Release Notes

System Software 7.1.12

Release Notes - System Software 7.1.12

Version 1.0

Purpose This document describes new features, changes, and solved problems of **System Software 7.1.12**.

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 Important Information

Please read the following information about System Software 7.1.12. As System Software 7.1.12 is based on System Software 7.1.1, the same conditions apply to the scope of features and the downgrade restrictions.

Please make sure to read all information about upgrading to System Software 7.1.12 which is available from our website.

⚠ Attention!

This document is published with a beta version of System Software 7.1.12. The document is accordingly of a temporary nature. In view of the status of the software, it may and probably does contain errors and inaccuracies. Funkwerk Enterprise Communications GmbH accepts no liability for problems and damage caused by the use of beta software and the accompanying documentation.

1.1 Scope of Features

System Software 7.1.12 can be used equally for both the new **VPN Access Series** devices and **X-Generation** devices. Please note, however, that the scope of features can differ between individual devices of a series or different series.

No version of **System Software 7.1.12** is available for the following devices:

- **BinGO! DSL**
- **X1000**
- **X1200**
- **X3200**
- all **BRICK** generation devices.

1.2 BOOTmonitor Update

Updating to **System Software 7.1.12** requires a BOOTmonitor update on all gateways of the **X2000** Family if the gateway is to be updated from a release earlier than 7.1.1. This does not apply to **X2301** and **X2302**.

You will find the necessary files in the Download section of your gateway. The BOOTmonitor can be updated just like the system software using the `update` command. A description can be found in the chapter "Configuration Management" in your gateway manual.

Attention!

The BOOTmonitor update must be carried out prior to the system software update, as otherwise the system software update is not possible.

Gateways of the X2000 Family need a BOOTmonitor version of 6.3.8 or higher.

1.3 Deleting DSL Logic

On devices of the **X2300** Family it is necessary to delete the DSL logic not required before carrying out the update to **System Software 7.1.12**. This does not apply to **X2301** and **X2302**

Proceed as follows:

1. Go to the flash ROM management shell: `update -i`.
2. Activate a list of all the files saved in the flash ROM: `ls -l`.

You receive the following shell output (e.g.):

```
Flash-Sh > ls -l
Flags      Version   Length  Date                Name ...
Vr-x-bc-B  6.3.04    1740353 2003/06/05 7:53:06  box155rel.ppc860
Vr---l--f  3.8.129   319696  2003/01/24 15:48:05 X2E-ADSLp.x2c
Vr---l--f  3.8.129   315904  2003/01/16 13:17:42 X2E-ADSLi.x2c
Flash-Sh >
```

File "X2E-ADSLp.x2c" is used by **X2300** (ADSL over POTS) and file "X2E-ADSLi.x2c" by **X2300i** and **X2300is** (ADSL over ISDN).

3. Delete the file that does not match your gateway type: `rm X2E-ADSLi.x2c` or `rm X2E-ADSLp.x2c`.

4. Make sure the file has been deleted: `ls -l`.

You now obtain the following shell output (if, for example, you have deleted the logic for ADSL over ISDN):

```
Flash-Sh > ls -l
Flags      Version   Length  Date                Name ...
Vr-x-bc-B  6.3.04    1740353 2003/06/05 7:53:06  box155rel.ppc860
Vr---l--f  3.8.129   319696  2003/01/24 15:48:05 X2E-ADSLp.x2c
Flash-Sh >
```

5. Carry out a "reorg" to finally delete the file from the flash ROM: `reorg`. You can activate a list of the saved files again as a check: `ls -l`.
6. Leave the flash ROM management shell: `exit`.

You have deleted the DSL logic not required.

If This Fails

Even though we try to keep updating procedures as simple as possible, more complicated situations cannot be completely ruled out. Under certain circumstances, the procedure described above will fail.

This is the case if the contiguous amount of space available in the Flash ROM is not enough for storing a software image larger than the old one. If this is the case, no error message is displayed, so what you will see is simply this:

```
 x2300ic:> update 192.168.1.10 s7104b04.x2c
 Starting TFTP File Transfer .x2300ic:>
```

This does by no means mean that you cannot update your gateway. Please refer to the **Bintec How To** describing how to prepare a **X2000**-Family Gateway for an update. You can find the document in the same location where you have found these Release Notes.

1.4 Downgrade Restrictions

It is not possible to downgrade directly from **System Software 7.1.12** to a previous version of the system software.

⚠ **Attention!**

Configurations created with System Software 7.1.12 are not compatible with older versions of system software.

Save a backup copy of your gateway configuration on a PC before you carry out an upgrade.

Please note that certain features will no longer be available after a downgrade.

It is possible to downgrade in stages:

1. Save a backup copy of your gateway configuration on a PC before you carry out an upgrade to **System Software 7.1.12**. Information on saving an external copy of your configuration can be found in the chapter "Configuration Management" in your gateway manual.
2. Now you can carry out the upgrade and still fall back on your old system software version if necessary. After a downgrade you must reload your gateway with the matching configurations for this system software. Information about the necessary steps can be found in your gateway manual.

Further information about upgrade or downgrade restrictions and the documentation for your gateway can be found at www.bintec.net.

1.5 BRICKware Wizard

Our system software has no longer supported the **BRICKware** Configuration Wizard since Release 7.1.1. A new HTML-based Configuration Wizard has been introduced with System Software 7.1.4.

1.6 Software Image Names

The names of the software images have changed and the device code is now placed before the actual release code. If your gateways are configured using the XAdmin configuration tool, you must initially still use the old image names. This is done by just deleting the device code from the name: "X1x00II-b7101.x2x" then becomes "b7101.x2x".

1.7 Prerequisites for Using the AUX Interface

Releases 7.1.1 and 7.1.4 of our system software support connecting an analog or GSM modem to the serial port of your gateway. There is a number of prerequisites that must be met, otherwise connecting a modem may fail.

Please refer to the Release Notes for System Software release 7.1.1 to learn about the supported options and possible restrictions. In particular, note the following:

- Only the modems specified in the Release Notes have been successfully tested and are certified by Funkwerk Enterprise Communications GmbH. XON/XOFF flow control must be fully supported and functional, otherwise a connection between the gateway and the modem will most probably fail.
- Make sure that the cable used for connecting gateway and modem complies with the specifications detailed in the Appendix to Release Notes 7.1.1. If in doubt, you can purchase a ready converted cable from Funkwerk Enterprise Communications GmbH.

2 New features

System Software 7.1.12 introduces a number of important new features like L2TP (Layer 2 Tunnelling Protocol), an Artem access point discovery function and TACACS+.

