RELEASE NOTES SYSTEM SOFTWARE 7.4.1

Release Notes - System Software 7.4.1
Version 1.0

Purpose

This document describes new features, changes, and solved problems of **System Software 7.4.1./7.4.2**

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.funkwerk-ec.com.

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.funkwerk-ec.com.

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.funkwerk-ec.com

1 Important Information

Please carefully read the following information about System Software 7.4.1 in order to avoid problems when updating to and using the software

1.1 Scope

System Software 7.4.1 supports the following gateways:

- **X1000 II**
- **X1200 II**
- **X2100**
- **X2250**
- **X2300 Series**
- **X2404**
- **X4x00**
- **X8500**
- **VPN Series.**

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.**

2 New Features

System Software 7.4.1 offers the following new features considerably expanding the scope of features previously available in System Software 7.2.1:

2.1 Dead Peer Detection

During the communication between two IPSec-Peers it may occur that one of the peers becomes unreachable, e.g. because of routing problems or a rebooting gateway. This will usually not be discovered before the SA Liftetime has ended and rekeying fails. Until then, data are lost. To avoid this situation, a number of mechanisms are available to verify the reachability of a peer.

Up to now, heartbeats were the only supported mechanism for the verification of a peer's reachability. Meanwhile, DPD (RFC 3706) has been established, shifting the initiative for the activation of an alive check completely to one of the peers.

System Software 7.4.1 offers two different modes of DPD: DPD Triggered and DPD Idle. DPD Triggered verifies the reachability of a peer only if data are to be sent to the peer. DPD Idle, however, verifies intervallicly and independently of

any pending data transfer. Peer gateways that do not support Heartbeats, but do support DPD can thus be checked for reachability, too.

The DPD mode to employ is chosen during the configuration of Phase 1 Profiles:

```
X2300is Setup Tool              Funkwerk Enterprise Communications GmbH
[PHASE1][EDIT]                                                MyGateway

Description (Idx 1)      : global (converted)
Proposal                 : 2 (DES3/MD5)
Lifetime Policy           : Propose this lifetime, accept use all
                            Seconds: 7200        KBytes: 0
Group                    : 1 ( 768 bit MODP)
Authentication Method    : Pre Shared Keys
Mode                     : aggressive
Alive Check              : Dead-Peer-Detection (DPD)
Block Time               : 0
Local ID                 : central
Local Certificate        : none
CA Certificates          :
Nat-Traversal            : enabled

View Proposals >

               SAVE                          CANCEL
```

The ***ALIVE CHECK*** parameter additionally offers *Dead-Peer-Detection (DPD)* and *Dead-Peer-Detection (DPD), Idle Mode*, where *Dead-Peer-Detection (DPD)* stands for DPD Triggered. If you choose any one of these options, only the chosen mechanism will be accepted for alive checks during Phase 1. If you choose *autodetect*, the gateway behaves as follows:

- If the peer gateway supports Heartbeats as well as DPD, Heartbeats are used in Phase 1.
- If the peer gateway supports only DPD, DPD is used in Phase 1.
- If the peer gateway supports only Heartbeats, Heartbeats are used in Phase 1.

Since DPD is not defined for Phase 2, there is no DPD option for the configuration of Phase 2 profiles. If ***ALIVE CHECK*** is set to autodetect for Phase 2, and DPD is used in Phase 1, no alive check is performed in Phase 2.

The following variables have been created for DPD control:

- ***IPSECGLOBDPDIDLETHRESHOLD***: Defines the time slice after which an alive check is performed. In Idle Mode this means that after the interval has ended, a check is performed if no authenticated data have been received, independently from whether any data are to be sent ot not. In Triggered Mode, the gateway checks for every packet that is to be sent (i.e. only if there are data to be sent) if the last packet was received more than ***IPSECGLOBDPDIDLETHRESHOLD*** seconds ago. If that is the case, the peer's reachability is verified. Possible values are *1* to *3600*, default is *15*.
- ***IPSECGLOBDPDMAXRETRIES***: Defines the number of tries the gateway makes to reach the peer (a value of 3 retries means 4 tries in sum). If the last query remains without an answer, the peer is considered dead and the relevant SAs are deleted. Possible values are *1* to *10*, default is *3*.
- ***IPSECGLOBDPDRETRYTIMEOUT***: Defines the interval between the single tries to reach the peer. Possible values are *1* to *3600* seconds, default is *2*.

