Release Notes System Software Release 6.3.4 X-Generation

June 2003

System Software Release 6.3.4

This document describes the new features, changes, bugfixes and known issues of System Software Release 6.3.4.

Table of Contents

1 Important Information

1.1 Downgrade Restrictions

It is not possible to directly downgrade from System Software Release 6.3.4 to System Software Release 6.2.2 or earlier. A staged downgrade, however, is possible:

- From System Software Release 6.3.4 downgrade to System Software 6.2.5.
- Save your configuration by entering `cmd=save` in the SNMP shell.
- Downgrade further to System Software Release 6.2.2 or earlier.

For further information on up- or downgrade restrictions see the download section of www.bintec.net.

1.2 Updating the ADSL-Firmware of X2300 Routers

Occasionally new logic files for the ADSL modem of your **X2300-Family** router will be available. We suggest updating your router, but highly recommend it if you are currently experiencing any problems. You can find new logic files in the download section for your router at www.bintec.net.

The process of updating the modem logic differs slightly from an update of the system software of your router. Please perform the following steps:

1.2.1 Deleting the Old Logic

It is crucial that the old ADSL modem logic is deleted before the new logic is imported.

First you need to delete the existing logic file from the Flash ROM (all commands must be called from the SMNP shell):

- Access the Flash ROM management shell: `update -i.`
- Call a listing of all files stored in the Flash ROM: `ls -l`.

  You will see something like this:

```
Flash-Sh > ls -l
  Flags   Version   Length                Date Name ...
Vr-x-bc-B  6.3.04  1740353 2003/06/05  7:53:06 box155rel.ppc860
Vr---l--f  3.8.129   319696 2003/01/24 15:48:05 X2E-ADSLp.x2c
Vr---l--f  3.8.129   315904 2003/01/16 13:17:42 X2E-ADSLi.x2c
Flash-Sh >
```

The file called X2E-ADSLp.x2c is used by **X2300** (ADSL over POTS), X2E-ADSLi.x2c is used by **X2300i** and **X2300is** (ADSL over ISDN).

- Delete the file you want to replace: `rm X2E-ADSLi.x2c` or `rm X2E-ADSLp.x2c.`
- Verify that the file has been removed: `ls -l`.

  Again, you will see something like this (if you have, e.g., deleted the logic for ADSL over ISDN):

```
Flash-Sh > ls -l
  Flags   Version   Length                Date Name ...
Vr-x-bc-B  6.3.04  1740353 2003/06/05  7:53:06 box155rel.ppc860
Vr---l--f  3.8.129   319696 2003/01/24 15:48:05 X2E-ADSLp.x2c
Flash-Sh >
```

- Perform a "reorg" to terminally delete the file from the Flash ROM: `reorg`. If you want to, you can again check the file listing by calling `ls -l`.

➤ Exit the Flash ROM management shell: `exit`.

You have now deleted the currently used modem logic.

1.2.2 Importing the New Logic

Importing the new logic is done exactly as any system software update. You can find detailed information on how to perform this kind of update in the User's Guide of your router ("Configuration Management" ➧ "Updating Software" – depending on your user's guide, the chapter name may differ slightly).

The new logic file you have to import is named according to a schema that differs from the one used for the old logic files: The file name now includes a version number:

- X2E-ADSLp_<version>.x2c, e.g. X2E-ADSLp_3.8.129.x2c
- X2E-ADSLi_<version>.x2c, e.g. X2E-ADSLi_4.10.04.x2c.

➤ Perform the update as is described in the user's guide.

1.2.3 Verifying the Update

After you have imported the new logic, you should verify that it has been successfully stored in the Flash ROM:

➤ Access the Flash ROM management shell: `update -i`.

➤ Call a file listing: `ls -l`.

You should see something like this:

```
Flash-Sh > ls -l
  Flags   Version   Length                Date Name ...
Vr-x-bc-B  6.3.04  1740353 2003/06/05  7:53:06 box155rel.ppc860
Vr---l--f  3.8.129   319696 2003/01/24 15:48:05 X2E-ADSLp.x2c
Vr---l--f  4.10.04   315904 2003/01/16 13:17:42 X2E-ADSLi_4.10.04.x2c
Flash-Sh >
```

➤ Exit the Flash ROM management shell: `exit`.

1.2.4 Rebooting the Router

In order to activate the new logic, you must reboot your router: `cmd=reboot`.

After the router has been rebooted, the new ADSL modem logic is activated.

2 New Features

System Software Release 6.3.4 is a major new release of our system software, and it contains a number of important new features:

- 2.1: "HTML User Interface (HUI)"
- 2.2: "Virtual LAN (VLAN)"
- 2.3: "BinTec Router Redundancy Protocol (BRRP)"
- 2.4: "DHCP over IPSec"
- 2.5: "Multi Interface PPPoE"

2.1 HTML User Interface (HUI)

System Software Release 6.3.4 introduces a Graphical User Interface for the configuration of our routers. It comes as an HTML interface accessible through a Java Script enabled browser.

As of now not all available browsers are supported by the HUI.

The following browsers have been successfully tested:

- Windows:
  - Opera 7
  - Mozilla 1 and above (browsers derived from Mozilla 1.0 should work, too)
  - Netscape 6.1 and above
  - Internet Explorer 5.0 and above
- Linux
  - Mozilla 1 and above (browsers derived from Mozilla 1.0 should work, too)
  - Netscape 6.1 and above.

In order to access the HUI, simply enter the IP address (or the hostname respectively, if it can be resolved) of your router in a web browser and append **/setup**. You will be prompted to login with a username (in order to configure your router, you must login as **admin**) and password (the admin password configured on your router).

If you enter the URL of your router as described above, but add the string "?pwd=" (e.g. ***http://router/setup?pwd=***), all passwords will be shown in plain text. This corresponds to the command `setup -p` in the SNMP shell when calling the Setup Tool.

Another way of accessing the HUI is through the HTML status page. This page is displayed by calling the IP address or resolvable hostname of your router in a browser. You can find a link that triggers the respective javascript below the "Hardware Interfaces" section.

The HUI is structured just as the ASCII Setup Tool of the router so that the information contained in your documentation is adequate for HUI configuration, too. The HUI is, however, significantly more convenient to use, since it displays all menus and information in a way well known through the Internet.

The setup is started in a pop-up window. Your browser must, therefore, be configured to accept pop-up windows, either in general or for the address or host name of the router you want to configure.

In several menus, the Setup Tool window needs to reload after you have changed the value for a specific parameter. All parameters that will cause the window to reload after a change are marked with a small Reload Icon (displaying the well known circular arrows).

