RELEASE NOTES SYSTEM SOFTWARE 7.2.2

Release Notes - System Software 7.2.2
Version 0.9

Purpose

This document describes new features, changes, and solved problems of **System Software 7.2.2**.

Liability

While every effort has been made to ensure the accuracy of all information in this manual, Funkwerk Enterprise Communications 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. Funkwerk Enterprise Communications 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 Funkwerk Enterprise Communications 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 Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +49 180 300 9191 0 Fax: +49 180 300 9193 0 Internet: www.funkwerk-ec.com	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

1 Important Information

Please carefully read the following information about System Software 7.2.2 in order to avoid problems when updating to and using the software

1.1 Scope

System Software 7.2.2 is available only for the following gateways and cannot be used on any other gateway:

- **X2301**
- **X2302**
- **X2301w**
- **X2302w.**

Many of the new features described here are also part of System Software 7.2.1 and are thus available for other gateways platforms, too.

1.2 Incompatibility

Configurations created or saved under **System Software 7.2.2** are incompatible with all older versions of our system software. Please carefully observe the following instructions when updating.

1.2.1 Preparations and Update

Proceed as follows to prepare and carry out an update to **System Software 7.2.2:**

1. Save the current configuration. Proceed in any of the following ways:
   a) Call `cmd=save path=boot.old` from the SNMP shell. This saves the current configuration to the Flash ROM of your gateway using "boot.old" as

file name.
b) Start an TFTP server on any PC inside your LAN and export the current configuration via the Setup Tool menu ***CONFIGURATION MANAGEMENT***. Choose the following settings:

- ***OPERATION*** *= put (FLASH -> TFTP)*
- ***TFTP SERVER IP ADDRESS*** *= <TFTP server IP address inside the LAN>*
- ***TFTP FILE NAME*** *= boot.old*
- ***NAME IN FLASH*** *= boot.*

2. Carry out the update to **System Software 7.2.2** as usual and reboot the gateway.
The gateway now boots into the new system software. The boot configuration has been converted and is now incompatible with all older versions of our system software.

1.2.2 Downgrade

In case you decide to downgrade again, proceed as follows:

1. Replace the current boot configuration with the one you have saved before updating. Proceed in any of the following ways:
a) Call `cmd=move path=boot.old pathnew=boot` from the SNMP shell. This overwrites the current boot configuration with the one previously saved. The configuration named "boot.old" is deleted from the Flash ROM (if you intend to keep "boot.old" use `cmd=copy` instead of `cmd=move`).
b) Start a TFTP server on a PC inside your LAN and import the configuration previously saved via the Setup Tool menu ***CONFIGURATION MANAGEMENT***. Choose the following settings:
   - ***OPERATION*** = get (TFTP -> FLASH)
   - ***TFTP SERVER IP ADDRESS*** *= <IP-Adresse des TFTP Servers im LAN>*
   - ***TFTP FILE NAME*** *= boot.alt*
   - ***NAME IN FLASH*** *= boot*.
2. Carry out the desired downgrade.
3. Reboot the gateway. It boots into the older version of our system software using the previously saved boot configuration.

2 New Features

System Software 7.2.2 offers the following new features, thus considerably expanding the scope of features previously available in System Software 7.1.15:

2.1 PKCS#12 Support

System Software 7.2.2 supports the import of PKCS#12 certificates by the IPSec certificate management. They can now be imported using the `cert` application as well as by the Setup Tool.

PKCS#12 supports the transfer of personal identification data like private keys and certificates using a number of security mechanisms (PKI or password protection). Mainly the password mechanism is relevant for an initial IPSec configuration, and PKCS#12 support by **System Software 7.2.2** is currently restricted to that mechanism. Importing a PKCS#12 certificate is carried out in the same way any other certificate is imported, i.e. it can either be downloaded from a TFTP server or it can be copy/pasted to the Setup Tool or the console. In both cases the gateway interactively prompts for the passwords required for decrypting the certificate (`cert` also offer the possibility of directly passing a password).