These variables cannot be configured using the Setup Tool.

2.2 WPA 2

System Software 7.4.1 introduces WPA 2 support for WLAN in Preshared Key mode as well as in combination with a 802.1x authentication server.

The menu ***WIRELESS LAN*** ➜ ***WIRELESS INTERFACES*** ➜ **ADD** now offers the following fields for WPA 2 configuration:

Parameter	Option
WPA/WPA2 mixed mode	Only for ***SECURITY MODE*** = *WPA PSK* and *WPA 802.1x* Here you select whether to apply WPA (with TKIP encryption), WPA2 (with AES encryption) or allow the negotiation of either of them. Possible values: ■ *WPA + WPA2* (default value) ■ *WPA only* ■ *WPA2 only*

Parameter	Option
WPA2 preauthentication	Only for ***SECURITY MODE*** = *WPA 802.1x* with ***WPA/WPA2 MIXED MODE*** = *WPA + WPA2* and *WPA2 only* With this option registered clients can preauthenticate at other access points in the same radio cell. Thus these clients can change faster to the other access point ("roaming"), as the RADIUS authentication can be omitted during registration. The preauthentication is only possible with the client being registered at the access point with WPA2. Possible values: ■ *enabled*: The Access Point allows preauthentication of clients at other access points. ■ *disabled* (default): Preauthentication requests of clients are ignored.

Tabelle 2-1: New fields in ***WIRELESS LAN*** ➜ ***WIRELESS INTERFACES*** ➜ ***ADD/EDIT***

Since WPA 2 supports key lengths of up to 256 Bits, the field ***PRESHARED KEY*** now allows entries of up to 63 ASCII characters.

2.3 WLAN Wizard

System Software 7.4.1 offers HTML Wizard support of WLAN Interfaces.

Our HTML Wizard guides you through the configuration of a single SSID on your gateway's WLAN interface. Extensive online help is available to inform you about the necessary steps.

2.4 SIP and MGCP Proxy

In order to allow IP telephones a connection to a VoIP provider, System Software 7.4.1 provides a SIP and MGCP Proxy which carries out the necessary NAT and firewall port mappings.

Proxy configuration is carried out in ***VoIP*** ➜ ***Application Level Gateways***:

```
X2300is Setup Tool       Funkwerk Enterprise Communications GmbH
[VOIP][ALG]: Application Level Gateway configuration
                                                  MyGateway

 Terminal administration

     MGCP Terminal configuration >
     SIP Terminal configuration >


Description     Type     Status    Destination Port
-------------------------------------------------------------
MGCP-Provider   MGCP     enable         2427
SIP-Provider    MGCP     enable         5400




     ADD               DELETE              EXIT
```

By choosing an existing proxy or via ***ADD***, you access the menu for proxy configuration. It contains the following fields

Parameter	Option
Description	Here you enter a proxy description.
Proxy Type	Here you choose the protocol the proxy is to relay. Available protocols are: ■ *MGCP* ■ *SIP.*

Parameter	Option
Adminstatus	Here you choose whether to activate the proxy. Available choices are: ■ *enable* (default) ■ *disable.*
Destination Port	Here you specify the port on which the VoIP provider listens for SIP or MGCP connections. You need to create a proxy for every port VoIP clients from your LAN should be allowed to connect to. Ports may be provider specific. Default is *2427*.

