Release Notes
System Software Release 6.1.2

September 2001

System Software Release 6.1.2

These Release Notes desribe new features, changes, bugfixes, and known issues of for System Software Release 6.1.2.

Table of Contents

Table of Contents

1 Introduction

With the release of System Software Release 6.1.2, BinTec Communications AG unifies the System Software for all routers of the X-generation. There are prominent new features like Quality of Service (QoS), Hardware Encryption for IPSec, a new licensing mechanism, changes and enhancements like a Multiuser WAN Partner, PPPoE Server Mode, a Silent Deny in NAT (Network Address Translation), and, of course, bugfixes. Depending on your type of router, the bugfixes described here relate to known issues of different versions of the system software. It may, therefore, be the case that a problem is mentioned which has been solved already in some builds of the system software, but not in others. Since not all bugfixes could be included in these release notes, please refer to earlier release notes and to our **Last Minute Information** which you can find at www.bintec.net, if you need further information.

1.1 How to Update to System Software Release 6.1.2

System Software Release 6.1.2 requires a more thorough update of your router's software than other updates have done so far. You have to update not only the System Software itself, but the BOOTmonitor and the Firmware Logic (for the basic unit and your expansion cards alike), as well. You can download all necessary files from www.bintec.net.

For updating to the initial release of system software version 6.1.2, BinTec will provide a single software file (BLUP = BinTec Large Update) that contains all necessary updates, i.e. the BOOTmonitor, the Firmware Logic (for the basic unit as well as for expansion cards) and the system software. You only need to complete the update process described in chapter 1.1.1, page 8 once to update all of your software. Later, the individual files will be available, too. Please, look for the update files on BinTec's webserver at http://www.bintec.net.

1.1.1 Updating to System Software Release 6.1.2 Using the BLUP

This chapter describes the procedure you need to follow when updating software images. For the initial update with the BLUP, you have to complete the update process only once.

Caution!

The update operation involves the risk that if updating one of these files fails, e.g. due to a power cut, it may no longer be possible to boot your router, i.e. it is damaged. You would then have to send your router in to your vendor.

The update is carried out using the BOOTmonitor. It is possible to update the Logic, BOOTmonitor and System Software, too, in one BOOTmonitor session.

- Configure a computer in your local network as TFTP server. For a Windows PC, you can use the TFTP server of **DIME Tools** (see documentation for **BRICKWare for Windows** which you can download from our webserver).
- Copy the update file (the BLUP, e.g. bl6102.x4a) downloaded from BinTec´s Web server to the TFTP folder on your TFTP server in your local network.
- Log in on your router from a computer serially connected and reboot the router by typing `cmd=reboot` in the SNMP shell.

`cmd=reboot` is not a command in the usual sense of the term. With this command the MIB-Variable **biboAdmConfigCmd** is assigned the value *reboot*. This leads to the termination of all currently running Flash operations and then to a restart of the system.

Your router restarts. When self tests are completed, the following line shows:

```
Press <sp> for boot monitor or any other key to boot system
```

➤ Now press **Space** within four seconds to enter BOOTmonitor mode (please note that all values shown here are examples only).

```
BINTEC X4000 Bootmonitor V. 5.1 Rev. 5 from 2000/08/07
Copyright (c) by BinTec Communications AG

(1) Boot System
(2) Software Update via TFTP
(3) Software Update via XMODEM
(4) Delete Configuration
(5) Default Bootmonitor Parameters
(6) Show system information

Your choice>
```

The menu `(6) Show system information` is only displayed when the BOOTmonitor has version 5.1.5 or higher.

It enables you to display some useful information about X4000, e.g. serial number, MAC address, current software, and so on.

➤ To carry out the update via TFTP choose 2 and confirm with **Return**. You must then enter the IP address of router, the IP address of the TFTP server and the file name of the file to be updated, e.g. the BLUP, and confirm each entry with **Return** (if the entries indicated in squared brackets are correct, you need not enter them again, just confirm with **Return**).

```
Your choice> 2
Enter local IP address [192.168.1.254]:
Enter IP address of TFTP server [192.168.1.1]:
Enter file name of image []: bl6102.x4a

Are your entries correct (y or n) ?
```

➤ Reexamine your settings. If they are correct, confirm with y and the **Return** key.

```
Starting file transfer ..OK (65588 bytes received)
Checking new image ... OK

Loaded new image has release 6.1.2

Now choose from the following:

(u) Update Flash ROM
(r) Write image to RAM and start it
(e) Exit

Enter (u, r or e):
```

➤ Choose `r` to load the new image into the RAM.

