RELEASE NOTES SYSTEM SOFTWARE 7.2.1

Release Notes - System Software 7.2.1
Version 0.9

1

Purpose

This document describes new features, changes, and solved problems of **System Software 7.2.1**.

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 Important Information 5

1.1 Scope 5

1.2 Feature Set 5

1.3 Updating Issues 6

2 New Features 9

2.1 PKCS#12 Support 9

2.1.1 Importing with the Setup Tool 10

2.1.2 Importing with "cert" 11

2.2 TCP Download Control 12

2.3 Switch Port Separation 16

2.4 New HTML Wizard Features 20

2.5 Cisco LMI 20

2.6 NewTrace Tool Function 20

2.7 Configurable Accounting Messages 21

3 Changes 23

3.1 QoS - Monitoring Menu 23

3.1.1 QoS Policy Statistics Submenu 24

3.2 New Option for Setup Tool Start 29

3.3 New DHCP Parameter 29

3.4 PPTP - Additional Configurable Parameters 29

3.5 IPSec - Configurable Log level 30

3.6 BRRP over VLAN 31

3.7 NAT - Session Count Control 31

3.8 Keepalive Monitoring - Flexible Default 31

3.9 BOOTP - CPU Load Reduced 32

4 Solved Problems 33

4.1 Setup Tool - Changes Applied Despite CANCEL 33
4.2 Factory Reset - Disfunctional for Some Gateways 33
4.3 Setup Tool - Individual Distribution Ratios Cannot be Set 33
4.4 DNS – Unrequested Name Cached 34
4.5 Setup Tool – Cobion Filter not Disabled 34
4.6 IPSec - Wrong Session Count 34
4.7 RIP - TOS Singaling not Possible 34
4.8 Bridging - Performance Loss 35
4.9 Setup Tool - Routing Entries Corrupted 35
4.10 Ethernet – Reception of Large Packets Faulty 35
4.11 Bridging - Bridge Filter not Matching 35
4.12 Setup Tool - Entries not Saved 36
4.13 Setup Tool – Use of “_” not Allowed 36
4.14 Setup Tool - Setup Tool Aborts 36
4.15 ARP - Wrong ARP Tell 36
4.16 Setup Tool - Load Balancing Configuration Incorrectly Written to MIB . . .37
4.17 SSHD - No Connection Possible 37
4.18 PPPoE - Problems with Two PPPoE Access Servers 37
4.19 Setup Tool - IPSec Wizard Settings not Saved Correctly 37
4.20 PPPoE - Connection Establishment Failure 38
4.21 HTML Setup Tool - GO Button Missing 38
4.22 DynDNS - Reboot with GnuDIP 38

4.23 Setup Tool - Stack Trace in IP Menu 38
4.24 IPSec - Phase 1 Errors 39
4.25 ATM -Virtual Interface Down 39
4.26 Ethernet - Virtual Interface Changed 39
4.27 Setup Tool - False MAC Address Displayed 39
4.28 HTML Wizard - Inactivity Timer Ineffective 40
4.29 Bridging - Packet Loss or Corruption 40
4.30 SIF - TCP Sessions Interrupted 40
4.31 Modems - Malfunction with False License Key 40
4.32 SIF - TCP Packets Using ECN Discarded 41
4.33 HTML Wizard - Only ISDN Connection Offered 41
4.34 SSHD - Impossible to Deactivate SSHD 41
4.35 IPSec Wizard - No Proposal Assigned 41
4.36 QoS - Misleading Entries in qosStatTable 42
4.37 PPPoE Credits - Panic on reaching Limit 42
4.38 X.25 - Write Queue Blocked 42
4.39 Bridging - Memory Loss 42
4.40 QoS - No entries in qosStatTable 43
4.41 IPSec - CRL Policy too Strict 43
4.42 Fax - Malfunction with Mapletree Modems 43
4.43 HTML Configuration - Link without Options 43
4.44 Setup Tool - IPSec Peer not Stored 44
4.45 SIF - Desired Connections Blocked 44
4.46 QoS - Panic 44

4.47 Keepalive Monitoring - Malfunction 44

1 Important Information

Please carefully read the following information about System Software 7.2.1 in order to avoid problems when updating to and using the software