2.1.1 Importing with the Setup Tool

Certificate import is carried out in the menu ***IPSec ➜ Certificate and Key Management ➜ Own/CA/Peer Certificate ➜ DOWNLOAD***:

```
BINTEC X2302 Setup Tool          Funkwerk Enterprise Communications GmbH
[IPSEC][CERTMGMT][OWN][GETCERT]: IPsec Configuration -
                                 Get Certificate        MyGateway

   Import a Certificate/CRL using:  TFTP

      Type of certificate: Own Certificate


     Server:
     Name:                                              auto
             START                                    EXIT
```

Note

Importing a certificate is described in the User's Guide of your gateway. You can either download the certificate form a TFTP server or copy/paste it into the menu window

When the gateway identifies a password encrypted PKCS#12 certificate, it interactively prompts for the required passwords:

```
BINTEC X2302 Setup Tool          Funkwerk Enterprise Communications GmbH
[IPSEC][CERTMGMT][OWN][GETCERT]: IPsec Configuration -
                                 Get Certificate        MyGateway

 Please Review retrieved Certificate:   [mycert]

 Encountered PKCS#12 password authenticated envelope



 please enter password for outer envelope       __________
```

The gateway successively prompts for the keys contained by the certificate (Outer Envelope, Internal Safe and Shrouded Key - the key last entered is kept

in the prompt so that you only need to enter it once in case all passwords are identical).

After decryption, the password is displayed in plain text:

```
BINTEC X2302 Setup Tool         Funkwerk Enterprise Communications GmbH
[IPSEC][CERTMGMT][OWN][GETCERT]: IPsec Configuration -
                              Get Certificate        MyGateway

Please Review retrieved Certificate:   [mycert]

Encountered PKCS#12 password authenticated envelope                    =
Certificate =                                                          |
 SerialNumber = 1                                                      |
 SubjectName = <CN=certtest, OU=no_dept., O=FEC GmbH, C=DE>            |
 IssuerName = <MAILTO=noob@fec.com, CN=Openssl Test-CA OU=no_dept      |
   O=FEC GmbH, L=Nuernberg, ST=Bayern, C=DE>                           |
 Validity =                                                            |
    NotBefore = 2004 Oct  5th, 08:07:36 GMT                            |
    NotAfter  = 2005 Oct  5th, 08:07:36 GMT                            |
 PublicKeyInfo =                                                       |
   Algorithm name (X.509) : rsaEncryptionv                             v

                IMPORT
```

After confirming by hitting ***IMPORT*** the certificate is installed and you return to the menu for entering or downloading the certificate. You can leave this by hitting ***EXIT*** and return to the list of installed certificate.

2.1.2 Importing with "cert"

The cert application that is called from the SNMP shell has equally been modified so that it supports PKCS#12 certificates. PKCS#12 certificates are automatically identified and any included passwords are interactively prompted for.

Certificate import is carried out as follows (import by copy/pasting the certificate data):

```
X2302:> cert get -p console test
Please enter certificate data:>

<the SNMP shell displays the encoded certificate data>

cert: Encountered PKCS#12 password authenticated envelope

please enter password for outer envelope (empty password cancels) >
please enter password for internal safe (empty password cancels) >
please enter password for shrouded key (empty password cancels) >
Received 2 certificate(s) 1 key(s). Accept all? (y/n) > y

X2302:>
```

Import by TFTP download is carried out as follows:

```
X2301:> cert get -p tftp://<Server IP Adresse>/1.pem test
cert: Encountered PKCS#12 password authenticated envelope

please enter password for outer envelope (empty password cancels) >
please enter password for internal safe (empty password cancels) >
please enter password for shrouded key (empty password cancels) >
Received 2 certificate(s) 1 key(s). Accept all? (y/n) > y

X2301:>
```

Using the option `-P <password>`, you can directly pass a password to the application within the import command. This password, however, is applied to all keys contained by the certificate so that the option is useful only if the passwords for Outer Envelope, Internal Safe and Shrouded Key are identical.

2.2 TCP Download Control

An increasing number of network services requires that data are transferred not only as fast as possible, but also at constant transfer rates (e.g. VoIP). System Software 7.2.2 offers a mechanism to obviate corresponding problems especially for ADSL connections.

Constant transfer rates for low latency data streams can be secured in basically two ways: On the one hand it is possible to reduce the download rate available for general usage so that a certain bandwidth is reserved for a High Priority QoS queue. On the other hand it is possible to use the available bandwidth as effectively as possible by prioritizing the upload of TCP ACK packets in the upstream

of asynchronous ADSL connections. This avoids latency that would be created as a result of the comparatively small upload bandwidth of ADSL connections.