The router boots.

```
Booting BOSS...
boss image started at 0x82a034

BINTEC X4000 BLUP V.6.1 Rev.2 from 2001/08/09 00:00:00
Copyright (c) 2001 by BinTec Communications AG

List of files in this update:
Version    Length  Name
    2.1     65588  Logic
  6.1.1    131124  Bootmon
  6.1.1   1231677  Boss
    2.0     70028  x4e_2pri.x4a
    1.2     12097  x4e_3bri.x4a

Proceed with update (y or n) ?
```

➤ Confirm with `y` to update all necessary files and save the files to the flash.

The following messages will be printed to the console window:

```
*** Don’t power-off your router while the update takes place
***


Updating Logic
New logic has release 2.1.
Erasing Flash-ROM . OK
Writing Flash-ROM . OK
Verify  Flash-ROM . OK

Updating Bootmon
New bootmonitor has release 6.1.2
Erasing Flash-ROM .. OK
Writing Flash-ROM .. OK
Verify  Flash-ROM .. OK

Updating Boss
New software release is 6.1.2
Erasing Flash-ROM ................... OK
Writing Flash-ROM ................... OK
Verify  Flash-ROM ................... OK

Updating x4e_2pri.x4a

Perform Flash-ROM update
Update  Flash-ROM .. OK
Verify  Flash-ROM .. OK

File update successfully finished

Updating x4e_3bri.x4a

Perform Flash-ROM update
Update  Flash-ROM . OK
Verify  Flash-ROM . OK

File update successfully finished
```

The router now reboots, loading the new system software, and you are presented with the login prompt.

1.1.2 Updating Individual Files

Once the individual update files are made available for download on www.bintec.net, you can update specific parts of your router’s software. If you do not want or do not need to update all software in a single BOOTmonitor ses-

sion, you need not reboot your router and enter the BOOTmonitor to update the system software. You can follow the procedure described in your **User's Guide**, chapter "Configuration Management".
Note, however, that the BOOTmonitor and the Firmware Logic for the basic unit cannot be updated with the `update` command. You can find information on how to update the routers's BOOTmonitor and Logic in the **Release Notes Logic** you can download from our web server.

2 New Features

The following new features have been implemented in System Software Release 6.1.2:

2.1 Easy Licensing

Beginning with System Software Release 6.1.2, BinTec introduces a new system of licensing your hardware and software products. The basic licenses your router comes with are no longer found in form of a license key, mask and serial number, but all of them are enabled by default. Only when you purchase additional hardware or software licenses do you have to go through the following procedure to enable them.

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

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

The licenses of the ex works state are reactivated.

License Data

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

Please note that with System Software Release 6.1.2 you must obtain your license data in the described way. You will no longer be able to enter license data of the kind you have previously found on the license data sheet.

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

Valid licenses that have been entered before updating to System Software Release 6.1.2, however, will be recognized and you need not reenter them.

Entering a License

To enter your license proceed as follows:

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

The licenses, which are already enabled on your router, are listed under **Available Licenses**. The field **Software License ID** displays the serial number of your router which you need to enter to enable any software licenses (in the case of **X8500** it displays the serial number of internal Smart Media Flash Card).