1.1 Scope

System Software 7.2.1 supports the following gateways:

- **Bingo DSL II**
- **X1000 II**
- **X1200 II**
- **X2100**
- **X2250**
- **X2300**
- **X2500**
- **X2400**
- **X4x00**
- **X8500**
- **VPN line.**

1.2 Feature Set

X.25 and H.323 have been removed from the IPSec versions of the software for the following gateways:

- **X1000 II**
- **X1200 II**

- **X2100**
- **X2300**
- **X2400**
- **X2500**
- **X4x00.**

1.3 Updating Issues

Due to changes made in **System Software 7.2.1**, the configuration of the Event Scheduler may be changed by an update.

Note

If you do not make use of the Event Scheduler or if your Event Scheduler configuration does not make use of time conditions, this information does not apply to your updating procedure.

Under two conditions **System Software 7.2.1** may require manually adjusting your Event Scheduler configuration:

You have used the "daily" condition and want to load a configuration e.g. per TFTP

If any of the events you have configured is based on a *daily* time condition (***CONDITION*** = *daily,* previously misspelled as *dayly*), the configuration will be updated correctly. If, however, you intend to load a configuration previously saved to a TFTP server, loading the configuration will fail. If you depend on loading a configuration from a TFTP server, open the configuration file with a text editor and replace any occurrence of "dayly" with "daily". The configuration should now be loadable via a TFTP download.

You have used other time conditions and want to run system software 7.2.1 with the configuration saved on the gateway

For certain events based on time conditions, the configuration will be changed by the update process as follows:

Initial Value	Resulting Value
sat-sun	mon_sat
day1	sat_sun
day2	day1
day3	day2
...	...
day31	day30

Configurations based on individual weekdays will not be changed by the update.

This change only takes place during the update of the system software; i.e. if you save the configuration to a TFTP server and then reload it by an TFTP download, the settings will be written to the MIB correctly.

1 Important Information

2 New Features

System Software 7.2.1 offers the following new features, thus considerably expanding the scope of features previously available in System Software 7.1.15:

- "PKCS#12 Support" on page 9
- "TCP Download Control" on page 12
- "Switch Port Separation" on page 16
- "New HTML Wizard Features" on page 20
- "Cisco LMI" on page 20
- "NewTrace Tool Function" on page 20
- "Configurable Accounting Messages" on page 21

2.1 PKCS#12 Support

System Software 7.2.1 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 7.2.1** 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 X2300s 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 X2300s 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 last key 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 X2300s 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):

```
X2300:> cert get -p console test
Please enter certificate data:>

<the SNMP shell displays the encodes 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

X2300:>
```

Import by TFTP download is carried out as follows:

```
X2300:> 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

X2300:>
```

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 is transferred not only as fast as possible, but also at constant transfer rates (e.g. VoIP). System Software 7.2.1 offers a mechanism to obviate corresponding problems especially for ADSL connections.

Constant transfer rates for low latency data streams can basically be secured in 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 X2300s 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 X2300s 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 X2300s 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 7.2.1 offers a logical separation and individual configuration of the four switch ports of X2300s and X2300is.

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).

Note

Note that this feature is only available for certain serial numbers:

X2300is: all serial numbers starting with X2Y25... and higher;

X2300s: alle serial numbers starting with X2Z25... and higher.

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

```
BINTEC X2300s Setup Tool        Funkwerk Enterprise Communications GmbH
[SWITCH]: Fast Ethernet Configuration                          MyGateway

    Fast Ethernet/en1-0>


    Switch Configuration >


              EXIT
```

After an update to **System Software 7.2.1**, 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 X2300s 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 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 con-fguration.

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

2.5 Cisco LMI

System Software 7.2.1 supports Cisco LMI for Frame Relay.

In the menu ***FR*** ➜ ***LINK CONFIGURATION*** ➜ ***ADD/EDIT*** you can choose *original_lmi* for ***LINE MANAGEMEN***t.

2.6 NewTrace Tool Function

System Software 7.2.1 offers new filter options as well as support for X.25 over ISDN interfaces.