2.2 Virtual LAN (VLAN)

A VLAN is an arbitrary group of network nodes that behave as if they were all connected to the same network segment. The members of a specific project

team may be spread across different locations of a building, but when assigned to the same VLAN, they can share network resources as if they were assigned to one and the same network section. Access to other network resources is entirely at the network administrator's discretion.

By offering a highly flexible means of segmenting a network, VLANs also increase the efficiency of network usage: They restrict the circulation of broadcast as well as host-to-host traffic, and extraneous traffic is reduced throughout the network, avoiding, e.g., broadcast storms. VLANs can also be used to increase network security, since a VLAN can be logically separated from other VLANs and security mechanisms as offered by routers can be applied.

There are different basic modes of how to determine to which VLAN a network node is assigned:

- Protocol based assignment: Network nodes are assigned to a VLAN on the basis of their Layer 3 addresses (like,e.g., IP addresses).
  This mode offers a very intuitive way of grouping together VLANs. Segmentation, however, is restricted; IP networks thus can only be segmented into subnets structured by network addresses and netmasks.
- MAC address based assignment: This method allows creating arbitrary VLANs based on physical or virtual MAC addresses. This mode does not really apply to routers, but is rather used with switches.
- Port based assignment: In this mode, a VLAN is created by the network nodes being attached to certain physical ports of a switch or a router.

The mode used by BinTec routers is a variant of the port based assignment: Every virtual interface is assigned a VLAN ID. This tag marks the traffic to and from the virtual interface as belonging to VLAN 1 or 2 or 3 etc. and makes it independent from the physical port the router is attached to.

If VLAN assignment by MAC address is desired, too, you must assign a virtual MAC address to every virtual interface. Note, however, that a switch needs to be configured to actually create the respective VLAN.

The configuration of VLAN interfaces can be completely carried out in the Setup Tool. To assign a router to a specific VLAN, a virtual LAN interface is created

with the parameters that group it together with the other members of the respective VLAN. This is done in the menu ***VIRTUAL INTERFACES*** which you can access from any menu for hardware ethernet interface configuration (e.g. ***LAN: CM-100BT, FAST ETHERNET*** or ***MODULE: X4E-100BT, FAST ETHERNET*** on **X4000** equipped with a fast ethernet module).

The first menu window shows a list of all virtual interfaces already configured and allows access to the **ADD/EDIT** menu which looks likes this:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[LAN][SLOT 1 UNIT 0 ETH][ADD]: Configure Virtual LAN
                               Interface # 1                  MyRouter


          IP-Configuration            VLAN
               Local IP-Number
               Local Netmask


               MAC Address           00a0f9
               VLAN ID               1


          Advanced Settings >

                    SAVE                                 CANCEL
```

The parameters available for configuration are basically the same as in the top-level ethernet configuration menus:

Field	Meaning
IP-Configuration	Here you can choose from four different configuration modes: ■ *Manual*: This mode allows for simple manual IP configuration just like any physical ethernet interface. See the user's guide of your router for a description of the parameters. ■ *VLAN*: In this mode the VLAN ID is configurable. This is vital for VLAN configuration, since assignment to a VLAN can best be determined using this ID. Specifying a MAC address is mandatory in this mode, though. ■ *BRRP*: In this mode, the state of the virtual interface does not depend on the Admin-State saved in the **ifTable**, but is determined by the BRRP Watchdog Daemon tasks. These are configured in the menu ***BRRP***. Specifying a MAC address is mandatory for BRRP mode. ■ *BRRP over VLAN*: In this mode you can configure a BRRP router within the specifications and boundaries of a virtual LAN. For more information on IP configuration for BRRP, see chapter 2.3.2, page 19.
Local IP-Number	Here you assign the IP address of the virtual interface.
Netmask	Here you enter the netmask corresponding to the IP address assigned to the virtual interface.

Field	Meaning
MAC Address	Here you enter the MAC address associated with the virtual interface. You may use the MAC address of the physical interface the virtual interface is created under. This is, however, not necessary. Assigning a virtual MAC address is possible, too. In VLAN and Manual mode, the first 6 digits of the MAC address are suggested (they can be edited, though).
VLAN ID	Accessible only if **IP-Configuration** is set to *VLAN* or *BRRP over VLAN*. Here you assign the virtual interface to a VLAN by entering the VLAN ID of the respective VLAN. Possible values are *1* to *4094*. A value of *0* means the packets from this virtual interface are not explicitly tagged.

Table 2-1: ***VIRTUAL INTERFACES*** ➧ **ADD/EDIT**

Note that each pair of a VLAN ID and a MAC address must be unique.

Moreover, you can access the ***ADVANCED SETTINGS*** menu for the virtual interface you are currently configuring. It contains the same options as the ***ADVANCED SETTINGS*** menu of the physical ethernet interface. See the user's guide of your router for a description of the available parameters.

Note that you must save the virtual interface before you can make any advanced settings. If you do not first save the virtual interface, none of the corresponding entries in the MIB have been made and all configuration in the ***ADVANCED SETTINGS*** menu is lost.

2.3 BinTec Router Redundancy Protocol (BRRP)

This feature is not available for the **X1000**, **X1200**, **X3200** and **BinGo! DSL**routers.

The main application of a router redundancy protocol is to back up a service offered by a single physical router to a LAN. The original router and all routers that can potentially act to back up the service provided by the original router form a logical entity called the Virtual Router. If the original router fails, any of the other routers joined together to form the Virtual Router takes over the service formerly provided by the original router.

Let us assume a simple scenario where Router A offers internet access to hosts in a LAN. If this router fails, all hosts that have no means of dynamically discovering an alternative route, but have statically configured routes are without access to the internet. To avoid this, Router B starts offering the same service previously offered by Router A to the hosts in the LAN. The entire set of tasks that allow setting up a Virtual Router as well as switching responsibility for services from one router to another is managed by a router redundancy protocol. The BRRP follows the specifications laid out by RFC 2338 and the corresponding Internet-Draft (you can find Internet-Drafts here: http://www.ietf.org/1id-abstracts.html).

Setting up a virtual router involves a number of steps:

- Configure a virtual interface for participation in the virtual router.
  A virtual interface is necessary, since the messages exchanged between the routers require the use of virtual MAC addresses. Physical MAC ad-

dresses cannot be used, since they are bound to a physical interface and cannot be assumed by other routers. This, however, is necessary if a back-up is to take over a service from another router.

- Configure the router to participate in a specific virtual router.
  This step includes defining the role of the virtual interface within the virtual router and specifying the settings required to act as master.
- Define the tasks that control the functions of the virtual router.
  This step includes the configuration of state transitions depending on a change of the state of the master.

Note that user data should always be transmitted via a virtual interface. Administrative multicasts (i.e. the keepalives sent between the participating routers) are transmitted via the master interface.

2.3.1 Terms and Definitions

The description of a virtual router requires a number of terms to be used. These terms are defined in the corresponding RFC and Internet-Draft.

Term	Definition
VRRP Router	"A router running the Virtual Router Redundancy Protocol. It may participate in one or more virtual routers."
Virtual Router	"An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and a set of associated IP address(es) across a common LAN. A VRRP Router may backup one or more virtual routers."

Term	Definition
IP Address Owner	"The VRRP router that has the virtual router's IP address(es) as real interface address(es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, etc." This means that the router that is given a priority of 255 is the "IP Address Owner".
Primary IP Address	"An IP address selected from the set of real interface addresses. One possible selection algorithm is to always select the first address. VRRP advertisements are always sent using the primary IP address as the source of the IP packet."
Virtual Router Master	"The VRRP router that is assuming the responsibility of forwarding packets sent to the IP address(es) associated with the virtual router, and answering ARP (Address Resolution Protocol) requests for these IP addresses. Note that if the IP address owner is available, then it will always become the Master."
Virtual Router Backup	"The set of VRRP routers available to assume forwarding responsibility for a virtual router should the current Master fail."

Table 2-2: Term definitions quoted from the VRRP Internet-Draft

2.3.2 Configure a Virtual Interface

Virtual Interface configuration is not carried out in the ***BRRP*** menu, but in the submenu ***VIRTUAL INTERFACES*** which you can access from any menu for hardware ethernet interface configuration. The configuration of a virtual interface

proceeds as is described in chapter 2.2, page 12. The following settings are mandatory when configuring a virtual interface for the use within a virtual router:

- The value for the field **IP-Configuration** must be set to *BRRP* or *BRRP over VLAN*.
- Specifying a MAC address is mandatory. If you do not enter a MAC address, the entry is incomplete and cannot be saved. The first 10 digits of the MAC address are suggested for maximum interoperability and RFC conformity. They can be edited if necessary, but you definitely should use the preset trunk. The last two (freely choosable) digits should be the VLAN ID (01, 02 ...).
- The IP address and the MAC address must be those of the virtual router master, irrespective whether you intend to use the virtual interface as master or as backup.

Once you have set up a virtual interface, you can proceed with BRRP configuration.

2.3.3 Configure Virtual Router Participation

Configuration of all processes controlled by BRRP is configured in the ***BRRP*** submenus, ***BRRP*** ➧ ***TASK DEFINITION*** and ***BRRP*** ➧ ***BRRP CONFIGURATION***. The first step is to configure participation in a virtual router (***BRRP CONFIGURATION***).

Upon entering the ***BRRP CONFIGURATION*** menu, you see a list of all virtual routers already configured. The **ADD/EDIT** menu for the configuration of virtual routers looks like this:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[BRRP][DAEMON][ADD]: Configure Virtual Router                  MyRouter


          Virtual Router ID           1
          Virtual Router State        down

          Priority                    100

          Interface                   en1-0-1
          Master IP-Address           192.168.1.254
          MAC-Address                 00005e000101

          Advertisement Interval      1
          Master Down Interval        3
          Pre-empt Mode               true
          Authentication Type         No Authentication


               SAVE                                CANCEL
```