The relevant menu in the Setup Tool looks like this:

```
X4000 Setup Tool                                BinTec Communications AG
[LICENSE]: Licenses                                              MyRouter

Available Licenses:

IP (builtin), STAC, CAPI, BRIDGE

Software License ID: X4A2001IWAN0020

Serialnumber     Mask     Key             Description      State
999999           55       88PNUPZ         composite        ok


ADD                       DELETE                        EXIT

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

To enter your license, proceed as follows:

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

  Another menu window opens.

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

- Confirm with **SAVE.**

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

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

➤ Try again.

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

Disabling a License

Proceed as follows to disable a license on your router:

➤ Go to ***LICENSES***.

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

➤ Confirm with **DELETE**.

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

2.2 Quality of Service (QoS)

The following chapters provide a survey of QoS only, and there is no configuration guide. For a complete description of BinTec's QoS implementation and its configuration, see the document **Quality of Service** which you can find on your BinTec Companion CD or download from www.bintec.net.

What is QoS?

Increasing Intra- and Internet traffic as well as a development towards converging voice and data networks call for intelligent bandwidth management. Quality of Service intelligently and efficiently takes control of available bandwidth and, if needed, reserves bandwidth and assigns it to specific services. This is what it can achieve:

- Avoiding network congestion (in either LAN or in WAN segments)
- Minimizing the loss of IP packets
- Optimizing the latency of certain services

In order to realize IP QoS, you should complete three steps. First you should identify the data traffic in your network segments, second you should quantify the traffic and third you should prioritize the services and assign the available bandwidth.

BinTec QoS

Our implementation of QoS offers support for the entire family of IP protocols. IP packets are processed according to the Differentiated Service Model, i.e. on the basis of a classification of IP packets (service recognition). By means of a set of rules, the IP packets of particular services are specified and divided into classes. This classification is performed for individual interfaces specifically and can be applied to LAN interfaces as well as to WAN interfaces. Once IP packets are classified, they are prioritized according to configurable strategies. The configuration of these strategies, however, is presently restricted to WAN interfaces. By means of packet level signalling, a router can communicate to adjacent network nodes that specific data must be handled in a specific way. Signalling is conducted by tagging the specified packets through the TOS field of the IP header. It is essential for coordinating data traffic shaped by other network nodes. Success of extensive end-to-end QoS services depends substantially on this kind of signalling.

Benefits

Quality of Service offers the following benefits:

- Time-critical data (e.g. VoIP) can be treated with high priority. For comparatively slow PPP connections, a particular algorithm reduces the latency of high priority packets (MLPPP Interleave, cf. "Multilink PPP (MLPPP)", page 23).

- The "normal priority" class of data traffic can be divided into up to 255 classes, allowing for highly differentiated data handling.
- It is possible to dedicate bandwidth to specific IP packets (and thus to specific services, Traffic Shaping).
- Network congestion is detected and resolved by various queuing algorithms (cf. "Scheduling Algorithms", page 20).
- Network Congestion can be avoided by means of Random Early Detection (RED). This reduces packet loss, especially when data traffic temporarily exceeds the assigned bandwidth limit (cf. "Congestion Avoidance", page 22).

2.2.1 Configuration Overview

QoS configuration is carried out in the ***QoS*** menu:

```
X4000 Setup Tool                                BinTec Communications AG
[QoS]: QoS Configuration                                        MyRouter

                        IP Filter
                        IP Classification and Signalling

                        Interfaces and Policies



                        Exit

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

IP filters are defined in ***QoS*** ➧ ***IP FILTER*** to specify particular IP packets (services). The procedure you should follow here is described in the **User's Guide** you have received upon purchasing your router, the relevant chapter is "Filters (Access Lists)".

Rule chains for classifying IP packets according to predefined filters are created in the ***QoS*** ➧ ***IP Classification and Signalling*** menu. Several filters can be combined and the data flow can be divided into different classes of packets. Likewise, different types of IP packets can be collected into a single class and can be treated with the same priority. TOS field signalling for devices other than the router itself (e.g. switches) is equally defined by these rule chains.

The ***QoS*** ➧ ***Interfaces and Policies*** is used to specify which rules apply to which interface. For example, all packets coming in through the Ethernet interface (en1) can be examined and classified, and all outgoing traffic of some WAN connection can be manipulated at the same time, but according to different rule chains.

Moreover, you can configure the following settings for either one or several WAN interfaces:

- Queuing strategies are defined in ***QoS*** ➧ ***Interfaces and Policies*** ➧ ***Edit*** ➧ ***QoS Scheduling and Shaping***.
- Bandwidth restriction and dedication are defined in ***QoS*** ➧ ***Interfaces and Policies*** ➧ ***Edit*** ➧ ***Class-Based QoS Policies*** ➧ ***Add***.
- Congestion Avoidance strategies like RED (Random Early Detection) are defined in ***QoS*** ➧ ***Interfaces and Policies*** ➧ ***Edit*** ➧ ***Class-Based QoS Policies*** ➧ ***Add***.
- To reduce the latency of high priority packets you can configure MLPPP Interleave (only for single link connections) in ***QoS*** ➧ ***Interfaces and Policies*** ➧ ***Edit***.

2.2.2 Classification and TOS Signalling

Upon classification the packets that have been specified by filters are assigned either to the high priority or to a normal priority class. By means of a Class ID, the normal priority class can be additionally divided into up to 255 subclasses. For each of these subclasses a specific policy can be defined for how packets are to be processed, especially during network congestion.

A maximum packet rate can be specified by TOS signalling. Packets that would exceed the limit of this rate are not manipulated, but are preferably discarded during network congestion, as long as they do not belong to the high priority class. Classification and TOS signalling are defined in ***QoS*** ➧ ***IP CLASSIFICATION AND SINGALLING*** ➧ ***ADD*** or in ***QoS*** ➧ ***IP CLASSIFICATION AND SINGALLING*** ➧ ***EDIT***.

2.2.3 QoS Bandwidth Management

If QoS is enabled on a WAN interface, additional settings can be made in ***QoS*** ➧ ***INTERFACES AND POLICIES***. These settings concern the manipulation of classified IP packets, e.g. queuing and discarding strategies.