The following new features have been added:

- "Layer 2 Tunneling Protocol (L2TP)" on page 11
- "TACACS+" on page 17
- "Artem Access Point Discovery" on page 20
- "New IPSec Peer Type" on page 27
- "Support for Registration Authority Certificates" on page 29
- "New Time Synchronization Options" on page 32
- "Continuous Ping" on page 35
- "Jitter Daemon" on page 35
- "ATM QoS - VBR 3" on page 35
- "DHCP Hostname" on page 36
- "HTML Wizard Rerun" on page 37
- "IPSec Peer Monitoring" on page 39
- "New X.25 Features" on page 42

2.1 Layer 2 Tunneling Protocol (L2TP)

System Software 7.1.12 supports the Layer 2 Tunneling Protocol which allows tunneling PPP connections through a UDP connection.

Our implementation covers the L2TP Network Server (LNS) functions as well as the functions of a client L2TP Access Concentrator (LAC). A client LAC is able to locally create the PPP data stream that is encapsulated in L2TP. Thus, it is possible that hosts in a LAN can connect to the gateway via all supported types of connection and still use L2TP. Presently our gateways support L2TP tunnels over UDP connections only.

WAN Partner Settings

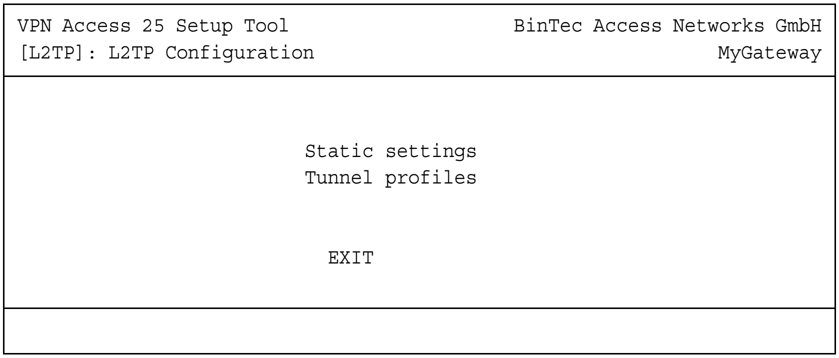
To configure a WAN Partner for the use of L2TP, two new options have been added for Layer 1 Protocol in the ***WAN Partner* ➜ *ADD/EDIT* ➜ *Advanced Settings*** menu:

- *PPP over L2TP (LNS mode)*: Using this option, the WAN Partner is used for accepting L2TP tunnels and terminating the encapsulated PPP data stream.
- *PPP over L2TP (LAC mode)*: Using this option, the WAN Partner is used to encapsulate a PPP data stream into L2TP and create an L2TP tunnel to a remote LNS.

If a WAN Partner is configured in L2TP LAC mode, it is necessary to choose a ***L2TP Tunnel Profile***.

L2TP Menu Settings

The list of profiles you can choose from is created in the ***L2TP*** menu which is accessible from the Setup Tool main menu.



```
VPN Access 25 Setup Tool                      BinTec Access Networks GmbH
[L2TP]: L2TP Configuration                                      MyGateway


                         Static settings
                         Tunnel profiles


                           EXIT
```

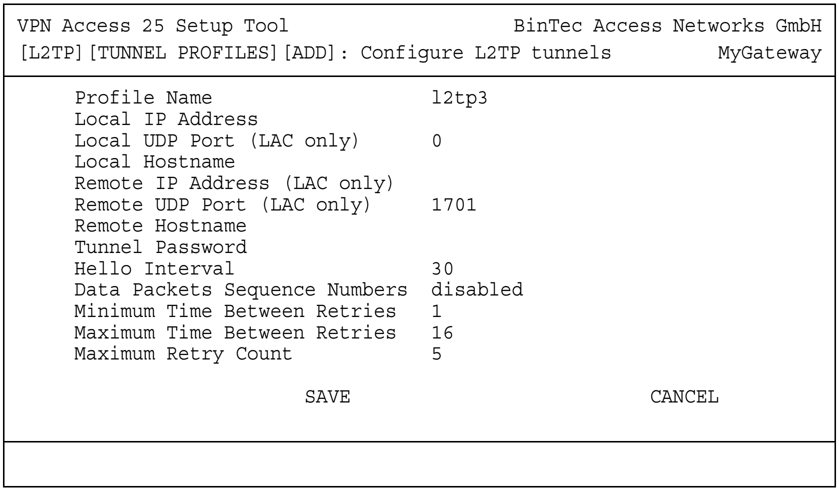
The submenu ***Static settings*** offers the following configuration options:

Field	Description
UDP port number for LNS mode	This is the port monitored by the LNS for incoming L2TP tunnel connections. Available values are all integers from *1* to *65535*, the default value is *1701* as detailed in RFC 2661.

Field	Description
Port usage for LNS mode	This parameter determines if the LNS will only use the monitored port (***UDP PORT NUMBER FOR LNS MODE***) as local source port for the L2TP call or if it chooses one of the available free ports.

Table 2-1: ***L2TP*** ➜ ***STATIC SETTINGS***

The L2TP tunnel profiles are created or edited in the ***TUNNEL PROFILES*** submenu:



```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[L2TP][TUNNEL PROFILES][ADD]: Configure L2TP tunnels             MyGateway

     Profile Name                   l2tp3
     Local IP Address
     Local UDP Port (LAC only)      0
     Local Hostname
     Remote IP Address (LAC only)
     Remote UDP Port (LAC only)     1701
     Remote Hostname
     Tunnel Password
     Hello Interval                 30
     Data Packets Sequence Numbers  disabled
     Minimum Time Between Retries   1
     Maximum Time Between Retries   16
     Maximum Retry Count            5

                    SAVE                          CANCEL
```

It offers the following configuration options:

Field	Description
Profile Name	Here you can enter a description for the current profile. The gateway automatically numbers the profiles "*l2tp..*", but this value can be changed.
Local IP Address	Here you enter the IP address that will be used as source address for all L2TP calls based on this profile. If left blank, the gateway uses the IP address of the associated interface.

Field	Description
Local UDP Port (LAC only)	Here you can enter the port number that is used as source port for all outgoing L2TP calls based on this profile. Available values are *0* to *65535*; the default value *0* means that ports will be dynamically allocated to calls using this profile.
Local Hostname	Here you enter the host name which is included in outgoing tunnel establishment messages for identifying this gateway. These messages are the SCCRQs sent by the LAC and SCCRPs sent by the LNS. The LNS uses this parameter to match the incoming SCCRQ to one of the available L2TP profiles. The maximum length of the entry is 35 characters.
Remote IP Address (LAC only)	Here you enter the IP address used as destination address for calls based on this profile. The destination must be a device capable of acting as LNS.
Remote UDP Port (LAC only)	Here you enter the destination port number used for all calls based on this profile. The remote LNS that receives the call must be listening for L2TP connections on this port.

