Release Notes System Software 7.1.15

Release Notes - System Software 7.1.15

Version 1.0

Purpose This document describes new features, changes, and solved problems of **System Software 7.1.15**.

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.

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 New Features

System Software 7.1.15 contains a number of new features that significantly enhance the scope of available features over System Software 7.1.14:

- "Free IPSec License" on page 3
- "New Time Synchronization Options" on page 3
- "TACACS+" on page 6
- "RADIUS" on page 10
- "QoS" on page 11
- ""ifstat" for Physical Interfaces" on page 11

1.1 Free IPSec License

With System Software 7.1.15, Bintec gateways support the use of two active IPSec tunnels as described in the User's Guide (cf. e.g. the X2250 User's Guide for a detailed description).

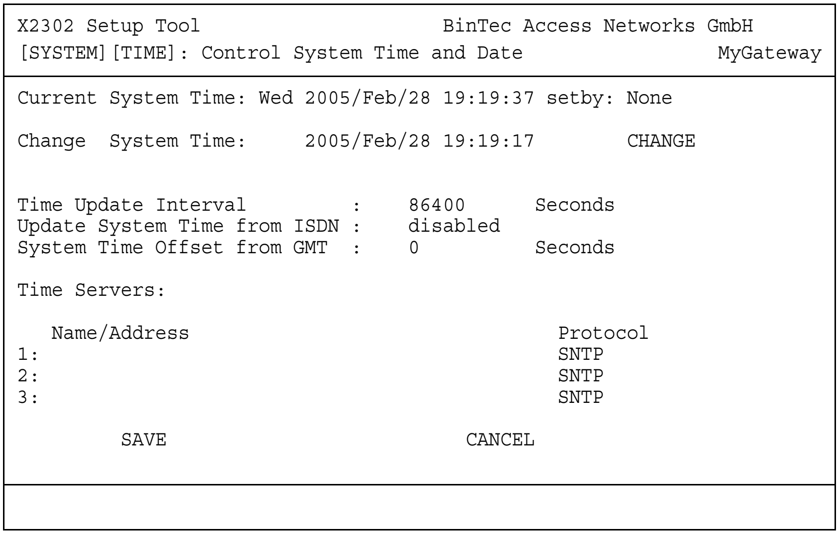
Note

Note that the license does not limit the number of IPSec peers that can be configured on your gateway, but rather limits the number of simultaneously active IPSec connections.

1.2 New Time Synchronization Options

The options for retrieving the system time of the gateway from different sources have been considerably expanded to allow querying multiple time servers.

The menu for the configuration of the time retrieval options has been extended, it is accessible via the ***System*** menu (***System*** ➜ ***Time and Date***):



```
X2302 Setup Tool                             BinTec Access Networks GmbH
[SYSTEM][TIME]: Control System Time and Date                   MyGateway

Current System Time: Wed 2005/Feb/28 19:19:37 setby: None

Change  System Time:     2005/Feb/28 19:19:17        CHANGE


Time Update Interval          :    86400      Seconds
Update System Time from ISDN :    disabled
System Time Offset from GMT   :    0          Seconds

Time Servers:

   Name/Address                                    Protocol
1:                                                 SNTP
2:                                                 SNTP
3:                                                 SNTP

         SAVE                          CANCEL
```

The first line in the menu window displays the current system time. This can be changed manually in the second line. Confirming with ***CHANGE*** applies the changes.

Since the system time is reset by a reboot on gateways that do not have a hardware Real Time Clock (cf. List of gateways without a Real Time Clock below), **System Software 7.1.15** supports synchronization with several time servers and via ISDN. The Setup Tool allows the configuration of three time servers, more can be configured via the SNMP shell. These options are configured in the lower half of the menu window. The menu offers the following configuration options:

Field	Description
Time Update Interval	Here you enter the interval at which the gateway will try to synchronize with one of the configured time servers (in seconds). Default value is *86400*.

Field	Description
Update System Time from ISDN	Here you can choose whether the time information sent at the end of an ISDN call is used to update the system time. This option is used only as long as no time update has been received from a time server since boot time. Available values are *enabled* and *disabled*, the default value is *disabled*.
System Time Offset from GMT	Here you enter the offset the local time has from GMT. Values are entered in seconds, but values between *1* and *23* are interpreted as hours and are converted to seconds upon saving the configuration. Positive values can be entered as well as negative ones, the default value is *0*.
Name/Address	Here you can enter up to three time servers, either by their domain name or by their IP address. There are no preconfigured servers.
Protocol	Here you choose the protocol used for querying the time server. Available choices are: ■ *SNTP* - This server uses the Simple Network Time Protocol. ■ *disabled* - This time server is currently not used for time retrieval. ■ *TIME/UDP* - This server uses the Time/UDP protocol. ■ *TIME/TCP* - This server uses the Time/TCP protocol.