The fields of this menu have the following relevance:

Field	Meaning
Virtual Router ID	Here you choose the Virtual Router Identifier. The VRID identifies the virtual router throughout the LAN and is part of every BRRP packet sent by the current master. A value for this parameter is assigned automatically when you create a new entry. The value can, however, be changed in the corresponding MIB table. Acceptable values are integers from *1* to *255*.

Field	Meaning
Virtual Router State	This parameter determines the state of the virtual router. Available choices are *up* and *down*. The state you set here does not affect the entire virtual router, but only the participation of this virtual interface in the virtual router. The default value is *down*. Note that the parameters of a virtual router can be configured only if the virtual router is *down*. In order to stop a running virtual router, you need to set **Virtual Router State** to *down* and confirm with **SAVE**. You can then return to the **ADD/EDIT** menu and change the parameters.
Priority	This parameter determines the logical priority of the virtual interface within the virtual router. Acceptable values are *1* to *255*. A value of *255* determines that this virtual interface functions as master. Any other value designates a virtual router slave (or backup): The higher the value, the higher the priority. The default value is *100*.
Interface	This parameter determines the interface which is to participate in the virtual router. You can choose from all virtual ethernet interfaces that are flagged for BRRP.
Master IP-Address	This field displays the IP address of the master. You cannot change this value, since it is determined by the interface you have chosen.
MAC-Address	This field displays the MAC address of the master. You cannot change this value, since it is determined by the interface you have chosen.

Field	Meaning
Advertisement Interval	This parameter determines how often a BRRP advertisement is sent if the virtual interface is acting as master. Only the current master sends BRRP advertisements. Acceptable values are integers from *1* to *255*. The value is in seconds, default is *1*.
Master Down Interval	The actual Master Down Interval is the time calculated from the number of expected, but omitted BRRP advertisement, the Advertisement Interval and a so called Skew Time which adds a minimal amount time depending on the priority of the virtual interface within the virtual router (the higher the priority, the shorter the time added, so that a backup with high priority reacts earlier than one with low priority). Once the Master Down Interval has elapsed, the backup considers the master down and assumes the role of master. The value you enter here determines the number of BRRP advertisements allowed to fail. Acceptable values are integers from *1* to *255*, the default value is *3*.
Pre-empt Mode	This parameter determines whether a higher priority backup preempts a lower priority master. Values are *true* to allow preemption and *false* to prohibit preemption. The default value is *true*. Note that there is an exception: The router that owns the IP address associated with the virtual router always pre-empts independently of the setting of this parameter.

Field	Meaning
Authentication Type	This parameter determines which kind of authentication is used for BRRP exchanges. Available choices are: ■ *none*: No authentication is used. ■ *Plain Text Password*: BRRP traffic is authenticated using a plain text password. All packets that fail authentication are discarded. (The VRRP RFC and Internet-Draft envisage the use of the IP Authentication Header. This option will be added later.)
Authentication Key	Accessible only if **Authentication Type** is not set to *none*. Here you enter the authentication key. Note that it needs to be the same for all virtual interfaces participating in the virtual router.

