RELEASE NOTES
System Software
7.1.4

Version 1.0

Purpose This document describes new features, changes, and solved problems of **System Software 7.1.4**.

Liability While every effort has been made to ensure the accuracy of all information in this manual, Bintec Access Networks GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information and changes can be found at www.bintec.net.

As multiprotocol gateways, Bintec gateways set up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. Bintec Access Networks GmbH accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks Bintec and the Bintec logo are registered trademarks of Bintec Access Networks GmbH.

Other product names and trademarks mentioned are usually the property of the respective companies and manufacturers.

Copyright

Guidelines and standards Bintec gateways comply with the following guidelines and standards:

R&TTE Directive 1999/5/EG

CE marking for all EU countries and Switzerland

You will find detailed information in the Declarations of Conformity at www.bintec.net.

How to reach Bintec

Bintec Access Networks GmbH Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +49 180 300 9191 0 Fax: +49 180 300 9193 0 Internet: www.bintec.net	Bintec France 6/8 Avenue de la Grande Lande F-33174 Gradignan France Telephone: +33 5 57 35 63 00 Fax: +33 5 56 89 14 05 Internet: www.bintec.fr

1 Important Information

Please read the following information about System Software 7.1.4. As System Software 7.1.4 is based on System Software 7.1.1, the same conditions apply to the scope of features and the downgrade restrictions.

Note

Please make sure to read all information about upgrading to **System Software 7.1.4** which is available from our website.

1.1 BOOTmonitor Update

Updating to **System Software 7.1.4** requires a BOOTmonitor update on all gateways of the **X2000** Family.

You will find the necessary files in the Download section of your gateway. The BOOTmonitor can be updated just like the system software using the `update` command. A description can be found in the chapter "Configuration Management" in your gateway manual.

Attention!

The BOOTmonitor update must be carried out before the system software update, as otherwise the system software update is not possible.

Gateways of the X2000 Family need a BOOTmonitor version of 6.3.8 or higher.

1.2 Deleting DSL Logic

On devices of the **X2300** Family it is necessary to delete the DSL logic not required before carrying out the update to **System Software 7.1.4**.

Proceed as follows:

1. Go to the flash ROM management shell: `update -i`.
2. Activate a list of all the files saved in the flash ROM: `ls -l`.

You receive the following shell output (e.g.):

```
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 >
```

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

3. Delete the file that does not match your gateway type: `rm X2E-ADSLi.x2c` or `rm X2E-ADSLp.x2c`.
4. Make sure the file has been deleted: `ls -l`.