Table 1-1: ***SYSTEM → TIME AND DATE***

List of gateways without a Real Time Clock

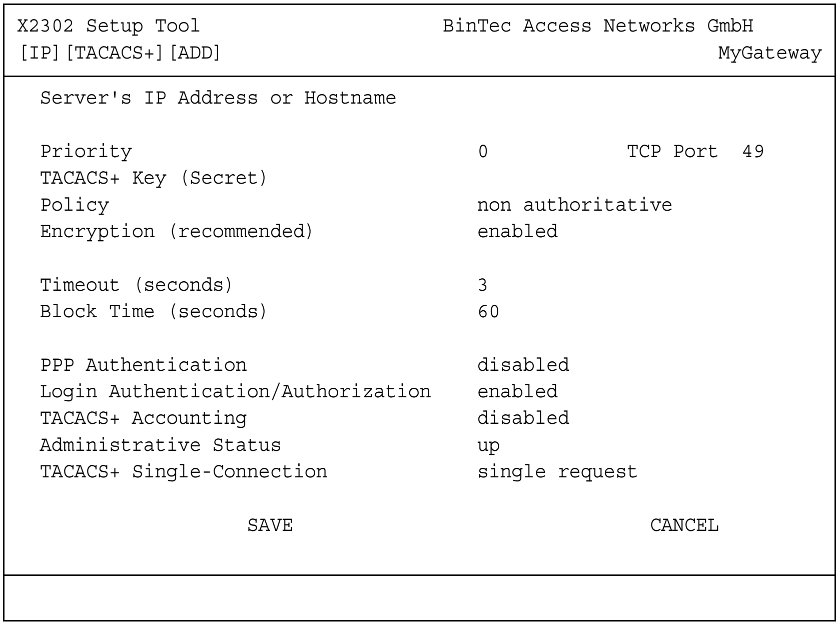
The following gateways or gateway types are not equipped with a Real Time Clock:

- **X1000 II**
- **X1200 II**
- **X2250**
- **X2300** compact with serial numbers equal to or higher than "X2C25...."
- **X2300s**
- **X2300i** compact with serial numbers equal to or higher than "X2I25..."
- **X2300is** compact with serial numbers equal to or higher than "X2Y25..."
- **X2404** compact with serial numbers equal to or higher than "X2D21..."
- **X2500**
- **VPN Access 5**, **25** and **100**
- **X2301**
- **X2302.**

1.3 TACACS+

The TACACS+ protocol provides access control for gateways, network access servers and other network devices via one or more centralized servers. TACACS+ provides authentication, authorization and accounting services.

Configuration of a TACACS+ server is carried out in the ***IP*** ➜ ***REMOTE AUTHENTICATION (RADIUS/TACACS+)*** ➜ ***TACACS+ AUTHENTICATION AND AUTHORIZATION*** ➜ ***ADD/EDIT*** menu.



```
X2302 Setup Tool                     BinTec Access Networks GmbH
[IP][TACACS+][ADD]                                     MyGateway

  Server's IP Address or Hostname

  Priority                             0            TCP Port  49
  TACACS+ Key (Secret)
  Policy                               non authoritative
  Encryption (recommended)             enabled

  Timeout (seconds)                    3
  Block Time (seconds)                 60

  PPP Authentication                   disabled
  Login Authentication/Authorization   enabled
  TACACS+ Accounting                   disabled
  Administrative Status                up
  TACACS+ Single-Connection            single request

                  SAVE                                CANCEL
```

It contains the following configuration options:

Field	Description
Server's IP Address or Hostname	Here you enter the IP address of the TACACS+ server that is to be queried for AAA (Authentication, Authorization, Accounting) request.
Priority	Here you assign a priority to the current TACACS+ server. The server with the lowest value is the first one used for a TACACS+ AAA request. If there is no response or the access was denied (in the non-authoritative case only, see also field ***POLICY***), the entry with the next lowest priority will be used. Available values are *0* to *9*, the default value is *0*.