Both mechanisms are configured in the menu ***IP ➜ BANDWIDTH MANAGEMENT (TDRC / LOAD BALANCING / BOD) ➜ TCP DOWNLOAD RATE CONTROL (TDRC). ADD/EDIT*** allows access to the actual configuration menu (the screenshot does not show the default values):

```
BINTEC X2302 Setup Tool          Funkwerk Enterprise Communications GmbH
[IP][TDRC][EDIT]: Configure TCP Download Rate Control        MyGateway

  Interface              50000   ethoa50-0

  Optimize Download Rate via TCP ACK prioritisation      no
  (recommended for ADSL)

  TDRC Mode      disabled

  Maximum TCP Download Rate (kbits/s)          1024

  Control all TCP Services                     no
  Select TCP Services >

         SAVE                                CANCEL
```

The menu contains the following fields:

Field	Description
Interface	Here you choose the interface the configuration is applied to.
Optimize Download Rate via TCP ACK prioritisation	Here you choose whether the download rate is to be optimized by prioritizing TCP ACK packets. If you choose *yes*, all of the following fields are no longer available. Available values are *yes* and *no*, default is *no*.

Field	Description
TDRC Mode	Only available for ***OPTIMIZE DOWNLOAD RATE VIA TCP ACK PRIORITISATION*** = *no.* Here you choose the TDRC (TCP Download Rate Control) policy. Available values are: ■ *static (fixed maximum rate for TCP download)* (default) - The download rate of TCP connections is statically restricted to the value specified by ***MAXIMUM TCP DOWNLOAD RATE (KBITS/S)***. ■ *dynamic (maximum rate less amount of high priority traffic)* - The download rate is restricted to a value dynamically determined. The value is computed from the value specified by ***MAXIMUM TCP DOWNLOAD RATE (KBITS/S)*** minus the bandwidth that is required by all QoS High Priority traffic over the current interface at the moment of adding or terminating a TCP session. This choice requires a QoS configuration for the respective interface. ■ *disabled* - The TCP download rate remains unrestricted.
Maximum TCP Download Rate (kbits/s)	Here you specify the maximum bandwidth for TCP connections over this interface. Available values are *1* to *100000*, default is *1024*.
Control all TCP Services	Here you choose if the download control configured is to be applied to all TCP connections. Available values are *yes* and *no*, default is *yes*.

Table 2-1: ***IP ➜ BANDWIDTH MANAGEMENT (TDRC / LOAD BALANCING / BOD) ➜ TCP DOWNLOAD RATE CONTROL (TDRC) ➜ ADD/EDIT***

If you choose *no* for ***CONTROL ALL TCP SERVICES***, ***SELECT TCP SERVICES*** allows access to the configuration of all services that TDRC is to be applied to (the screenshot shows the preconfigured services):

```
BINTEC X2302 Setup Tool         Funkwerk Enterprise Communications GmbH
[IP][TDRC][SERVICES]: Configure TCP Services          MyGateway

 TCP Port                                Status

    80              HTTP                   builtin
    443             HTTPS                  builtin
    20              FTP Data               builtin
    110             POP3                   builtin
    143             IMAP2                  builtin


     ADD                DELETE              EXIT
```

ADD allows access to the configuration of further services:

```
BINTEC X2302 Setup Tool         Funkwerk Enterprise Communications GmbH
[IP][TDRC][SERVICES][ADD]: Configure TCP Services          MyGateway

     TCP Service Port              1

     Status                        enabled

     Alias Name (Description)



            SAVE                                  CANCEL
```

The menu contains the following fields:

Field	Description
TCP Service Port	Here you enter the TCP port of the service you want to configure. Available values are *1* to *65535*, default is *1*.

Field	Description
Status	Here you choose if the service configured is to be actually controlled. Available values are *enabled* and *disabled*, default is *enabled*.
Alias Name (Description)	Here you enter a description for the service you have configured, the maximum length of the entry is 20 characters.

Table 2-2: ***IP ➜ BANDWIDTH MANAGEMENT (TDRC / LOAD BALANCING / BOD) ➜ TCP DOWNLOAD RATE CONTROL (TDRC) ➜ ADD/EDIT ➜ SELECT TCP SERVICES ➜ ADD***

2.3 Switch Port Separation

System Software 7.2.2 offers a logical separation and individual configuration of the four switch ports of X2301(w) and X2302(w).

