X1000

Release Notes

System Software Release 5.3.1

December 13, 2000

New System Software

System Software Release 5.3.1

This document describes the features, changes, bugfixes and known issues of the system software in release 5.3.1 for **X1000**.

1 Updating System Software

- Get the system software release 5.3 version 1 from BinTec's Web server at www.bintec.de (Products/Download section).
- You can then update **X1000** with this system software (see chapter 9.3 "Updating Software" in your User's Guide).
- When you have installed release 5.3 version 1, you will certainly want to obtain the latest documentation as well (in Adobe's PDF format). You will also find this in the Download section of BinTec's WWW server.

When you update the system software, it is recommended that you also use the latest version of BRICKware for Windows. You can load this from BinTec's WWW server.

2 New Features in 5.3.1

The following new features are included in release 5.3.1 for **X1000**:

- IPSec (with extra license)
- leased lines (with extra license)
- ADSL connection via PPTP
- AO/DI
- strong encryption via VPN license
- PPPoE credits
- revised Activity Monitor with extended functions for monitoring and control of **X1000**

For Information about these features, refer to your **X1000** User's Guide.

2.1 Time Stamp

With release 5.3.1, a trailing time stamp for syslog messages is available displaying the local system time of **X1000**. In the Setup Tool, **Timestamp** can be set under ***SYSTEM*** ➧ ***EXTERNAL SYSTEM LOGGING*** ➧ ***ADD.***

The following part of the menu is relevant for the configuration:

Field	Meaning
Timestamp	System time of **X1000**.

Table 2-1: ***SYSTEM*** ➧ **External System Logging** ➧ ***ADD***

The **Timestamp** field includes the following options:

Possible Values	Meaning
all	system time consisting of date and time
time	system time without date
none	no time stamp

Table 2-2: **Timestamp**

To activate the time stamp function, proceed as follows:

- Go to ***System*** ➧ ***External System Logging*** ➧ ***add***
- Select **Timestamp**: *all* or *time*.
  All syslog messages called up in the Setup Tool under ***Monitoring and Debugging*** ➧ ***Messages*** will be displayed with the predefined time stamp format.

2.2 Session Timeout

In release 5.3.1, a session timeout for PPP connections is available via MIB variable **biboPPPSessionTimeout**.

The variable **biboPPPSessionTimeout** gives the maximum number of seconds before terminating the established PPP session regardless of any data throughput on the corresponding link(s). The default value zero of the variable means there is no time limit on the PPP session.

2.3 SNMP Shell

In release 5.3.1, blanks between quotation marks in command line arguments (on the SNMP shell) will be accepted, e.g. `cert get ldap://trustcenter.de "cn=me, o=my company, c=de"`.

2.4 NAT

If source port mapping is not desired for outgoing NAT sessions, a fixed external port may be specified in the **ipNatOutTable** in release 5.3.1.

The external port for outgoing NAT sessions generated by an entry in the **ipNatOutTable** may be specified in the **ipNatOutExtPort** variable.

Furthermore, you can specify an additional internal port for NAT **ipNatIntPort** in the **ipNatOutTable**, which further narrows down the selection of packets to only those matching the entry to a special internal port.

2.5 Boot Sequence

In release 5.3.1, an additional function is available as point 6 in the BOOTmonitor.

```
X1000 Bootmonitor V.5.3 Rev. 1 from 2000/11/20 00:00:00
Copyright (c) 1999-2000 by BinTec Communications AG

(1) Boot System
(2) Software Update via TFTP
(3) Software Update via XMODEM
(4) Delete Configuration
(5) Default Bootmonitor Parameters
(6) Show System Information

Your Choice>
```

Figure 2-1: BOOTmonitor functions

The function (6) calls up information about the system, e.g. serial number, software version, company etc.

For information about the BOOTmonitor functions in general, refer to your **X1000** User's Guide, chapter 11.5.