You now obtain the following shell output (if, for example, you have 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 >
```

5. Carry out a "reorg" to finally delete the file from the flash ROM: `reorg`. You can activate a list of the saved files again as a check: `ls -l`.
6. Leave the flash ROM management shell: `exit`.

You have deleted the DSL logic not required.

1.3 Downgrade Restrictions

It is not possible to downgrade directly from **System Software 7.1.4** to a previous version of the system software.

⚠ **Attention!**

Configurations created with System Software 7.1.4 are not compatible with older versions of system software.

Save a backup copy of your gateway configuration on a PC before you carry out an upgrade.

Please note that certain features will no longer be available after a downgrade.

It is possible to downgrade in stages:

1. Save a backup copy of your gateway configuration on a PC before you carry out an upgrade to **System Software 7.1.4**. Information on saving an external copy of your configuration can be found in the chapter "Configuration Management" in your gateway manual.
2. Now you can carry out the upgrade and still fall back on your old system software version if necessary. After a downgrade you must reload your gateway with the matching configurations for this system software. Information about the necessary steps can be found in your gateway manual.

Further information about upgrade or downgrade restrictions and the documentation for your gateway can be found at www.bintec.de.

1.4 Scope of Features

System Software 7.1.4 can be used identically for both the new VPN Access series devices and X-Generation devices. Please note, however, that the scope of features can differ between individual devices of a series or different series.

No version of **System Software 7.1.4** is available for the following devices:

- **BinGO! DSL**
- **X1000**

- **X1200**
- **X3200**
- all **BRICK** generation devices.

The following restrictions also exist:

- **BinGO! DSL II** does not have the "IP Address Transfer over ISDN" feature, as **BinGO! DSL II** is not IPSec-capable.

1.5 BRICKware Wizard

Our system software has no longer supported the **BRICKware** Configuration Wizard since Release 7.1.1. A new HTML-based Configuration Wizard is introduced with **System Software 7.1.4**.

1.6 Software Image Names

The names of the software images have changed and the device code is now placed before the actual release code. If your gateways are configured using the XAdmin configuration tool, you must initially still use the old image names. This is done by just deleting the device code from the name: "X1x00II-b7101.x2x" then becomes "b7101.x2x".

1.7 Prerequisites for Using the AUX Interface

Releases 7.1.1 and 7.1.4 of our system software support connecting an analog or GSM modem to the serial port of your gateway. There is a number of prerequisites that must be met, otherwise connecting a modem may fail.

Please refer to the Release Notes for System Software release 7.1.1 to learn about the supported options and possible restrictions. In particular, note the following:

- Only the modems specified in the Release Notes have been successfully tested and are certified by Bintec. XON/XOFF flow control must be fully supported and functional, otherwise a connection between the gateway and the modem will most probably fail.
- Make sure that the cable used for connecting gateway and modem complies with the specifications detailed in the Appendix to Release Notes 7.1.1. If in doubt, you can purchase a ready converted cable from Bintec.

2 New Features

System Software 7.1.4 is a Major Release and contains a number of important new features.

These are described in the following chapters:

- "HTML Wizard" on page 11
- "Transfer of IP Address over ISDN" on page 13
- "NAT Traversal" on page 17
- "Event Scheduler" on page 19.

2.1 HTML Wizard

System Software 7.1.4 offers am HTML-based Configuration Wizard, which makes basic configuration tasks considerably easier for you and ensures a workable configuration for your router or gateway.

The HTML Wizard is available on the following devices:

- **VPN Access 5/25/100**
- **BinGO! DSL II**
- **X1000 II**
- **X1200 II**
- all devices in the **X2000** Family.

Bintec routers and gateways are supplied with a default IP configuration (IP address: *192.168.0.254*, netmask: *255.255.255.0*). Start the 192.168.0.254/wizard to start the HTML configuration assistant (**HTML Wizard**). This guides you through a basic configuration, which includes all the important settings of the gateway, access to the Internet via an Internet Service Provider (ISP) and connection to a WAN partner (e.g. a head office). Detailed knowledge of networking is not necessary. A detailed online help system gives you extra support.

Note The HTML Wizard has a default timeout of 5 minutes, i.e. the HTML session is ended after 5 minutes inactivity and you must carry out the complete configuration again.

2.1.1 Changing the Language

When updating a device with **System Software 7.1.4**, only the English version of the HTML Wizard is loaded initially. Other languages (for the time being German only) can be installed later. Devices delivered with System Software 7.1.4 installed already contain the relevant language files.

