number of static entries, no further dynamic entries are possible!
Maximum TTL for Pos Cache Entries	Is assigned to a positive dynamic entry in the cache as **TTL** if the field of the DNS record has the value 0 or exceeds **Maximum TTL for Pos Cache Entries**.
Maximum TTL for Neg Cache Entries	Is assigned as **TTL** to a negative dynamic entry in the cache.

Table 2-11: ***IP*** ➧ ***DNS*** ➧ ***ADVANCED SETTINGS...***

IP ➧ ***DNS*** ➧ ***GLOBAL STATISTICS...*** contains the following fields (the menu is updated every second):

Field	Meaning
Received DNS Packets	Displays the number of received DNS packets, including the answer packets for forwarded requests.
Invalid DNS Packets	Displays the number of invalid DNS packets received.
DNS Requests	Displays the number of correct DNS packets received.
Cache Hits	Displays the number of requests that could be answered with static or dynamic entries from the cache.
Forwarded Requests	Displays the number of requests forwarded to other name servers.
Cache Hitrate (%)	Displays the number of **Cache Hits** per **DNS Request** in %.
Successfully Answered Queries	Displays the number of successful requests (positive and negative) answered.
Server Failures	Displays the number of requests that could not be answered by any name server (either positively or negatively).

Table 2-12: ***IP*** ➧ ***DNS*** ➧ ***GLOBAL STATISTICS...***

The following part of ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings*** is of interest for this configuration step:

Field	Meaning
Dynamic Name Server Negotiation	In the event of dynamic name server negotiation, defines whether the BinTec router receives IP addresses for **Primary Domain Name Server**, **Secondary Domain Name Server**, **Primary WINS** and **Secondary WINS** from the WAN partner or sends them to the WAN partner.

Table 2-13: ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***

The **Dynamic Name Server Negotiation** field contains the following selection options:

Possible Values	Meaning
off	The BinTec router does not send or answer requests for name server addresses.
yes	The response is linked to the mode for issuing/ receiving an IP address (setting in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** under **IP Transit Network**): ■ The BinTec router sends requests for name server addresses to the WAN partner if *dynamic client* is selected. ■ The BinTec router answers requests for name server addresses from the WAN partner if *dynamic server* is selected. ■ The BinTec router answers but does not send requests for name server addresses if *yes* or *no* is selected.
client (receive)	The BinTec router sends requests for name server addresses to the WAN partner.
server (send)	The BinTec router answers requests from the WAN partner for name server addresses.

Table 2-14: **Dynamic Name Server Negotiation**

2.6.8 Procedure for Configuration with the Setup Tool

To do

Proceed as follows to configure name resolution with DNS Proxy on a BinTec router:

Name resolution on a BinTec router

If applicable, first enter the global name servers on the BinTec router:

- Go to ***IP*** ➧ ***STATIC SETTINGS***.
- Enter **Domain Name**, e.g. ***mycompany.com***.
- Enter **Primary** or **Secondary Domain Name Server**, if applicable.
- Enter **Primary** or **Secondary WINS**, if applicable.

If you do not have a Secondary DNS or Secondary WINS server, you can enter the IP address of the Primary DNS or WINS server in the **Secondary Domain Name Server** or **Secondary WINS** field again.

This may be necessary for connection to some data communications

- Press **SAVE**.

Activate or deactivate the cache function and define general settings for DNS Proxy:

- Go to ***IP*** ➧ ***DNS***.
- Select **Positive Cache** and **Negative Cache**, e.g. *enabled*.
- Select **Overwrite Global Nameservers**, e.g. *yes*, if you do not wish to enter any static global name servers under ***IP*** ➧ ***STATIC SETTINGS***.
- Select **DHCP Assignment**, e.g. *self*.
- Select **IPCP Assignment**, e.g. *global*.

Defines the values for the static and dynamic entries:

- Go to ***IP*** ➧ ***DNS*** ➧ ***ADVANCED SETTINGS...***.
- Enter **Maximum Number of DNS Records**.
- Enter **Maximum TTL for Pos Cache Entries**.
- Enter **Maximum TTL for Neg Cache Entries**.
- Press **SAVE**.

How to create static entries:

- Go to ***IP*** ➧ ***DNS*** ➧ ***STATIC HOSTS***.
- All the existing static entries are listed here.
- You can create a new entry with **ADD**.
- Enter **Name**.
- Select **Response**.
- Enter **Address**, if applicable.
- Enter **TTL**.
- Press **SAVE**.

How to create forwarding entries:

- Go to ***IP*** ➧ ***DNS*** ➧ ***FORWARDED DOMAINS***.
- All the existing forwarding entries are listed here.
- You can create a new entry with **ADD**.
- Enter **Name**.
- Select **Interface**.
- Enter **TTL**.
- Press **SAVE**.
- Select **EXIT**.
- Press **SAVE**.

BinTec router <–––> WAN partner

Proceed as follows if you would like to configure a WAN partner so that the address of a name server is sent from the BinTec router to the WAN partner or from the WAN partner to the BinTec router, as applicable:

- Go to ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***.
- Select **Dynamic Name Server Negotiation**.
- Confirm with **OK**.
- Press **SAVE**.

Monitoring and statistics

How to obtain a list of dynamic entries in the cache:

- Go to ***IP*** ➧ ***DNS*** ➧ ***Dynamic Cache***.
- This menu contains a list of all the dynamic entries in the cache.
- To convert a dynamic entry into a static entry, tag the entry with the **Space** bar and confirm with **STATIC**.
- The entry disappears from the list of dynamic entries and is listed as a static entry under ***IP*** ➧ ***DNS*** ➧ ***Static Hosts***.
- How to obtain a list of some static parameters:
- Go to ***IP*** ➧ ***DNS*** ➧ ***Global Statistics...***.
- Here you will find some statistics for DNS Proxy.

3 Changes

3.1 PPP

3.1.1 Inconsistent Encryption Configuration Leading to Repeated Connection Attempts

If a dialout partner tries to negotiate an encryption protocol, but that encryption is not enabled by the WAN partner, the connection is correctly terminated and the state of the interface of the client turns to *blocked*.

Problems occurred in the reverse case, however, where the dialout partner did not enable MPPE encryption, although the WAN partner required it. The connection was terminated by the WAN partner. The state of the client interface, however, did not turn to *blocked*, as it did not know the reason for the failure to connect. Continued attempts to establish the connection from client to server were made.

Now in the latter case, the dialout client partner not supporting encryption receives notification of an encryption requirement, causing the state of the client interface to turn to the *blocked* state. Thus, the repeated connection attempts are prevented.

This proprietary solution can only function provided both sides are BinTec routers and both sides are running Release 5.2.1 or greater.

3.1.2 VPN Performance Issues Addressed

Considerable Improvements have been made to the VPN implementation. Several modules have been overhauled, and problems causing poor performance and unreliable connections have been resolved.

The corresponding documentation has also been overhauled. The new text has been rewritten with increased emphasis on accuracy, clarity and specific configuration scenarios.

This represents the first installment in a new-look, user-friendly online Software Reference that can be retrieved from BinTec´s web site.