3 Changes

3.1 License Mechanism

For the features VPN, IPSec or leased lines you need an extra license (see **X1000** User's Guide) which you can purchase from your dealer. In release 5.3.1, a new license mechanism is available. Exchange your VPN license, if it was delivered before 01.12.00. For information about the exchange mechanism and the current license mechanism, refer to www.bintec.de and to the license information delivered with your license.

If you have got the extra license data, activate the license on your **X1000**. To enter the data (license serial number and license key) in the Setup Tool, proceed as follows:

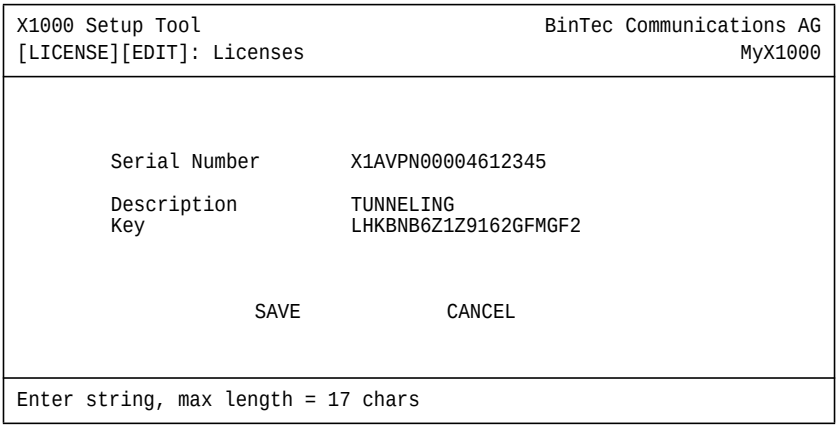
➤ Go to ***LICENSE*** ➧ ***ADD***.

```
X1000 Setup Tool                              BinTec Communications AG
[LICENSE][ADD]: Licenses                                      MyX1000


        Serial Number
        Mask                  0
        Description           default
        Key


                      SAVE              CANCEL

Enter string, max length = 17 chars
```

In release 5.3.1, the **Description** field is added.

➤ Type in the license **Serial Number**, e.g. *X1AVPN00004612345*.
Under **Description**, the system will identify the type of license, e.g. *TUNNELING* for a VPN license.

➤ Type in the **Key**, e.g. *LHKBNB6Z1Z9162GFMGF2*.



➤ Press **Save**.
The extra license will be available.

3.2 Windows PPTP Client Mode

In release 5.3.1, you may configure *PPTP PNS* (the only option available in former software versions) or *Windows PPTP client mode* (new feature) via Set-up Tool and not only on the SNMP shell (setting the values *pptp_pns* or *pptp_pac*, respectively, in the variable **layer1protocol** of the MIB table **biboPPPTable**). With the *Windows PPTP client mode*, you may dial in via **X1000** to a VPN server (master).

To configure *PPTP PNS* or *Windows PPTP client mode* via Setup Tool, proceed as follows:

➤ Go to ***VPN*** ➧ ***ADD*** ➧ ***ADVANCED SETTINGS.***

➤ Select **PPTP Mode**: *PPTP PNS* or *Windows PPTP client mode*.

➤ Confirm with **OK**.

3.3 Boot Process

There are two different boot modes on **X1000** :

- the normal boot process after switching on
- the boot process in “factory reset” mode (see the user´s guide, chapter 9.2).

From system software 5.3.1 each device will have up to three different boot configurations which **X1000** will use for either the normal boot process or for the boot process in "factory reset" mode. The device selects one of the existing configurations. The order by which the selection is made is fixed (see chapter 3.3.1, page 14 or chapter 3.3.2, page 16).

In addition to the default configuration, there are two configuration files with the following names on **X1000**:

- boot
- boot_fac (optional, new from release 5.3.1)

The boot configuration file named "boot" contains the configuration that was last saved over Setup Tool under **Exit ➧ Save as boot configuration and exit**. For this reason, no “boot” configuration is available on devices being brought into initial operation.

From system software 5.3.1 there is a so-called “factory boot” file option on **X1000** with a special configuration saved in the Flash memory in the factory. This configuration allows **X1000** to establish a connection to a corporate headquarters, for example. From there a remote configuration of the device can be carried out.