Field	Description
Remote Hostname	Here you enter the host name which is expected in incoming tunnel establishment messages (SCCRQs received by the LNS and SCCRPs received by the LAC) for identifying the remote gateway. The maximum length of the entry is 35 characters. The ***Local Hostname*** configured on the LAC has to match the ***Remote Hostname*** configured for the intended profile on the LNS, and vice versa. However, a blank ***Remote Hostname*** specified on the LNS qualifies the associated profile as a default entry that is used for all incoming calls for which no profile with a matching ***Remote Hostname*** can be found.
Tunnel Password	Here you enter the password that is used for tunnel authentication. Authentication between LAC and LNS is two-way, i.e. the LNS checks the ***Local Hostname*** and the ***Tunnel Password*** contained in the LAC SCCRQ against the ones specified in the relevant profile. The LAC does the same for the respective fields of the LNS SCCRP. If this field is left blank, authentication data will neither be sent nor considered in tunnel establishment messages.
Hello Interval	Here you enter the interval (in seconds) between sending two L2TP HELLO messages in order to keep the tunnel open. Available values are *0* to *255*, the default value is *30*. A value of *0* means that no L2TP HELLO messages are sent.

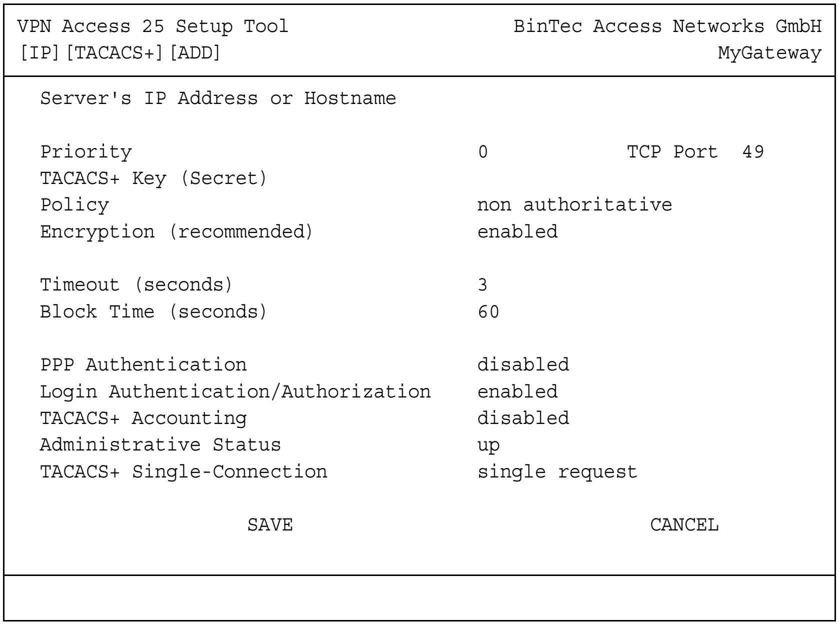
Field	Description
Data Packets Sequence Numbers	Here you can choose if the gateway uses sequence numbers for data packets sent through a tunnel based on this profile. Available choices are *disabled* (default value) and *enabled*.
Minimum Time Between Retries	Here you enter the minimum time (in seconds) the gateway waits before resending an L2TP control packet to which it has received no reply. Wait time will be dynamically increased until it reaches the ***Maximum Time Between Retries***. Independently of the current wait time, no more retries are sent if ***Maximum Retry Count*** has been reached. Available values are *1* to *255*, the default value is *1*.
Maximum Time Between Retries	Here you enter the maximum time (in seconds) the gateway waits before resending an L2TP control packet to which it has received no reply. Available values are *8* to *255*, the default value is *16*.
Maximum Retry Count	Here you enter the maximum number of times the gateway retransmits an L2TP control packet it has not received an acknowledgement for. If this number is reached without receiving a reply, the tunnel times out. Available values are *1* to *255*, the default value is *5*.

Table 2-2: ***L2TP → Tunnel profiles → ADD/EDIT***

2.2 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.



```
VPN Access 25 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.

Field	Description
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*.
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.

Field	Description
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.
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 7.1.12**. 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*.

Field	Description
TACACS+ Accounting	This function is not supported by **System Software 7.1.12**. It may be included in a later version of our system software.
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 2-3: ***IP* ➜ *Remote Authentication (RADIUS/TACACS+)* ➜ *TACACS+ Authentication and Authorization* ➜ *ADD/EDIT***

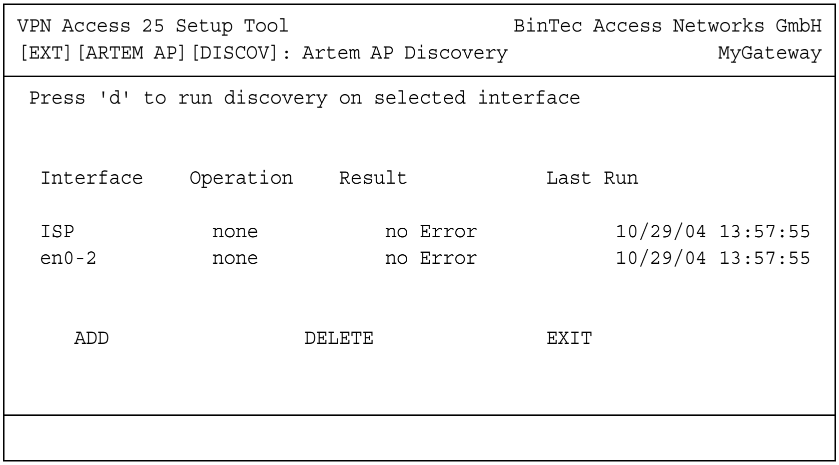
2.3 Artem Access Point Discovery

A new subsystem has been added to the Setup Tool main menu: External Systems. With System Software 7.1.12, it contains a menu for the discovery of Artem Access Points that are located in the same network as your gateway. Once an access point has been discovered, a number of basic

parameters can be configured on the access point (given that you know the administrative password).

Discovery

Once you have run an access point discovery, you can configure the discovered devices (node name, IP address, netmask and gateway address). Discovery is triggered in the menu ***External Systems*** ➜ ***Artem Access Point Discovery/Configuration*** ➜ ***Initiate Discovery***:



```
VPN Access 25 Setup Tool                     BinTec Access Networks GmbH
[EXT][ARTEM AP][DISCOV]: Artem AP Discovery                    MyGateway

 Press 'd' to run discovery on selected interface


  Interface     Operation     Result             Last Run

  ISP             none          no Error               10/29/04 13:57:55
  en0-2           none          no Error               10/29/04 13:57:55