The send-side operates with at least three queues: one queue for high priority data, 1 to 255 queues for normal priority data, and a default queue for all unclassified data. The number of normal priority queues equals the number of policies entered for this class in ***QoS*** ➧ ***INTERFACES AND POLICIES*** ➧ ***EDIT*** ➧ ***CLASS-BASED QOS POLICIES*** ➧ ***ADD***. All packets that are not assigned to a class and for which there is no preset policy are assigned to the default queue. A single policy can be defined for the default queue, and packets not assigned to either the high or the normal priority class can thus be integrated into the queueing and scheduling procedure. No policy, however, can be defined for the high priority queue, since configuring discarding and queueing strategies for data that are to be processed as quickly as possible would not be reasonable. Only a bandwidth restriction can be applied.

Scheduling Algorithms

Presently three scheduling algorithms have been implemented:

- Priority Queuing (PQ): The order in which packets are processed is determined only by the priority of the queue they are assigned to. Any queue is processed only once all higher priority queues have been emptied.
- Weighted Round-Robin Scheduling (WRR): According to a configurable weighting routine all classes will be handled in relation to one another.

- Weighted Fair Queueing (WFQ): Different traffic flows are processed as "fairly" as possible, so that within a queue or class a single connection cannot consume bandwidth to an unproportional expense of other connections.

Only available bandwidth is assigned by these algorithms. Queues which are not yet using all of the bandwidth dedicated to them are served first, and independently of the queueing and scheduling chosen, high priority queues are always preferred.

Traffic Shaping

Traffic Shaping specifies a maximum transfer rate (in bits) for a single interface. This limit is applied to all kinds of data, i.e. it includes high priority packets as well as normal priority ones, but also system messages like keepalive or RIP packets. Traffic Shaping is especially useful for limiting the bandwidth of virtual (WAN)interfaces which are realized via an interface with larger bandwidth, like e.g. PPP over PPTP or PPPoE.

Policies

A policy can be defined for each class, determining to which queue a packet is assigned during the preconfigured scheduling process. The kind of queue and the kind of configuration which is possible is determined by the priority class the policy is supposed to be valid for. As with classification, high priority and the up to 255 normal priority classes are distinguished, as well as the default class to which all previously unassigned packets are assigned.

It is possible to assign a certain portion of the overall bandwidth to each queue and thus to each class.

High priority packets are always preferred over any other kind of data. Therefore, bandwidth that has been dedicated to normal priority classes may be used for transmitting high priority data if the configuration is inconsistent (i.e. if the sum of individual bandwidth shares assigned to all classes is larger than the overall bandwidth available).

Congestion Avoidance

TCP connections typically react to network congestion with a (temporary) reduction of the negotiated transfer rate. If packets are discarded with a probability that is proportional to the average fill level of the queue they belong to, the queue averages a shorter length and the maximum length allowed is reached less often. After the maximum queue length has been reached, packets are discarded. Moreover, this procedure achieves a smaller average transit delay and significantly smaller packet loss rates in case queue bursts lead to the application of dropping algorithms. RED (Random Early Detection) is activated (if it has been configured) with queue lengths that vary between the Lower Queue Treshold and the Upper Queue Treshold values.

This algorithm is effective only if the data flow is predominantly composed of TCP based data and the respective TCP implementations are consistent with TCP standards, i.e. if they cooperate with this specific kind of signalling. Data flows other than TCP (like UDP flows) remain unaffected.

Treshold Levels

As long as a queue is shorter than the Lower Treshold Value suggests, neither dropping nor congestion avoidance algorithms are applied.

Once a queue is longer than the Lower Treshold value suggests, but shorter than the Upper Queue Treshold suggests, QoS tries not to allow the queue to grow any longer (depending on what dropping algorithms have bee configured).

If the Upper Queue Treshold is exceeded, packets are dropped according to the configured dropping policy.

The following dropping algorithms are available:

- *tail-drop*: The packet last added to the queue is discarded..
- *head-drop*: The oldest packet in the queue is discarded.
- *random-drop*: A randomly chosen packet is discarded.

Multilink PPP (MLPPP)

MLPPP is a special PPP mode for comparatively low bandwidth connections like ISDN or X.21. It is useful for reducing the transit delay of high priority packets in comparison to a conventional PPP connection. This is achieved by fragmenting normal priority packets as soon as they have a certain size. If needed, a high priority packet can then be inserted between the fragments for immediate transmission.

2.3 New RADIUS Features

2.3.1 Login Authentication via RADIUS

With System Software Release 6.1.2 user authentication on the login shell is performed through a RADIUS authentication request. The router proceeds as follows:

When a login name and a password are entered in a login-shell (of e.g. ISDN Login, Telnet, Console or Minipad), the router checks if a RADIUS server is configured for login authentication.