The so-called default configuration is always available. It will be loaded if there is no other boot configuration.

From system software 5.3.1 several new syslog messages give information about the boot configuration currently in use and the corresponding password.

3.3.1 Normal Boot Process

The following graphic and the accompanying text explain the order in which the existing boot configurations on **X1000** are requested during a normal boot process:

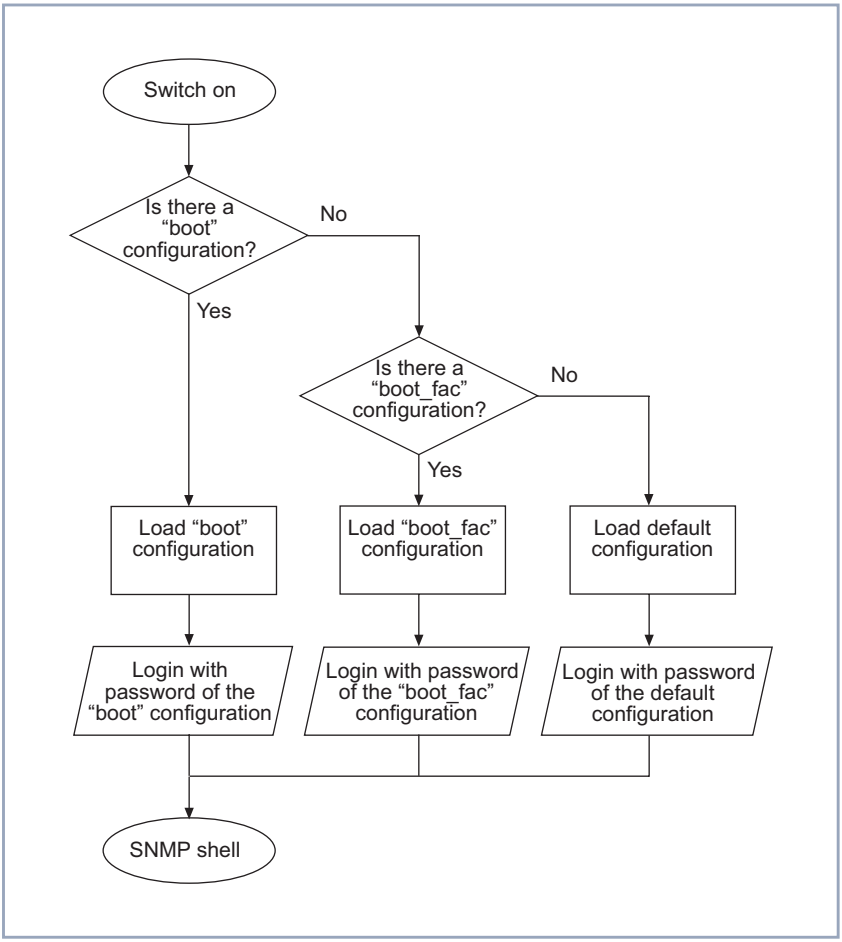


Figure 3-1: Boot configurations in the normal boot process

3 Boot Process

After switching on, **X1000** performs a boot process for which the device uses a certain boot configuration. Depending on which boot configurations are available, **X1000** selects its configuration according to the order illustrated in figure 3-1, page 14. **X1000** boots with the first configuration it finds. The graphic also includes the place in the process of the respective password required to enter the SNMP shell.

3.3.2 Booting in "factory reset" Mode

The following graphic, together with the accompanying text, explains the order in which existing boot configurations on **X1000** are requested during the boot process in "factory reset" mode.