     ADD                  DELETE                 EXIT
```

The menu displays the following details about the configured entries:

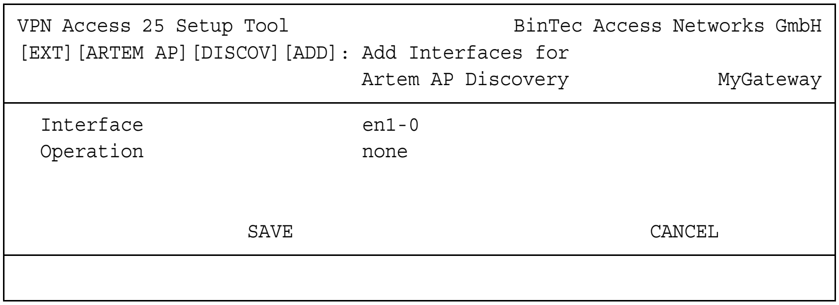
Column	Description
Interface	This column displays the name of the interface which is configured for Artem access point discovery. The name shown to identify the interface is the ***ifDescr*** from the ***ifTable***.
Operation	This column displays whether a discovery is running. It is updated automatically to indicate, when the discovery operation has finished. It can assume the following (read-only) values: ■ *none*: Discovery is not running on this interface. ■ *discovery*: Discovery is currently running on this interface.

Column	Description
Result	This column displays the result of the operation. It is updated automatically; the values are read-only: ■ *no Error*: No discovery initiated or discovery was a success. ■ *Dest. unreachable*: The interface is currently not usable, i.e. the interface is not operational, has no IP address assigned or has no associated direct route. The request could not be sent. Specific failure reason can be found in the syslog.
Last Run	This column displays the date and time of the last successful discovery. An empty string is displayed if no discovery has been performed yet or the initial discovery has been unsuccessful.

Table 2-4: ***External Systems → Artem Access Point Discovery/Configuration → Initiate Discovery***

By highlighting an entry and pressing the **d** key on your keyboard, you can initiate the discovery process for the selected entry.

You can add an instance of the access point discovery or edit an existing one in the menu ***External Systems → Artem Access Point Discovery/Configuration → Initiate Discovery → ADD/EDIT***:



```
VPN Access 25 Setup Tool                     BinTec Access Networks GmbH
[EXT][ARTEM AP][DISCOV][ADD]: Add Interfaces for
                              Artem AP Discovery                MyGateway

  Interface                   en1-0
  Operation                   none


                     SAVE                                 CANCEL
```

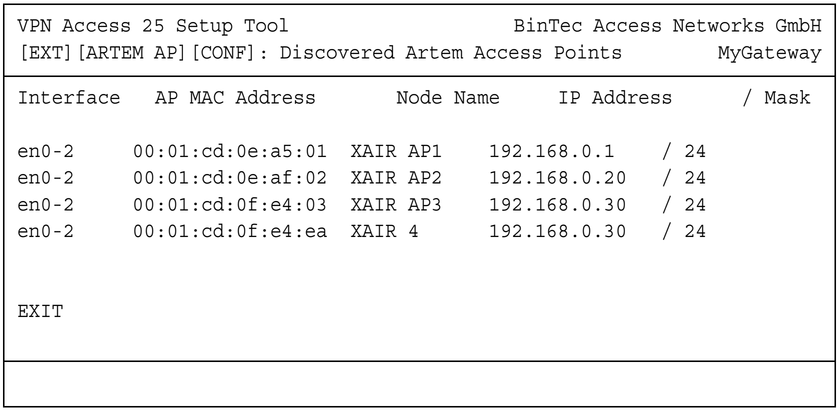
The menu contains the following fields:

Field	Description
Interface	Here you can choose for which of the IP interfaces the discovery is to be performed. All access points to which the gateway connects via this interface will be discovered.
Operation	Here you can choose if the discovery is to be triggered immediately when the entry is saved, i.e. as soon as you confirm with ***SAVE***. Note that discovered access point are not stored in the MIB, i.e. the discovery has to be repeated after a reboot of your gateway. Available choices are: ■ *none* (default value): No operation is performed when the entry has been saved. The discovery can later be triggered as described above. ■ *discovery*: Discovery on this interface is performed immediately after the entry has been saved.

Table 2-5: ***EXTERNAL SYSTEMS ➜ ARTEM ACCESS POINT DISCOVERY/CONFIGURATION ➜ INITIATE DISCOVERY ➜ ADD/EDIT***

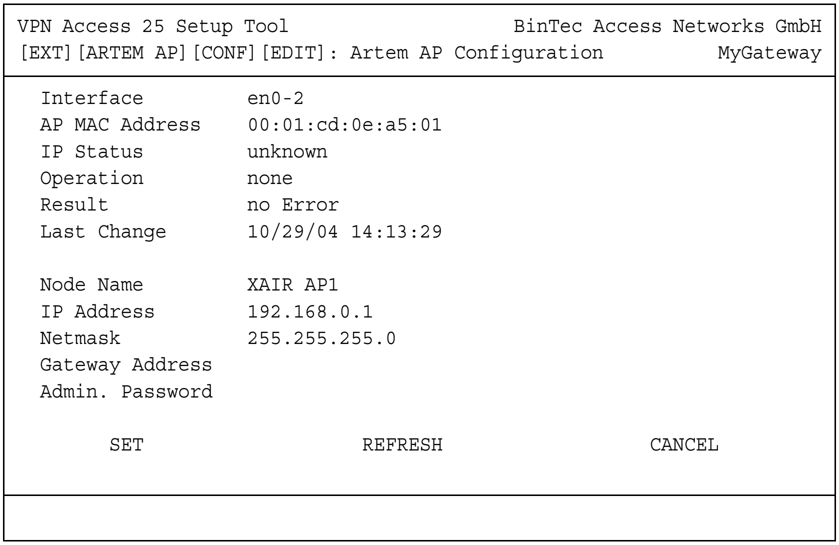
Configuration

Once you have run the discovery on all desired interfaces, you can view the result of the discovery and configure the discovered access points in the menu ***EXTERNAL SYSTEMS ➜ ARTEM ACCESS POINT DISCOVERY/CONFIGURATION ➜ VIEW/CONFIGURE***:



```
VPN Access 25 Setup Tool                           BinTec Access Networks GmbH
[EXT][ARTEM AP][CONF]: Discovered Artem Access Points            MyGateway

Interface   AP MAC Address       Node Name     IP Address      / Mask

en0-2     00:01:cd:0e:a5:01  XAIR AP1    192.168.0.1    / 24
en0-2     00:01:cd:0e:af:02  XAIR AP2    192.168.0.20   / 24
en0-2     00:01:cd:0f:e4:03  XAIR AP3    192.168.0.30   / 24
en0-2     00:01:cd:0f:e4:ea  XAIR 4      192.168.0.30   / 24


EXIT
```

The list displays all discovered access points, the interface they have been found at, their MAC address, their current node name and their current IP configuration. You can change a number of values by highlighting an entry and confirming with **Return**:



```
VPN Access 25 Setup Tool                           BinTec Access Networks GmbH
[EXT][ARTEM AP][CONF][EDIT]: Artem AP Configuration              MyGateway

  Interface          en0-2
  AP MAC Address     00:01:cd:0e:a5:01
  IP Status          unknown
  Operation          none
  Result             no Error
  Last Change        10/29/04 14:13:29