Tabelle 2-2: ***VoIP ➜ Application Level Gateways ➜ ADD***

In ***MGCP Terminal Configuration*** and ***SIP Terminal Configuration*** you can survey the MGCP or SIP clients currently connected through your gateway as well as those that have successfully connected through your gateway before:

```
X2300is Setup Tool       Funkwerk Enterprise Communications GmbH
[VOIP][ALG][MGCP]: Application Level Gateway configuration
                                              MyGateway

All known connected MGCP Terminals:


Ident    Alias    Status    IP-Address    Gateway
-------------------------------------------------------


            DELETE                              EXIT
```

The menu serves as a display of clients known to the gateway and of basic connection parameters. You can remove unneeded or undesired clients, though.

The list of known clients is stored on the gateway so that all NAT and Firewall settings can be recreated after a reboot. VoIP clients inside your LAN will be

reachable from the outside again immediately after the reboot, even if they have not yet registered with the proxy again.

2.5 GPRS Backup

With System Software 7.4.1, you can use GPRS for backup connections via the Auxiliary interface.

For the configuration of a WAN Partner using GPRS, it is merely necessary to set ***Layer 1 Protocol*** to *GPRS over GSM* in the ***Advanced Settings*** menu of the WAN Partner configuration.

Note that you must specify an ***Access Point Name (APN)*** when configuring the respective modem profile in the ***Auxiliary*** menu.

2.6 HTTP Update

System Software 7.4.1 supports updating the gateway system software via an HTTP connection.

Up to now, the system software of your gateway could only be updated via TFTP or a serial connection. The update application has been changed so that HTTP connections can now be used for that purpose, too. E.g.:

```
update   http://www.funkwerk-ec.com/downloads/X2300/X2x00-
s7401.x2c.
```

Moreover, it is possible to perform an HTTP update from a default location: The variable ***biboExtAdmUpdatePath*** specifies a standard path leading to the respective most current release. The command to update from this location is simply:

```
update http:
```

The gateway automatically expands the path specified by ***biboExtAdmUpdatePath*** with the following elements (if the path specified ends with a "/"):

- "<System Name>/<System Name>-b_current" for standard images
- "<System Name>/<System Name>-s_current" for IPSec images

Note

"System Name", in this case, is not the value of the MIB variable ***SYSNAME***, but a system internal value that cannot be changed. If applicable, blanks are replaced with a "-", so that "X2300i compact" becomes "X2300i-compact".

On the web server that is to provide the updated software, symlinks have to be created that point to the most current release image (z. B x2300i-compact-s_current -> X2x00-s7401.x2c). The preconfigured value for ***BIBOEXTADMUPDATEPATH*** is *http://www.funkwerk-ec.com/static/files/*.

Finally, the update command can be called with two new options:

- `-a` - The update is carried out without any prompts. For this purpose, an incremental update is being performed which writes the new system software directly into the Flash ROM. The gateway must not be powered off during this process.
- `-r` - In order to activate the new system software, the gateway is automatically rebooted after an update.

2.7 Extended Scheduler Functions

Our Event Scheduler is now capable of calling all commands (or applications) that can be called from the SNMP shell.

The menu ***SCHEDULE COMMANDS ➜ ADD*** accordingly offers a number of new fields or options:

Parameter	Option
Execute Command	In order to execute a shell application, this field can now take the value *exec application*.
Appl. name	Here you specify the command, the scheduler is to execute, e.g. `update`.
Argum.list active	Here you can specify arguments (options) the scheduler is to use with the command as soon as the Schedule Event becomes active and the command is to be executed.
Argum.list inactive	Here you can specify arguments (options) the scheduler is to use with the command as soon as the Schedule Event becomes inactive and the command is to be executed.

Tabelle 2-3: New fields/optons in ***SCHEDULE COMMANDS ➜ ADD/EDIT***

Moreover, the scheduler functions have been expanded by the following capabilities. Configuration is carried out on the SNMP shell:

- The scheduler can set several variables (separated by ";").
- Accordingly more than one index variable can be specified to identify the entries that are to be changed.
- The scheduler is capable of adding a row to a MIB table as well as of replacing an existing one. For this, a "+" is prefixed to the table name. The new entry is created with the values specified for ***VARINDEXVAL*** and ***ACTIVEVALUE*** or ***INACTIVEVALUE..***

2.8 XoT - Source IP Address Configurable

System Software 7.4.1 supports specifying an interface indepedent IP source address for the TCP connections of outgoing XoT links.