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)
```

Moreover, support for tracing X.25 over ISDN interfaces (interface index numbers 27000 to 29999) has been added.

2.7 Configurable Accounting Messages

System Software 7.2.1 allows customizing IP Accounting syslog messages.

Using the variable ***biboAdmAcctlogFormat,*** it is possible to combine the following kinds of information at will:

```
%d      Date the session opened; in DD.MM.YY format.
%t      Time the session opened: in HH:MM:SS format
%a      session age in seconds
%c      protocol type
%i      source IP address
%r      source port
%f      source interface index
%I      destination IP address
%R      destination port
%F      destination interface index
%p      outgoing packets
%o      outgoing octets
%P      incoming packets
%O      incoming octets
%s      message sequence counter
%%      '%'
```

The desired format can be created with the following command:

`biboAdmAcctlogFormat="<fmt>"`

followed by

`cmd=save`.

2 New Features

3 Changes

The following changes have been made to our system software in order to enhance its performance and usability:

- "QoS - Monitoring Menu" on page 23
- "New Option for Setup Tool Start" on page 29
- "New DHCP Parameter" on page 29
- "PPTP - Additional Configurable Parameters" on page 29

3.1 QoS - Monitoring Menu

The ***MONITORING AND DEBUGGING*** ➜ ***IP QOS*** menu shows QoS-specific statistics information for interfaces which have been configured for Quality of Service. These values cannot be changed.

```
X2300s Setup Tool              Funkwerk Enterprise Communications GmbH
[MONITOR][IP QOS]: IP QoS Interface Monitoring                MyGateway

  Interface                          ethoa50-0
  Operational Status                 up

  Nominal Transmit Rate              2048000
  Maximum Transmit Rate              192000

  Received Packets                   1075
  Received Octets                    66650

  Transmit Packets                   2334382
  Transmit Octets                    144731684

  QoS Policy Statistics >


  EXIT
```

The following values are shown:

Field	Description
Interface	Selection of the interface for which QoS has been configured and whose QoS statistics are to be displayed.
Operational Status	Shows the operational status of the selected interface.
Nominal Transmit Rate	The maximum overall data transmission rate in bits per second.
Maximum Transmit Rate	The maximum data rate specified for this interface in bits per second in the transmit direction (see User's Guide chapter **QoS** in the ***INTERFACES AND POLICIES*** ➜ *<Interface>* ➜ ***QOS SCHEDULING AND SHAPING*** submenu).
Received Packets	The number of packets received over the selected interface since the last change to the *up* status.
Received Octets	The number of octets received over the selected interface since the last change to the *up* status.
Transmit Packets	The number of packets sent over the selected interface since the last change to the *up* status.
Transmit Octets	The number of octets sent over the selected interface since the last change to the *up* status.

Table 3-1: ***IP QOS*** menu fields

3.1.1 QoS Policy Statistics Submenu

The *QOS POLICY STATISTICS* submenu is described below.

Opening the ***MONITORING AND DEBUGGING*** ➜ ***QOS POLICY STATISTICS*** menu normally shows a view of the distribution of the whole bandwidth in the form of a bar graph.

```
X2300s Setup Tool                Funkwerk Enterprise Communications GmbH
[MONITOR][IP QOS][STATISTICS]: QoS Bandwidth                   MyGateway
                               Distribution (ethoa50-0)

load          ::: agreed      XXX agreed but bounded     *** overbooked
  ^
  |       42        41   19
  + 100
  |
  |
  |
  |       :::       ***
  |       :::       ***
  |       :::       ***
  |       :::       ***  ***
  |       :::       XXX  XXX
  +-------------------------------------------------------------->
HP   1    2    3    DEF                          classes