  Node Name          XAIR AP1
  IP Address         192.168.0.1
  Netmask            255.255.255.0
  Gateway Address
  Admin. Password

        SET                    REFRESH                   CANCEL
```

The menu offers the following configuration options:

Field	Description
Interface	The value of this field is read-only. This field displays the interface to which the access point is connected.
AP MAC Address	The value of this field is read-only. This field displays the MAC address of the access point.
IP Status	The value of this field is read-only. This field displays by which mechanism the access point has received its IP configuration. Possible values are: ■ *unknown*: The information cannot be collected from the access point. ■ *static*: The IP configuration was carried out manually. ■ *DHCP Lease*: The IP configuration was established by DHCP. ■ *DHCP Failed:* IP configuration by DHCP has failed and a fallback IP configuration is used.
Operation	The value of this field is read-only. This field displays the operation that is currently carried out, it is updated depending on the operation state, when you hit ***REFRESH***. Possible values are: ■ *none*: No operation is currently running. ■ *set in progress*: A "set" operation is running, i.e. parameters are being configured on the access point.

Field	Description
Result	The value of this field is read-only. This field displays the result of a "set" operation. Possible values are: ■ *no Error*: The access point has reported success or has not been configured yet. ■ *no Reply*: The access point has not replied. ■ *Access denied*: The access point has reported an authorization failure. ■ *invalid IP parameters*: There is a problem with the intended IP parameters (IP address, netmask or gateway address). ■ *Dest. unreachable*: The acces point cannot be reached because of internal reasons (e.g. the interface the access point is connected to is down). A set request cannot be sent to the access point. ■ *other AP error*: The access point replies with an unexpected or unspecific error to the set request. ■ *internal Error*: A gateway internal problem has prevented the set operation.
Last Change	The value of this field is read-only. This field displays the date and time when the access point has been discovered or has last been configured.
Node Name	Here you can change the name of the discovered access point.
IP Address	Here you can change the IP address of the discovered access point.

Field	Description
Netmask	Here you can change the netmask of the discovered access point.
Gateway Address	Here you can change the gateway address of the discovered access point.
Admin. Password	Here you must enter the admin password of the access point. Otherwise the set operation cannot be carried out.

Table 2-6: ***External Systems*** ➜ ***Artem Access Point Discovery/Configuration*** ➜ ***View/Configure*** ➜ ***EDIT***

After starting the set operation with the SET button, the help line displays the message `Set in progress...` and the value of ***Operation*** changes to *set in progress*. To view the result of the set request, hit REFRESH: ***Operation*** will change back to *none* and ***Result*** will display the outcome of the set request.

2.4 New IPSec Peer Type

In order to allow more than one IPSec partner to connect on an IPSec gateway using one and the same peer configuration on the gateway, System Software 7.1.12 introduces a "dynamic peer".

By means of a special peer configuration, a number of clients can connect to an IPSec gateway using the same peer configuration on the gateway. A single parameter determines if a peer is treated as a dynamic peer or not: ***IPSec*** ➜ ***Configure Peers*** ➜ ***APPEND/EDIT*** ➜ ***Peer specific Settings*** now offers the parameter ***Special Peer Type***. It can assume two values: *None* (default value) and *Dynamic Client*.

Apart from specifying *Dynamic Client* when configuring a peer for the use as a dynamic peer a number of points have to be considered:

- The dynamic peer configuration on the gateway must not specify a peer ID or a peer IP address.
  Clients connecting to the gateway, however, must have a peer ID specified

in the client peer configuration, since the ID is still used to differentiate the tunnels created via the dynamic peer.

- The resulting gateway peer would match all incoming tunnel requests. It is, therefore, essential to put it at the end of the IPSec peer list on the gateway. Otherwise all peers that follow the dynamic peer in the peer list would be inactive.

This means that ***IPSEC* ➜ *CONFIGURE PEERS* ➜ *ADD/EDIT***: ***PEER ADDRESS*** and ***PEER IDS*** have to remain void when configuring a dynamic peer.

The gateway handles requests that match the dynamic peer as follows:

- Whenever an incoming IKE request matches a peer which has ***SPECIAL PEER TYPE*** set to *Dynamic Client*, the peer entry is duplicated and a temporary peer is created.
- The peer ID of the new peer is set to the ID of the connecting client.
- The peer type of the newly created (temporary) peer is set to *fixed* in the MIB tables.
- The peer priority is set to a value that assures that the temporary peer is treated with a higher priority than other peers, including the parent dynamic peer. This makes sure that the connecting client is definitely associated with the temporary peer.
- Depending on the the dynamic peer's setting for ***VIRTUAL INTERFACE***, the following settings are created:
  - For ***VIRTUAL INTERFACE***: *yes* - A host route is created for the temporary peer with the connecting client's Phase 1 IP address as destination.
  - For ***VIRTUAL INTERFACE***: *no* - The traffic list entries associated with the dynamic peer are copied to the temporary peer's traffic list.

After the new peer and its traffic list entries or route respectively have been created, IPSec processing continues in the same way as with a fixed IPSec peer.

Attention!

As, in this case, there is no difference between the client configurations, all clients use the same authentication information.

With Preshared Key authentication, this may be a problem, since authentication information is symmetric, i.e. both sides (client and gateway) use the same secret. If only a single client's configuration is compromised, the authentication data of the entire infrastructure based on the dynamic peer is known to a potential intruder.

We, therefore, strongly advise against using Preshared Key authentication with dynamic peers.

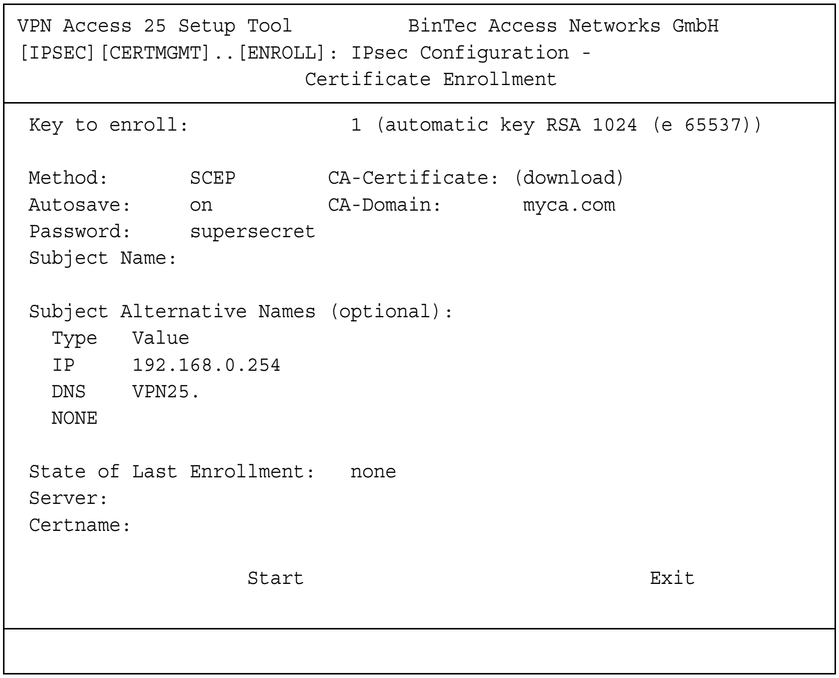
2.5 Support for Registration Authority Certificates

System Software 7.1.12 adds support for Registration Authority Certificates for SCEP. This facilitates SCEP controlled certification, since all Certificate Authorities that use RAs for the administration of certificate requests are supported by our SCEP implementation.

In general, if a CA manages certificate requests by means of a separate RA, the client (in this case the Bintec gateway) needs to know which certificates to use for communication with the RA.

RA certificates may either be automatically detected by the gateway (***CA-Certificate*** = *(download)*) or specified manually (select required data in ***CA-Certificate***).

Specification of RA certificates applies to SCEP governed certificate enrollment only, so the relevant configuration options are in the ***IPSec* ➜ *Certificate and Key Management* ➜ *Key Management* ➜ *REQUEST CERT*** menu:

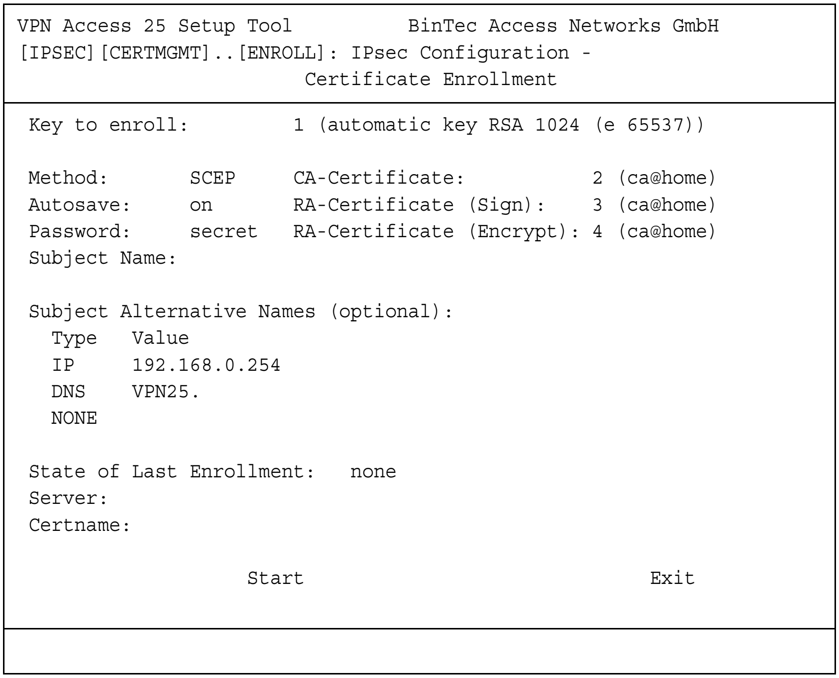