To support this function, the variable ***xotSrcIpAddr*** has been created. It can be configured through the use of ***Source IP Address*** in ***X.25 ➜ XOT ➜ ADD/EDIT*** of the Setup Tool, too.

Note

This function has been available from system software release 7.1.12 on.

2.9 X.25 Statistics

In order to allow a better analysis of errors on and the load of an X.25 gateway, MIB tables have been added for the display of X.25 statistics.

The following tables have been added:

- ***x25SwStats,***
- ***x25MuxStats and***
- ***x25ToTcpStats.***

Note

These tables have been available from system software release 7.2.1 on.

2 New Features

3 Changes

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

3.1 PPP Redesign

The PPP subsystem has undergone a major redesign in order to account for the increasing demands of broadband applications and the resulting requirements. A number of PPP-related errors have been removed in this process, you can find the respective descriptions in "Solved Problems" on page 31.

3.2 SIF Enhancements

The Stateful Inspection Firewall has undergone a major redesign in order to account for the increasing demands of broadband applications and the resulting requirements. A number of SIF-related errors have been removed in this process, you can find the respective descriptions in “Solved Problems” on page 31.

3.3 BLUP Procedure

The BLUP procedure has been changed so as to delete identically named imgaes of our system software in the Flash ROM before writing the new image. This has been done to avoid update errors like e.g. lack of Flash space.

3.4 Additional SIF Table

A new MIB table (***IPSIFSTATS***) has been added to expand the statistical information available. It contains the follwoing variables:

```
x2301:> ipsifstat
ipSifStatCurrSessions( ro):                 0
ipSifStatCurrUdpSessions( ro):              0
ipSifStatCurrTcpSessions( ro):              0
ipSifStatCurrOtherSessions( ro):            0
ipSifStatCurrExpectedSessions( ro):         0
ipSifStatTotalUdpSessions( ro):             0
ipSifStatTotalTcpSessions( ro):             0
ipSifStatTotalOtherSessions( ro):           0
ipSifStatTotalExpectedSessions( ro):        0
x2301:ipSifStat>
```

3.5 HTML Wizard - Easier Handling

The HTML wizard has been changed so as to properly detect the javascript capabilities of the browser used. Additionally, the APPLY procedure has been simplified when the wizard is run in Quick mode.

Moreover, the options for configuration management have been removed from the Quick Mode version of the wizard: only old wizard configuration is stored on the gateway and overwritten by the next wizard run.

3.6 IPSec - ID String Syntax Extended

The PSec ID String Syntax has been extended by defining new delimiters to explicitly specify the ID type regardless of its syntax:

Syntax:

- X500 distinguished name:
  <obj-name=obj-value, obj-ID=obj-value, ...>
- IPV4-Address:
  |123.456.789.012| with or without '|'
- IPV4 Address Range:
  |123.456.789.012-123.456.789.013| with or without '|'
- IPV4 Address Subnet:
  |123.456.789.012/255.255.255.0| with or without '|'
  or:
  |123.456.789.012/24| with or without '|'
- Key-ID: arbitrary length hexadecimal string with even number of digits:
  { 01 23 45 67 89 ab cd ef }
- Fully Qualified User Name (FQUN):
  (anything) or user@domain with mandatory '@'
- Fully Qualified Domain Name (FQDN):
  [anything] or any name without '@' not matching any other syntax

3.7 IPSec - Lifetime Configuration

The configuration of the IPSec Phase 1 and Phase 2 Lifetimes has been changed and is now configured per profile. Therefore, the ***IPSECLIFETIMETABLE***

is obsolete and all necessary parameters are stored in the ***IKEPROFILETABLE*** and ***IPSECPROFILETABLE***.