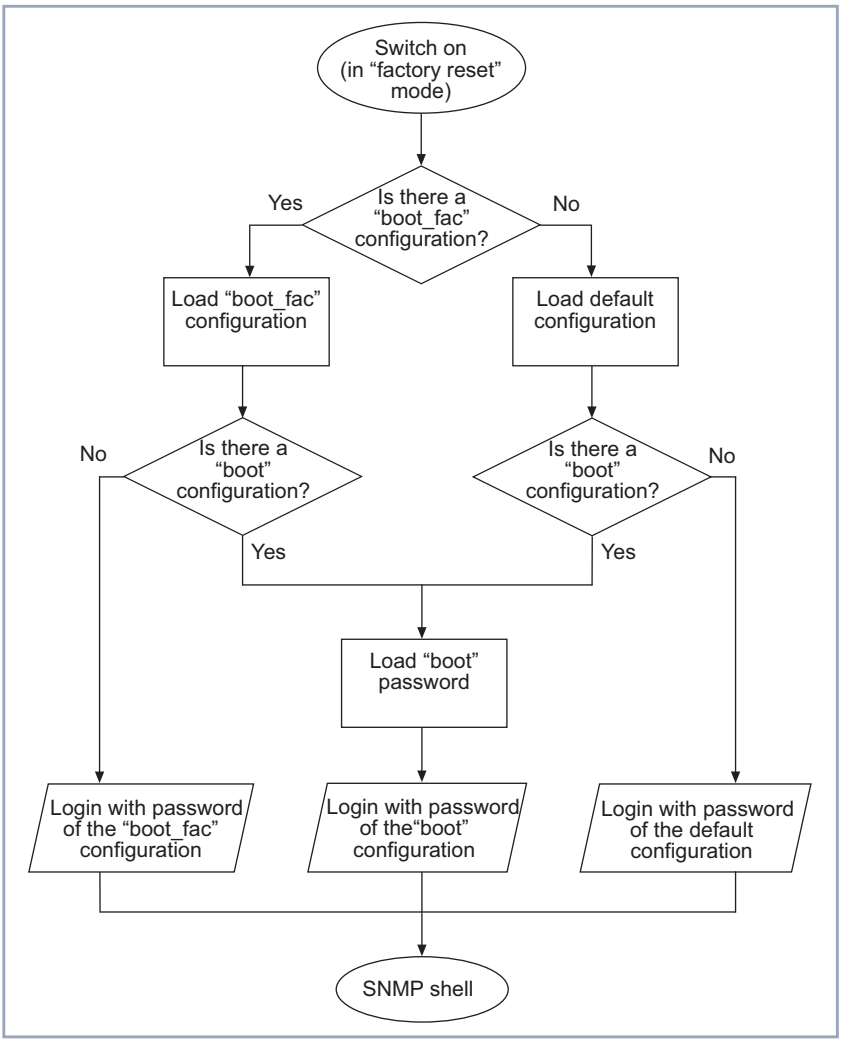


Figure 3-2: Boot configurations in "factory reset" mode

By using a special reset sequence (switching on and off), it is possible to reset **X1000** to the so-called "factory reset" state (see user´s guide, Kapitel 9.2). If **X1000** boots in the "factory reset" state, **X1000** loads one of up to three boot

configurations according to the illustrated conditions in figure 3-2, page 17. The graphic also includes the place in the process of the respective password required to enter the SNMP shell. In order to log on, the password of the boot configuration in the previous step of the process is required.

Normally, a configuration loaded with “factory reset” mode should not be changed or saved as it is essentially a hybrid of two configurations.

Be aware that the name of the configuration loaded with “factory reset” is not “boot”. In no case should you leave Setup Tool via **Save as boot configuration and exit**, this would save the loaded configuration under the name "boot" and would thus overwrite the original boot configuration. As the password of the “factory reset” configuration would come from another configuration, the original password would also be overwritten on saving.

The loading of a new configuration is perfectly possible.

3.3.3 Boot Configuration Used

From system software 5.1.6 the following message will appear during the boot process: "Cfg: <config>", where <config> specifies the boot configuration used.

3.3.4 Password Used

From system software 5.1.6 the following message will appear during the boot process in “factory reset” mode “Sec: <passwd>", where <passwd> specifies the configuration whose password was loaded.

3.4 Syslog Messages

3.4.1 Boot Configuration

From system software 5.1.6 the syslog messages include information about which configuration **X1000** has booted.