Separating the switch ports allows a completely independent configuration of the resulting interfaces. All configuration options are identical to those available for the configuration of a single Ethernet interface (for information on the configuration of Ethernet interfaces see your User's Guide).

The Ethernet Menu has been changed to support the new feature:

```
BINTEC X2302 Setup Tool          Funkwerk Enterprise Communications GmbH
[SWITCH]: Fast Ethernet Configuration                          MyGateway

    Fast Ethernet/en1-0>


    Switch Configuration >


              EXIT
```

After an update to **System Software 7.2.2**, the switch still is in single interface mode, i.e. there is just one configuration for all switch ports.

Note

Note that the configuration of the interface ***MODE*** is no longer carried out in the interface configuration menu but in the menu ***SWITCH CONFIGURATION***.

You can change the switch configuration in the menu ***SWITCH CONFIGURATION***:

```
BINTEC X2302 Setup Tool          Funkwerk Enterprise Communications GmbH
[SWITCH][ASSIGN]: Switch Interface Assigment                    MyGateway

     Switch Port    Assigned Interface   Switch Port Mode


     Port 1         en1-0                full autonegotiation

     Port 2         en1-0                full autonegotiation

     Port 3         en1-0                full autonegotiation

     Port 4         en1-0                full autonegotiation




                    SAVE                      CANCEL
```

The menu contains the following fields:

Field	Description
Switch Port	Here the switch port numbers are displayed. The numbering corresponds to the numbering of the ports on the rear of your gateway.
Assigned Interface	Here you can assign an ethernet interface to the switch port. Four interfaces are available: *en1-0* to *en1-3*. The default configuration assigns *en1-0* to all four switch ports. The pre-update Ethernet configuration is applied to interface *en1-0*. If you do not create or if you remove this interface, the configuration is not inherited.

Field	Description
Switch Port Mode	Here you choose the mode the interface is to be operated in. Available values are: ■ *full autonegotiation* (default) ■ *auto 100 mbps only* ■ *auto 10 mbps only* ■ *auto 100 mbps/full duplex* ■ *auto 100 mbps/half duplex* ■ *auto 10 mbps/full duplex* ■ *auto 10 mbps/half duplex* ■ *fixed 100 mbps/full duplex* ■ *fixed 100 mbps/half duplex* ■ *fixed 10 mbps/full duplex* ■ *fixed 10 mbps/half duplex* ■ *suspend* - The interface is set to *disabled* and disconnected from the power supply. ■ *disabled* - The interface is created but remains inactive.

Table 2-3: ***IP ➜ BANDWIDTH MANAGEMENT (TDRC / LOAD BALANCING / BOD) ➜ TCP DOWNLOAD RATE CONTROL (TDRC) ➜ ADD/EDIT ➜ SELECT TCP SERVICES ➜ ADD***

After switch configuration, the menu ***XEY-100SW, FAST ETHERNET*** changes and displays the Ethernet interfaces assigned to the switch ports. You can now configure the interfaces individually.

Please note: The separation of the switch ports into Ethernet interfaces is a logical one, i.e. the maximum overall bandwidth available across all switch ports or Ethernet interfaces remains unchanged (100 Mbit/s Full Duplex). If you, e.g.,

separate all switch ports, each of the resulting interfaces can use only part of the overall bandwidth.

If you collect several switch ports into a single interface, the bandwidth available between these ports is a full 100 Mbit/s Full Duplex.

2.4 Universal Plug and Play

Universal Plug and Play (UPnP) enables a client within your LAN to prompt a NAT enabled gateways to open ports and create port mappings that are required by current messenger services like real time video conferencing. System Software 7.2.2 supports UPnP.

Configuring your gateway for UPnP is carried out using only a few new parameters in the menu ***IP*** ➜ ***UPnP***:

```
BINTEC X2302 Setup Tool          Funkwerk Enterprise Communications GmbH
[IP][UPNP]: UPnP Configuration                                  MyGateway

     UPnP status                          disabled

     TCP port number for UPnP             5678

           SAVE                            CANCEL
```

The menu contains the following fields:

Field	Description
UPnP status	Here you choose the which policy the gateway applies to UPnP requests from the LAN. Available values are: ■ *disabled* (default) - The gateway discards UPnP requests, there are no changes to NAT. ■ *restricted* - The gateway opens ports and creates port mappings exclusively for the requesting host. ■ *enabled* - The gateway creates UPnP NAT settings for the entire LAN.
TCP port number for UPnP	Here you enter the port number on which the gateway listens for UPnP requests. Possible values are *1* to *65535*, default is *5678*.