Existing configurations are converted so that all existing profiles are initiated with those values from the ***IPSECLIFETIMETABLE*** which are referenced in the respective profile. If ***IKE-/IPSECPROFILEFLIFEPOLICY*** is set to *use_default_lifetime*, all (if any) lifetime variables are taken from the default profile.

Additionally, the parameters for the configuration of profile lifetimes in the Setup Tool has been enhanced and is now carried out with the following parameters:

Field	Description
Lifetime Policy	Here you specify the method the lifetime is achieved by, that may expire before a phase 1 key must be renewed with another Diffie-Hellman key calculation. Possible values: ■ *Use default lifetime settings* (default value): No lifetime is proposed and the lifetime is set to eight hours according to RFC. Different proposals of the IPSec peer are accepted and used. ■ *Propose this lifetime, accept and use all proposals*: The proposal says that the key is renewed when either the value specified in ***SECONDS*** has elapsed or the value in ***KBYTES*** has been processed, depending on which event occurs first. Different proposals of the IPSec peer are accepted and used. ■ *Propose this lifetime, reject different proposals*: The proposal says that the key is renewed when either the value specified in ***SECONDS*** has elapsed or the value in ***KBYTES*** has been processed, depending on which event occurs first. Different proposals of the IPSec peer are rejected.

Field	Description
Lifetime Policy (cont.)	■ *Use this lifetime, accept all proposals, notify*: The proposal says that the key is renewed when either the value specified in ***SECONDS*** has elapsed or the value in ***KBYTES*** has been processed, depending on which event occurs first. Different proposals of the IPSec peer are accepted, but not used. The IPSec peer is informed about the different lifetime values by means of a "responder lifetime" message.
Seconds	Only for ***LIFETIME POLICY*** = *Propose this lifetime, accept and use all proposals* or *Propose this lifetime, reject different proposals* or *Use this lifetime, accept all proposals, notify* Enter the lifetime for phase 1 key in seconds. Possible values are whole number from *0* to *2147483647. 900* is default value.
Kb	Only for ***LIFETIME POLICY*** = *Propose this lifetime, accept and use all proposals* or *Propose this lifetime, reject different proposals* or *Use this lifetime, accept all proposals, notify* Enter the lifetime for phase 1 key as amount of data processed in kB. Possible values are whole number from *0* to *2147483647. 0* is default value.

3.8 IPSec - Support for Per-Proposal Key Sizes

Support for the configuration of key sizes on a per-proposal basis has been added in **System Software 7.4.1**. It currently cannot be configured useing the Set-

up tool, but has to be configured using the SNMP shell. The relevant varibales can be found in the ***ikeProposalTable*** and in the ***ipsecProposalTable***.

3.9 Rijndael Changed to AES

The description of the algorithm formerly known as Rijndael has been changed to AES in order to account for the more commonly known name of the algorithm.

3.10 New Option in Flash Management Shell

The `ls` command did so far not display the patch level of a file stored in the Flash ROM. The option `-e` has been introduced to display this property of a file,:

```
Flash-Sh > ls -eal
Flags   Version        Length               Date Name ...
Vr-x-bc-B  7.4.02      3071906 2005/10/21  9:09:31 boss.bin
Vr---l--f  3.0.14.000   268818 2004/12/14 20:09:05 XEY-ADSLp.xey
Vr---l--f  3.0.14.249   266802 2005/10/12  7:27:48 XEY-ADSLp.xey
Flash-Sh >
```

3.11 SNMP Foreign Agent Disabled

Before **System Software 7.4.1**, it was possible to configure a remote SNMP agent address. This feature was hardly ever used and caused problems when listening on address *0.0.0.0.* It has been removed.

3.12 MRU for PPPoA Interfaces

If an interface is configured for PPPoA permanent mode, the MRU is read from the respective entry in the ***biboAdmDeviceTable***. If the interface is configured for on demand mode, the MRU is set to *4096 Bytes.* If a value other than *0* is configured for ***pppExtIfMru***, however, this value has highest priority.