3.1.3 Local IP Address in IPCP Negotiation

If the local IP address variable in ***STATIC SETTINGS*** ➧ ***UNIQUE SOURCE IP ADDRESS*** (**biboAdmIpAddr**) is set, its value is used as the source address of all IP packets and transmitted to the WAN partner in the course of the IPCP negotiation. When a transit network is configured to the WAN partner, however, the transmission of the local IP address prevents a PPP connection from being made.

From this release, the ***UNIQUE SOURCE IP ADDRESS*** variable (**biboAdmIpAddr**) will only be used for IPCP negotiations if no corresponding entry has been made in the **ipRouteTable** for the interface over which the IP packet is to be transmitted, or if there are no entries in the **ipAddrTable**.

3.1.4 Asynchronous PPP over X.75

A new value has been added to the variable **isdnDspItem** of the **isdnDispatchTable**: *ppp_x75*. This makes possible asynchronous PPP over X.75 with PPP partners dialing in, even if these partners are authenticated in-band (non-CLID).

3.1.5 Debugging and Status Info of PPP Connections

The pppSessionTable

A new MIB table has been added to the PPP group. The **pppSessionTable** has been implemented to simplify the debugging of PPP connections and to provide a means of getting reliable status information about active PPP connections. The table is read only.

Variable	Meaning
IfIndex (*ro)	The correlating PPP interface index.
Mlp (ro)	Indicates negotiation of multillink PPP.
Mru (ro)	Peer´s MRU/MRRU LCP option.
LcpCallback (ro)	Callback option inside LCP negotiation.
AuthProt (ro)	The negotiated PPP authentication protocol.
Compression (ro)	The negotiated CCP compression mode.
Encryption (ro)	The negotiated CCP encryption mode.
CbcpMode (ro)	The negotiated Callback Control Protocol (CBC/P) mode.
CbcpDelay (ro)	The negotiated (CBCP) callback delay in seconds.
LocIpAddr (ro)	The negotiated local IP address.
RemIpAddr (ro)	The negotiated remote IP address.
DNS1 (ro)	The negotiated first name server IP address. In dynamic client mode, the DNS address dynamically assigned by the partner is used here.
DNS2 (ro)	The negotiated second name server address. In dynamic client mode, the DNS address dynamically assigned by the partner is used here.
WINS1 (ro)	The negotiated first NetBIOS name server IP address. In dynamic client mode, the WINS address dynamically assigned by the partner is used here.
WINS2 (ro)	The negotiated second NetBIOS name server IP address. In dynamic client mode, the WINS address dynamically assigned by the partner is used here.

Variable	Meaning
VJHeaderComp (ro)	The negotiation of Van Jacobsen TCP/IP header compression.
IpxcpNodeNumber (ro)	Unique IPX node ID dynamically assigned to the client.
BacpFavoredPeer (ro)	The negotiated BACP favored-peer.

Table 3-1: **pppSessionTable**

Extensions to bibopppLinkTable

The **bibopppLinkTable** has been extended to display characteristics specific to a link.

Variable	Meaning
Accm (ro)	Asynchronous Control Character Map according to RFC 1548
Lqm (ro)	Indicates the successful negotiation of the Link Quality Monitoring protocol.
LcpComp (ro)	Address and protocol field compression.
LocDiscr (ro)	Local LCP multilink endpoint discriminator, class 3 according to RFC 1990.
RemDiscr (ro)	Peer´s LCP multilink endpoind discriminator, class 3 (IEEE. 802.1 MAC Address) according to RFC 1990.

pppLinkTable extensions

3.2 RADIUS

3.2.1 OSPF and Connections over RADIUS

The new variable **ospfAreaLSAOriginateDelay** has been added to the **ospfAreaTable**. This variable controls the origination of OSPF Link State Advertisements (LSA) for connections over a RADIUS server. It only affects the interplay between OSPF and RADIUS and has no effect on other areas.

The feature is intended for a situation in which the RADIUS server generates more than one route: if, for example, the RADIUS server generates one host route for the PC that is calling and one for that PC´s remote access server. As soon as the first host route, sent by the RADIUS server, is generated in the **ipRouteTable** of the BinTec router, an LSA is sent; OSPF, however, can not send an LSA for the second incoming host route because the default interval to wait between sending LSAs is 5 seconds: the second host route would ordinarily be discarded in the meantime.

In such a case, **ospfAreaLSAOriginateDelay** can be set to delay the sending of the first LSA so as there is enough time for the second host route to be generated before the first LSA is sent.

The default value is 0.

3.2.2 New and Changed RADIUS Attributes

NAS-PORT

- Authentication Request: corresponds to the **isdnIfIndex** of the controller used for the connection.
- Accounting Start or Accounting Stop: is the sum of the variables **isdnCallIsdnIfIndex** and **isdnCallChannel**

NAS-PORT-TYPE

- Data 64k, Data 56k = NAS_PORT_TYPE_ISDN_SYNC
- Modem = NAS_PORT_TYPE_ASYNC
- V110 = NAS_PORT_TYPE_ISDN_ASYNC_V110

FRAMED-IP-ADDRESS

This attribute is now also sent for Radius accounting.

ACCT-TERMINATE-CAUSE

This attribute is now also sent for accounting stop.

- Shorthold = ACCT_TERMINATE_CAUSE_IDLE_TIMEOUT
- Termination backup/BOD link = ACCT_TERMINATE_CAUSE_PORT-UNNEEDED
- Callback = ACCT_TERMINATE_CAUSE_CALLBACK
- Termination for Priority Voice (PV) = ACCT_TERMINATE_CAUSE_PORT_PREEMPTED
- Remote side terminates the connection = ACCT_TERMINATE_CAUSE_USER_REQUEST
- Termination due to PPP keepalive = ACCT_TERMINATE_CAUSE_PORT_ERROR
- Authentication problems, other problems concerning link establlishment and PPP negotiation = ACCT_TERMINATE_CAUSE_USER_ERROR
- Administrative interface in the ´down´ state, deletion of an interface (on an open connection), changing of an ISDN leased line interface = ACCT_TERMINATE_CAUSE_ADMIN_RESET

- Now also in Accounting, the relevant numbers are taken from the variables **isdnCallLocalNumber** or **isdnCallRemoteNumber** = CALLING_STATION_ID and CALLED_STATION ID

3.2.3 RADIUS Dialout Protocols

The following encapsulations are now supported for Radius dialout:

```
FRAMED_PROTOCOL_IP_LAPB          17825796
FRAMED_PROTOCOL_IP_HDLC          17825798
FRAMED_PROTOCOL_MPR_LAPB         17825799
FRAMED_PROTOCOL_MPR_HDLC         17825800
FRAMED_PROTOCOL_X75_PPP          17825803
FRAMED_PROTOCOL_X75BTX_PPP       17825804
```

3.2.4 RADIUS and Callback ´delayed´

The Callback option *delayed* is now supported for Radius dialin. The prerequisite for this is of course the identification of the partner by CLID (outband Radius).

Configuration in the Radius users file is as follows:

```
´BinTec-biboPPPTable = "callback=delayed"´
```

3.2.5 Automatic Loading of Dialout Routes

The **radiusServerTable** has been extended with the variable **ReloadInterval**. The value for this variable specifies the interval in minutes to wait after which the initial Radius dialout routes are reloaded.