Table 2-3: ***BRRP*** ➧ ***BRRP CONFIGURATION*** ➧ **ADD/EDIT**

2.3.4 Configure Tasks

Once you have configured a virtual interface to participate in a virtual router, you need to configure the Watchdog Daemon, i.e., determine how monitoring master availability and state transitions are handled.

The Watchdog Daemon configuration includes the following specifications of the virtual router master:

- which IP address is to be monitored for availability - this is either determined by the Virtual Router ID that points at a configuration made in the ***BRRP CONFIGURATION*** menu; or it is determined by specifying an interface description that points to an entry in the **ifTable**

- by which mechanism the state of the master can be detected - this can either be the BRRP advertisements sent by the master or the **operStatus** of the respective interface
- which master state triggers the action configured for the backup.

The Watchdog Daemon configuration includes the following specifications of the virtual router backup:

- which interface is to react to the master state configured as trigger – the interface can again be specified by a VRID pointing at a BRRP Configuration or the interface description
- the mechanism by which the backup reacts to the trigger – this can either be a BRRP state or an interface state
- which action the backup carries out.

These details are specified in the ***BRRP*** ➧ ***TASK DEFINITION*** menu.

Upon entering the menu, you see a list of all configured tasks. You can add and edit tasks in the **ADD/EDIT** menu. It looks like this:

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[BRRP][TASKS][ADD]: Redundancy Task Definition                 MyRouter


          Task ID                      1

          Master Interface Protocol    BRRP
          Master Action                Initialize
          Virtual Router ID            1

          Slave Interface Protocol     BRRP
          Slave Admin Action           down
          Virtual Router ID            2


               SAVE                                  CANCEL
```

The fields of this menu have the following relevance:

Field	Meaning
Task ID	You can arbitrarily assign Task IDs. They are not used for router internal processes and serve to define logical sets of tasks.
Master Interface Protocol	This parameter determines which mechanism is used for Keepalive Monitoring of the master. Available choices are: ■ *BRRP*: The BRRP specific state advertisements are used to determine the state of the master. The master sends advertisements according to its configuration in the ***BRRP CONFIGURATION*** menu. ■ *IFC - operStatus*: The **OperStatus** of the interface acting as master is queried. The **OperStatus** is found in the **ifTable**.
Master Action	This parameter determines the trigger of the task you are configuring. Depending on your choice of Master Interface Protocol, the available choices vary: ■ **Master Interface Protocol** = *BRRP*: – *Initialize* – *Backup* – *Master* For details on the BRRP states, see "BRRP States", page 29 below. ■ **Master Interface Protocol** = *IFC-operStatus:* – *up*: The interface is up. – *down*: The interface is down.

Field	Meaning
Virtual Router ID	This field is accessible only if **Master Interface Protocol** is set to *BRRP.* This parameter determines which interface is to be monitored by specifying the VRID. The Watchdog Daemon will check the configuration made in the ***BRRP CONFIGURATION*** menu for details.
Master Interface	This field is accessible only if **Master Interface Protocol** is set to *IFC - operStatus.* This parameter determines which interface is to be monitored by specifying the interface description. The Watchdog Daemon will check the **ifTable** for details.
Slave Interface Protocol	This parameter determines by which mechanism the backup reacts to the trigger: ■ *BRRP*: The backup transitions to the BRRP state specified by the parameter chosen for **Slave Admin Action**. ■ *IFC - adminStatus*: The backup transits to the **adminStatus** specified by the parameter chosen for **Slave Admin Action**.

Field	Meaning
Slave Admin Action	The available choices for this parameter do not depend on the trigger mechanism chosen for **Slave Interface Protocol**. They in both cases are: ■ *up*: – For *BRRP* this means that the virtual router is *enabled*. It transitions to the Initialize state. – For *IFC- adminStatus* this means the router interface is set to *up*. ■ *down*:. – For *BRRP* this means that the virtual router is *disabled*. – For *IFC- adminStatus* this means the router interface is set to *down*. ■ *none*: – For *IFC- adminStatus* only: this means that no action is triggered.
Virtual Router ID	This field is only accessible if **Slave Interface Protocol** is set to *BRRP*. The backup gathers the information whether to start or stop the virtual router from the BRRP advertisements sent by the master. Thus the VRID needs to be specified
Slave Interface	This field is only accessible if **Slave Interface Protocol** is set to *IFC - adminStatus*. The backup cannot determine whether to start or stop the virtual router. Thus the interface needs to be specified.

Table 2-4: ***BRRP*** ➧ ***TASK DEFINITION***

BRRP States

The BRRP specifies three different states BRRP routers can assume. Depending on the state, the behavior of the BRRP router changes. The different kinds of behavior are complex, exhibiting a large number of dependencies (this is especially true of the Master state).

These are the states and the respective behavior of the router:

State	Relevance
Initialize	The purpose of this state is to wait for a Start-up event. When the BRRP router is activated, it behaves as follows: ■ If the local Priority is *255*, the router: – sends an BRRP advertisement – broadcasts a gratuitous ARP (Address Resolution Protocol) packet containing the virtual router MAC address for each IP address associated with the virtual router. – sets the Advertisement Timer to the configured Advertisement Interval – transitions to the Master state. ■ In every other case, the router: – sets the Master Down Timer to the calculated Master Down Interval – transitions to the Backup state.

State	Relevance
Backup	The purpose of the Backup state is to monitor the availability and state of the master. While in this state, a BRRP router behaves as follows: ■ It does not respond to ARP requests for the IP address(s) associated with the virtual router. ■ It discards packets with a destination link layer MAC address equal to the virtual router MAC address. ■ It does not accept packets addressed to the IP address(es) associated with the virtual router. ■ If the BRRP router is deactivated: – it cancels the Master Down Timer – it transition to the Initialize state.

State	Relevance
Master	While in the Master state the router functions as the forwarding router for the IP address(es) associated with the virtual router. While in this state, a BRRP router behaves as follows: ■ It responds to ARP requests for the IP address(es) associated with the virtual router. ■ It forwards packets with a destination link layer MAC address equal to the virtual router MAC address. ■ It does not accept packets addressed to the IP address(es) associated with the virtual router if it is not the IP address owner. If the BRRP router is deactivated: ■ It cancels the Advertisement Timer. ■ It sends an advertisement with Priority = *0*. ■ It transition to the Initialize state. If the Advertisement Timer fires: ■ It sends an advertisement. ■ It resets the Advertisement Timer to Advertisement Interval.

State	Relevance
Master (cont.)	If an advertisement is received: ■ If the Priority in the advertisement is *0*: – it sends an Advertisement – it resets the Advertisement Timer the to Advertisement Interval. ■ If the Priority in the advertisement is greater than the local Priority: – it cancels the Advertisement Timer – it sets the Master Down Timer to the calculated Master Down Interval – it transitions to the Backup state. ■ If the Priority in the advertisement is lower than the local Priority: – it discards the advertisement.

Table 2-5: BRRP states

2.4 DHCP over IPSec

When running an IPSec client on a Windows PC, it may be desirable to obtain the IP configuration for remote network access through DHCP. The SSH IPSec client (formerly distributed as BinTec IPSec Client) offers a virtual interface for this purpose. RFC 3456 specifies a way to perform DHCP over an IPSec tunnel that is specifically created for this purpose.

For this purpose a new value (*dhcp*) for the variable **RemoteAddressType** has been created in the **ipsecTrafficTable**. Configuration through the Setup Tool is possible (***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT** (traffic list)):