3.4.2 Output of Syslog Messages

From system software 5.1.6 the complete list of all syslog messages can be generated over the serial interface.

3.5 SNMP Shell Command: showmib

From system software 5.1.6 the command `showmib` displays the number of lines of the table at the end of the table.

4 Bugfixes

4.1 Windows 2000

4.1.1 PPP Callback

Under Windows 2000, PPP callback to a Windows 2000 client failed.

This problem has been fixed.

4.1.2 DNS Proxy Could Not Resolve DNS Requests

When PCs running Windows 2000 sent DNS requests to the **X1000**'s DNS Proxy and a negative static name entry existed for a requested name, the **X1000** tried to resolve the name instead of answering the request negatively and not passing it to another name server. In this way, unwanted connections may have been established, generating costs.

This problem has been fixed.

4.2 DNS Proxy

DNS Proxy interpreted static name entries case sensitively. This way unwanted connections may have been established, generating costs.

This problem has been fixed.

4.3 Syslog Message "TX Underrun"

In some cases, an Ethernet problem caused the syslog message "TX underrun".

This problem has been fixed.

4.4 BackRouteVerify at an AppleMAC

X1000 could not route IP pakets from an AppleMAC when BackRouteVerify was switched on.

This problem has been fixed.

4.5 Channel Bundling

If **X1000** was configured for static or dynamic channel bundling, but the router of an ISP did not accept channel bundling, the first channel was connected, but the second one was established and dropped. **X1000,** however, continued dialling. This way unwanted connections were established, generating costs.

This problem has been fixed.

4.6 Setup Tool

4.6.1 WAN Interface

It was not possible to open the Setup Tool menu ***CM-1BRI, ISDN S0*** ▶ ***ADVANCED SETTINGS***.

This problem has been fixed.

4.6.2 WAN Partner

In the Setup Tool menu, the submenu ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings*** ➧ ***Extended Interface Settings (optional)*** was not available in any case.

This problem has been fixed.

4.6.3 WAN Partner

If entries were made in the Setup Tool menu ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings*** and then the following menu was opened ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings*** ➧ ***Extended Interface Settings (optional)***, the entries were lost as soon as one left ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings*** ➧ ***Extended Interface Settings (optional)*** via **Save** or **Cancel** .

This problem has been fixed.

4.6.4 Channel bundling

In the ***WAN Partner*** ➧ ***ADD*** ➧ ***Advanced Settings*** ➧ ***Extended Interface Settings (optional)*** Setup Tool menu, the value under **Maximum Number of Dialup Channels** was not shown if one had previously left that menu via **Save**.

This problem has been fixed.

4.7 SNMP

Disabling the SNMP port or the SNMP trap port failed. If the SNMP port or the SNMP trap port was set to zero, **X1000** lost these values after a reboot. Instead of zero, the default values 163 and 164 were active again.

This problem has been fixed.

4.8 MIB Variable ifOperStatus

The MIB variable **ifOperStatus** displaying the physical link of a LAN interface was not implemented in conformity with RFC 1213.

This problem has been fixed, now the MIB variable **ifOperStatus** is in conformity with RFC 1213.

4.9 MIB Variable ifLastChange

The MIB variable **ifLastChange** displayed the period of time passed since an interface changed its state.

With release 5.3.1, the MIB variable **ifLastChange** displays the system time when the state of an interface has changed in conformity with RFC 1213.

4.10 10 Base-T Ethernet Interface

The 10 Base-T Ethernet interface was blocked during high traffic, e.g. Spray.

This problem has been fixed.

4.11 DHCP after Reboot

If a DHCP client (PC) communicated with **X1000** and had got its IP address via DHCP from the router, the router lost its information of offered IP addresses after a reboot. A window was displayed with the message "DHCP could not get an IP address" while working at the PC, because **X1000** couldn't reassign the

same address previously assigned to the PC as requested. In some cases, the PC could not get an IP address until the previously assigned IP address was available again.

This problem has been fixed.