3.3 CAPI

3.3.1 DTMF Signals Transmission over CAPI

Introduction

DTMF stands for Dual Tone Multi Frequency and refers to a form of signalling in which standard set combinations of two specific voice band frequencies, one high, one low, are used. DTMF signals can pass through the entire connection to the destination user.

BinTec Communications AG now supports the transmission of DTMF signals over its CAPI interface.

At the CAPI interface a string of DTMF tones can be specified in a FACILITY_REQ in order to send them on a B-channel. It is also allowed (though not advised) to send a sequence of FACILITY_REQs one after the other instead of concatenating the strings in the individual FACILITY_REQs and sending a single request.

Details not covered by the CAPI specification

- It is not necessary to wait for confirmation to a FACILITY_REQ for DTMF-send before sending the next one. Up to 64 FACILITY-REQs are queued internally.
- The default tone length as specified in the CAPI specification in 40 ms. Experience has shown, however, that 40 ms is not sufficient in many cases. In BinTec´s implementation, the default tone length and the gap between two tones is fixed at 100 ms.
- While a FACILITY_REQ for DTMF-send is running, DATAB3_REQs are not permitted. They will be released and confirmed with a bad returncode.

3.3.2 New CAPI Variables

Three new variables have been added to the **capiConfigTable.**

1. **Fax12000(rw)**: This enables or disables the 12000bps mode for fax transmission. If the value of the variable is set to *on*, the fax speed will fall back from 14400 to 12000 bps during a retrain. If set to *off*, it will fall straight back to 9600 bps. The default value is *off*.
2. **FaxTXLevel(rw)**: The transmission level can be set to -x dB (*db0* = 0 dB, *db3* = -3 dB). The default value and the value normally used for fax transmission in Germany is -6 dB (*db6*).
3. **FaxModulation(rw)**: With this variable you can set the following default transmission protocols for fax. The default value is v17.
   - v17 max. 14400 bps new standard
   - v33 max. 14000 bps early standard
   - v29 max. 9600 bps fax standard
   - v17s: v17 with extended fax-on-demand capability
   - v33s: v33 with extended fax-on-demand capability

3.3.3 Terminal Portability over CAPI

Terminal portability provides the possibility to suspend a call of a terminal, move it to another socket and resume the call there. When the call is made over a CAPI interface, terminal portability is used to pass a call from one CAPI application to another. The call is suspended on the one application and resumed on the other.

Terminal portability is applicable at the basic rate interface (S_0) only. In the CAPI specification, refer to Supplementary Services.

3.3.4 Virtual Terminal Portability over CAPI

While terminal portability is applicable on basic rate interfaces only, virtual terminal portability is an extension of it for primary rate interfaces (S2M). In the CAPI specifications, refer to Supplementary Services.

3.3.5 B-Channel Selection

In the ISDN standard it is possible to choose the B-channel of outgoing calls. This feature is now supported by BinTec´s CAPI implementation. In the CAPI specifications, refer to Connect Req.

3.3.6 Error Correction Mode for G3 Faxing = On

The default value for **capiConfigFaxG3ECM** is now *on.* This specifies whether ECM (Error Correction Mode) should be used for the T30 protocol in G3 facsimile transmissions.

3.4 XBRI

3.4.1 Fax Server on 2XBRI Connections

4 channels can be used over a CM 2XBRI with modem functionality. With the maximum number of two installed CM 2XBRIs, the number of channels has increased to eight.

3.5 Setup Tool

3.5.1 DHCP Menu Name Changes

The names of two submenus have changed to better reflect the configuration options for each.

- Formerly ***IP*** ➧ ***DYNAMIC IP ADDRESSES (SERVER MODE)*** has been renamed as ***IP ADDRESS POOL WAN (PPP)***.
- Formerly ***IP*** ➧ ***DHCP SERVER*** has been renamed as ***IP ADDRESS POOL LAN (DHCP)***.

```
BinTec router Setup Tool                        BinTec Communications AG
[IP][DYNAMIC][ADD]: IP address pool WAN (PPP)                    MyBrick

        Pool ID                             0
        IP Address                          172.16.98.1
        Number of consecutive addresses     1


            SAVE                        CANCEL

Enter integer range 0..9
```

Table 3-2: ***IP*** ➧***DYNAMIC*** ➧***ADD***

3.5.2 Keepalive Monitoring

The Keepalive Monitoring feature can now be configured over Setup Tool. The fields in ***SYSTEM*** ➧***KEEPALIVE MONITORING*** ➧***ADD*** correspond to the variables in the **ipHostsAliveTable**.

```
BinTec router Setup Tool                        BinTec Communications AG
[SYSTEM][KEEPALIVE MONITORING][ADD]: Keepalive Monitoring      MyBrick


        Group               0
        IPAddress           172.16.98.1
        Interval            300
        DownAction          down
        FirstIfIndex        10001
        Range               4999


            SAVE                        CANCEL

Enter integer range 0..9
```

Table 3-3: ***SYSTEM ➧ KEEPALIVE MONITORING ➧ ADD***

3.5.3 Time and Date

Time and date can now be manually configured over Setup Tool. Remember the time set here may be overwritten by the time protocol configured in ***IP ➧ STATIC SETTINGS***.

```
BinTec router Setup Tool                        BinTec Communications AG
[SYSTEM][TIME]: Set System Time and Date                       MyBrick


        Time is currently controlled by: TIME/UDP

        Current Time:
        Mon Mar 27 12:00:52 2000


        New Time 11:58

        New Date 03/27/2000

                SET                         BACK

Enter integer range 0..23
```

Table 3-4: ***SYSTEM ➧ TIME***

3.5.4 Transit Network Settings

A new field has been added to the ***WAN*** ➧***EDIT*** ➧***IP*** menu in Setup Tool. If you are not using a transit network (and **no** is selected after **IP Transit Network**), it is nevertheless possible to enter a local IP address: the new field **local IP Address** appears.

```
BinTec router Setup Tool                        BinTec Communications AG
[WAN][EDIT][IP]: IP Configuration (bgo)                          MyBrick

    IP transit Network                no


    local IP Address              10.1.1.1


    Partner´s LAN IP Address      12.2.2.9
    Partner´s LAN Netmask

    Advanced Settings

                SAVE                        CANCEL

Use <Space> to select
```

This field does not appear if either **yes**, **dynamic client** or **dynamic server** is selected after **IP Transit Network**. An entry is then required in the new field if:

1. there are other WAN partners with transit networks
2. there are several Ethernet modules
3. there is another IP configuration for which the BRICK has several different IP addresses.