```
BinTec Router Setup Tool                    BinTec Access Networks GmbH
[IPSEC][PEERS][EDIT][TRAFFIC][EDIT]: Edit Traffic Entry       MyRouter


     Description:   1

     Protocol:      dont-verify

     Local:
          Type: net   Ip:                / 0

     Remote:
          Type: dhcp

     Action:        protect

     Special Settings >


      SAVE                               CANCEL
```

In order to create a traffic list entry for DHCP over IPSec, the value of the field **Remote: Type** merely has to be set to *dhcp*.

If this address type is specified in a traffic list entry, an implicit rule is assumed which allows the setup of an IPSec tunnel mode Security Association (SA) from the remote peer's (dynamic) internet address to anywhere for UDP packets and the DHCP ports (remote: *68*, local: *67*). If the DHCP configuration is completed, SAs may be established with the assigned address as remote address only.

The procedure is as follows:

- The remote side (the PC running the IPSec client) creates a phase 1 (IKE) SA.
- The remote side creates a phase 2 (IPSec) DHCP SA.
- The remote side performs DHCP over the tunnel.

- The Bintec router snoops the DHCP communication and remembers the assigned address and lease.
- The Bintec router enters the snooped DHCP address into the DHCP traffic list entry.
- The Bintec router adds a route to the remote client towards the external interface of the PC.
- The client establishes a phase 2 SA with the DHCP address as **RemoteAddress**
- After the lease expires or there has been a DHCPRELEASE from the client, the Bintec machine deletes the route, clears the DHCP address in the traffic list entry and clears the IPSec tunnel.

The use of this feature requires one peer and one traffic specification for each IPSec client. It is not possible to work with a wildcard peer entry for all clients.

Moreover the IPSec client must have the DHCP IPSec tunnel configured as a "VPN Connection". For details on how to configure the IPSec client refer to the IPSec Client manual.

If you have defined DHCP pools for an internal network, IPSec clients can be assigned IP numbers from the same pool. You must make sure, however, to enable Proxy ARP for the local interface (***LAN*** ➧ ***ADVANCED SETTINGS***: **Proxy Arp** *on*). Otherwise the IPSec clients are not visible to the internal network.

DHCP Server Extension

The DHCP server function of BinTec routers has been expanded to account for the needs of DHCP over IPSec. Two newly created MIB variables allow to adjust the DHCP server to your needs:

- **ipDhcpHwType** – This variable allows to restrict an IP address pool to a certain kind of clients. Available values are:
  - *ipsec*
  - *non_ipsec*

– *any*

This parameter can be configured in the ***IP*** ➧ ***IP ADDRESS POOL LAN (DHCP)*** ➧ **ADD/EDIT** menu. The relevant field there is **Type**.

- **ipDhcpId** – This variable allows to specify a DHCP Client Identifier as an alternative to specifying the client's MAC address, since a MAC address may not always be available, e.g. if the IPSec client is running on a PC without Ethernet equipment.
  This parameter can be configured in the Setup Tool. The field description **MAC Address** in the menu ***IP*** ➧ ***IP ADDRESS POOL LAN (DHCP)*** ➧ **ADD/EDIT** can be highlighted and changed to **Client Identifier**. You can then enter an arbitrary string.

2.5 Multi Interface PPPoE

BinTec routers offer the possibility to act as PPPoE client as well as PPPoE server. For both modes System Software Release 6.3.4 introduces an enhanced way of handling PPPoE configurations.

PPPoE Client Mode

So far it was not possible to use more than one Ethernet interface for the configuration of PPPoE WAN partners. All PPPoE WAN partners had to use the same globally defined PPPoE interface (the definition is made in the ***PPP*** menu). System Software Release 6.3.4 significantly enhances the configuration options by introducing the possibility to assign a specific Ethernet interface to a WAN partner for the use of PPPoE. The menu ***WAN PARTNER*** ➧ ***ADVANCED SETTINGS*** ➧ ***EXTENDED INTERFACE SETTINGS*** now includes the field **PPPoE Ethernet Interface** which allows choosing from all available Ethernet interfaces (physical ones as well as virtual ones).

Note that the field **PPPoE Ethernet Interface** is displayed only if you have chosen *PPP over Ethernet (PPPoE)* for the field **Layer 1 Protocol** in the ***WAN Partner*** ➧ ***Advanced Settings*** menu.

Thus, two ways of configuring a PPPoE WAN partner are available: You can still use the "old" way and define a global PPPoE interface which is used by all PPPoE WAN partners; or you can assign a specific Ethernet interface to every PPPoE WAN partner.

It is also possible to combine the two kinds of configuration: For every WAN partner the router first checks for a WAN partner specific setting. If no interface has been specifically assigned, the router uses the global setting made in the ***PPP*** menu.

If you access the ***WAN Partner*** ➧ ***Advanced Settings*** ➧ ***Extended Interface Settings*** menu, but do not want to use a WAN partner specific PPPoE interface, make sure not to leave this menu by hitting **SAVE**. The default value is set to the first Ethernet interface, and if you save this setting, you will have defined a specific PPPoE interface for this WAN partner.

PPPoE Server Mode

This feature is currently available for our **X4000**-Family routers and for **X8500** only.

As well as acting as a PPPoE client, the modular routers can act as a PPPoE server. Configuring a router as PPPoE server requires little configuration, which, however, needs to be carried out in the SNMP shell. To enable the PPPoE server mode on a physical or virtual Ethernet interface, an entry in the **pppoeAcTable** must be created. Optionally, the **pppAcServiceTable** offers the possibility to manage client access.

The **pppoeAcTable** table contains the following variables:

Variable	Meaning
pppoeAcEthIfIndex	Here you specify which Ethernet interface is to accept PPPoE connections from PPPoE clients.You do so by entering the Interface Index of the interface in question. You can find the Index in the **ifTable**. A value for this variable must be specified for the router to act as PPPoE server.
pppoeAcChkService	The value of this variable determines which kinds of connections the PPPoE server accepts. Available choices are: ■ *accept-all* – Regardless of the PPPoE "SERVICE-NAME" tag (see RFC 2516) all PPPoE Active Discovery Initiation (PADI) packets will be accepted and answered with a PPPoE Active Discovery Request (PADR) packet. ■ *accept-from-list* – Only PADI packets with a "SERVICE-NAME" tag matching one of the services specified by the **Name** variable in the **pppoeAcServiceTable** (see table 2-7, page 38) will be accepted and answered. ■ *delete* – this entry will be removed and PADI packets received on the associated Ethernet interface will be ignored.