  EXIT

 (d)istribution   (c)lasses   (t)os   (i)nterface statistics
```

The graph shows the percentage share of the individual configured QoS packet classes in terms of the total bandwidth. The bars contain the bandwidth distribution of the QoS packet classes.

The meaning of the different graphical representation of the bars is as follows:

- *agreed*: Share of the packets within the guaranteed bandwidth for this QoS packet class.
- *agreed but bounded*: Share of the packets within the maximum guaranteed bandwidth for this QoS packet class.
- *overbooked*: Overbooking of the guaranteed (not bounded) or maximum (bounded) bandwidth. This overbooking is only allowed in the "not bounded" mode.

Detailed statistics values can still be displayed. You can change the display with the following commands as described in the help line:

- *c* = Classes: Display of statistics values for classes
- *t* = TOS: Display of statistics values for TOS
- *i* = Interface Statistics: Display of statistics values for interfaces.

The **RESET STATISTICS** button resets all values in the respective window to *0*.

CLASSES

```
X2300s Setup Tool                Funkwerk Enterprise Communications GmbH
[MONITOR][IP QOS][STATISTICS]: QoS Class                        MyGateway
                               Statistics (ethoa50-0)

Class Pkts Send   Dropped Queued Octs Send    Dropped  Queued

DEF        0       0       0          0        0        0
N 1        0       0       0          0        0        0
N 2        167550  355049  22         6702000  19172646 880
N 3        292021  735122  405        11680840 39696588 16200
HP         1969580 0       13         78783200 0        520









  EXIT                    RESET STATISTICS

 (d)istribution      (c)lasses      (t)os      (i)nterface statistics
```

The following values are shown:

Field	Description
Class	The ID of the configured QoS packet class. The abbreviations in front of the entries have the following meaning: ■ N = Normal ■ HP = High Priority ■ DEF = Default
Pkts	Number of packets of this QoS packet class: ■ *Send*: Packets sent ■ *Dropped*: Packets dropped ■ *Queued*: Packets in the queue

Field	Description
Octs	Number of octets of this QoS packet class: ■ *Send*: Octets sent ■ *Dropped*: Octets dropped ■ *Queued*: Octets in the queue

Table 3-2: ***QoS Policy Statistics → Classes*** menu fields

TOS

```
X2300s Setup Tool                Funkwerk Enterprise Communications GmbH
[MONITOR][IP QOS][STATISTICS]: TOS Statistics                 MyGateway
                               (ethoa50-0)

TOS OutPkts OutOctets InPkts InOctets PktsDropped OctetsDropped

00    0       0        0      0          0           0
01    0       0        1135   68100      0           0

  EXIT                    RESET STATISTICS

 (d)istribution      (c)lasses      (t)os      (i)nterface statistics
```

The following values are shown:

Field	Description
TOS	The value in the TOS field of the IP packet.
OutPkts	Number of packets sent with the value entered under TOS.
OutOctets	Number of octets sent with the value entered under TOS.

Field	Description
InPkts	Number of packets received with the value entered under TOS.
InOctets	Number of octets received with the value entered under TOS.
PktsDropped	Number of packets dropped with the value entered under TOS.
OctetsDropped	Number of octets dropped with the value entered under TOS.

Table 3-3: ***QoS Policy Statistics ➜ TOS*** menu fields

Interface Statistics

```
X2300s Setup Tool                Funkwerk Enterprise Communications GmbH
[MONITOR][IP QOS][STATISTICS]: QoS Interface                    MyGateway
                               Statistics (ethoa50-0)