Field	Description
TCP Port	Here the default TCP port used for the TACACS+ protocol is set to *49*. The value cannot be changed.
TACACS+ Key (Secret)	Here you enter the password used to authenticate and (if applicable) encrypt the data exchange between the TACACS+ server and the Network Access Server (your gateway). The maximum length of the entry is 32 characters.
Policy	Here you can choose the interpretation of the TACACS+ reply. Available values are *authoritative* and *non authoritative*. If set to *authoritative*, a negative answer to a request is accepted. This is not necessarily true when set to *non authoritative* (default value). In this case, the next TACACS+ server is queried until there is an authoritative reply. If ***Policy*** is set to *non authoritative* and none of the servers delivers a positive reply, or if none of the servers can be reached, the locally configured SNMP communities are checked for relevant access information.
Encryption (recommended)	Here you can choose whether the data exchange between the TACACS+ server and the NAS is encrypted. Available values are *enabled* (default value) and *disabled*. If set to *enabled,* the TACACS+ packets are MD5 encrypted. Otherwise - if set to *disabled* - the packets and therefore all related information are sent unencrypted. Unencrypted transfer is not recommended for standard usage.

Field	Description
Timeout (seconds)	Here you enter the time the NAS waits for a TACACS+ response. If no reply is received during waiting time, the next configured TACACS+ server is queried and the current server is set into a *blocked* state (***TACACSPSERVEROPERSTATUS*** = *blocked*). Available values are *1* to *60*, the default value is *3*.
Block Time (seconds)	Here you enter the amount of time for which the current server is set to a blocked state. After the block time has ended, the server is set to the state specified for the field ***ADMINISTRATIVE STATUS*** (see below). Available values are *0* to *3600*, the default value is *60*. A value of *0* means that the server is never set to a *blocked* state.
PPP Authentication	This function is not supported by **System Software 7.1.15**. It may be included in a later version of our system software.
Login Authentication/Authorization	Here you can choose whether to use the current TACACS+ server for login authentication to a gateway. Available choices are *enabled* (default value) and *disabled*.
TACACS+ Accounting	This function is not supported by **System Software 7.1.15**. It may be included in a later version of our system software.

Field	Description
Administrative Status	Here you can choose the status the server is to be put in: If set to up the associated server is used for authentication, authorization and accounting according to the priority (see field ***Priority***) and the current operational status. Otherwise this entry will not be considered for TACACS+ AAA requests. Available choices are *up* (default value) and *down*.
TACACS+ Single-Connection	Here you can choose if multiple TACACS+ sessions (subsequent TACACS+ requests) may be supported simultaneously over a single TCP connection. If multiple sessions are not being multiplexed over a single TCP connection, a new connection will be opened for each TACACS+ session and closed at the end of that session. Available choices are *multiple requests* and *single request* (*single request* is the default value and is recommended for most applications).

Table 1-2: ***IP ➜ Remote Authentication (RADIUS/TACACS+) ➜ TACACS+ Authentication and Authorization ➜ ADD/EDIT***

1.4 RADIUS

System Software 7.1.15 supports RADIUS for authentication, accounting, IPSec Peer Retrieval and shell login as described in the User's Guide (cf. e.g. the X2250 User's Guide for a detailed description).

1.5 QoS

System Software 7.1.15 supports Quality of Service as described in the User's Guide (cf. e.g. the X2250 User's Guide for a detailed description).

1.6 "ifstat" for Physical Interfaces

The `ifstat` command has not been available for physical interfaces before System Software 7.1.15. `physifstat` now offers the same options as `ifstat` for physical interfaces.

The command is used with the following syntax:

```
x2301:> physifstat -?
Usage:
        physifstat [ -lud ] [<interface>]
Options:
        -l              long interface names
        -u              only up interfaces
        -d              only down interfaces
Usage:
        physifstat <interface> up|down
             up: set <interface> to up
           down: set <interface> to down
x2301:>
```

For **X2301** and **X2302** the Ethernet and the ATM interfaces support the command:

```
x2301:> physifstat -l
Index  Descr     Typ Speed  St Ipkts Ies Opkts Oes ChgTime
001000 XEY-100BT eth 100M   up 15561 5   77    0   0 00:00:00
003000 ar7sar-3  atm    0   dn 0     0   0     0   0 00:00:00
  total: 2
x2301:>
```

Ies and ***Oes*** stand for Incoming or Outgoing errors respectively, ***ChgTime*** displays the time of the last state change..

Note

Please note that only those Ethernet interfaces ending in -0 are displayed, e.g. en1-0. Virtual interfaces (e.g. en1-1) are not covered.

Moreover, the operative status of an Ethernet interface cannot be changed.

2 Changes

The following changes have been made in order to enhance performance and ease of use of your gateway:

- "PPTP - Additional Configurable Parameters" on page 13
- "ATM Standard Profile" on page 14
- "New Option for Setup Tool Start" on page 14
- "New DHCP Parameter" on page 14

2.1 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 table 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.