Table 2-4: ***IP ➜ UPnP***

2.5 SNMP V. 2/V. 3

In addition to SNMP V. 1 System Software 7.2.2 now supports the SNMP versions 2(c) and 3. SNMP V. 3, above all, offers support for authenticating and encrypting the transferred SNMP data.

Attention!

After an update to System Software 7.2.2 the configuration of your gateway is no longer compatible with any older version of our system software, i.e. a direct downgrade to an earlier version is not possible.

Follow the directions in “Preparations and Update” on page 5 **and** “Downgrade” on page 6**!**

SNMP V. 1 and V. 2 support access control through the commonly known SNMP communities (*admin*, *write*, *read*) while SNMP V. 3 supports three different access levels and respective security levels:

- no authentication, no privacy (encryption): *noAuthNoPriv*
- authentication (MD5 or SHA1): *authNoPriv*
- authentication and privacy (DES or AES): *authPriv.*

Moreover, SNMP V. 3 supports "real" user management. Currently there are three preconfigured users (corresponding to the SNMP communities) with statically assigned security levels:

- *admin* - full access with MD5 authentication und DES encryption (*authPriv*)
- *write* - write access with MD5 authentication (*authNoPriv*)
- *read* - read access with MD5 authentication (*authNoPriv*).

Encryption and authentication are automatically applied by the gateway when using SNMP V. 3. The keys used for this purpose correspond to the user passwords and must have a length of at least 8 characters (so the user passwords should have the required length). If a user password is shorter than eight characters, it has to be repeated in the SNMP command, i.e. *bintecbintec* instead of *bintec* (see the example of a corresponding SNMP command: All versions).

The configuration of the newly created SNMP parameters is carried out mainly on the SNMP shell, only ***SNMPADMINVERSION*** can be configured in the menu ***IP*** ➜ ***SNMP***. The following MIB tables are available in **System Software 7.2.2**:

- ***SNMP***
- ***SNMPADMIN***
- ***SNMPENGINE***
- ***USMSTATS.***

Information on the tables and their parameters can be found in the HTML MIB reference published together with the software.

Mainly ***SNMPADMIN*** is relevant for SNMP configuration; here the following parameter is of prime importance:

Parameter	Description
snmpAdminVersion(rw)	This parameter determines which SNMP version the gateway allows for external SNMP connections. Available values are: ■ *All* (default) - The gateway accepts SNMP V. 1, 2c and 3. ■ *None* - The gateway accepts no external SNMP commands, i.e. SNMP access is possible exclusively from the console of the gateway (e.g. via SSH or the serial interface). ■ *v1 (0)* - The gateway accepts only SNMP V. 1. ■ *v2c (1)* - The gateway accepts only SNMP V. 2c. SNMP V. 2c supports 64 bit counters and access control through SNMP communities. ■ *v3 (2)* - The gateway accepts only SNMP V. 3, supporting "real" user management and access control through access levels. When entering the desired value, it is possible to combine single values using the pipe symbol ("|"). If e.g. a combined support of SNMP V. 1 and V. 3 is intended, this an be realized by entering `snmpAdminVersion=v1|v3`.

Table 2-5: ***SNMPADMIN*** ➜:***SNMPADMINVERSION***

SNMP commands have e.g. the following form, depending on the version applied:

SNMP V. 1

```
$ snmpget -v1 -c bintec 192.168.0.254 iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0

SNMPv2-MIB::sysDescr.0 = STRING: X2302
```

SNMP V. 2

```
$ snmpget -v2c -c bintec 192.168.0.254 system.sysDescr.0 system.sysName.0 iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus.1000

SNMPv2-MIB::sysDescr.0 = STRING: X2302

SNMPv2-MIB::sysName.0 = STRING: myrouter

IF-MIB::ifOperStatus.1000 = INTEGER: up(1)
```

SNMP V. 3

```
$ snmpget -v3 -a MD5 -A publicpublic -u write -l authNoPriv 192.168.0.254 system.sysDescr.0

SNMPv2-MIB::sysDescr.0 = STRING: 2302
```

All versions

```
$ snmpget -m ALL -M /usr/share/snmp/mibs -M /opt/bintec/mib/7.2.2/ -v3 -a MD5 -A bintecbintec -u admin -l authPriv -x DES -X bintecbintec 192.168.0.254 iso.org.dod.internet.private.enterprises.bintec.bibo.admin-2 .snmpAdminMIB.snmpAdmin.snmpAdminVersion.0

BINTEC-ADMIN-MIB::snmpAdminVersion.0 = BITS: E0 v1(0) v2c(1) v3(2)
```

(The examples above have been created using the command line version of NET-SNMP. See http://www.net-snmp.org).