  Transmit Packets  2469015
  Transmit Octets   98760600

  Queued Packets    417
  Queued Octets     16680

  Dropped Packets   1090901
  Dropped Octets    43636040









  EXIT                    RESET STATISTICS

 (d)istribution      (c)lasses      (t)os     (i)nterface statistics
```

The following values are shown:

Field	Description
Transmit Packets	Number of packets sent over the selected interface.
Transmit Octets	Number of octets sent over the selected interface.

Field	Description
Queued Packets	Number of packets in the queue of the selected interface.
Queued Octets	Number of octets in the queue of the selected interface.
Dropped Packets	Number of packets dropped at this interface.
Dropped Octets	Number of octets dropped at this interface.

Table 3-4: ***QoS Policy Statistics*** ➜ ***Interface Statistics*** menu fields

3.2 New Option for Setup Tool Start

Under **System Software 7.2.1**, the Setup Tool can be started with the option `-I`. This starts the Setup Tool in the menu ***Monitoring and Debugging*** ➜ ***Interfaces*** and does not allow access to any other menus of the Setup Tool.

3.3 New DHCP Parameter

Using the new MIB variable ***ipDhcpUseDefaultHostname***, it is possible to determine if your gateway includes a standard host name in DHCP replies. If ***ipDhcpUseDefaultHostname*** is set to *disabled*, no host name is transmitted, if set to *enabled*, the gateway transmits a host name created from the IP address of the client. The default value is *enabled*.

3.4 PPTP - Additional Configurable Parameters

The following parameters relevant for PPTP control connections can be configured from the SNMP shell by means of the ***pptpProfileTable***. Entries in this ta-

ble are optional, and as long as no values have been explicitly configured, system inherent default values are used:

- ***HOST*** - If no value for ***HOST*** is configured, the gateway transmits the ***SYSNAME*** found in the ***SYSTEMTABLE***. Otherwise, the value configured for ***HOST*** is transmitted.
- ***VENDOR*** - If no value for ***VENDOR*** is configured, the gateway creates an ID from the string "Bintec" and a system inherent value from the ***BIBOADMBOARDTABLE***.
- ***FIRMREV*** - For ***FIRMREV***=*-1* the firmware revision *0* is transmitted, for ***FIRMREV***=*0* (and if no entry has been created here) the revision implied by the system software is transmitted. For any other value (between *1* and *999*) exactly the value specified is transmitted.

3.5 IPSec - Configurable Log level

Using the variable ***CERTGLOBLOGLEVEL***, the detail of syslog messages concerning certificate management can be customized:

Log Level	Detail in Syslog Messages
3	important events like e.g. an invalid certificate
4	extended information about events logged in level 3
5	cache and search events
6	extended information about successful cache events
7	output of certificates after sucessful search events

Table 3-5: Details contained in certificate management syslog messages

Messages from level 3 (and lower) are displayed on the global syslog level *Info*, all others on the syslog level *Debug*.

3.6 BRRP over VLAN

If no IP configuration was assigned to the physical interface of a virtual router (e.g. if it was to be used for bridging only), using BRRP over VLAN was not possible because no BRRP advertisements were sent over this interface.

To enable sending BRRP advertisements over a different interface, a new parameter has been created: ***BRRP ➜ CONFIGURATION: ADVERTISEMENT INTERFACE***. It allows choosing the interface BRRP advertisements are to be sent over.

3.7 NAT - Session Count Control

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

System Software 7.2.1 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.

3.8 Keepalive Monitoring - Flexible Default

With a default of only three attempts to reach a host with an ICMP Echo Request, Keepalive Monitoring has proved too inflexible. The number of attempts can now be configured at will (between *1* and *65535*) using the variable ***IPHOSTSALIVETRIALS.***

3.9 BOOTP - CPU Load Reduced

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

4 Solved Problems

The following problems have been solved in System Software 7.2.1:

4.1 Setup Tool - Changes Applied Despite CANCEL

(ID 221 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 Factory Reset - Disfunctional for Some Gateways

(ID 3068)

Resetting the gateway configuration by switching the gateway off and on again three or five times respectively did not work.

4.3 Setup Tool - Individual Distribution Ratios Cannot be Set

(ID 3169)

When choosing *individual for all interfaces of the group* for the field ***DISTRIBUTION RATIO*** in a configuration of ***IP LOAD BALANCING OVER MULTIPLE INTERFACES***, the individual values entered for the interfaces were not in all cases stored correctly.

4.4 DNS – Unrequested Name Cached

(ID 3364)

For some DNS queries only the Fully Qualified Domain Name (FQDN, e.g moon8.bintec.de) was cached by the DNS Proxy and the Canonical Name (CNAME, e.g. www.bintec.de) was discarded.

4.5 Setup Tool – Cobion Filter not Disabled

(ID 3434)