If a RADIUS server is configured on the router, an alive check is performed, and, if successful, an authentication request is sent. If the RADIUS server is unreachable, the router continues with local authentication as described below. If the RADIUS servers responds, it checks the login-data, if it does not respond, the router again proceeds with local authentication. If the RADIUS server performs the authentication and the login data are valid, access to the shell prompt is granted. If the data are invalid, the user is presented with a new login prompt.

If no RADIUS server is configured, it checks the login name and which access level is assigned to it. Next, it checks the entered password and whether it matches the password configured for the access level. If authentication is successful, access to the shell prompt is granted. If authentication, however, fails the user is presented with a new login prompt.

The following figure represents this procedure:

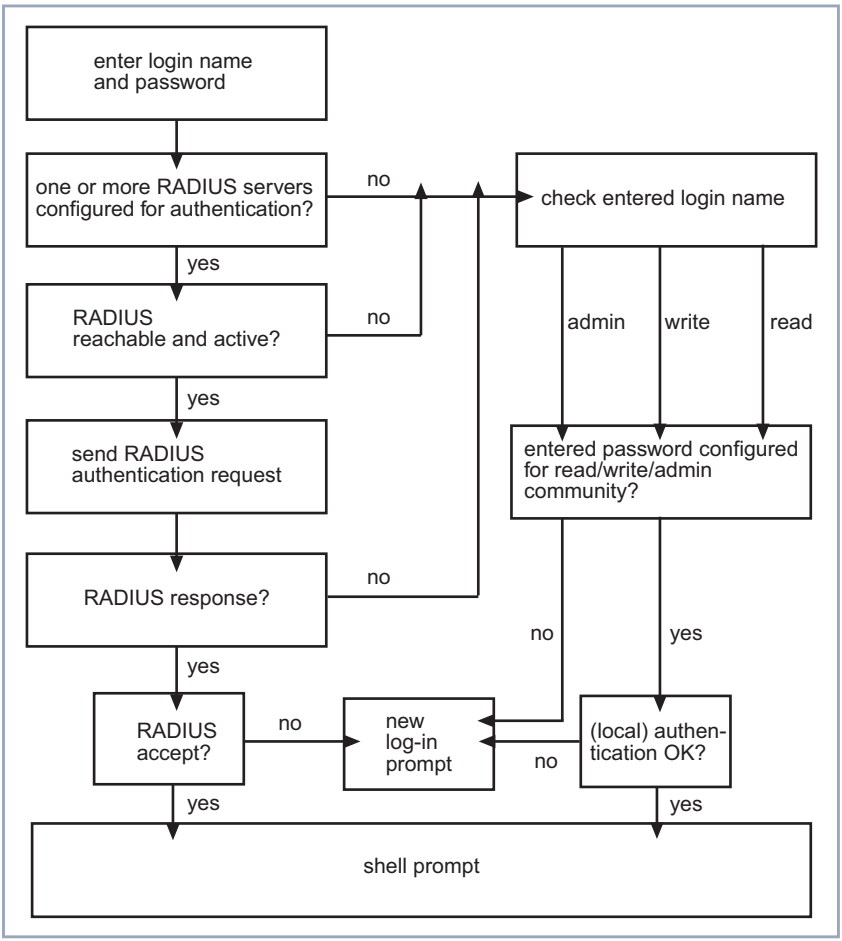

Figure 2-1: RADIUS login authentication

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

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

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

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

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

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

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

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

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

2.3.2 Client Authentication during Callback

Prior to System Software Release 6.1.2 it was mandatory for PPP authentication during a callback that BinTec specific RADIUS attributes were used to transmit the necessary protocol/ID/password triple. These settings were then sent back to the remote access server. This procedure had some drawbacks, since there were compatibility issues with certain user data bases a RADIUS server may have to interact with (especially Windows NT), as well as with the Microsoft IAS RADIUS server. Moreover, with this configuration sensitive data were sent unencrypted from the RADIUS servers to the remote access server.

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

2.4 Hardware Encryption

BinTec's modular routers of the X-generation can be equipped with expansion cards or resource modules that carry the HiFn chip for hardware encryption and MAC (Message Authentication Code) in IPSec. Hardware encryption, e.g., raises the throughput of an IPSec Ethernet/Ethernet connection through a **X4000** by at least 100% in case of small packet sizes and up to 800% in case of large packets sizes (1280 bit). With System Software Release 6.1.2, the HiFn chip is now supported, and offers a significant increase in the availability of security features. It operates without any further configuration whenever an supported algorithm is used (i.e. DES, 3DES, SHA-1 or MD5).