To additionally install a language file after a system software update, you need a TFTP server to enable the gateway to load the file. A TFTP server is included in the **Dime Tools**, which are part of **BRICKware for Windows**.

Your gateway must have a working IP configuration to be able to transfer the language file by TFTP.

To do Proceed as follows:

1. Download the relevant language file from our Web server. The file name is based on the relevant language and your gateway type (e.g. german.x2c for a German language file for X2x compact).
2. Copy or drag the file into the root directory of the TFTP server and start the server.
3. Log in to your gateway as `admin`.
4. Download the file from your PC (make sure you use the IP address of your PC): `update <IP address of TFTP server> german.x2c`.

The language file is now available on your gateway and no more steps are necessary.

2.1.2 ASCII Wizard

If access to your gateway is not possible over the LAN or you cannot access the HTML Wizard for other reasons, you can start an ASCII-based version of the Wizard in the SNMP shell. You can then also use all the Wizard functions over a serial connection.

To do You can start an ASCII version of the Wizard regardless of how you are connected to the gateway: Your gateway connection can be over the LAN, over a serial connection or over ISDN login. You must log in as `admin` and be able to access the SNMP shell.

Proceed as follows:

1. Log in to your gateway as `admin`.
2. Enter the command `wizard` after the command prompt and press **Return**.

The ASCII version of the Wizard is started. This offers the same configuration possibilities as the HTML Wizard and the help texts are also available via the **HELP** button.

2.2 Transfer of IP Address over ISDN

Transferring the IP address of a gateway over ISDN (in the D-channel and/or B-channel) opens up new possibilities for the configuration of IPSec VPNs, as the limitations that occur in IPSec configuration with dynamic IP addresses can be avoided.

Until now, IPSec ISDN callback only supports tunnel setup if the current IP address of the initiator can be determined by indirect means (e.g. via DynDNS). However, DynDNS has serious disadvantages, such as the latency until the IP address is actually updated in the database. This can mean that the IP address propagated via DynDNS is not correct. This problem is avoided by transferring the IP address over ISDN. This type of transfer of dynamic IP addresses also enables the more secure ID Protect mode to be used for tunnel setup.

2.2.1 Method of Operation

Various modes are available for transferring your own IP address to the peer: The address can be transferred free in the D-channel or in the B-channel, but here the call must be accepted by the remote station and therefore incurs costs.

If a peer whose IP address has been assigned dynamically wants to arrange for another peer to set up an IPSec tunnel, it can transfer its own IP address as per the settings described in “Configuration” on page 15. Not all transfer modes are supported by all telephone companies. If you are not sure, automatic selection by the gateway can be used to ensure that all the available possibilities can be used.

Note

The callback configuration on the two gateways should be identical so that the gateway of the called peer can identify the IP address information.

The IP address transfer and the start of IKE phase 1 negotiation take place in the following steps:

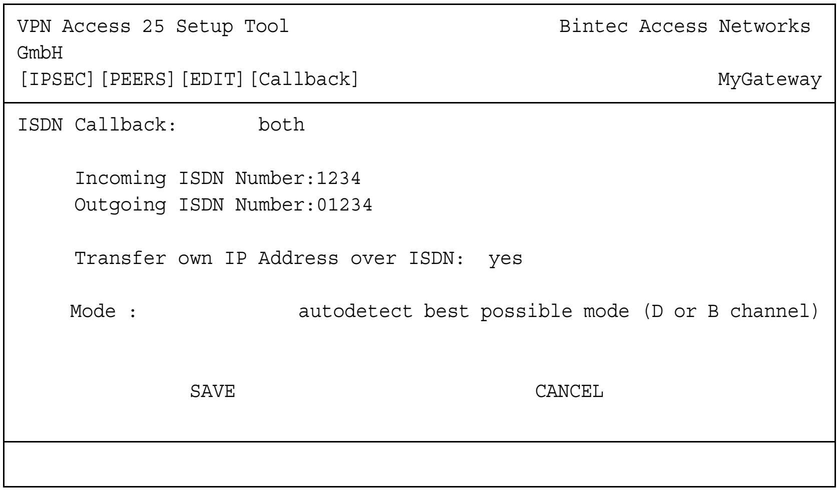
1. Peer A (the callback initiator) sets up a connection to the Internet in order to be assigned a dynamic IP address and be reachable for peer B over the Internet.
2. The gateway creates a token with a limited validity and saves it together with the current IP address in the MIB entry belonging to peer B.
3. The gateway sends the initial call to peer B, which transfers the IP address of peer A and the token as per the callback configuration.
4. Peer B extracts the IP address of peer A and the token from the ISDN call and assigns them to peer A based on the calling party number configured (the ISDN number used by peer A to send the initial call to peer B).
5. The IPSec Daemon at peer B’s gateway can use the transferred IP address to initiate phase 1 negotiation with peer A. Here the token is returned to peer A in a part of the payload in IKE negotiation.
6. Peer A is now able to compare the token returned by peer B with the entries in the MIB and so identify the peer without knowing its IP address.

As peer A and peer B can now mutually identify each other, negotiations can also be conducted in ID Protect mode using preshared keys.

2.2.2 Configuration

The configuration is carried out in the context of IPSec callback configuration in the ***IPSEC* ➜ *CONFIGURE PEERS* ➜ *APPEND/EDIT* ➜ *IPSEC CALLBACK*** menu.

The menu is shown below (the screenshot contains example values):



```
VPN Access 25 Setup Tool                               Bintec Access Networks
GmbH
[IPSEC][PEERS][EDIT][Callback]                                      MyGateway