```
VPN Access 25 Setup Tool          BinTec Access Networks GmbH
[IPSEC][CERTMGMT]..[ENROLL]: IPsec Configuration -
                         Certificate Enrollment

 Key to enroll:             1 (automatic key RSA 1024 (e 65537))

 Method:       SCEP        CA-Certificate: (download)
 Autosave:     on          CA-Domain:       myca.com
 Password:     supersecret
 Subject Name:

 Subject Alternative Names (optional):
   Type   Value
   IP     192.168.0.254
   DNS    VPN25.
   NONE

 State of Last Enrollment:   none
 Server:
 Certname:

                   Start                             Exit
```

Note that *SCEP* must be selected for ***METHOD*** to access the options for RA certificate configuration.

As long as the CA Certificate is to be downloaded *(download)*, there are still no changes to the menu, since all possibly relevant certificates are automatically extracted from the certificate chain.

If, however, a certificate already installed on the gateway is specified as CA certificate, the menu changes (the screenshot shows example values):



```
VPN Access 25 Setup Tool          BinTec Access Networks GmbH
[IPSEC][CERTMGMT]..[ENROLL]: IPsec Configuration -
                         Certificate Enrollment

 Key to enroll:         1 (automatic key RSA 1024 (e 65537))

 Method:       SCEP     CA-Certificate:           2 (ca@home)
 Autosave:     on       RA-Certificate (Sign):    3 (ca@home)
 Password:     secret   RA-Certificate (Encrypt): 4 (ca@home)
 Subject Name:

 Subject Alternative Names (optional):
   Type   Value
   IP     192.168.0.254
   DNS    VPN25.
   NONE

 State of Last Enrollment:   none
 Server:
 Certname:

                    Start                              Exit

```

The menu now contains the following additional fields:

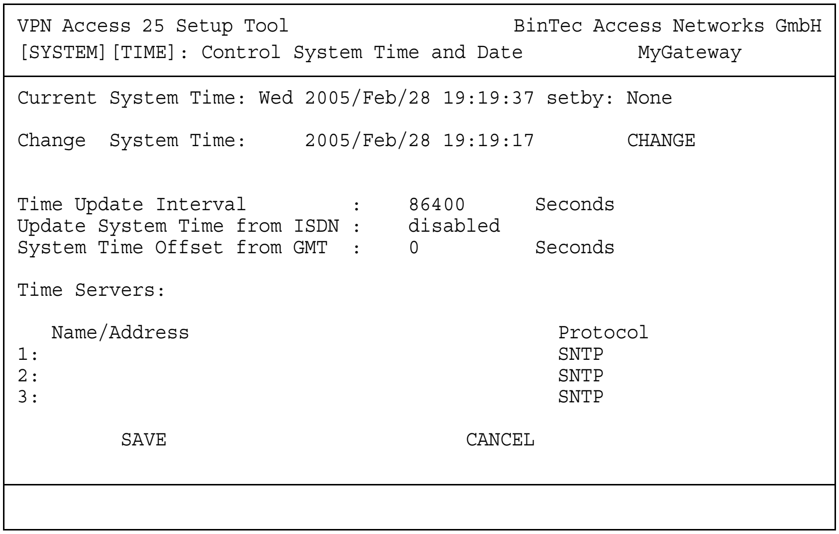
Field	Description
RA-Certificate (Sign)	Only if ***CA-CERTIFICATE*** is not = *(download)*. Here you can choose a certificate to use for signing the communication with the RA. The default is to use the CA certificate here.

Field	Description
RA-Certificate (Encrypt)	Only if ***RA-Certificate (Sign)*** is not = *(use CA cert)*. If you specify a discrete certificate for signing the communication with the RA, you get the option to specify another certificate for encrypting the communication. The default is to use the same certificate as used for signing, but you can choose any other certificate installed on the gateway.

2.6 New Time Synchronization Options

The options for retrieving the system time of the gateway from different sources have been considerably expanded to allow for 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***):



```
VPN Access 25 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 7.1.12** 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*.
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.