2.2 ATM Standard Profile

System Software 7.1.15 contains a standard ATM profile that eases the configuration of a DSL WAN Partner.

Depending on whether your gateway is connected to an ADSL over POTS or ADSL over ISDN network, there is a standard ATM profile in the ***ATM*** ➜ ***ETHERNET OVER ATM*** menu that covers the settings of many ADSL connections offered. For ADSL over ISDN, there is an entry with ***VPI****=1* and ***VCI****=32*. For ADSL over POTS, no entry is created.

2.3 New Option for Setup Tool Start

Under **System Software 7.1.15**, 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.

2.4 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 Solved Problems

The following problems that could arise with earlier versions of our system software have been solved in System Software 7.1.15:

- “SNMP Shell - No Syslog Output with "message"” on page 16
- “MIB - Memory Leak” on page 16
- “DNS – Unrequested Name Cached” on page 16
- “Setup Tool – Use of “_” not Allowed” on page 16
- “HTML Wizard - Broadcasts Blocked by Access Filters” on page 17
- “DCHP - Reboot” on page 17
- “ARP - Wrong ARP Tell” on page 17
- “Event Scheduler - Minor Problems” on page 18
- “Setup Tool - Load Balancing Configuration Incorrectly Written to MIB” on page 18
- “Setup Tool - X.25 Monitoring Menu Removed” on page 18
- “PPPoE - Problems with Two PPPoE Access Servers” on page 19
- “Setup Tool - Irrelevant Menu Item Removed” on page 19
- “Setup Tool - IP Accounting Information Wrong” on page 19
- “PPPoE - Connection Establishment Failure” on page 20
- “ADSL - No Data Traffic” on page 20
- “DNS - First DNS Resolution Failure” on page 20

3.1 SNMP Shell - No Syslog Output with "message"

(ID n/a)

Calling `message` on the SNMP shell should have displayed the collected syslog messages, but instead displayed a MIB table.

This problem has been solved.

3.2 MIB - Memory Leak

(ID 3144)

Frozen processes could lead to a memory leak.

This problem has been solved.

3.3 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.

This problem has been solved.

3.4 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.

This problem has been solved.

3.5 HTML Wizard - Broadcasts Blocked by Access Filters

(ID 3654)

IP Access Lists created by the HTML Wizard blocked broadcast traffic on the WAN interface. This was a problem if the gateway was to obtain its IP configuration via DHCP.

This problem has been solved.

3.6 DCHP - Reboot

(ID 3670)

When handling a DHCP renew request from a client, the gateway occasionally rebooted.

This problem has been solved.

3.7 ARP - Wrong ARP Tell

(ID 36714)

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.

This problem has been solved.

3.8 Event Scheduler - Minor Problems

(ID 3679)

There were several minor bugs in the Event Scheduler implementation:

a) a typo where it read “dayly” instead of “daily”;

b) it was not possible to select a WAN interface in ***SCHEDULE COMMANDS*** ➜ ***ADD: INTERFACE*** when configuring an interface specific command;

c) the ***BIBOEXTADMSCHEDULEINTERVAL*** was reset when saving a scheduler configuration created with the Setup Tool;

d) there was no “Monday to Saturday” condition for scheduled events.

These problems have been solved.

3.9 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.

This problem has been solved.

3.10 Setup Tool - X.25 Monitoring Menu Removed

(ID 3696)

The menu ***X.25 MONITORING*** was included in the Setup Tool, even though **X2301** and **X2302** do not support X.25.

This problem has been solved.

3.11 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.

This problem has been solved.

3.12 Setup Tool - Irrelevant Menu Item Removed

(ID 3703)

Menus for the configuration of Bandwidth on Demand were included in the Setup Tool of **X2301** and **X2302** even though neither gateway supports this function.

This problem has been solved.

3.13 Setup Tool - IP Accounting Information Wrong

(ID 3737)

Monitoring and Debugging ➜ ***Interfaces*** ➜ ***EXTENDED*** displayed a wrong value for ***SrcPrt***.

This problem has been solved.

3.14 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.

This problem has been solved.

3.15 ADSL - No Data Traffic

(ID 3761)

Occasionally, data traffic over an ATM interface was impossible. At the same time, the responsiveness of the SNMP shell was dragging.

This problem has been solved.

3.16 DNS - First DNS Resolution Failure

(ID 3809)

After the initial configuration of an gateway in the ex works state, connecting to the internet failed because no connection was established for an initial DNS resolution.

This problem has been solved.