3.13 Additional Debug Options

When a driver generates a burst of syslog messages, a `trap queue 0x12345678 full` message is displayed on the console and some syslogs are not displayed. This happens if the amount of syslog messages generated by the driver exceeds the limit of the trap queue, which is set to *32768* on most routers. **System Software 7.4.1** adds a `-l <size>` option to the debug application for extending the size of the trap queue to a maximum of *256000*.

There was no comfortable way of displaying the content of the ***BIBOADMSYSLOGTABLE***. **System Software 7.4.1** adds a `-s` option to the debug application for displaying the existing content of the ***BIBOADMSYSLOGTABLE*** instead of new entries in real time, but with the same convenient formatting.

3.14 Support for Additional IPSec Licenses

Additional IPSec licenses are now available (allowing 25 or 50 additional active tunnels). They can be added up to obtain the maximum number of tunnels possible on a gateway.

3.15 GPRS supported

Using a GPRS modem connected to the AUX port of your gateway is now supported. The respective options have been added to modem profile and WAN Partner configuration menus.

3 Changes

4 Solved Problems

The following problems have been solved in System Software 7.4.1:

4.1 Important: IPSec Vulnerability Fixed

Funkwerk gateways were affected by an ISKAMP vulnerability that was detected at http://www.ee.oulu.fi (see http://www.ee.oulu.fi/research/ouspg/protos/testing/c09/isakmp/). They failed the following test cases: #16, #427, #1681 and #2970.

Susceptibility to the vulnerability has been removed.

4.2 SIF - Enhanced Performance

(ID 2800)

Under certain conditions, the CPU load created by the SIF could rise significantly and cause a loss in overall gateway performance.

This problem has been solved.

4.3 RADIUS - Accounting Messages

(ID n/a)

When RADIUS accounting was used for PPP-over-L2TP connections, and the RADIUS servers was reachable only through the L2TP tunnel, the ACCOUNTING OFF message did not reach the RADIUS server if the user deactivated the respective interface.

This problem has been solved.

4.4 Keepalive Monitoring - Setup Tool Failure

(ID 3358)

The configuration of Keepalive Monitoring for IPSec interfaces (having an index of *100001* and above) failed with the message "Integer value too large" when enteirng the interface index for ***FIRSTIFINDEX***..

This problem has been solved.

4.5 QoS - TOS Error

(ID 4148)

Due to a TOS value not being handled as expected, QoS could show inconsistent behavior.

This problem has been solved.

4.6 PPP - Deadlock

(ID 4071)

When connecting to a misconfigured LNS, a PPP-over-L2TP connection using a shorthold of *-1* could not be realized. Instead, the PPP subsystem entered a deadlock after a number of connection attempts.

This problem has been solved.

4.7 QoS - Enhanced Weighted Fair Queuing

(ID n/a)

Using WFQ for QoS configurations could lead to unexpected gateway behavior (including stack traces).

This problem has been solved.

4.8 NAT - Superfluous MIB Entries

(ID 4210)

Changeing the NAT state for an interface lead to additional, but redundant entries in the ***PPPEXTIFTABLE***.

This problem has been solved.

4.9 RPoA - IP Advanced Settings Menu Missing

(ID 4275)

When configuring an RPoA interface, the link to the IP ***ADVANCED SETTINGS*** Menu was missing before the profile had not been saved.

This problem has been solved.

4.10 Ethernet - Error in Switch Configuration

(ID 4181)

Obsolete ***IPROUTETABLE*** entries were created after resetting a port separation.

This problem has been solved.

4.11 QoS - Reboot when Changing Priorities

(ID 4287)

Changing the ***QOSPOLICYPRIORITY*** value(s) of entries associated with the same interface could lead to a gateway reboot.

This problem has been solved.

4.12 Decimal Notation for OIDs

(ID n/a)

By using the `x` command on the SNMP shell, it is possible to enter OIDs in a decimal notation. This led to errors in the identification of the intended MIB.

This problem has been solved.

4.13 ATM - Reboot when Changing VPI/VCI

(ID 4323)

When changing the settings for VPI and VCI either in the Setup Tool or on the SNMP shell, the gateway rebooted.