Field	Description
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 2-7: ***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.**

2.7 Continuous Ping

Before System Software 7.1.12, the ping daemon could be used only for a limited number of echo requests (between 1 and 65535). This has been changed so that a continuous ping can be sent to a remote host.

Note

Note that the ping daemon is not identical with the ping command you can use from the SNMP shell. The ping daemon is configured through entries in the ***BIBOPINGTABLE*** and runs in the background only.

To configure the ping daemon to send a continuous ping, the variable ***BIBOPINGPACKETCOUNT*** can now assume the value *0*. This will set the ping count to "unlimited".

2.8 Jitter Daemon

System Software 7.1.12 includes a Jitter Daemon.

In order to calculate the "jitter" (the variance in the round trip time between two hosts), ICMP Echo Requests are sent by the gateway to a certain remote host.

The configuration of this feature is not supported by the Setup Tool. You can find information on the available configuration parameters in the **MIB Reference** for **System Software 7.1.12**, section **IP**: ***BIBOJITTERADMINTABLE***, ***BIBOJITTERCTRLTABLE*** and ***BIBOJITTERSTATSTABLE***.

2.9 ATM QoS - VBR 3

ATM QoS offers a number of service categories according to which traffic shaping is performed. System Software 7.1.12 introduces support for the VBR.3 category.

VBR.3 changes the original behavior of VBR.1 in that it adds Best Effort Scheduling by CLP (Cell Loss Priority) Tagging.

Note

Information on the ATM QoS service categories can be found in the **Release Notes 7.1.1** which are available for download from www.bintec.net.

VBR.3 implies the following behavior:

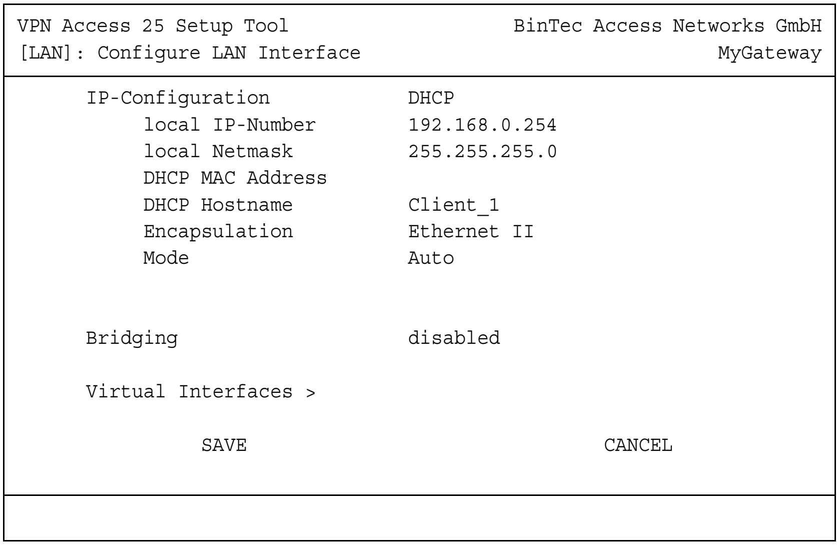
Using the traffic parameters PCR (Peak Cell Rate), SCR (Sustainable Cell Rate) and MBS (Maximum Burst Size) as limiting factors, the gateway transmits all traffic that lies within the limits of the traffic contract with the CLP flag set to *0*, i.e. the ATM cells are not flagged for potential discarding by the ATM network connected to the gateway. Any traffic that exceeds the PCR is discarded by the gateway itself while traffic exceeding <SCR+MBS> have the CLP flag set to *1*, i.e. they may be discarded by the ATM network connected to the gateway.

To apply VBR.3 to an ATM profile (determined by a combination of VCI and VPI) you can choose the option *Variable Bit Rate (VBR.3)* for ***ATM*** ➜ ***ATM QoS*** ➜ ***ADD/EDIT***: ***ATM SERVICE CATEGORY***.

2.10 DHCP Hostname

Some ISPs require that DHCP messages sent by the client contain a host name (DHCP option 12). Without this host name being transferred, no IP address is assigned to the client. System Software 7.1.12 meets this requirement.

The Setup Tool menu for the configuration of an Ethernet interface has been changed accordingly. If ***IP-CONFIGURATION*** is set to *DHCP*, the field ***DHCP HOSTNAME*** is displayed (the screenshot shows example values):



```
VPN Access 25 Setup Tool                           BinTec Access Networks GmbH
[LAN]: Configure LAN Interface                                       MyGateway

      IP-Configuration            DHCP
           local IP-Number        192.168.0.254
           local Netmask          255.255.255.0
           DHCP MAC Address
           DHCP Hostname          Client_1
           Encapsulation          Ethernet II
           Mode                   Auto


      Bridging                    disabled

      Virtual Interfaces >

                SAVE                                CANCEL
```

In this field you can enter the host name required by the ISP. The maximum length of the entry is 45 characters.

2.11 HTML Wizard Rerun

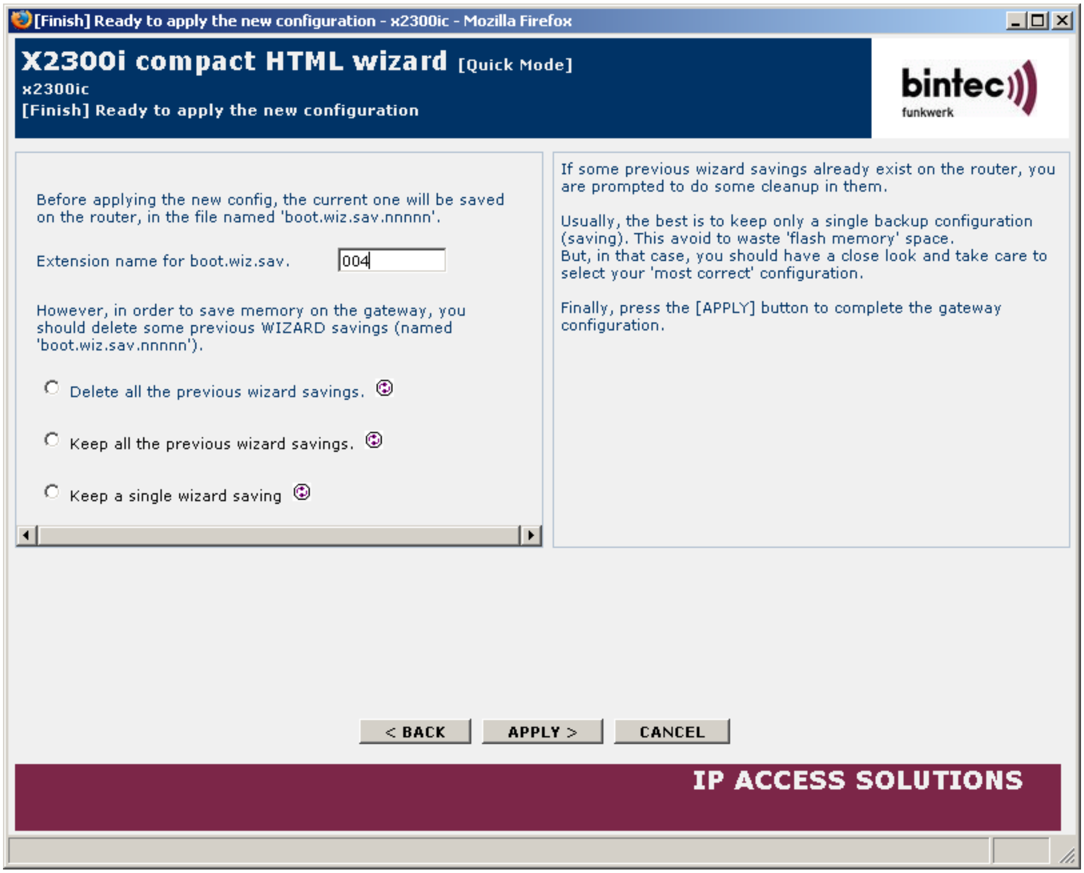
Up to now it was not possible to use a Wizard configuration already stored on the gateway as a template for a rerun of the HTML Wizard. Every time the HTML Wizard was run, it ignored the parameters of an already existing configuration. System Software 7.1.12 introduces a HTML Wizard "rerun" which allows keeping certain parameters of an earlier Wizard configuration while changing others.