3.5.5 Extended Routes

It is now possible to add extended routes in ***IP*** ➧ ***ROUTING*** ➧ ***ADDEXT***. The fields additional to ***IP*** ➧ ***ROUTING*** ➧ ***ADD*** correspond to variables of the **ipExtRtTable**.

```
BinTec router Setup Tool                        BinTec Communications AG
[IP][ROUTING][ADD]: IP Routing - Extended Route                  MyBrick


    Route type                    Host Route
    Network                       LAN

    Destination IP-Address

    Gateway IP-Address
    Metric                        1
    Source Interface              dont verify
    Source IP-Address
    Source Mask
    Type of Service (TOS)         00000000     TOS Mask     00000000
    Protocol

                SAVE                        CANCEL
```

Table 3-5: ***IP*** ➧ ***ROUTING*** ➧ ***ADDEXT***

3.5.6 TFTP Server IP Address Suggestions

In the Configuration Management submenu, the **TFTP Server IP Address** field appears if *put*, *get* or *state* is selected. Now one of the following IP addresses appears as a proposal in the corresponding entry field:

biboAdmLogHostAddr is used, if not

biboAdmTrapHostAddr is used, if not

biboAdmTimeServer is used, if not

biboAdmipAddr is used.

```
BinTec router Setup Tool                          BinTec Communications AG
[CONFIG]: Configuration Management                                MyBrick

        Operation                       put (FLASH -> TFTP)

        TFTP Server IP Address          172.14.93.39
        TFTP File Name                  BRICK.cf

        Name in Flash                   boot

        Type of last operation          save (MEMORY -> FLASH)
        State of last operation         done

            START OPERATION                 EXIT

Enter IP address (a.b.c.d or resolvable hostname)
```

3.5.7 User Name Dependent on Item

In the Setup Tool submenu ***WAN*** ➧ ***INCOMING CALL ANSWERING*** ➧ ***ADD***, the user name field is now dependent on the Item selected. Only if a CAPI item is selected does the CAPI Username field appear.

```
BinTec router Setup Tool                          BinTec Communications AG
[WAN][INCOMING][ADD]: Incoming Call Answering                      MyBrick


        Item                    CAPI 1.1 EAZ 0 Mapping
        Number
        Mode                    right to left
        CAPI Username
        Bearer                  any


                SAVE                CANCEL

Enter string, max length = 42 chars
```

3.5.8 2nd IP Address on LAN Interface

From Release 5.2.1, it is possible to configure a second IP address for a LAN interface over Setup Tool.

```
BinTec router Setup Tool                          BinTec Communications AG
[LAN]: Configure LAN Interface                                    MyBrick

        IP-Configuration
            local IP-Number           178.14.98.126
            local Netmask             255.255.255.0
            Second Local IP-Number    178.14.98.122
            Second Local Netmask      255.255.255.0

            Encapsualtion             Ethernet II
            Mode                      Auto

        IPX-Configuration
            local IPX-NetNumber
            Encapsulation

        Bridging                      disabled

        Advanced Settings >

                    SAVE                        CANCEL

Enter IP address (a.b.c.d or resolvable hostname)
```

3.5.9 Number of Syslog Messages

The maximum number of Syslog messages that can be configured in Setup Tool, **Maximum Number of Syslog Entries** in the ***SYSTEM*** menu has increased to 1000.

3.5.10 ISP Configuration

When *Async PPP over X.75* or *Async PPP over X.75/T.70/BTX* is selected as **Encapsulation**, the submenu ***PROVIDER CONFIGURATION*** in ***WAN*** ➧ ***ADD*** ➧ ***ADVANCED SETTINGS*** has changed.

- The name of the submenu has been changed from ***PROVIDER CONFIGURATION*** to ***COMPUSERVE LOGIN***.
- *Compuserve via T-Online* has been removed from the list.

- *Compuserve II* and *Compuserve II Germany (Unique No.)* have both been added to the list.

3.5.11 IP Interface Display for NAT Configuration

The ***IP*** ➧ ***NAT CONFIGURATION*** menu has changed. Now it is possible to view at a glance whether NAT has been activated for each available IP interface as well as the number of session profiles (**static mappings**) configured for each interface.

```
BinTec router Setup Tool                        BinTec Communications AG
[IP][NAT]: NAT Configuration                                    MyBrick

    Select IP Interface to be configured for NAT

    Name             Nat          static mappings


    en1              off
    en1-snap         off
    MyHQ             on           1
    SalesO           on           3


    EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

3.5.12 Duplex Settings for 100BT Ethernet Modules

There is a new configuration option for 100BT Ethernet modules over Setup Tool. It is now possible to configure the following duplex settings, although the default value *Auto* is recommended.:

- 10 MBit Half Duplex
- 10 MBit Full Duplex
- 100 MBit Half Duplex
- 100 MBit Full Duplex

- Auto

3.5.13 Compression Options

The availability of compression options is now dependent on the presence of STAC module or a license. In the ***WAN*** ➧ ***EDIT*** ➧ ***ADD*** menu, the Compression option MPPC can only be selected if there is a STAC module present. The Compression options STAC and MS-STAC are only available if there is a STAC module or a valid license present.

3.5.14 Response Options for Access Violations

Two configuration options have been added to the ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES*** ➧ ***EDIT*** menu. Both options deal with how to respond to access violations.

- **Deny Silent** specifies whether to respond with an ICMP error message for packets violating an access rule (*no*) or to ignore the violation (*yes*).
- **Reporting Method** specifies whether violations should be reported, and if so in what way.
  - *info* specifies the creation of a syslog message with some brief information about the packet.
  - *dump* specifies the creation of a syslog message with the complete content of the packet included.
  - *none* specifies that no report of the access list violation is made.

```
BinTec router Setup Tool                        BinTec Communications AG
[IP][ACCESS][INTERFACES][EDIT]: Configure First Rules            MyBrick


        Interface             MyHq
        First Rule            none

        Deny Silent           no
        Reporting Method      info

            SAVE                          CANCEL

Use <Space> to select
```

3.5.15 Local Filters

A new submenu has been added to the ***IP*** menu. ***Local Services Access Control*** allows the user to control access to local services (e.g. telnet, capi tapi, http) for specific interfaces via Setup Tool. As long as this is empty, access to local services is possible via all interfaces, provided it is not prohibited by the use of NAT or global filters.

Local filters therefore provide an additional instrument that is easier to handle than global filters and also that does not adversely affect performance in normal routing.

The Setup Tool configuration options correspond to variables and values from the MIB tables **localTcpAllowTable** and **localUdpAllowTable**.