Setting ***Security*** ➜ ***Cobion Orange Filter:Admin Status*** to *disable* after the filter had been enabled before did not completely disable the filter. Access to web sites could still be blocked.

4.6 IPSec - Wrong Session Count

(ID 3487)

If IP Load Balancing was activated for IPSec connections, more sessions were counted than were necessary for the created IPSec tunnels.

4.7 RIP - TOS Singaling not Possible

(ID 3491)

It was not possible to customize the TOS field of RIP packets for TOS signaling.

4.8 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.

4.9 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.

4.10 Ethernet – Reception of Large Packets Faulty

(ID 3583)

The reception of packets larger than 1518 bytes was not initialized and handled correctly.

4.11 Bridging - Bridge Filter not Matching

(ID 3584)

The bridge filter mechanism did not function properly because a wrong interpretation of filter lengths prevented adequate matching.

4.12 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.

4.13 Setup Tool – Use of "_" not Allowed

(ID 3619)

When entering a host name in the DynDNS menus, the use of "_" (underscore) was not allowed even though it is an acceptable character for FQDNs.

4.14 Setup Tool - Setup Tool Aborts

(ID 3661)

When entering ***MONITORING AND DEBUGGING*** ➜ ***MESSAGES***, the Setup Tool session was aborted. Syslog messages could still be viewed on the SNMP shell.

4.15 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.

4.16 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.

4.17 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.

4.18 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.

4.19 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 correct-

ly. When entering the IPSec Setup Tool menus, the IPSec Wizard started over again.

4.20 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.

4.21 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***.

4.22 DynDNS - Reboot with GnuDIP

(ID 3762)

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

4.23 Setup Tool - Stack Trace in IP Menu

(ID 3793, 3793, 3794)

Setting ***REMOTE CAPI SERVER TCP PORT*** to *0* in ***IP*** → ***STATIC SETTINGS***, confirming with ***SAVE*** and then re-entering the menu and saving again caused a stack trace.

4.24 IPSec - Phase 1 Errors

(ID 3800)

When establishing an IPSec tunnel, the Phase 1 authentication failed if a Distinguished Name Peer ID was to be verified.

4.25 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.

4.26 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.

4.27 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.

4.28 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.

4.29 Bridging - Packet Loss or Corruption

(ID 3875)

After activating Bridging data transfer on the Ethernet interfaces could be lossy or corrupted.

4.30 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.

4.31 Modems - Malfunction with False License Key

(ID 3919)

When trying to use a modem license starting with *X4AMOD* on a **X4300**, no connections were allowed.

Now all licenses starting with *X4*MOD* are accepted by the gateway.

4.32 SIF - TCP Packets Using ECN Discarded

(ID 3948)

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

4.33 HTML Wizard - Only ISDN Connection Offered

(ID 3975)

On certain gateways (e.g. **X1200 II**) only an ISDN connection was offered when configuring an ISP. An xDSL connection was not configurable.

4.34 SSHD - Impossible to Deactivate SSHD

(ID 4024)

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

4.35 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.

4.36 QoS - Misleading Entries in qosStatTable

(ID n/a)

When activating QoS on physikal as well as on virtual interfaces, wrong entries were written into the ***QOSSTATTABLE***.

4.37 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.

4.38 X.25 - Write Queue Blocked

(ID n/a)

When clearing a connection, the X.25 driver was sending too many Clear Requests or Clear Confirms. This blocked the write queue, and no data could be sent over the X.25 interface.

4.39 Bridging - Memory Loss

(ID n/a)

The activation of bridging led to a memory loss.

4.40 QoS - No entries in qosStatTable

(ID n/a)

When manually adding entries to the QoS Table using the SNMP shell, it could happen that the QoS module did not create any entries in the ***QOSSTATTABLE***.

4.41 IPSec - CRL Policy too Strict

(ID n/a)

If a CA certificate was not marked as such in the ***CERTTABLE*** (***CERTISCERT***=*false*), the gateway strictly required a CRL, even if ***CERTNOCRLS*** was set to *true*. This setting is now respected.

4.42 Fax - Malfunction with Mapletree Modems

(ID n/a)

Fax mode was disfunctional if using Mapletree modems.

4.43 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.

4.44 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***.

4.45 SIF - Desired Connections Blocked

(ID n/a)

Even though the Stateful Inspection Firewall did not control locally initiated connections (***LOCAL FILTER*** = *off*), TCP connections locally initiated on the gateway were blocked.

4.46 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.

4.47 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.