ISDN Callback:       both

     Incoming ISDN Number:1234
     Outgoing ISDN Number:01234

     Transfer own IP Address over ISDN:  yes

     Mode :              autodetect best possible mode (D or B channel)


              SAVE                          CANCEL
```

It contains the following new fields:

Field	Description
Transfer own IP Address over ISDN:	Here you select whether the IP address of your own gateway is to be transferred over ISDN for IPSec callback. Possible values: ■ *yes* - The IP address is transferred according to the settings in the following fields. ■ *no* - (Default value) The IP address is not transferred.

Field	Description
Mode	Only visible if ***Transfer own IP Address over ISDN*** = *yes*. Here you select the mode in which the gateway tries to transfer its IP address to the peer. Possible values: ■ *autodetect best possible mode (D or B channel)* - (Default value) The gateway determines the best mode automatically. All D-channel modes are tried first before the B-channel is used (using the B-channel incurs costs). ■ *autodetect best possible mode (D channel only)* - The gateway determines the best D-channel mode automatically. The use of the B-channel is excluded. ■ *use specific D channel mode* - The gateway tries to transfer the IP address in the mode set in the ***D-Channel Mode*** field. ■ *try specific D channel mode,* *fall back on B* - The gateway tries to transfer the IP address in the mode set in the ***D-Channel Mode*** field. If this does not succeed, the IP address is transferred in the B-channel (this incurs costs). ■ *use B channel* - The gateway transfers the IP address in the B-channel. This incurs costs.

Field	Description
D-Channel Mode	Only visible if ***Mode*** = *use specific D channel mode* or *try specific D channel mode, fall back on B*. Here you select the D-channel mode in which the gateway tries to transfer the IP address. Possible values: ■ *LLC* - (Default value) The IP address is transferred in the LLC information elements of the D-channel. ■ *SUBADDR* - The IP address is transferred in the subaddress information elements of the D-channel. ■ *LLC-and-SUBADDR* - The IP address is transferred in both the LLC and subaddress information elements.

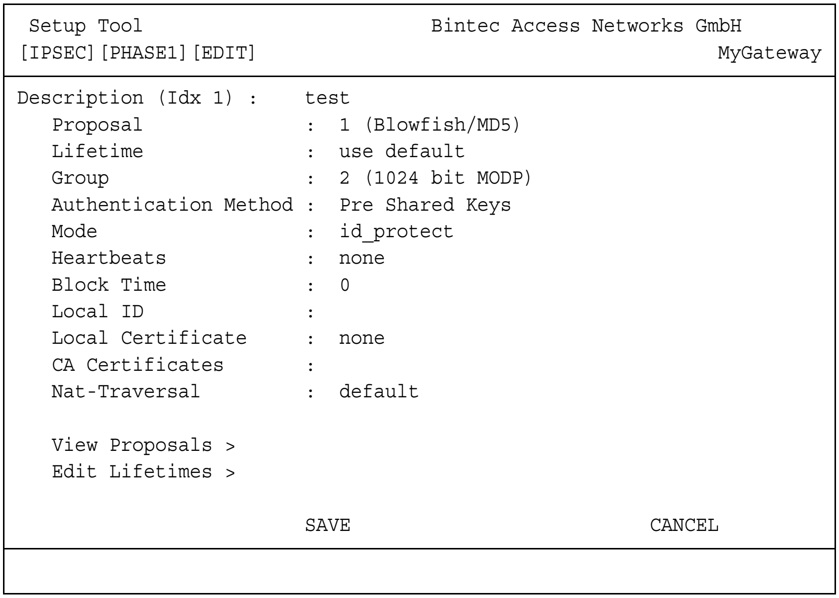
Table 2-1: ***IPSec → Configure Peers → APPEND/EDIT → IPSec Callback***

2.3 NAT Traversal

NAT Traversal (NAT-T) allows the creation of IPSec tunnels across one or more gateways that have Network Address Translation activated.

Without NAT-T there may be incompatibilities between IPSec and NAT (cf. RFC 3715, section 2). These especially constrict the creation of an IPSec tunnel from a host inside a LAN and behind a NAT gateway to another host or another gateway outside the LAN. NAT-T allows establishing such tunnels without any conflicts: the IPSec Daemon automatically detects active NAT and uses NAT-T.

The configuration of NAT-T is as simple as activating or deactivating it in the settings of Phase 1 profiles. A respective parameter has been added to Phase 1 profile configuration:



```
 Setup Tool                              Bintec Access Networks GmbH
[IPSEC][PHASE1][EDIT]                                          MyGateway

Description (Idx 1) :    test
   Proposal              :   1 (Blowfish/MD5)
   Lifetime              :   use default
   Group                 :   2 (1024 bit MODP)
   Authentication Method :   Pre Shared Keys
   Mode                  :   id_protect
   Heartbeats            :   none
   Block Time            :   0
   Local ID              :
   Local Certificate     :   none
   CA Certificates       :
   Nat-Traversal         :   default