```
BinTec router Setup Tool                        BinTec Communications AG
[LOCALSRV][EDIT]: Local Services Access Control                  MyBrick


        Service                         http(tcp)

        Verify IP Address               verify
            IP Address                  172.16.86.12
            Mask                        255.255.255.0

        Verify Interface                verify
            Interface                   sales


                SAVE                        CANCEL

<Space> to select
```

3.5.16 Selection of Filterable Protocols Extended

The list of protocols that can be filtered over Setup Tool ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER*** ➧ ***ADD*** has been supplemented by the following:

ip, igp, chaos, tlsp, skip, kryptolan, iso-ip, ipip, ipx-in-ip,vrrp.

3.5.17 Monitoring IP Sessions

IP sessions have been added to the ***MONITORING AND DEBUGGING*** ➧ ***INTERFACES*** ➧ ***EXTENDED*** menu. Currently active IP sessions monitored by the router are displayed.

The Setup Tool monitoring display of IP sessions corresponds to variables and values from the MIB table **ipSessionTable**.

3.6 IP

3.6.1 Limited ICMP Source Quenches

In order to reduce traffic congestion between sender and receiver, Source Quench messages are sent. These messages inform a sending side that is causing congestion on the receiving side to reduce the speed at which its packets are being sent. If, however, there is no limitation to the rate at which the Source Quench messages are sent, these messages can, in turn, cause traffic congestion on the sending side.

In order to both provide a controlling mechanism for congestion without the drawback of thereby creating more congestion in the other direction, Source Quench messages are now limited to respond to TCP packets and are only sent once every second for each sender/receiver pair.

This now conforms with the recommendations stipulated in RFC 1812.

3.6.2 NAT

1. Up to now a limitation of 230 active NAT sessions was supported on one interface. This limitation of NAT sessions has increased to 4000.
2. The aging interval for entries to the TCP port 1723 (PPTP) has been increased to 24 hours. This value is fixed and can no longer be adjusted.

3.6.3 DHCP Gateway Setting

Normally, a BinTec router acts as both a DHCP server and as the default gateway for the workstations in the LAN. In some cases, however, it is desirable for the router to act as a DHCP server, but not as the default gateway for the LAN. For this reason, the **ipDhcpGateway** has been added to the **ipDhcpTable**. If a value is given to this new variable, the router does not act as the default gateway. If no value is set, the router is specified by DHCP as the default gateway.

3.7 System

3.7.1 BinTec Router Ready for New Activity Monitor

The new BRICKware for Windows release available soon will include a new-look Activity Monitor that will improve the clarity and ease of interface monitoring, as well as allow the manipulation of the states of selected interfaces.

In order to be able to use this improved Windows application, the system software running on the BinTec router has been specially extended. It will thus only be possible to use the new features of the Activity Monitor when running this release (5.2.1) or higher.

3.7.2 Changes to the ifstat Application

Two changes have been made to the ifstat application:

- The final column of the ifstat application display is now divided into two parts: physical (MAC) address and change time: **PhyAddr/ChgTime**
  - On non-LAN interfaces, ifstat now shows the amount of time since the last change in the state of that interface.
    For example, if the interface is up, the length of time the interface has been up is displayed.
  - On LAN interfaces, on the other hand, the application will continue to display the physical (MAC) address.
- Secondly, the total number of available interfaces is displayed.
  By using the -u option, only the total number of interfaces that are currently up is displayed.

3.7.3 netstat and Extended Routes

The output for the netstat *-r* option now includes extended routes. The new option *-e* shows extended routes options.

3.7.4 New Ping Options

The following options have been added to the ping program:

- -i: incremental. Each successive packet is sent with one additional byte.
- -f: flood. Each packet(s) is sent immediately after one is received. <precount> sets the number of packets to be sent without acknowledgement. The command -f 1 without -d nn sends/receives nearly half of the bandwidth.
- -d: delay. The time in milliseconds to wait before the next packet is sent (default is 1000).
- -c: count. Only a specified number of packets is sent.

3.8 Modem FM-8MOD

3.8.1 Firmware Update

A new modem Firmware version is now available: the Rockwell/Conexant code version is V2.1.11B.

It is generally advisable to use the latest modem firmware.

3.9 CSM56K

3.9.1 Idle Timer For Modem Driver Now Configurable

Configuration options for the idle timer of the modem (CSM) driver of the BIANCA-BRICK-XL/XL2 have been implemented.

The idle timer is used to specify the duration of an interval between successive characters received from the modem which, when exceeded, will cause the modem driver to terminate the assembly of a data packet and to forward it to the higher-layer protocols.

The following new SNMP configuration options have been added to the **mdmProfileTable**.

Variable	Meaning
IdleTimerMode	Two values can be given to this variable: *static*: the idle time is taken from the object **IdleTimerFixedDelay** (default value). *dynamic*: the idle time is set to the duration a number of **IdleTimerCharDelay** characters would take to be transmitted at the transmission rate of the modem used.
IdleTimerFixedDelay	This object specifies the duration of the idle timer in milliseconds between the last data received and the forwarding of that data (default=5).
IdleTimerCharDelay	This object specifies the number of characters (octets), corresponding to the current transmission rate, before which data forwarding takes place (default=3).

Table 3-6: **Extensions to the mdmProfileTable**

4 Bugfixes

4.1 PPP

4.1.1 Connections to Certain Internet Service Providers

Manifestation: Accessing the Internet over certain ISPs (such as Online Dienst Nürnberg) may have failed.

Preconditions: When clients were dynamically assigned IP addresses and/or DNS/WINS addresses from the provider. The BinTec router used was running system software 5.1.1.

Current status: This bug has been fixed.

4.1.2 No Connection to Compuserve

Manifestation: Access to "Compuserve Network", "Compuserve Corporate Network", Compuserve II" and "Compuserve II Germany (Unique No.)" failed.

Preconditions: The BinTec router used was running system software 5.1.1.

Current status: This bug has been fixed.

4.1.3 VPN Links Disconnected

Manifestation: In some isolated cases, after precisely 7,200 seconds or if the BinTec router on one side rebooted, for example, VPN links were incompletely disconnected.

The result of this type of disconnection was that the state of the VPN interface on the side that booted was set to *dormant*, while the state of the VPN interface

on the other remained *up*. Once these inconsistent states were reached, no further VPN connection could be made.

Current status: Now the inconsistency is determined and resolved: the VPN interface with the *up* state is reset to *dormant* and the VPN connection can be reestablished.

4.1.4 Setting Short Hold to -1 on a VPN Interface

Background: By setting **biboPPPShortHold** to *-1,* it has been possible, since release 5.1.1, to automatically initiate a dial-up connection and reestablish the link directly after termination of the link.

Caution!

This immediate reestablishment of the link should be expressly wished as setting **PPPShorthold** to *-1* can obviously have considerable financial implications.

➤ If you wish to prevent constant reestablishment of a link, make sure to set **PPPShorthold** to a value other than *-1.*

Manifestation: Setting Short Hold to *-1* on a VPN interface led to a system crash. In addition, this setting would lead to a panic after booting the router.

Current Status: This bug has been fixed.

4.1.5 Regular Rebooting Problems

Manifestation: In some cases, if the wrong number was configured for the dial-in partner, incoming connections may have led to the **biboDialTable** being overwritten with the loss of the **biboDialNumber** entries and/or the router rebooting.

Current status: This bug has been fixed.

4.1.6 PPP Callback and WIN2000

Manifestation: MS-Callback was not possible between a WIN2000 Client and a LAN-side BinTec router.

Current status: This bug has been fixed.

4.1.7 Transmission of RIP V1 & V2 Packets

Manifestation: During the establishment phase of a PPP connection, RIP packets were generated, but may have been discarded before transmission. Initial transmission of RIP packets may have taken up to 30 seconds.

Preconditions: This problem occurred if RIP was configured on a WAN interface.

Current status: This bug has been fixed; now RIP V1/V2 packets are automatically transmitted at connection time.

4.1.8 BOD not Activated due to Load Error

Manifestation: When calculating the load of a channel bundle, no load (**pppExtIfLoad**) was calculated. This meant that BOD could not be activated.

Preconditions: This problem only occurred when **pppExtIfAlgorithm** was set to *proportional*.

Workaround: If you do not want to upgrade to Release 5.2.1, to ensure a load is calculated and BOD works correctly with Release 5.1.1, it is necessary to leave **pppExtIfAlgorithm** set to the default value *equal.*

Current status: This bug has been fixed; **pppExtIfAlgorithm** can be set to *proportional* or *equal*.

4.1.9 Link Quality Monitoring Set to "0"

Manifestation: Concerning leased lines, when the variable **biboPPPLQMonitoring** in the **biboPPPTable** was set to the invalid value '*0*' instead of "off (*01*)", certain SNMP managers experienced problems.

Current status: This bug has been fixed.

4.1.10 Loopback Recognition for PPP Connections

Manifestation: the loopback condition was not recognized by the BinTec router, making it impossible for the status of the interface to be switched to *down*, in turn making it impossible for a backup connection to be established.

Current status: The loopback condition is now recognized by BinTec routers.

4.2 RADIUS

4.2.1 RADIUS for Dialout

Manifestation: In very rare cases, the problem may have occurred where on booting, the BRICK failed to load dialout routes from the RADIUS server. Subsequent authentication requests could not be made, causing the BRICK to reboot.

Connection problems may also have occurred after a temporary failure of the RADIUS server.

Current status: These bugs have been fixed.

4.2.2 RADIUS Dialout Causing Reboot

Manifestation: Directly after a dialout connection established over a Radius server is terminated, the BinTec router booted.

Preconditions: This problem occurred, and will reoccur, if customers using a Radius server for dialout make the following entry in the ´users file´.