2.5 Multiuser WAN Partner

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

Creating a Multiuser WAN Partner

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

On how to create a WAN partner, please refer to the **User's Guide** of your router. You can find the relevant information in the "Basic Configuration" chapters.

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

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

```
inx IfIndex(ro)              Type(*rw)              Encapsulation(-rw)
    Keepalive(rw)            Timeout(rw)            Compression(rw)
    Authentication(rw)       AuthIdent(rw)          AuthSecret(rw)
    IpAddress(rw)            RetryTime(rw)          BlockTime(rw)
    MaxRetries(rw)           ShortHold(rw)          InitConn(rw)
    MaxConn(rw)              MinConn(rw)            Callback(rw)
    Layer1Protocol(rw)       LoginString(rw)        VJHeaderComp(rw)
    Layer2Mode(rw)           DynShortHold(rw)       LocalIdent(rw)
    DNSNegotiation(rw)       Encryption(rw)         LQMonitoring(rw)
    IpPoolId(rw)             SessionTimeout(rw)

 02 10001                    multiuser              ppp
    off                      3000                   none
    chap                     "user"                 "geheim"
    dynamic_server           4                      300
    5                        20                     1
    2                        1                      disabled
    data_64k                                        disabled
    auto                     0
    enabled                  none                   off
    0                        0
```

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

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

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

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

On how to create an IP address pool, please refer to the **User's Guide**. You can find the relevant information in the "Advanced Configuration" chapters.

Channel Bundling and Callback

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

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

2.6 Mutual PPP Authentication

Prior to System Software Release 6.1.2, authentication was only required from the calling party, but not from the called party (with the exception of negotiated callback). Mutual authentication must be enabled through the newly created MIB variable **pppExtIfAuthMutual**, the default value is *1*=disabled (*2*=enabled). During the LCP (Link Control Protocol) negotiation, the router tries to negotiate and use the same authentication protocol for both authentications.

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

2.7 PPPoE Server Mode

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

2.8 Flash File System

System Software Release 6.1.2 introduces a new flash file system which allows to dynamically store different kinds of data in the Flash ROM of your router. It facilitates handling the Firmware Logic of expansion cards and resource modules.

By entering `update -i` in the SNMP command prompt, you can access the Flash ROM management shell. Here you can list, update and organize all files currently stored. An online help is accessible by entering `help` in the command prompt.

2.9 Additional MIB Tables CPU and Memory

With System Software Release 6.1.2, information about the CPU and memory usage of your router is stored in the newly created **CpuTable** and **MemoryTable**. All information is read only.

The **CpuTable** contains the following variables (values are examples):

```
inx Number(*ro)
    TotalSystem(ro)         Descr(ro)             TotalUser(ro)
    LoadUser(ro)            TotalStreams(ro)      TotalUser(ro)
    LoadIdle(ro)            LoadSystem(ro)        LoadStreams(ro)
    LoadStreams10s(ro)      LoadUser10s(ro)       LoadSystem10s(ro)
    LoadSystem60s(ro)       LoadIdle10s(ro)       LoadUser60s(ro)
                            LoadStreams60s(ro)    LoadIdle60s(ro)

 00 1
    2                       "Onboard MPC 860"     4
    0                       8                     6595
    100                     0                     0
    0                       0                     0
    0                       100                   0
                            0                     100
```

The **MemoryTable** contains the following variables (values, again, are examples)

```
inx Type(*ro)
    Inuse(ro)           Descr(ro)          BlockSize(ro)   Total(ro)
    NFails(ro)          DramUse(ro         NAllocs(ro)     NFrees(ro)

00  flash
    0                   "Onboard Flash"    0               4194304
    0                   0                  0               0

 01 dram
    4833681             "Main Memory"      0               16711680
    0                   0                  69313           69056

 02 dpool
    2                   "STREAMS Class 0"  0               32
    0                   3072               23050           23048
```

2.10 Silent Deny in NAT (Network Address Translation)

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

If Silent Deny in NAT is enabled, however, neither message is sent. This option has been common in the configuration of IP Access Rules, and is now made available for NAT. It is useful when much unsolicited incoming traffic has to be handled, and the originators of the packets need or should not be informed that the traffic has been blocked. Not informing a packet originator of discarded packets can be a vital security function if the ports of inactive services are supposed to be in stealth mode.

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

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

2.11 Keepalive for Multi-Protocol HDLC Framing

With System Software Release 6.1.2, there now is a keepalive for encapsulation *Multi-Protocol HDLC Framing*. Thus the keepalive of Cisco routers operating on the remote side is supported. It is configured through the **biboPPPKeepalive** variable in the **biboPPPTable**. The default value *1* (off) means that the keepalive is in passive mode. In this mode all received keepalive packets are answered with a keepalive request, and no checks are performed upon outstanding remote keepalive requests.