This problem has been solved.

4.14 PPTP - Compatibilty

(ID 4337)

PPTP connection establishment to DrayTek devices failed.

This problem has been solved.

4.15 RIP - Endless Replies

(ID 4338)

Even though the gateway received acknowledgements for triggered RIP responses, it continued to resend the responses so that no other RIP routes were sent.

This problem has been solved.

4.16 Debug - NAT Messages Suppressed

(ID 4268)

NAT debug messages were erroneously suppressed when e.g. calling `debug all`.

This problem has been solved.

4.17 QoS - Interfaces Omitted in Monitoring

(ID 4328)

Some interfaces which had QoS enabled were not displayed in the respective monitoring menus.

This problem has been solved.

4.18 TDRC - Port Range Insufficient

(ID 4317)

When configuring a service for TDCR (TCP Download Rate Control), the parameter ***TCP SERVICE PORT*** allowed only port numbers up to *999*. The correct range is *1 .. 65535*.

This problem has been solved.

4.19 Setup Tool - IPSec Remote Type not Configurable

(ID 3934

The type of the remote side of Post IPSec Traffic configuration was not configurable.

This problem has been solved.

4.20 GRE - Memory Leak

(ID 4301)

GRE sessions that were not controlled by the PPTP subsystem could lead to a memory leak when used with SIF, Load Balancing or TDRC.

This problem has been solved.

4.21 SIF - Activity Monitor Packets Blocked

(ID 4384)

Locally generated messages sent by the statusd were blocked although an accept rule was configured.

This problem has been solved.

4.22 MIB - Enums Renamed

(ID 4365)

Some of the MIB enums started with capital letters which is not standard compliant.

This problem has been solved.

4.23 Syslogs - Stack Trace

(ID n/a)

A stack trace was occasionally created when Syslog tried to access certain traps.

This problem has been solved.

4.24 Ethernet - Virtual MAC Address Error

(ID 4175)

Erroneously, the virtual MAC addresses created for ETHoA interfaces were identical with the ones assigned to the Ethernet interfaces.

This problem has been solved.

4.25 IPSec - Certificate Server Cannot be Deleted

(ID 4428)

Once an entry had been created in the ***CERTSERVERTABLE*** (either via the Setup Tool or on the SNMP shell), it could no longer be deleted.

This problem has been solved.

4.26 NAT - Session Restriction not Applied Correctly

(IFD n/a)

Restricting the maximum number of NAT sessions (by setting ***ipExtIfNatMaxSessions***) did not work exactly as expected: One additional session was allowed.

This problem has been solved.

4.27 TCP - Poor Performance with High Speed xDSL

(ID 4348)

The download rate actually achieved with high bandwidth xDSL connections (6 Mbit/s and more) was lower than expected.

This problem has been solved.

4.28 WLAN - Creating New WLAN Interface not Possible

(ID n/a)

Creating a new WLAN interface was not possible using either the SNMP shell or a SNMP manager. Only the Setup Tool allowed this.

This problem has been solved.

4.29 SNMP - "Decode failed" Error Message

(ID 4235)

Under certain conditions, all UDP packets coming from the network(s) connected to the gateway were treated as SNMP responses causing the gateway to display an error on accessing the MIB.

This problem has been solved.

4.30 PPP - MRU Settings Ignored

(ID 4588)

The MRU configuration was ignrored for PPPoE interfaces, since the MRU was fixed at 1492 Bytes.

This problem has been solved.

4.31 IPSec - Impossible to Add Post IPSec Rule

(ID 4586)

Once a first Post IPSec Rule had been configured, the gateway crashed when trying to add a further one.

This problem has been solved.

4.32 IPSec - Certificate / CRL Download Failed

(ID 4598)

An automatic download of a certificate or a CRL from a server in the ***CERTSERVERTABLE*** failed because the request was sent to a wrong port.

This problem has been solved.