```
BinTec-biboDialTable = "direction=incoming number=1234"
BinTec-biboDialTable = "direction=both number=1234"
```

Prevention: The correct configuration will ensure that the problem does not reoccur. Make sure that the **BinTec-biboDialTable** in the users file on the Radius server is set to *outgoing* for Radius dialout connections. Thus, for example:

```
BinTec-biboDialTable = "direction=outgoing number=1234"
```

Current status: Now despite the aforementioned configuration error, the BinTec router will not reboot.

4.2.3 RADIUS Users Saving Configurations

Manifestation: If a configuration was saved (cmd=save) while Radius connections were active with temporary WAN partners created on the BinTec router, the entries for those WAN partners loaded in the **biboDialTable** were also permanently saved in the configurtion. As Radius dynamically assigns the interface index, the interface settings saved on the router may have caused problems with Callback, for example.

Current status: This bug has been fixed: temporary entries loaded from a Radius server can no longer be saved as part of a currrent configuration.

4.2.4 Authentication Caused Memory Leakage

Manifestation: Incoming PPP calls authenticated via RADIUS caused a memory leakage of approx. 100 bytes for every connection establishment. This could lead to a restart of the BinTec router because of insufficient RAM available.

Current status: This bug has been fixed.

4.3 IPX

4.3.1 Netware Login on Booting

Manifestation: On attempting to connect to a BRICK from a dialup workstation (Win 95 or NT) installed as a Novell Netware client, logging in to the netware server or the NDS tree failed on booting, i.e. at the same time as the local login. The error message "*The tree or server cannot be found"* appeared.

Current status: This bug has been fixed.

4.3.2 ipxCircType Reset by Setup Tool Entry

Manifestation: If a value either *dynamic* or *ipxcpWS* was given to the variable **ipxCircType** in the SNMP shell and subsequently a change was made to the WAN partner configuration in Setup Tool, the value in the MIB table was automatically and unintentionally reset to either an unnumbered RIP or a WAN RIP. Do bear in mind, however, that when **type** = *ipxcpWS* and **NetNumber** = *0:0:0:0,* the value is correctly reset to an unnumbered RIP after such a Setup Tool entry.

Current status: This bug has been fixed.

4.3.3 BRICK IPX and Service Name Recognition

Manifestation: Services in an IPX network can be defined and distinguished by means of their network address, node address, socket number, the type and the service name. It is permissible for services to be distinguished merely by their service name. The BRICK IPX, however, did not allow the distinguishing of services by means of the service name.

Current status: Services can now be distinguished by means of the service name.

4.3.4 Memory Leakage

Manifestation: With an active IPX module, incoming PPP calls authenticated via RADIUS caused a memory leakage of approx. 100 bytes for every connection establishment. This could lead to a restart of the BinTec router because of insufficient RAM available.

Current status: This bug has been fixed.

4.3.5 New WAN Partner Causing Unwanted Connections

Manifestation: On configuring and saving for the first time a new WAN partner, a debug syslog message would report "no outgoing dial entry" although one had been configured. On saving a second time, a connection to the newly configured WAN partner was established, causing unintentional charges. This behaviour would cease after saving a third time.

Current status: This bug has been fixed.

4.3.6 IPX NetBIOS Rebroadcasting Error

Manifestation: Despite the fact that a connection to the WAN partner already existed, every rebroadcast of a NetBIOS packet resulted in the establishment of another connection.

Current Status: This bug has been fixed.

4.3.7 IPX Enabled After New Interface Configured

Manifestation: On configuring a new WAN partner over the SNMP shell, IPX was automatically enabled. This led to connections being established after every boot.

Precondition: The problem only occurred if a WAN partner was configured over the SNMP shell and not over Setup Tool.

Current Status: This bug has been fixed: IPX remains disabled when a new WAN partner is configured.

4.4 OSPF

4.4.1 Border Router Address Not Sent

Manifestation: A remote access server may not have learned the default route to the Internet. The ASBR (autonomous system border router) address was not learned by other areas in the system as the ASBR-Summary-LSA was not sent.

Preconditions: This problem affected autonomous systems communicating routes over OSPF.

Current status: This bug has been fixed.

4.4.2 Duplication of Areas

Manifestation: If an Area that already existed in the **ospfAreaTable** was created a second time (in the **ospfAreaTable** in the SNMP shell), these two entries for the same Area were dealt with separately. When one of these entries was deleted, however, all structures relevant to both of these Areas were also deleted, making the remaining entry ineffectual.

Current Status: This bug has been fixed: it is no longer possible for the same area to be duplicated. A syslog message is generated in such a case.

4.4.3 Summary LSAs not Sent to Areas

Manifestation: Summary LSAs (OSPF configuration packets) were not always sent to the appropriate Areas.

Current Status: The sending of Summary LSAs has been improved.

4.4.4 Reboot After Disabling and Enabling OSPF

Manifestation: In rare cases, after OSPF was disabled and then enabled again (in Setup Tool **IP** ➧ **OSPF** ➧ **STATIC SETTINGS**), the BinTec router may have responded with a reboot.