pppoeAcName	Here you can specify a name for the PPPoE server running on the specified interface.

Table 2-6: **pppoeAcTable**

If *accept-from-list* has been chosen for the **pppoeAcChkService** variable, the client needs to send a Service Name for the connection to be accepted. If you configure a PPPoE client on a BinTec router, you can specify the **PPPoE Service Name** in the menu ***WAN Partner*** ➧ ***Advanced Settings*** ➧ ***Extended Interface Settings.***

BinTec currently recommends using the *accept-all* value for PPPoE servers.

The **pppoeAcServiceTable** is used to map Service Names to physical or virtual Ethernet interfaces. It contains two variables:

Variable	Meaning
pppoeAcServiceEthIfIndex	Here you specify the Ethernet interface to which one or more Service names are assigned.
pppoeAcServiceName	Here you enter the Service Name for the interface in question. It is possible to map more than one **Name** to a single interface.

Table 2-7: **pppoeAcServiceTable**

Note that it is not recommended to configure one or more PPPoE clients and a PPPoE server on the same interface.

3 Changes

In addition to new features introduced with System Software Release 6.3.4, there has been a number of changes enhancing the functionality of your router:

- 3.1: "STAC and MPPC License"
- 3.2: "CAPI 1.1 Removed"
- 3.3: "Factory Reset"
- 3.4: "Update Command"
- 3.5: "PPP"
- 3.6: "Bandwidth Allocation Protocol – Link Termination"

3.1 STAC and MPPC License

When System Software 6.3.3 or 6.3.4 is used on routers of a new hardware revision, the STAC and MPPC licenses are no longer included and activated by default. You can, however, obtain a free (combined) license from www.bintec.net. You will find the respective web page in the Service/Support section. When you enter the hardware serial number of your router, our web application will verify whether you actually need a license. If this is the case, the license key will be sent to you by email.

3.2 CAPI 1.1 Removed

The CAPI 1.1 implementation has been removed from System Software Release 6.3.4, since it must be considered an outdated standard without practical relevance.

Setup Tool integration for CAPI 1.1 was already removed in System Software 6.3.1, but CAPI 1.1 was still configurable in the MIB tables.

3.3 Factory Reset

This feature is available for our non-modular routers only.

You can reset your router to the "factory reset" state (delivery status) with a special reset sequence (switching on and off). You can then dial in to the router from any location using ISDN Login. In "factory reset" state, the default configuration is used and any existing boot configuration is ignored but not deleted.

For information on how to proceed, refer to the User's Guide of your router.

To protect your router against unauthorized access in the "factory reset" state, you need to enter the password of the last active boot configuration for dial in. Optionally, you can enter `erase bootconfig` at the first login prompt after the reset. This command deletes all existing configurations.

With System Software Release 6.3.4, the same effect can now be created without access to the SNMP shell. While you have to restart your router three times for the "normal" factory reset (retaining the passwords of the last active boot configuration), restarting it five times has the same effect as the `erase bootconfig` command. All values are reset to the factory defaults.

3.4 `Update` Command

Before System Software Release 6.3.4 it was not possible to update BOOTmonitor and Logic of our routers using the `update` command in the SNMP shell. These software modules had to be updated using the respective function of the BOOTmonitor. It was, therefore, not possible to update BOOTmonitor and Logic during a remote login session.

System Software Release 6.3.4 introduces the possibility to perform this kind of update with the `update` command, too. Thus, remote software updates are now available for all software modules.

3.5 PPP

3.5.1 Additional Callback Mode

In order to facilitate callback negotiation with clients expecting the use of the MS Callback Control Protocol (CBCP), System Software Release 6.3.4 offers a new value for the variable **bibopppCallback**: *expected_cbcp*. If a client is incapable of using the Link Control Protocol (LCP) according to RFC 1570, or for some other reason expects the use of CBCP, your router can now be configured to react accordingly. Configuration, however, needs to be carried out in the SNMP shell.

3.5.2 Layer 1 Protocol Selection

Before System Software Release 6.3.4 it was possible for every configured WAN partner to authenticate access to any interface, irrespective of the interface type. This behavior has been changed, and now clients dialing in with a specific Layer 1 protocol are restricted to interfaces with the same Layer 1 protocol. The protocol a client is allowed to authenticate for is specified by the variable **pppExtIfDialinL1Protocol**.

Every dialin attempt is checked for the Layer 1 protocol used, and if it does not match the one specified for the WAN partner, then the attempt is rejected.

3.6 Bandwidth Allocation Protocol – Link Termination

With System Software Release 6.3.4 a link is terminated after a timeout even if the client does not answer the Link Drop request.

Note, however, that only the following BACP/BAP modes are affected:

- *bap-active*
- *bap-both*
- *bap-client*
- *bap-first*

In all other modes the router does not send a BAP Link Drop Request.

You can find detailed information on the BACP/BAP modes in the **User's Guide** of your router.

4 Bugfixes

The following problems have been solved in System Software Release 6.3.4:

- 4.1: "IPSec"
- 4.2: "Stateful Inspection Firewall"
- 4.3: "Flash File System – File Names"
- 4.4: "MSS Clamping - Malfunction"
- 4.5: "MPPE – Negotiation"
- 4.6: "VoIP – False Syslog Message"
- 4.7: "TAF – Authentication Freezes Router"
- 4.8: "DynDNS"
- 4.9: "Channel Bundling – Second B-Channel Used for Rx Only"
- 4.10: "QoS"
- 4.11: "Fax G3 – Sporadic Receive Malfunction"
- 4.12: "Fax – First Attempt to Send a Fax Fails"
- 4.13: "PPP Keepalive - Interface not Set Down"
- 4.14: "PPP – Keepalives Erroneously Activated"
- 4.15: "PPPoE – LCP Establishment Error"
- 4.16: "X.25 over CAPI – File Transfer Fails"

The ID numbers specified below each heading indicate the Error ID in our action request system. If you want to inquire about any of the bugfixes, this ID will help our support team to identify the problem.

4.1 IPSec

A number of problems in the field of IPSec have again been solved in System Software Release 6.3.4. They include:

- 4.1.1: "Peer Specific Local ID Ignored"
- 4.1.2: "IKE Requests Keep Connection Alive"
- 4.1.3: "Distorted Setup Tool Menu"
- 4.1.4: "False Messages with IPSec Callback"
- 4.1.5: "Setup Tool – Pre Shared Key not Saved"
- 4.1.6: "Wrong Setting in ipsecDialTable"
- 4.1.7: "Peers Loaded twice from RADIUS"
- 4.1.8: "Setup Tool – Field Descriptions"
- 4.1.9: "Key and Certificate Load/Reload Behavior"
- 4.1.10: "IPSec-Callback Sporadically Fails"
- 4.1.11: ""Ghost Peer" Created"

4.1.1 Peer Specific Local ID Ignored

(ID n/a)

This problem applied to certificate based authentication, only.

If a special **ipsecPeerLocalId** was configured and no **ipsecPeerLocalCert** was stored on the router (**ipsecPeerLocalCert** is *0*), the Local Peer ID was ignored and the default local ID (**ipsecGlobDefaultLocalId**) was used.

This problem has been solved.

4.1.2 IKE Requests Keep Connection Alive

(ID n/a)

When the router received IKE packets in ID Protect Mode, the reply packets sent by the router kept the connection alive, even if the request was not accepted and no tunnel creation was started.

This problem has been solved. If the router acts as responder in an IKE negotiation, replies to IKE requests are no longer allowed to keep the connection alive.

4.1.3 Distorted Setup Tool Menu

(ID 2548)

When entering the ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT** menu, the menu display appeared distorted and unreadable. This was due to displaying debugging output.

This problem has been solved.

4.1.4 False Messages with IPSec Callback

(ID 2566)

When viewing the debug level syslog messages of two routers performing an IPSec callback, misleading messages were displayed concerning dispatch table entries (an entry was reported as missing even though it existed). Moreover, the missing entry was reported for the PPP subsystem which was not involved in this case.

This problem has been solved.

4.1.5 Setup Tool – Pre Shared Key not Saved

(ID 2577)

After modification of a peer's pre shared key (PSK) in the menu ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **EDIT** and after saving the changes, the new PSK occasionally was not saved to the MIB.

This problem has been solved.

4.1.6 Wrong Setting in ipsecDialTable

(ID 2583)

Every time an IPSec peer was created with the Setup Tool, and ISDN Callback was activated for that peer during the initial configuration, a wrong interface index (*0*) was stored in the corresponding entry of the **ipsecDialTable**.

While this problem did not affect the functions of your router directly, it created superfluous entries in the MIB tables. It has been solved.

4.1.7 Peers Loaded twice from RADIUS

(ID 2613)

The IPSec peers stored on the RADIUS server are retrieved every time the router is rebooted or the IPSec daemon is reset (e.g. caused by a reconfiguration). The reset deletes all IPSec/RADIUS peers from the router so that upon the next retrieval all entries are stored only once.

In a single case the IPSec/RADIUS peers were not deleted: If you reset the IPSec daemon with the command `kill -10`, the peers already stored were not deleted and double entries were created upon the retrieval from the RADIUS.

This problem has been solved.

4.1.8 Setup Tool – Field Descriptions

(ID 2621)

When editing an existing IPSec peer (***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **EDIT**), the field descriptions of the menu could be focused with the cursor.

This problem has been solved.

4.1.9 Key and Certificate Load/Reload Behavior

(ID 2648)

If a configuration was loaded with `cmd=load`, the automatic assignment of keys to certificates was occasionally destroyed.

This problem has been solved.

4.1.10 IPSec-Callback Sporadically Fails

(ID 2656)

If a pair of IPSec peers was configured both with dynamic addresses and ISDN Callback together with DynDNS, an initiating call sporadically failed. The Phase 1 Security Association was established correctly, but the phase 2 SA was inoperative.

This problem has been solved.

4.1.11 "Ghost Peer" Created

(ID 2689)

When creating a new IPSec peer with IPSec Callback enabled, a ghost peer entry was created under specific circumstances:

- You tried to save the entry with callback enabled (***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **APPEND/EDIT**: **IPSec Callback** set to any value but *disabled*)
- The callback parameters were still incomplete (no or invalid callback numbers specified).

Even though the Setup Tool displayed a warning and did not seem to save the entry to the MIB, an entry actually was created. Moreover, this entry could not be deleted using the Setup Tool.

This problem has been solved.

4.2 Stateful Inspection Firewall

The Stateful Inspection Firewall has been enhanced by a configurable syslog level, and a number of problems have been solved in System Software Release 6.3.4.

4.2.1 Configurable Syslog Level

(ID n/a)

The operation of the SIF generates a considerable number of syslog messages if a larger number of rules is configured. This may in some cases reduce the performance of the router.

In order to reduce the impact of syslog messages, the syslog level can now be specified in a more fine grained way. The available values for the respective variable (**ipSifSyslogLevel**) are:

- *deny* – only rejcets and ignores are displayed
- *accept* – only accepts are displayed
- *verbose* – all SIF activity is displayed (default)
- *none* – syslogs are disabled, only attack warnings are displayed.

4.2.2 Establishing Unwanted WAN Connections

(ID 2383)

Before System Software Release 6.3.4 it was possible that a packet triggered a WAN connection even though the same packet was then rejected by the SIF.

This problem has been solved: With System Software Release 6.3.4, the packet is first inspected by the SIF, and only if it is accepted a WAN connection is established.

4.2.3 Misspelling in Service Alias List

(ID 2616)

The Service Alias "Terminal Server" was displayed as "ierminal Server".

This problem has been solved.

4.2.4 Wrong Index Numbers assigned

(ID 2626)

When adding or deleting entries of the **ipSifAliasAddressTable** or **ipSifAliasServiceTable**, the indices assigned were unpredictable. This occasionally lead to inoperative configurations.

This problem has been solved.

4.3 Flash File System – File Names

(ID n/a)

If more than 30 entries were made in a subdirectory, some of the files were displayed with distorted names.

This problem has been solved.

4.4 MSS Clamping - Malfunction

(ID 2559 and 2567)

If bridging was enabled for the LAN interface of the router, Maximum Segment Size (MSS) Clamping was functional only in the receive direction (Rx) of a DSL connection. This may have had the effect that certain HTTP sites of the Internet were inaccessible. Moreover, MSS Clamping did not function properly in specific LAN-LAN connection scenarios.