4.33 PPPoE - Call Direction Wrong

(ID n/a)

The direction of an outgoing PPPoE call was set to *incoming*.

This problem has been solved.

4.34 HTML Wizard - Wrong Images

(ID n/a)

The GIF used for the SIF was not the correct one.

This problem has been solved.

4.35 PPP - Problems with Two-Step Authentication

(ID 4667)

Two-step PPP authentication procedures occasionally led to connection problems.

This problem has been solved.

4.36 WLAN - Radio Band Configuration

(ID 4764)

The field ***USAGE AREA*** was displayed for both, 2,4 and 5 GHz interfaces, even though it should have been available only for 5 GHz interfaces.

Moreover, if selecting any other value than *default* in ***USAGE AREA***, confirming with ***SAVE*** did not result in storing the desired value.

These problems have been solved.

4.37 WLAN - Channel Selection

(ID 4713)

In some versions of our system software, choosing *auto* for Channel in WLAN configuration was not possible. This was not intended.

The problem has been solved.

4.38 WLAN - WPA-PSK Configuration

(ID 4765)

The Setup Tool field for the Preshared Key for ***SECURITY MODE*** = *WPA PSK* was:

1) too small: only 46 digits could be visibly entered

2) showing wrong information in the help line: "...max length = 64 chars". The actual maximum length is *63* characters since the final *0* of each key is not entered.

These problems have been solved.

4.39 PPP - Authentication Failure

(ID 4771)

When authentication was carried out in a multi-step process, occasional failures occurred.

This problem has been solved.

4.40 SNMP - MIB Search Operations Failed

(ID 4767)

Search operations inside the MIB could fail.

This problem has been solved.

4.41 VJH Compression - Stack Trace with ISDN PPP

(ID 4798)

With VJHC enabled, stack traces and reboots could occur.

The problem has been solved.

4.42 TACACS+ - Instable System

(ID 4822)

When using TACACS+, starting a random application could cause a reboot.

This problem has been solved.

4.43 Content Filtering - Fixes

(ID n/a)

1. Cobion's format of the server list has been extended. This caused an entry with IP address *0.0.0.0* in the ***cofServerTable***, and this entry led to occasional panics and sometimes to long delays when requesting the category of an URL from Cobion.

2. In rare cases, the Cobion server responded with an unsuitable answer to our license requests. This lead to an invalid license state and no more queries were sent to the cobion server.

3. If the internet connection is not up only a few seconds after booting, as may be the case with, e.g., ADSL connections, the license request to the content filter server failed and the URL filter was not usable.

These problems have been solved.

4.44 IPSec / RADIUS - Peers Deleted

(ID n/a)

After a failed IPSec preset reload, the peers which had not been reloaded yet were deleted. This was probably not intended by the user, and it is better to keep the rest of the old peers than to discard them.

The problem has been solved.

4.45 Multi Link PPP - Panic with LCP Echo Check Failure

(ID n/a)

A failing LCP echo check via a MLPPP connection could lead to a panic.

This problem has been solved.

4.46 SNMP - MIB Entries Inaccessible

(ID n/a)

RIPFILTERTABLE entries could not be deleted via SNMP, using the Setup Tool was mandatory for that purpose.

This problem has been solved.

4.47 PPTP - Reboot

(ID 5130)

If dialing in to the gateway with a Linux PPTP client, termination of the connection could lead to a reboot (without or with a stack Trace).

This problem has been solved.

4.48 ADSL - MIB Entries

The direction of the output power was reversed when the output power was written into the MIB. This means the ***ATUC*** mib held the atur's output power and vice versa.

This problem has been solved.

4.49 Compatibility - Errors with ECI DSLAMs

(ID 4368)

When connected to an ECI DSLAM, data traffic was heavily affected.

This problem has been solved.

4.50 Activity Monitor - Interfaces not Supported

(ID 4149, 4224, 4709)

The Activity Monitor delivered with our **BRICKware** did not properly detect and support all interfaces of either our new products or when using new software versions on older gateways.

This problem has been solved.

4 Solved Problems