You can find further information on all SNMP versions in the corresponding RFCs and Drafts:

- SNMP V. 1: RFC 1157
- SNMP V. 2c: RFC 1901 – 1908
- SNMP V. 3: RFC 3410 – 3418.

2.6 New HTML Wizard Features

The Bintec HTML Wizard for gateway configuration supports a number of new features that allow the configuration of more complex functions like firewall configuration.

The following features have been added:

- configuration of the Stateful Inspection Firewall
- configuration of multiple LAN to LAN connections
- country profiles for pre-selecting common ISPs during internet access confguration.

During configuration, detailed online help texts inform you about the necessary steps.

2.7 New Trace Tool Function

System Software 7.2.2 offers new filter options.

The trace application now allows tracing only the traffic transmitted from, to or between two specific IP addresses inside your LAN. The following options have been created for this purpose:

```
-S      set source IP address filter (LAN only)
-U      set destination IP address filter (LAN only)
-Ba,b   filter IP packets between a and b (LAN only)
```

2 New Features

3 Changes

3.1 NAT - Session Count Control

Up to now a gateway could reboot if the number of NAT sessions became too high.

System Software 7.2.2 allows controlling the maximum number of NAT sessions acceptable for a specific interface. Configuration is carried out using the varibale ***ipExtIfNatMaxSessions***. If the maximum number is reached, the gateway tries to close old sessions. If that is impossible, new sessions are no longer accepted.

3.2 BOOTP - CPU Load Reduced

BOOTP NetBIOS relaying has been changed in order to reduce the CPU load created by the BOOTP service.

3 Changes

4 Solved Problems

The following problems have been solved in System Software 7.2.2:

4.1 Setup Tool - Changes Applied Despite CANCEL

(ID 2211 and 3728)

After discarding changes made in the ***WAN PARTNER*** menu either by **CANCEL** or by **Esc Esc**, these changes were nevertheless applied and stored when the WAN Partner was saved later.

4.2 Setup Tool - Entries not Saved

(ID 3343 and 3605)

After confirming changes made in ***IP*** ➜ ***DNS*** ➜ ***FORWARDED DOMAINS*** ➜ ***ADD*** these were not saved to the MIB. Occasionally a stack trace was displayed, but the gateway did not reboot.

4.3 Bridging - Performance Loss

(ID 3525)

When using an ETHoA connection with either *bridged-fcs* or *bridged-nofcs* encapsulation, the performance of the gateway gradually decreased.

4.4 Setup Tool - Routing Entries Corrupted

(ID 3576

When a WAN partner route with transit network was edited in ***IP*** ➜ ***ROUTING*** ➜ ***ADD/EDIT***, the route type was nevertheless displayed as *route without transit network*. When confirming with ***SAVE***, the transit network configuration was lost.

4.5 ARP - Wrong ARP Tell

(ID 3671)

If a gateway had multiple interfaces (e.g. a physical and a virtual one), it occasionally created wrong ARP tells, using the IP address of one, and the MAC address of the other interface.

4.6 Setup Tool - Load Balancing Configuration Incorrectly Written to MIB

(ID 3680)

When configuring ***IP LOAD BALANCING OVER MULTIPLE INTERFACES*** with ***DISTRIBUTION POLICY*** *service/source-based routing*, wrong entries were written to the ***IPEXTRTTABLE***. This could lead to a Load Balancing malfunction.

4.7 SSHD - No Connection Possible

(ID 3694)

After a certain uptime no SSH connections to the gateway were possible. This was induced either by a memory loss or by changing the IP address of the gateway.

4.8 PPPoE - Problems with Two PPPoE Access Servers

(ID 3698)

When a gateway was configured to use two PPPoE Access Servers, the PPP layer could not be established.