These problems have been solved.

4.5 MPPE – Negotiation

(ID 2491)

Maximum flexibility and tolerance (e.g. start a negotiation with MPPE V1 but accept also V2 and vice versa) for MPPE (Microsoft Point to Point Encryption) negotiations lead to a number of problems, especially on connections to Windows clients. In many cases the result of the MPPE negotiation was not transparent for the user.

The most frequent error was that no data transfer was possible even though the connection had been established. This was caused by an "asynchronous" result of the MPPE negotiation (V1 for one and V2 for the other direction).

MPPE negotiation has been enhanced as to avoid such problems.

4.6 VoIP – False Syslog Message

(ID 2578 and 2662)

When booting the router, a syslog warning concerning the VoIP daemon being unable to resolve a certain IP address (0.0.0.0:53) was displayed. This message was misleading, and it did not affect the functionality of your router.

This problem has been solved.

4.7 TAF – Authentication Freezes Router

(ID 2655)

In very specific cases a TAF authentication occasionally lead to a freeze of **X8500**. This occurred either if **X8500** expected a client to perform a TAF authentication, but the client did not run the TAF application, or if the PPP shorthold

was activated before the client had answered the TAF Keepalive message from the router.

This problem has been solved.

4.8 DynDNS

A number of problems found in our DynDNS implementation have been solved in System Software Release 6.3.4:

4.8.1 DynDNS Service Entry not Deleted

(ID 2398)

If a WAN interface used for propagating a dynamic IP address was deleted, the respective DynDNS entry was not deleted from the **ipPublishTable**. This caused problems if the interface number of the original WAN interface was then assigned to another interface over which the IP address could not be propagated.

This problem has been solved.

4.8.2 Reboot with Misconfigured DynDNS Server

(ID 2417)

If a DynDNS server had been misconfigured and did not send the kind of data expected by the router (e.g. an error message instead of protocol data), the router occasionally rebooted.

This problem has been solved.

4.8.3 Unnecessary DynDNS Updates

(ID 2503)

When using the DynDNS service, the IP address was updated in the DynDNS provider's database after every redial, even if the IP address assigned by the ISP was the same as it had been before. This was not only unnecessary, but occasionally lead to problems with DynDNS providers, since they might decide to block your account due to abuse.

This problem has been solved.

4.9 Channel Bundling – Second B-Channel Used for Rx Only

(ID 2563)

Under specific circumstances, a BinTec router was unable to send data over the second B channel when a PC dialed in to the router using channel bundling.

Receiving data over both channels was possible, though. This happened if the second B-channel was created before the Link Control Protocol negotiation of the first B-channel had been completed.

This problem did not occur between two BinTec routers, but only between a BinTec router and a client/router that did not wait for the first channel to be successfully established before establishing a second one.

This problem has been solved.

4.10 QoS

Three problems found in our QoS (Quality of Service) implementation have been solved in System Software Release 6.3.4:

4.10.1 Classification Inoperative

(ID n/a)

If a value involving the *keep TOS* option was chosen for the field **Action** in the ***QoS*** ➧ ***IP Classification and Signalling*** ➧ **ADD/EDIT** (corresponding to setting the variable **ipQosAction** variable in the MIB), the classification was inoperative.

This problem has been solved.

4.10.2 Stack Trace with Frame Relay

(ID n/a)

When QoS was used for a Frame Relay WAN partner, an `ifconfig <interface> down` command for this WAN partner resulted in an error message and a stack trace.

This problem has been solved.

4.10.3 Classified Data Corrupted

(ID 2684)

Before System Software Release 6.3.4 it was possible that after configuring a QoS classification for certain services, the data of exactly that service were corrupted and the service was inaccessible.

This problem has been solved.

4.11 Fax G3 – Sporadic Receive Malfunction

(ID 2494)

Receiving G3 faxes with software products like, e.g., RVS-COM lite occasionally failed. The problem occurred randomly, i.e. it was possible that several consecutive attempts to receive a fax failed. Sending G3 faxes was trouble-free.

This problem has been solved.

4.12 Fax – First Attempt to Send a Fax Fails

(ID 2594)

Sending faxes basically worked correctly, but occasionally the first attempt to send a fax failed. This occurred if a Remote Access Service (RAS) connection had been terminated or a data file transfer had been completed immediately before. A second attempt at sending the fax was successful.

This problem has been solved.

4.13 PPP Keepalive - Interface not Set Down

(ID 2557)

Under specific circumstances, when a connection from one router to another via internet was interrupted, the interface was not set *down* after the PPP Keepalive had failed. Instead, it remained in a *dormant* state with the **AdminStatus** set to *dialup*. This had the effect that the interface was no longer triggered to dial out, and could not be used before a reboot was performed.

This problem has been solved.

4.14 PPP – Keepalives Erroneously Activated

(ID 2215)

Upon leaving the menu ***WAN PARTNER*** ➧ **ADD/EDIT** ➧ ***PPP*** with **SAVE** after adding or editing a WAN partner, the **Keepalives** were set to *on* even if the settings had not been changed.

This problem has been solved.

4.15 PPPoE – LCP Establishment Error

(ID 2340)

Occasionally, a WAN partner with **Static Shorthold** set to a value of *-1* (***WAN PARTNER*** ➧ **ADD/EDIT** ➧ ***ADVANCED SETTINGS***) was inoperative. Debug messages showed Link Control Protocol failures.

This problem has been solved.

4.16 X.25 over CAPI – File Transfer Fails

(ID 2642)

When sending data across an X.25 over CAPI or over RCAPI connection, the file transfer sometimes failed.

This problem occurred with specific clients only. It has been solved.

5 Known Issues

Even though we thoroughly test our system software, the possibility of problems arising during every day use cannot be completely eliminated. BinTec has, therefore, created a mailing list (**release-info**) which will keep you informed on problems, solutions and workarounds verified in our laboratories. If you want to subscribe to this mailing list, you will find a respective link on the download pages of www.bintec.net.

5 Known Issues