   View Proposals >
   Edit Lifetimes >

                         SAVE                          CANCEL
```

You can choose from three values for the field ***Nat-Traversal***:

- *default* - If you choose this value when configuring peer specific parameters (in ***Configure Peers ➜ ADD/EDIT ➜ Peer specific Settings ➜ IKE (Phase 1) Defaults: edit***), the gateway uses the value chosen for the global default profile (in ***IPSec ➜ IKE (Phase 1) Defaults: edit***). A global profile cannot be saved with this value. If there already is any Phase 1 profile when updating to **System Software 7.1.4**, Nat-Traversal is set to *default* for this profile. For a global profile this means that NAT-T remains deactivated.
- *enabled* - NAT-T is activated in this profile.
- *disabled* - NAT-T is deactivated in this profile.

When configuring an IPSec connection by means of the HTML Wizard or by means of the Setup Tool IPSec Wizard, NAT-T is activated. The Setup Tool IP-

Sec Wizard, however, does not change the the NAT-T settings of an already existing default profile.

Note

If you want to allow IPSec connections starting with the gateway as well as connections starting with a host inside the LAN, you must remove such entries pertaining to IKE traffic from the ***ipNatOutTable***. Otherwise all IKE sessions will be directed to the same internal IP address, and only the session initiated last is really established.

Deleting the NAT entries, however, has the effect that you may experience difficulties with IPSec connections from the gateway to other hosts or gateways which do not support NAT-T, since the source port of the IKE connection is now changed by NAT.

2.4 Event Scheduler

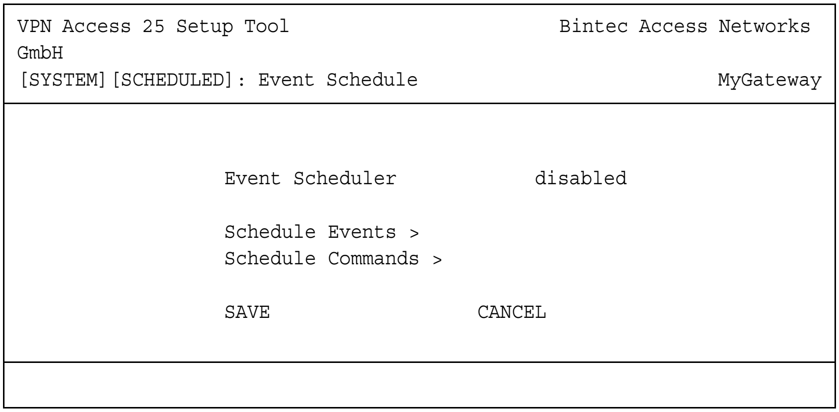
To enable events like deactivating an Internet access on exceeding a certain transfer volume, System Software 7.1.4 offers an event scheduler. This makes it possible to assign any action to any event.

Apart from default and easily configured standard applications like time- or volume-controlled activation of interfaces, the event scheduler permits access to any MIB parameter. This means that any event in the MIB can be defined as the trigger of any desired action.

Attention!

Configuration of actions that are not available as defaults requires extensive knowledge of the method of operation of our gateways. An incorrect configuration can cause considerable disturbances in operation. If applicable, save the original configuration on a PC.

The event scheduler is configured in the ***System* ➜ *Schedule & Monitor* ➜ *Event Scheduler (Time & SNMP)*** menu:



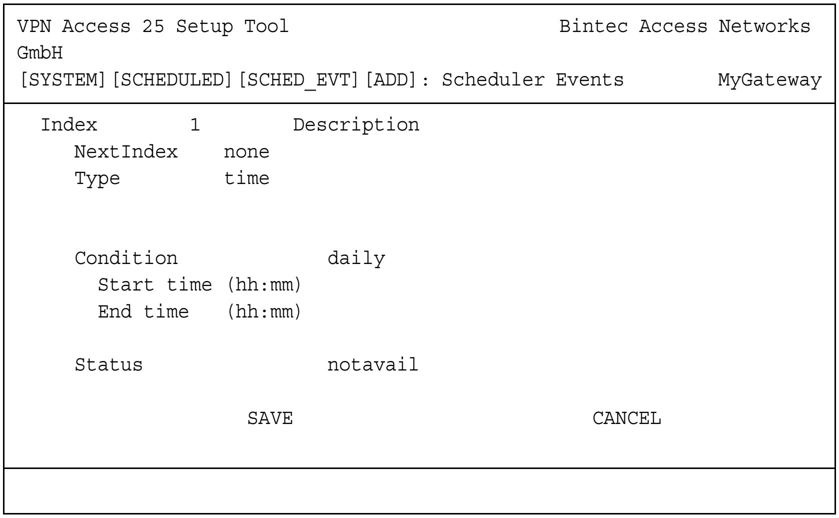
```
VPN Access 25 Setup Tool                        Bintec Access Networks
GmbH
[SYSTEM][SCHEDULED]: Event Schedule                          MyGateway


                  Event Scheduler            disabled

                  Schedule Events >
                  Schedule Commands >

                  SAVE                  CANCEL

```

Activate or deactivate the scheduler in the ***Event Scheduler*** field; the default setting is *enabled*. Configure the events that are to trigger a certain action at the gateway in the ***Schedule Events*** menu and the actions to be executed in the ***Schedule Commands*** menu. The triggers (events) can be linked to event chains, so that complex conditions for initiating an action can also be created.

2.4.1 Configuration of Triggers (Events)

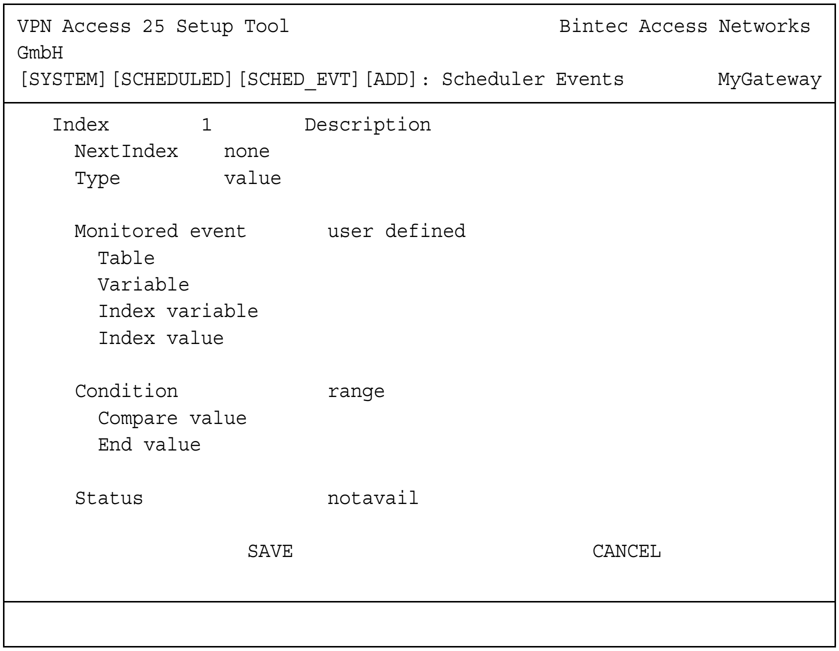
The events that trigger a relevant action are created and edited in the ***System* ➜ *Schedule & Monitor* ➜ *Event Scheduler (Time & SNMP)* ➜ *Schedule Events* ➜ *ADD/EDIT*** menu.

The default menu opens with the mask for configuration of an event of the *time* type:



```
VPN Access 25 Setup Tool                                Bintec Access Networks
GmbH
[SYSTEM][SCHEDULED][SCHED_EVT][ADD]: Scheduler Events             MyGateway

  Index         1        Description
     NextIndex     none
     Type          time


     Condition               daily
       Start time  (hh:mm)
       End time    (hh:mm)

     Status                  notavail

                     SAVE                          CANCEL
```

If you select ***Type*** = *value*, the menu changes as follows:



```
VPN Access 25 Setup Tool                               Bintec Access Networks
GmbH
[SYSTEM][SCHEDULED][SCHED_EVT][ADD]: Scheduler Events          MyGateway

   Index        1        Description
     NextIndex     none
     Type          value

     Monitored event       user defined
       Table
       Variable
       Index variable
       Index value

     Condition             range
       Compare value
       End value

     Status                notavail

                    SAVE                          CANCEL
```

The menu contains the following fields depending on the setting:

Field	Description
Index	The gateway assigns an index number for the entry automatically. This value can also be edited. Possible settings are all values from *1* to *65535*.
Description	Here you enter the desired description for the event. The maximum length of the entry is 30 characters.

Field	Description
Next Index	Here you enter which entry is to follow the current entry in an event chain. The entries in an event chain form a complex condition for an action to be executed. How the event chain leads to an action is configured in the ***SYSTEM* ➜ *SCHEDULE & MONITOR* ➜ *EVENT SCHEDULER (TIME & SNMP)* ➜ *SCHEDULE COMMANDS*** menu.
Type	Here you select which type of event is to trigger an action: Possible settings: ■ *time* - The action is triggered at certain times (default value). ■ *value* - The action is triggered as soon as an MIB variable assumes a certain value.

Field	Description
Monitored event	Only for ***TYPE*** = *value*. Here you can choose between different events. Possible settings: ■ *user defined* - You can choose which of the possible values of a MIB variable the scheduler is to respond to with an action (default value). ■ *WAN interface total charge* - An action is executed if certain costs are incurred at a WAN interface (the interface is selected on configuring the action). The gateway must receive metering pulses from the provider for this purpose. ■ *WAN interface total duration* - An action is executed if a WAN interface has been active for a certain time. ■ *WAN interface total RX traffic* - An action is executed if a WAN interface has received a certain amount of data (in bytes). ■ *WAN interface total TX traffic* - An action is executed if a WAN interface has sent a certain amount of data (in bytes).
Table	Only for ***MONITORED EVENT*** = *user defined*. Here you enter the MIB table containing the MIB variable that is to be used for the trigger, e.g. ***PPPTABLE***.
Variable	Only for ***MONITORED EVENT*** = *user defined*. Here you enter the MIB variable that is to be used for the trigger, e.g. ***PPPMAXCONN***.

Field	Description
Index variable	Only for ***MONITORED EVENT*** = *user defined*. Here you enter the index variable of the previously selected MIB table. This is the variable marked with an asterisk (*) in the table view of the desired MIB table, e.g. ***PPPTYPE***. The entries in an MIB table are indexed internally. This indexing is not shown in the normal table view. Enter `y` in the shell to deactivate the table mode. If you now, for example, enter `pppTable`, the entries are listed in a format that shows the indexing (e.g. ***BIBOPPPTYPE.1.1(RW): ISDN_DIALUP***). The unique identification of a certain table entry is given by the combination of the index variable (including the internal index) and its value (see ***INDEX VALUE*** below).
Index value	Only for ***MONITORED EVENT*** = *user defined*. Here you enter the value of the index variable for the table entry that is to be used for the trigger, e.g. ***ISDN_DIALUP***.

Field	Description
Condition	For ***Type*** = *time*: ■ *daily* - The action is triggered daily (default value). ■ *<day of week>* - The action is triggered repeatedly on a certain day of the week. ■ *mon-fri* - The action is triggered daily from Monday to Friday. ■ *sat_sun* - The action is triggered repeatedly on Saturdays and Sundays only. ■ *day <1 .. 31>* - The action is triggered repeatedly on a certain day of the month. For ***Type*** = *value*: ■ *range* - The action is triggered if the value of the variable lies between two certain values (default value). ■ *greater* - The action is triggered if the value of the variable exceeds a certain value. ■ *equal* - The action is triggered if the value of the variable is a certain value. ■ *less* - The action is triggered if the value of the variable remains below a certain value. ■ *notequal* - The action is triggered if the value of the variable is not a certain value.
Compare value	The value at which the value of the variable bears the relationship determined by ***Condition***. If ***Condition*** = *range*, this is the start value of the range of values.

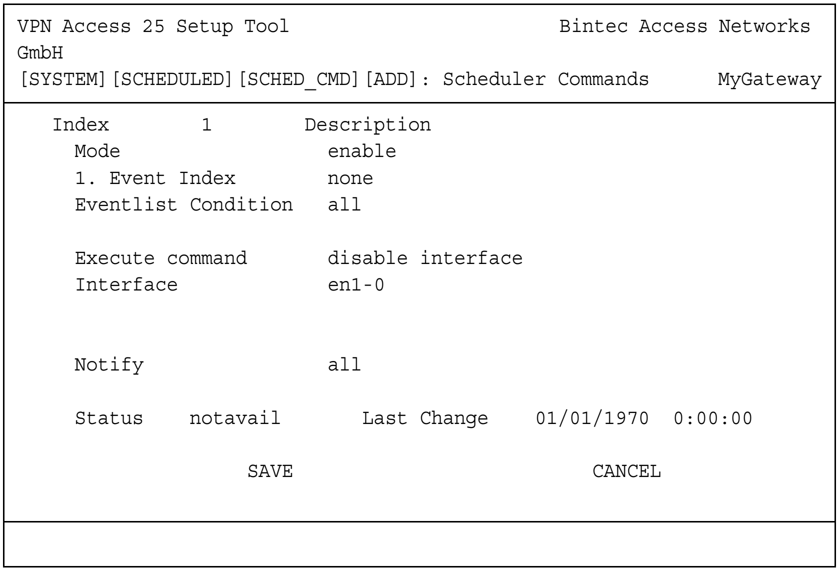
Field	Description
End value	If ***CONDITION*** = *range*, this is the end value of the range of values.
Start time (hh:mm)	Only for ***TYPE*** = *time*. Here you enter the time at which the action is to be started.
End time (hh:mm)	Only for ***TYPE*** = *time*. Here you enter the time at which the action is to be ended.
Status	This field cannot be edited and shows the status of the trigger. Possible values: ■ *active* - The trigger is currently active. ■ *inactive* - The trigger is inactive. ■ *notavail* - The status cannot be determined, e.g. if the scheduler is not activated. ■ *error* - An error has occurred; the configuration of the trigger is not consistent.
Last Change	Shows the time of the last status change. This field cannot be edited.

Table 2-2: ***SYSTEM ➜ SCHEDULE & MONITOR ➜ EVENT SCHEDULER (TIME & SNMP) ➜ SCHEDULE EVENTS ➜ ADD/EDIT***

2.4.2 Configuration of the Action (Command)

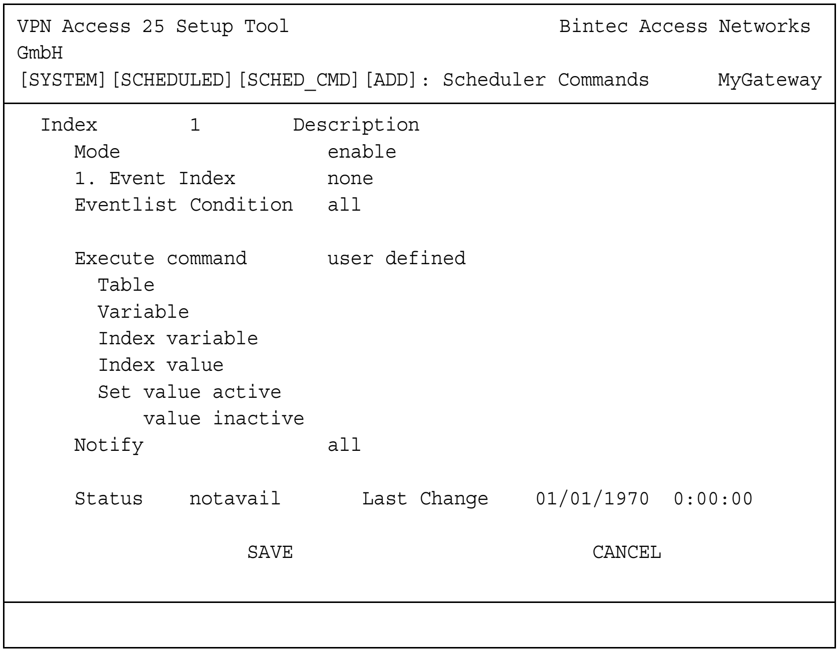
The action executed as soon as one of the events configured as trigger occurs is created or edited in the ***SYSTEM ➜ SCHEDULE & MONITOR ➜ EVENT SCHEDULER (TIME & SNMP) ➜ SCHEDULE COMMANDS ➜ ADD/EDIT*** menu.

The default menu opens with the options for selecting one of the default actions:



```
VPN Access 25 Setup Tool                               Bintec Access Networks
GmbH
[SYSTEM][SCHEDULED][SCHED_CMD][ADD]: Scheduler Commands      MyGateway

   Index        1        Description
     Mode                  enable
     1. Event Index        none
     Eventlist Condition   all

     Execute command       disable interface
     Interface             en1-0


     Notify                all

     Status    notavail       Last Change    01/01/1970  0:00:00

                    SAVE                          CANCEL
```

If you select the value *user defined* for the ***Execute Command*** field, the menu changes as follows:



```
VPN Access 25 Setup Tool                               Bintec Access Networks
GmbH
[SYSTEM][SCHEDULED][SCHED_CMD][ADD]: Scheduler Commands      MyGateway

  Index         1        Description
     Mode                     enable
     1. Event Index           none
     Eventlist Condition      all

     Execute command          user defined
       Table
       Variable
       Index variable
       Index value
       Set value active
           value inactive
     Notify                   all

     Status    notavail       Last Change    01/01/1970  0:00:00

                    SAVE                          CANCEL
```

The menu contains the following fields depending on the setting selected:

Field	Description
Index	The gateway assigns an index number for the entry automatically. This value can also be edited. Possible settings are all values from *1* to *65535*.
Description	Here you enter the desired description for the event. The maximum length of the entry is 30 characters.

Field	Description
Mode	Here you select if the configured action is to be active or inactive. Possible settings: ■ *enable* (default value) ■ *disable.*
1. Event Index	Here you define the first event of an event (trigger) chain. The event chain is activated only for this entry and the following ones, preceding entries are ignored. The default value is *none*.
Eventlist Condition	Here you define whether all the entries of an event chain must occur before an action is executed. Possible settings: ■ *all* - All events of an event chain must occur if the action is to be executed (default value). ■ *one* - At least one of the events of an event chain must occur if the action is to be executed. ■ *none* - None of the events of an event chain may occur if the action is to be executed. ■ *one_not* - At least one of the events of an event chain must not occur if the action is to be executed.

Field	Description
Execute command	Here you define the action that is executed by an trigger. Possible settings: - *disable interface* - The interface set in the ***INTERFACE*** field is deactivated (its ***ADMINSTATUS*** is set to *down*, default value). - *enable interface* - The interface set in the ***INTERFACE*** field is activated (its ***ADMINSTATUS*** is set to *up*). - *user defined* - The action is configured as desired in the following fields.
Interface	Here you select which interface is to be activated or deactivated if *disable interface* or *enable interface* is selected for ***EXECUTE COMMAND***. The default value is *en1-0*.
Table	Only for ***EXECUTE COMMAND*** = *user defined*. Here you enter the MIB table containing the variable to be set.
Variable	Only for ***EXECUTE COMMAND*** = *user defined*. Here you enter the MIB variable to be set.

Field	Description
Index variable	Only for ***Execute Command*** = *user defined*. Here you enter the index variable of the previously selected MIB table. This is the variable marked with an asterisk (*) in the table view of the desired MIB table. The entries in an MIB table are indexed internally. This indexing is not shown in the normal table view. Enter `y` in the shell to deactivate the table mode. If you now, for example, enter `pppTable`, the entries are listed in a format that shows the indexing (e.g. ***biboPPPType.1.1(rw): isdn_dialup***). The unique identification of a certain table entry is given by the combination of the index variable (including the internal index) and its value (see ***Index value*** below).
Index value	Only for ***Execute Command*** = *user defined*. Here you enter the value of the index variable for the table entry that is to be changed by the action.
Set value active	Only for ***Execute Command*** = *user defined*. Here you enter the value the ***Variable*** is to be assigned by the action. The value is set as soon as an appropriate trigger becomes active and is retained until the trigger becomes inactive again.
Value inactive	Only for ***Execute Command*** = *user defined*. Here you enter the value the variable is to become as soon as the trigger becomes inactive. This value is also assigned to the variables after a gateway restart or if the system time is not set correctly.

Field	Description
Notify	Here you select the mechanisms to be used to notify actions. Possible settings: ■ *all* - Both SNMP traps and syslog messages are generated. ■ *snmptrap* - Only SNMP traps are generated. ■ *syslog* - Only syslog messages are generated. ■ *none* - No messages are generated.
Status	This field cannot be edited and shows the status of the action. Possible values: ■ *active* - The action is currently performed. ■ *inactive* - The action is not performed. ■ *notavail* - The status cannot be determined, e.g. if the scheduler is not activated. ■ *error* - An error has occurred; the configuration of the action is not consistent.
Last Change	Shows the time of the last status change. This field cannot be edited.

Table 2-3: ***SYSTEM ➜ SCHEDULE & MONITOR ➜ EVENT SCHEDULER (TIME & SNMP) ➜ SCHEDULE COMMANDS ➜ ADD/EDIT***

3 Changes

In addition to new features, there are a number of changes that extend the scope of features and services of our software.

These changes are described in the following chapters:

- "New Commands" on page 35
- "HTML Wizard - LAN-LAN Connection via IPSec" on page 36
- "New Mechanism for PMTU Discovery and MSS Clamping" on page 37

3.1 New Commands

To make it possible to export and import sensitive data like preshared keys of an IPSec configuration with the configuration file, two new commands have been incorporated into the *biboAdmConfigTable*: `put_all` **and** `get_all`**.**

Attention!

Note that the file is saved on the PC in unencrypted form and sensitive data can therefore be read in plain text. Secure your PC accordingly to prevent unauthorized access to the saved files.

put_all The following syntax is used for saving the `boot` configuration:

`cmd=put_all host=<IP address of TFTP server> path=<name of file to be sent from flash> file=<name of file on PC>`.

For example:

```
x2300ic:biboAdmConfigTable> cmd=put_all host=192.168.0.1 path=boot
file=boot.cf
01: biboAdmConfigCmd.3.7( rw):        put_all
01: biboAdmConfigHost.3.7( rw):       192.168.0.1
01: biboAdmConfigPath.3.7( rw):       "boot"
01: biboAdmConfigFile.3.7( rw):       "boot.cf"
x2300ic:biboAdmConfigTable>
```

get_all The syntax for loading a file is accordingly:

`cmd=get_all host=<IP address of TFTP server> path=<name of file to be saved in flash> file=<name of file on PC>`.

For example:

```
x2300ic:> cmd=get_all host=192.168.0.1 path=boot file=boot
00: biboAdmConfigCmd.4.10( rw):        get_all
00: biboAdmConfigHost.4.10( rw):       192.168.0.1
00: biboAdmConfigPath.4.10( rw):       "knut"
00: biboAdmConfigFile.4.10( rw):       "knut"
x2300ic:>
```

3.2 HTML Wizard - LAN-LAN Connection via IPSec

For a LAN-LAN connection via IPSec it was up to now necessary to configure Internet access via ISDN or DSL. Internet access through a second gateway (i. e. through an Ethernet connection) was not supported by the HTML Wizard.

System Software 7.1.4 introduces the possibility of such a configuration. If the location to be connected uses a second gateway (i. e. an Ethernet connection) for internet access, proceed as follows.

1. Start the HTML Wizard.
2. After choosing a language, choose *Advanced* for **CONFIGURATION MODE**.
3. Select all three ***CONFIGURATION SECTIONS*** (*General settings*, *Internet access*, *Connection to Corporate Network*).
4. Proceed with the configuration until you reach Internet access configuration. In the first configuration window, choose *by third party gateway* for ***INTERNET ACCESS***.
   The windows now refreshes and allows the configuration of further parameters.
5. Specify the IP address at which the third party gateway can be reached from inside your LAN.
6. If you have not specified a DNS server during the configuration of the general settings, you need to do so here.

You have now prepared your gateway for a LAN-LAN connection via IPSec without ISDN or DSL Internet access.

7. Proceed with the configuration of your gateway until you reach the LAN-LAN configuration. In the first configuration window, choose IPSec for ***AVAILABLE CONNECTION TYPE***.

3.3 New Mechanism for PMTU Discovery and MSS Clamping

Since problems with discovering the correct PMTU for IPSec connections because of missing ICMP messages have been reported, the respective mechanisms have been reworked.

Basically it is now ensured that PMTU discovery functions properly even for IPSec connections. Moreover, the PMTU discovery behavior of your gateway can be fine-tuned with a new MIB variable.

The new variable (***IKEPRFMTUMAX***) allows specifying a default value for a peer's MTU. This value also designates the maximum value accepted during PMTU discovery. It can assume any integer value from *0* to *65536*, where all values <*214* are adjusted to a value of *214* (the smallest acceptable value). The default value (*0*) implies a MTU of 1418 Bytes.

In any existing profile, the variable assumes the default value (*0*) when a system software update is performed. Likewise, the default value is assumed for all IPSec configurations performed with either the Setup Tool IPSec Wizard or the HTML Wizard. Setting a value for ***IKEPRFMTUMAX*** in the Setup Tool is otherwise not supported.

The peer MTU currently used is displayed in ***IPSECPEERMTU***.

MSS Clamping is activated dynamically according to a peer's configuration. If you have created a virtual interface peer (***IPSECPEERVIRTUALINTERFACE*** = *enabled*), MSS Clamping will be activated for incoming as well as for outgoing traffic, and the value specified in ***IPSECPEERMTU*** will be assumed, if no differing setting has been made in ***IPEXTIFTXPMSSCLAMPING*** (i.e. if the value there is *0*).

For peers created with a traffic list, MSS Clamping will not be used.

4 Solved Problems

The following problems have been solved with System Software 7.1.4:

- “Memory Loss” on page 40
- “ATM - Route Points to Wrong Interface” on page 40
- “SNMP Shell - Command "t 0" Does not Disable Autologout” on page 40
- “NAT -PMTU Discovery Fails” on page 41
- “IPSec Setup Tool Wizard - Wrong Values Displayed” on page 41
- “Setup Tool - Advanced Interface Settings not Saved” on page 41
- “SSH Daemon Dies after Connection Failure” on page 42
- “IPSec - Memory Leak” on page 42
- “RIP - Route Import Restricted” on page 42
- “BOOTP Relay - Inform Packets not Handled Properly” on page 43
- “BRRP- Reboot” on page 43
- “QoS - Wrong Length for Input Field” on page 43
- “AUX - PPP Connections Interrupted” on page 44
- “LED - HA LED Dead” on page 44
- “PPP - MTU Ignored on Responder Side” on page 44
- “QoS - Problems with X8E-SYNC” on page 44
- “Configuration Management - Configuration File Cannot Be Imported” on page 45
- “PPTP - Incorrect IP Settings in PPTP Partner Configuration” on page 45

4.1 Memory Loss

(ID n/a)

An internal function caused a memory leak when using the IPSec version of our system software.

This problem has been solved.

4.2 ATM - Route Points to Wrong Interface

(ID n/a)

A new IP entry was created in one of the following menus:

- ***ATM* ➜ *ETHERNET OVER ATM* ➜ *ADD/EDIT* ➜ *IP AND BRIDGING* ➜ *ADD/EDIT***
- ***ATM* ➜ *ROUTED PROTOCOLS OVER ATM* ➜ *ADD/EDIT* ➜ *IP* ➜ *ADD/EDIT***.

Any IP route referring to one of the interfaces that were created by this new entry pointed to a wrong interface.

This problem has been solved.

4.3 SNMP Shell - Command "t 0" Does not Disable Autologout

(ID 2668)

Under specific circumstances an autologout occurs even though it should have been disabled by entering `t 0` in the SNMP shell.

This problem has been solved.

4.4 NAT -PMTU Discovery Fails

(ID 2792)

The discovery of the Path Maximum Transfer Unit failed for interfaces for which NAT (Network Address Translation) was activated, possibly causing packet loss.

This problem has been solved.

4.5 IPSec Setup Tool Wizard - Wrong Values Displayed

(ID 3260)

When configuring the advanced interface settings of a virtual interface peer during an IPSec wizard run, the values displayed differed from the ones actually used. Only if the displayed settings were confirmed by hitting SAVE, the values are stored in the MIB and activated.

This problem has been solved.

4.6 Setup Tool - Advanced Interface Settings not Saved

(ID 3266)

When configuring the Advanced Interface IP settings in any of the contexts where they are available (e.g. WAN Partner configuration), the values were not saved to the MIB. Configuration via the SNMP shell was possible, though.

This problem has been solved.

4.7 SSH Daemon Dies after Connection Failure

(ID 3301)

After a failed connection attempt the SSH daemon sporadically died without respawning. Moreover, SSH connections failed through interfaces on which NAT was activated, causing the same effect.

This problem has been solved.

4.8 IPSec - Memory Leak

(ID 3318)

Activating IPSec on a gateway could cause a significant memory leak and lead to the gateway rebooting.

This problem has been solved.

4.9 RIP - Route Import Restricted

(ID 3325)

Route import via RIP (Routing Information Protocol) was restricted to 100 routes.

This problem has been solved.

4.10 BOOTP Relay - Inform Packets not Handled Properly

(ID 3327)

DHCP Inform Packets were generated by a Windows PC and were relayed correctly to the central side DHCP server. The response packets from the DHCP server, however, were not routed to the PC client.

This problem has been solved.

4.11 BRRP- Reboot

(ID 3356)

Entering the menu ***BRRP*** ➜ ***CONFIGURATION*** ➜ ***ADD*** sporadically caused the gateway to reboot without a stacktrace.

This problem has been solved.

4.12 QoS - Wrong Length for Input Field

(ID 3366)

If the field ***SPECIFY TOS SET RATE LIMITATION*** was set to *packets* in the ***QOS*** ➜ ***IP CLASSIFICATION AND SIGNALLING*** ➜ ***ADD/EDIT*** ➜ ***SIGNALLING (TOS)*** menu, the Setup Tool specifies a maximum value of 256000 (six digits) for the fields ***MAXIMUM RATE (PACKETS PER SECOND)*** and ***MAXIMUM BURST SIZE (NUMBER OF PACKETS)***. It was, however, only possible to enter five digits.

This problem has been solved.

4.13 AUX - PPP Connections Interrupted

(ID 3369)

PPP connections via the AUX interface occasionally experienced interrupted data transfer or the connection to the modem was lost completely.

This problem has been solved.

4.14 LED - HA LED Dead

(ID 3377)

The LED labeled "HA" did not behave as is described in the user’s guide: It did not respond to any internal state of the gateway and, therefore, never lit up.

This problem has been solved.

4.15 PPP - MTU Ignored on Responder Side

(ID 3400)

In case of inband authentication (and identification) of incoming PPP connections the MTU adjustment determined by the variable ***PPPExtIfMtu*** was carried out only by the gateway initiating the PPP session.

This problem has been solved.

4.16 QoS - Problems with X8E-SYNC

(ID 3412)

When handling a high amount of traffic, a QoS configuration for priority queues with a bandwidth restriction did not work properly.

This problem has been solved.

4.17 Configuration Management - Configuration File Cannot Be Imported

(ID 3417)

When an error occurring in the context of the Email Alert feature was stored in the MIB, this prevented the gateway from re-importing the same configuration file from a TFTP server.

This problem has been solved.

4.18 PPTP - Incorrect IP Settings in PPTP Partner Configuration

(ID 3438)

When configuring a PPTP Partner, wrong IP settings were occasionally saved to the MIB (*static* instead of *dynamic client* for ***IpAddress*** in the ***biboPPPTable***).

This problem has been solved.