4.9 Setup Tool - IPSec Wizard Settings not Saved Correctly

(ID 3733)

While the Setup Tool IPSec Wizard asked for a ***LOCAL ID*** during the configuration if PSK was to be used as authentication, the setting was not saved correctly. When entering the IPSec Setup Tool menus, the IPSec Wizard started over.

4.10 PPPoE - Connection Establishment Failure

(ID 3756)

Due to an overly brief timeout, certain types of PPPoE connections (e.g. wireless connections) could not be established.

4.11 HTML Setup Tool - GO Button Missing

(ID 3757)

When running the Setup Tool IPSec wizard, the GO button used to confirm the settings made disappeared after entering the ***LOCAL ID***.

4.12 ADSL - No Data Traffic

(ID 3761)

Due to an extremely high number of interrupts the following errors occurred:

- The PPP interface could not be set from *dormant* to *up*.
- Only outgoing traffic could be seen on the ATM interface.
- Setup Tool and SNMP shell were lagging.

4.13 DynDNS - Reboot with GnuDIP

(ID 3762)

When using DynDNS over the GnuDIP HTML protocol, the gateway rebooted.

4.14 ATM -Virtual Interface Down

(ID 3829)

After creating a virtual PPPoE interface in ***ATM*** ➜ ***ETHERNET OVER ATM*** ➜ ***ADD/EDIT*** ➜ ***IP AND BRIDGING*** ➜ ***VIRTUAL INTERFACES***, this interface was not set to *up* after a reboot.

4.15 Ethernet - Virtual Interface Changed

(ID 3840)

A virtual Interface could not be saved without an IP configuration. Encapsulation was reset from *None* to *Ethernet II* when leaving the respective menu.

4.16 Setup Tool - False MAC Address Displayed

(ID 3846)

After specifying a MAC address for any of the Ethernet interfaces, the menus for the configuration of the remaining interfaces showed the same MAC Address.

4.17 HTML Wizard - Inactivity Timer Ineffective

(ID 3872)

When calling the HTML Wizard, specifying an Inactivity Timer with a value larger than 300 seconds rendered the timer ineffective.

4.18 SIF - TCP Sessions Interrupted

(ID 3895)

After activating the Stateful Inspection Firewall, TCP sessions (like e.g. a Telnet connection to the gateway) were interrupted even if ***FULL FILTERING*** was disabled.

4.19 SIF - TCP Packets Using ECN Discarded

(ID 3948)

The Stateful Inspection Firewall discarded TCP packets that had their ECN flag set (ECN = Explicit Congestions Notification).

4.20 SSHD - Impossible to Deactivate SSHD

(ID 4024)

It was not possible to deactivate the SSHD by setting ***BIBOEXTADMPROCSSHD*** to *disabled*.

4.21 VLAN - False Frame Format

(ID 4046)

If VLAN tags were used for an ETHoA interface, the format of the ATM frames was corrupted. This could lead to a loss of data.

4.22 IPSec Wizard - No Proposal Assigned

(ID 4048)

After configuring IPSec with either the HTML or the ASCII wizard, the Default Profile was not assigned any IPSec Proposal.

4.23 QoS - TOS Changed

(ID 4148)

The TOS field of a connection from LAN to WAN was not set according to the QoS configuration.

4.24 Bridging - Memory Loss

(ID n/a)

The activation of bridging led to a memory loss.

4.25 PPPoE Credits - Panic on reaching Limit

(ID n/a)

If a time based restriction was configured for PPPoE connections, the gateway rebooted as soon as the limit was reached.

4.26 HTML Configuration - Link without Options

(ID n/a)

If a timeout had terminated an HTML session, the link for creating a new session was not generated with all the options used in the previous session.

4.27 Setup Tool - IPSec Peer not Stored

(ID n/a)

It could occur that a peer configuration that was carried out too slowly was deleted again when confirming with ***SAVE***.

4.28 QoS - Panic

(ID n/a)

Using QoS for the classification of a high priority queue on a LAN interface, and routing the packets over an ETHoA, PPPoA, RPoA or PPTP interface could lead to a panic.

4.29 Keepalive Monitoring - Malfunction

(ID n/a)

Depending on the time interval between state transitions it could occur that slave interfaces did not change their state correctly.

4.30 NAT - WLAN Packets Discarded

(ID n/a)

TCP packets that were to be routed from a WLAN interface to a WAN interface (PPPoA or IPoA) were discarded if NAT was active on the WAN interface.