Precondition: After OSPF had been running for a longer time.

Current Status: This bug has been fixed.

4.4.5 Incorrect Value assigned to ospfIfMetricStatus

Manifestation: Instead of one of the two possible values *valid* or *invalid*, the value *0* was assigned to the variable **ospfIfMetricStatus** in the **ospfIfMetricTable**.

Current Status: This bug has been fixed.

4.5 Bridging

4.5.1 Bridging and ISDN Channel Bundles

Manifestation: Bridging packets could not be sent over more than one B-channel, for example over the Setup Tool setting: **ISDN Switch Type: Leased Line B1+B2 Channel (64S2).**

Preconditions: The error affected the second and all subsequent dynamically switched B-channels.

Current status: This bug has been fixed.

4.5.2 Filtering with more than 2 Interfaces

Manifestation: After the first filter was checked, subsequent filters configured for bridging interfaces were ignored.

Preconditions: There were at least 2 interfaces involved for which filters were set.

Current status: This bug has been fixed.

4.5.3 Timer not Conforming to Standard

Manifestation: Entries in the **dot1dTpFdbTable** are removed from the table after a certain time if they are not updated. The waiting time set is an adjustable value set in **dot1dTpAgingTime**. If, however, there is a topology change, the bridge must react faster so that all addresses remain reachable. In order to achieve this quicker reaction, the value in **dot1dStpForwardDelay** should be used instead of the value in **dot1dTpAgingTime**. Prior to release 5.2.1, this was not the case.

Current status: Now the correct value is used after a topology change.

4.6 IP

4.6.1 Interface 2 Invalid for ipExtRtTable

Manifestation: The values 1 (Local) or 2 (Ignore) for **DstIfIndex** in the **ipExtRtTable** were ineffectual. Instead packets thus configured were sent over the default route configured in the **ipRouteTable**.

Preconditions: This error occurred only when **DstIfIndex** was set toeither *1* or *2*.

Current status: This bug has been fixed and the values *1* or *2* for **DstIfIndex** in **ipExtRtTable** respond appropriately.

4.6.2 Back Route Verify Malfunction

Manifestation: A BinTec router could not receive dynamically assigned IP addresses from a DHCP server.

Preconditions: The IP address of the DHCP server was not entered on the BinTec router, causing the router to send a BootP request. Back Route Verify was activated on the router. The BinTec router used was running system software 5.1.1.

Current status: This bug has been fixed.

4.6.3 Back Route Verify Causing Unintentional Connections

Manifestation: Back Route Verify packets were not routed "back" to their source, but were sent on the default route, causing unintentional connections.

Preconditions: Back Route Verify was activated.

Current status: This bug has been fixed.

4.6.4 File Transfer by TFTP

Manifestation: A file transfer from the BinTec router to a TFTP server may have failed.

Preconditions: The configuration file was first saved by Xmodem. The BinTec router used was running system software 5.1.2 or lower.

Current status: This bug has been fixed.

4.6.5 Last Host IP address Not Assignable

Manifestation: The maximum number of IP addresses could not be assigned by DHCP. The final configured number in **Number of consecutive addresses** was miscalculated to the detriment of one. This meant that the last host IP address in the given range could not be assigned.

Current status: This bug has been fixed. Now all addresses in the given range can be assigned.

4.7 System

4.7.1 Flash Files Deleted

Manifestation: In very rare cases, all Flash files of the **biboAdmConfigDirTable** may have been deleted after repeated attempts were made to save new configuration files to Flash with the `cmd=save` command (**save as boot configuration** in Setup Tool). A reorganization would have been done automatically leading to the deletion error.

Workaround: If you have experienced this problem and are saving a configuration file without running system software 5.2.1, verify the file has been correctly saved to Flash by either looking for the file in the **biboAdmConfigDirTable** or by checking if the error "`CONFIG: err flash-get`" is reported in the

biboAdmSyslogTable. If your configuration file has not been saved, simply save the configuration file again with `cmd=save`.

Current status: The bug has been fixed.

4.7.2 Hieroglyphics After Failed CHAP Authentication

Manifestation: Characters of the ´debug´ Syslog message reporting a failed CHAP authentication request in a hyperterminal or a Telnet session appeared as hieroglyphics.

Current status: All non-printable characters will be represented as a period "." from this release on.

4.7.3 Y2K Compliance

Manifestation: The date in the SNMP shell was not Y2K compliant. The year number was incorrectly displayed. The following MIB tables and variables were affected:

- **msgForwardTable**
- **msgDirTable**
- **biboAdmSyslogTimeStamp**
- **isdnCallHistoryTime**
- **biboPPPLinkEstablished**
- **ipTafAuthTime**
- **X25CallHistoryTime**

Preconditions: The BinTec router used was running system software 5.1.1. or lower.

Current status: These inaccuracies have been corrected.

4.7.4 Ping Fails After Time Reset

Manifestation: The ping program failed, erratic negative ping times were recorded, no further data readout was exchanged. The session had to be ended with Ctrl-C.

Precondition: ISDN was the method used to retrieve the current time (**biboAdmTimeProtocol**=*isdn*) and a time update took place.

Current Status: This bug has been fixed.

4.7.5 Trace with a Specified Interface

Manifestation: If a trace command with a specified interface name was given, for example,