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

2.12 New Restart Delay Timer in X.25

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

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

3 Changes

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

- Bridging and X.25 Availability (chapter 3.1, page 34)
- HP OpenView Compatibility (chapter 3.2, page 35)
- IPX no Longer Supported (chapter 3.3, page 35)
- Changes in RADIUS Implementation (chapter 3.4, page 36)
- Configurable MTU and MRU Values (chapter 3.5, page 36)
- Interface Blocked with Inconsistent Encryption Configurations (chapter 3.6, page 37)
- Interdependent Configuration of PPP Encapsulation, Encryption and Compression (chapter 3.7, page 42)
- New Activity Monitor Password (chapter 3.8, page 43)
- New License State "*not supported*" (chapter 3.9, page 43)
- Discarding Link Level Broadcast Packets (chapter 3.10, page 43)

3.1 Bridging and X.25 Availability

With System Software Release 6.1.2, Bridging of IP protocols is available on all X-Generation routers without a software license.

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

In bridging each bridge makes its own routing decisions and is therefore transparent to the communicating hosts on the end networks. Additionally, a trans-

parent bridge configures itself (in terms of routing information) after coming into service. Because a bridge forwards complete frames between connected networks many different protocols can coexist on either network, the messages are forwarded unchanged (protocol information is passed as raw data in the Ethernet frames). Bridges are used when multiple-protocol packets need to be shared among networks.

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

Moreover, X.25 will be available per default on all **X1000**, **X1200** and **X3200** routers.

3.2 HP OpenView Compatibility

To enhance the compatibility of the BinTec SNMP implementation with HP OpenView, the SNMP behavior of System Software Release 6.1.2 has been changed so as to allow all basic HP OpenView functions. Moreover, the **SysObjectID** has bee changed so that HP OpenView can now correctly identify the different types of BinTec routers.

3.3 IPX no Longer Supported

IPX which is used in Novell networks is no longer supported by System Software Release 6.1.2, just as Novell has discontinued work on this protocol. To enable data transfer between IPX and IP networks you can still use the bridging function that is now available on all BinTec routers.

3.4 Changes in RADIUS Implementation

3.4.1 RIP Update of RADIUS Dial-out Routes

Prior to System Software Release 6.1.2, any change of a RADIUS dial-out IP route was immediately propagated by the RIP (Routing Information Protocol). Since all routes, and not only those that had actually changed were updated up to several thousands of routes were propagated each time, leading to an unnecessary increase in traffic. Now only such routes that have actually changed are updated, and the update of RADIUS dial-out routes takes place together with the cyclical RIP updates which takes place every 30 seconds.

3.4.2 Configurable RADIUS Keepalive

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

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

3.5 Configurable MTU and MRU Values

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

on its MRU (Maximum Receive Unit) size. Where this information is unavailable the MTU is set to a default size of *1500*.

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

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

3.6 Interface Blocked with Inconsistent Encryption Configurations

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

The conditions under which an interfaced is blocked are:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.7 Interdependent Configuration of PPP Encapsulation, Encryption and Compression

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

3.8 New Activity Monitor Password

With System Software Release 6.1.2, a password for the **Activity Monitor** has been introduced. It is needed to set any interface of a monitored router into an up or down state respectively. As long as no Activity Monitor password is configured on your router, you need the admin password to do so.

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

3.9 New License State "*not supported*"

When a license is entered for a feature which is not supported by the currently loaded software image or the router's hardware, the state of that license is now no longer shown as *not_ ok*, but as *not_supported*.

3.10 Discarding Link Level Broadcast Packets

According to RFC 1812 link level broadcast packets must be discarded if they are not directed towards an IP multicast address. With System Software Release 6.1.2, BinTec routers follow this recommendation. This also fixes a problem that occurred when IP routing was configured on two Ethernet interfaces and bridging was then enabled on these interfaces. The router rebooted at the arrival of the first IP broadcast packet. Since link level broadcast packets are now discarded, this will no longer happen.

4 Bugfixes

Since System Software Release 6.1.2 is a release for all routers of the X-Generation, the problems and their solution described here do not relate to a single router type or to a certain system software release only. Thus, you will find bugfixes that pertain to system software release 5.3.1 (for the **X1000** and **X1200**), 5.5.1 (for the **X3200**), and 5.1.6 (for the **X4000**).

The following problems have been solved:

4.1 Radius Issues Solved

Several problems of the RADIUS implementation have been solved in System Software Release 6.1.2.