4.12 LED L1 Blinking

If, in the menu ***CM-1BRI, ISDN S0***, the field **ISDN Switch Type** was set to *leased line B1 channel (64S)*, the LED L1 would blink continuously.

This problem has been fixed.

4.13 Boot Process

During the boot process of **X1000**, several debug messages were issued on the console of **X1000**.

This problem has been fixed.

5 Known Issues

5.1 PAP and Encrypted PPP Connections

In release 5.3.1, **X1000** will reboot, if PAP authentication is used within PPP connections using one of the following **Encryption** settings:

- *MPPE V2 128*
- *DES 56*
- *DES3 168*
- *Blowfish 56*
- *Blowfish 168*

With the setting **Encryption** *MPPE 128*, **Encryption** *none* is negotiated but not displayed.

For the above reasons and to ensure security, it is highly recommended to avoid PAP authentication together with encryption, because otherwise the passwords are sent unencrypted and therefore encryption makes no sense.

5.2 Authentication with MS-CHAP V2

In release 5.3.1, authentication with MS-CHAP V2 over leased lines fails.

5.3 Windows 98: VPN

When trying to establish a PPTP connection under Windows 98 to a **X1000** VPN server, the PPTP negotiation fails. No VPN connection will be set up.

5.4 Windows 2000: VPN

When dailing up from a **X1000** to a Windows 2000 server, no PPTP connection will be established, because TCP negotiation fails.

5.5 SNMP Shell Command Trace

5.5.1 Aborting Trace

In release 5.3.1, the command `trace` used over the telnet service or the serial console cannot be aborted if characters are typed in via keyboard while the trace is running.

Use `trace&` instead of `trace` to operate the process in the background and thus avoid the problem.

5.5.2 State Blocked or Down

If an interface is in the *blocked* or *down* state, the `trace` command can not give any information about the reason for the state; instead, the result is a stack trace.

Use the `debug` command to find out why the interface is not available.

5.6 Setup Tool

5.6.1 Leased Lines

In release 5.3.1, using leased lines (with selection *leased line B1 + B2 channel (64S2)* or *leased line D + B1 + B2 channel (TS02)*) and changing the authenti-

cation in the Setup Tool under ***WAN PARTNER*** ➧ ***ADD*** ➧ ***PPP*** causes stack traces and/or a lot of error messages in the following cases:

- changing the **Authentication** from *none* to *MS-CHAP*
- changing the **Authentication** from *MS-CHAP* V2 to *CHAP + PAP*
- changing the **Authentication** from *PAP* to *CHAP*

If you change the **Authentication** from *CHAP + PAP + MS-CHAP* to *MS-CHAP V2*, no connection will be established and a warning is displayed.

Unplugging the ISDN connection, changing the authentication in the MIB table **biboPPPTable**, saving it and plugging in the ISDN connection again will solve the problem.

5.7 DHCP after Reboot

5.7.1 X1000 Blocked

If a DHCP client communicates with **X1000** as DHCP server and the client has got its IP address from **X1000** , a reboot of **X1000** blocks the router when the client sends a DHCP request to renew the IP address.

Remove the IP address on each client and reboot **X1000** again.

To avoid this problem, do not switch off **X1000** during running.

5.7.2 Stack Trace

If a DHCP client communicates with **X1000** as DHCP server, a reboot of **X1000** sometimes causes a stack trace under following conditions:

- The client has got its IP address from Windows and then requests an IP address from the address pool of **X1000**.
- `ipconfig /release` and `ipconfig /renew` is typed in on the client.

5.8 DHCP Request on Booting

If **X1000** is acting as a DHCP server and Windows computers are being used as DHCP clients, **X1000** can not end its boot process if a DHCP client sends a DHCP request to **X1000** during the boot process.

To avoid this problem, firstly boot **X1000** and then the DHCP clients.

5.9 Syslog Messages

The first syslog messages during the boot process are not transmitted over the LAN**.**

Switch on the output of syslog messages on the console to get a complete list of syslog messages. After logging in, you can also list all syslog messages with the SNMP command `message`.