```
trace -hip T-Online
```

the application waited for the next call to any interface and not that specified interface.

Current Status: This bug has been fixed. The trace command now waits for the next call to the specified interface.

4.8 SetupTool

4.8.1 System Crash After File Loaded

Manifestation: If, after getting and loading a configuration file by TFTP that has been initially created with the Configuration Wizard, a Setup Tool crash may have occurred on leaving the ***PPP*** ➧ ***PPP PROFILE CONFIGURATION*** menu via ***SAVE***:

```
BRICK-XS Setup Tool                          BinTec Communications AG
[PPP] PPP Profile Configuration                                  MyXS


        Authentication Protocol          CHAP+PAP+MS-CHAP
        Radius Server Authentication     none

        PPP Link Quality Monitoring      no


                SAVE                          CANCEL

Use <Space> to select
```

Current status: This bug has been fixed.

4.8.2 System Crash After PPP Menu Entry

Manifestation: Attempts to configure PPP entries over Setup Tool led to a system crash.

Preconditions: The loading of a configuration file that had been created by the Configuration Wizard and saved in the Flash led to the deletion of entries previously configured in the **pppProfileTable**. The table would remain empty until the next reboot.

Current status: This bug has been fixed.

4.9 ISDN

4.9.1 Credits Based Accounting: Connections not Terminated

Manifestation: The settings **MaxOutDuration** and **MaxInduration** in ***ISDN*** ➧ ***CREDITS*** ➧ ***EDIT*** are designed to limit the total length of all incoming/outgoing calls. Although no further connections could be made, existing connections were not terminated after reaching the values set for these variables.

Current status: This bug has been fixed.

4.9.2 X.31 Connections on ISDN B-Channel Could Not be Established

Background: When establishing an X.31 connection on the ISDN B-channel, SABM collisions can occur. In this case, both sites (DCE and DTE) should send a UA response as soon as possible.

The BinTec router, when configured as DCE, should migrate to the next state

1. after receiving the UA response or
2. after sending the UA response or
3. after sending the UA response and the UA response of the remote site was not received within the timeout.

Manifestation: Until now the BinTec router behaved according to 1 and 3. In some cases, the connection to some terminal adapters could not be established because the BinTec router did not change to the next state after sending a UA response (2) and therefore could not accept the RESTART packet sent by the remote site.

Current status: With Release 5.2.1 the BinTec router also behaves according to 2, the connection can be established to every terminal adapter.

4.10 CAPI

4.10.1 Transmitting Faxes with FM-8MOD

Manifestation: The transmission level of the FM-8MOD modems was set too high which may have caused problems when transmitting faxes.

Current Status: This bug has been fixed. The value of the transmission level is adjustable now (see chapter 3.3.2, page 74) and the default value is set to *db6* which is normally used for fax transmission in Germany.

4.10.2 Video-Telephony: Transmitting Data with CM-PRI in Transparent Mode

Manifestation: In rare cases, when transmitting data with the CM-PRI module in transparent mode, the data transmission may have failed due to additional bytes that might have been sent in the beginning of data transmission. This problem was only encountered in connection with video-telephony.

Current status: This bug has been fixed.

5 Known Issues

5.1 Problems with Windows NT 4.0 SP 6A

5.1.1 Authentication with MS-CHAP V2

When the **Domain** name is activated when using MS-CHAP V2 and Windows NT 4.0 Service Pack 6A, inband authentication fails.

This Microsoft problem does not occur if the dial-in client is initially identified by CLID (outband) or a RADIUS server is used in the case of inband authentication.

5.2 Windows 2000

5.2.1 DNS Proxy Cannot Resolve DNS Requests from Windows 2000

When PCs running Windows 2000 send DNS requests to the BinTec router's DNS Proxy and a negative static name entry exists for a requested name, the BinTec router tries to resolve the name instead of answering the request negatively and not passing it to another name server. This way unwanted connections are established, generating costs.

5.2.2 Callback and the User-Specified Number

Another problem when using Windows NT 4.0 Service Pack 6A is that the user-defined callback number is not recognized by the Windows NT computer. Only callback numbers configured by the administrator on the BinTec router at the central-site can lead to a successful callback call.

5.3 FM-8MOD

5.3.1 No Module Detected

If two modem shuttles for FM-8MOD modules were installed in a BIANCA/BRICK-XL2, after starting or restarting, in rare cases, the BinTec router can not detect the modems of one of the shuttles.

5.4 FTP

5.4.1 Outgoing FTP Connections via NAT

When outgoing FTP connections occur via NAT, data transfer does not work with some FTP servers. The connection is established, the FTP client can register with the server. Commands such as `cd` and pwd work, but others such as `dir` and `get` do not.

The problem can be dealt with if the client is switched to the passive mode. This is not, however, possible with all FTP clients.

5.5 Setup Tool

5.5.1 *WAN INTERFACE* ➧ *ADVANCED SETTINGS* Inaccessible

Products affected: BIANCA/BRICK-XS2, -XM2, -XL, -XMP.

With System Software Release 5.2.1 the Setup Tool menu ***WAN INTERFACE*** ➧ ***ADVANCED SETTINGS*** is erroneously not visible and thus not accessible via Setup Tool.

In order to change the X.31 TEI service for your external interface, use the **isdnDChanX31Table** in the SNMP shell.

To change the X.31 TEI service, proceed as follows:

isdnDChanX31Table

- Type **isdnDChanX31Table** into the SNMP shell, press **Return**.
- Change the service for which you want to use X.31 TEI in the variable **AssignedTo** by entering the variable name, the table index number containing the wrong entry, and the new value via the following syntax:
  Example: `AssignedTo:00=capi`
- Press **Return** and save your changes by typing `cmd=save`.
- Verify your new settings by typing again `isdnDChanX31Table`, press **Return**.

isdnIfTable

- Type **isdnIfTable** into the SNMP shell, press **Return**.
  Check if the variable **UsePowerDetector** has its default value *use* and the variable **Autoconfig** has its default value *on*.
  If this is not the case, change the values by entering the variable name, the table index number containing the wrong entry, and the new value via the following syntax:
  Example: `UsePowerDetector:00=use Autoconfig:00=on`
- Press **Return**.
- Reboot your BinTec router with the `halt` command.
- Verify your settings in the **isdnDChanX31Table**.

5.5.2 WAN Partner: IP Address Pool Erroneously Reset to 0

In the Setup Tool field **IP Address Pool** in the menu ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***, it is not sufficient to select **OK** to save your changes, but you must **SAVE** the complete WAN partner configuration, i.e. se-

lect **SAVE** twice. If you only select **OK** to save your changes, the new value is reset to 0 with the next entry.

You can also change the IP Address Pool settings via the **biboPPPTable** in the SNMP Shell.

To change and save your settings, proceed as follows:

- Type **biboPPPTable** into the SNMP shell, press **Return**.
- Type in **IpPoolId**, press **Return**.
- Change the value for **IpPoolId** by entering the variable name, the table index number containing the wrong entry, and the new **IpPoolId** value via the following syntax:
  Example: `IpPoolId:00=5`
- Verify your new settings by typing in again `IpPoolId`, press **Return**.

5.6 RADIUS

5.6.1 RADIUS Server Configuration

Products affected: BIANCA/BRICK-XS2, -XM2, -XL, -XMP

If you want to configure your BinTec router as a RADIUS server, go to Setup Tool menu ***IP*** ➧ ***RADIUS SERVER***. If you try to configure the RADIUS server in ***IP*** ➧ ***STATIC SETTINGS*** in the field **Radius Server** you will not be able to save your settings.

5.7 SNMP

5.7.1 Wrong Default Value for Variable FaxG3ECM

With System Software Release 5.2.1, the default value for the MIB variable **FaxG3ECM** in the **capiConfigTable** is erroneously set to *on*. It is highly recommended to change the value to *off* as the ECM does not work perfectly yet.

To change the value to *off* in the SNMP shell, proceed as follows:

- Type in `capiConfigTable`, press **Return**.
- Change the value for **FaxG3ECM** to *off* by entering the variable name, the table index number containing the wrong entry, and the new value via the following syntax:
  Example: `FaxG3ECM:00=off`
- Press **Return**.
- Verify your new settings by typing in again `capiconfigtable`, press **Return**.

5.8 CAPI

5.8.1 BRICK-XM: Outgoing CAPI Connections Cause Reboots

In some cases, outgoing CAPI connections cause reboots of a BRICK-XM.

5.9 Setup Tool

5.9.1 BRICK-XM: Setup Tool can not be Called Up

In some cases, Seutp Tool cannot be called up on BRICK-XM due to a lack of memory, the message `cannot execute command, Not enough space` is displayed instead.

As a workaround you can reboot the BRICK-XM or upgrade system memory to 8 MB. Afterwards Setup Tool can be called up again.

5.9.2 *MENU CM-1BRI, ISDN S0*: Selection Under B-Channel 1 is Displayed Wrongly

If you configure an ISDN interface in the Setup Tool menu ***CM-1BRI, ISDN S0*** and select the following:

ISDN Switch Type = *leased line B1 channel (64S)* and
B-Channel 1 = *leased dce*,

it is displayed wrongly, when you leave the menu with **SAVE** and enter it again:

B-Channel 1= *leased dte*.

The BinTec router accepts the setting correctly, but does not display it in the Setup Tool menu mentioned above.

5.10 Frame Relay

5.10.1 Frame Relay Not Working

The feature Frame Relay does not work with Release 5.2.1.