4.1.1 Temporary Entries in pppExtIfTable Become Static

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

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

- **ifEntryTable**

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

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

4.1.2 Missing RADIUS Attribute Now Transmitted

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

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

4.1.3 Wrong Calculation of RADIUS Dial-out Reload Interval

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

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

4.2 PPTP: Memory Leakage Removed

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

This problem has been solved.

4.3 PPPoE: Memory Leakage Removed

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

This problem has been solved.

4.4 PPPoE Credits

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

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

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

4.5 Multilink PPP with Cisco 4500

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

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

4.6 Calculation of MRU Size for PPP Interfaces

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

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

4.7 Data Transfer with DES or Blowfish Encryption

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

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

4.8 MPP Encryption with Windows NT/2000

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

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

4.9 Portscan on Port 1723

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

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

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

4.10 ICMP Fragment Unreachable Messages

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

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

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

4.11 Transparent ISDN Login

In System Software Release 6.1.2 certain problems concerning the Transparent ISDN Login have been solved. All routers that lie in between the local and the targeted router can be operated in a transparent mode so that data are in no way modified (e.g. interpreted as commands that require execution). Thus, e.g., a file transfer over several hops is possible.

4.12 RFC Compliance with CHAP Reauthentication

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

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

4.13 Calls through PRI Interface Now Possible

If ISDN Line Framing was set to *special (no CRC)*, this setting had been changed to ISDN Line Framing *unknown* when the CM-PRI menu was entered again. This had the effect that even though layer establishment was successful, no calls could be made on this interface.

This problem has been solved, the PRI interface can now be configured correctly.

4.14 DDI Called Party Numbers

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

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

4.15 Second Logical Channel with X.25 and CAPI

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

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

4.16 X4000 and CAPI Applications

Certain CAPI applications did not work with the PMX expansion card for the **X4000**. The internal buffer was chosen too large, resulting in a delay time the software did not support.

The Problem has been solved, the buffer size is now determined according to the software requirements.

4.17 Activity Monitor (X4000)

There were several problems with the Activity Monitor not displaying information about the status of a **X4000**:

- The expansion cards and resource modules of a **X4000** and their respective status where not displayed at all in the Activity Monitor.
- Information about currently used ISDN channels was not displayed in the Activity Monitor.
- The Activity Monitor was "informed" about the system name of the router only with every 256th message, so that changes of the **sysName** variable in the **systemTable** sometimes were displayed too late.

All these problems have been solved, and the Activity Monitor displays the relevant information immediately.

4.18 ISDN Autoconfiguration for "E1ON1" Switches

If the router was connected to an "E1ON1" ISDN switch, the automatic detection could not discover the relevant DSS1 protocols, since the switch did not answer a Release message with a Release Complete message.

This problem has been solved, and DSS1 is used as a default if no protocols are detected by the autoconfiguration routine.

4.19 X.21 Interfaces

When a X.21 link was temporarily lost (e.g. due to a reboot of the remote router), the PPP interface was blocked.

This problem has been solved, and the PPP interface is set in an up state once the link is available again. Moreover, several other changes have been made to enhance the X.21 performance of BinTec routers.

4.20 Removed Memory Leakage with DNS Requests

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

This problem has been solved.

4.21 DHCP: Stacktrace After Reboot

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

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

4.22 Error `dl_look: len 0`

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

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

4.23 Full RIP V2 Multicast Support on Ethernet Interfaces

The **ipExtIfRipSend** variable could not be set to *ripV2mcast* with the Setup Tool. With System Software Release 6.1.2 it is possible to set the **RIP Send** field in the ***Ethernet*** ➧ ***Advanced Settings*** menu to *RIP V2 multicast*.

Moreover, RIP V2 messages were sent to the IP address 224.0.0.9 in compliance with RFCs 1388 and 1723 when RIP V2 Multicast was enabled, but they were sent as MAC broadcast instead of Link Level multicast packets. System Software Release 6.1.2 now complies with RFC 1812 and forwards IP multicast packets as Link Level multicasts.

4.24 V.35 Problems Solved

When using V.35, it could happen that connections were unreliable. The software has been changed so as to reliably support V.35 connections.

4.25 Bridging Fully Functional

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

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

4.26 Missing or Damaged Ethernet Cable

A missing or damaged Ethernet cable is now signalled as if the interface was down.

Since a backup line or route is activated only when the interface which is not available is signalled as down, the use of backup lines and routes was not possible.

5 Known Issues

5.1 V.110 Problems

When accessing a BinTec router from a mobile phone using the HSCSD protocol for communication between the phone and the base station, and V.110 for the ISDN connection, there were transfer problems, partly based on software incompatibilities.

This problem is taken care of, and it will be fixed in a future release of system software version 6. Please look for software updates at www.bintec.net.