At the end of each wizard run you are now prompted to specify an extension for the file the old wizard configuration will be saved to in the Flash ROM. It is possible to store any number of wizard configurations, but note that Flash ROM space is limited. Since the wizard uses only the most recent among the saved configurations as a basis for a rerun (there is no choice among configurations), it is not reasonable to store any greater number of configurations.

Note

Note that the extension you choose for a configuration does not influence the choice the wizard makes in terms of which configuration it chooses as the basis for a rerun. It always chooses the most recent configuration.

The prompt for saving the previous configuration looks like this:



[Finish] Ready to apply the new configuration - x2300ic - Mozilla Firefox

X2300i compact HTML wizard [Quick Mode]
x2300ic
[Finish] Ready to apply the new configuration

Before applying the new config, the current one will be saved on the router, in the file named 'boot.wiz.sav.nnnnn'.

Extension name for boot.wiz.sav. 004

However, in order to save memory on the gateway, you should delete some previous WIZARD savings (named 'boot.wiz.sav.nnnnn').

○ Delete all the previous wizard savings.

○ Keep all the previous wizard savings.

○ Keep a single wizard saving

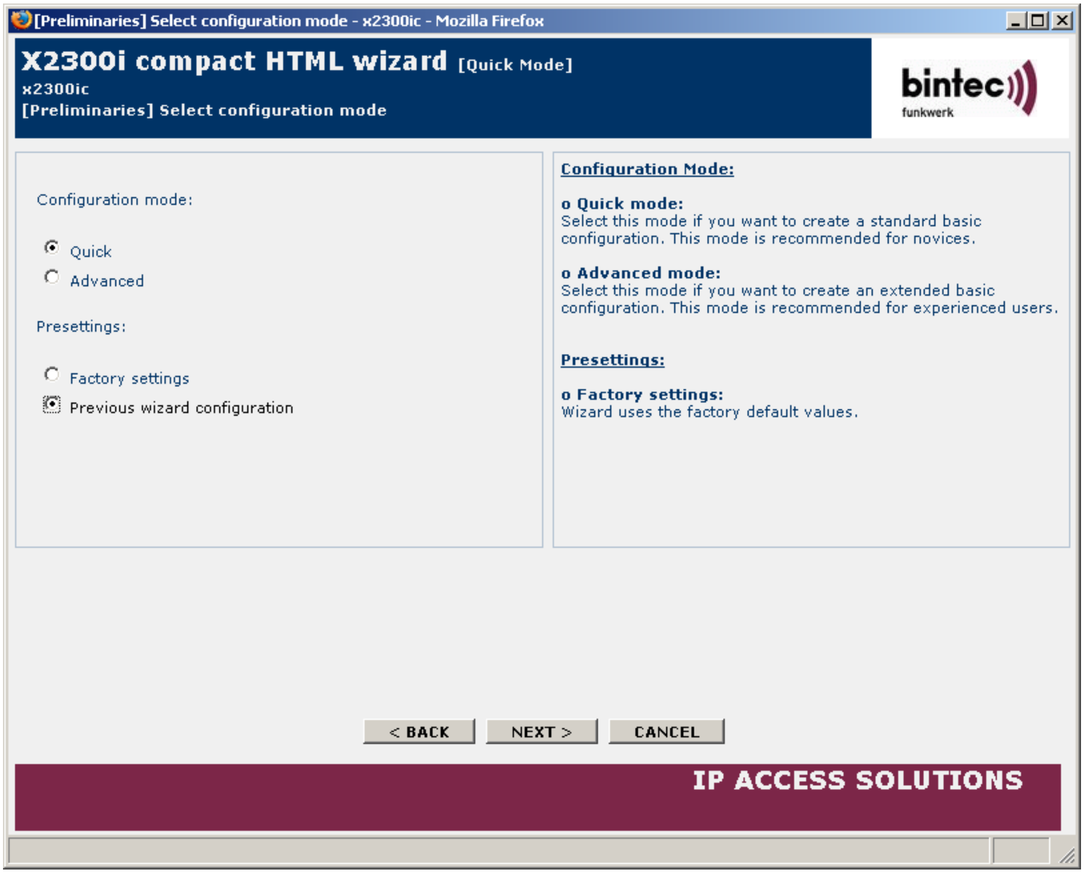
If some previous wizard savings already exist on the router, you are prompted to do some cleanup in them.

Usually, the best is to keep only a single backup configuration (saving). This avoid to waste 'flash memory' space.
But, in that case, you should have a close look and take care to select your 'most correct' configuration.

Finally, press the [APPLY] button to complete the gateway configuration.

Figure 2-1: HTML Wizard prompt for configuration saving options

If you now restart the HTML Wizard, you will be prompted to choose whether the wizard is to start assuming only factory settings or if it is to use the settings made during the last wizard configuration:



[Preliminaries] Select configuration mode - x2300ic - Mozilla Firefox

X2300i compact HTML wizard [Quick Mode]
x2300ic
[Preliminaries] Select configuration mode

Configuration mode:

● Quick
○ Advanced

Presettings:

○ Factory settings
● Previous wizard configuration

Configuration Mode:

o Quick mode:
Select this mode if you want to create a standard basic configuration. This mode is recommended for novices.

o Advanced mode:
Select this mode if you want to create an extended basic configuration. This mode is recommended for experienced users.

Presettings:

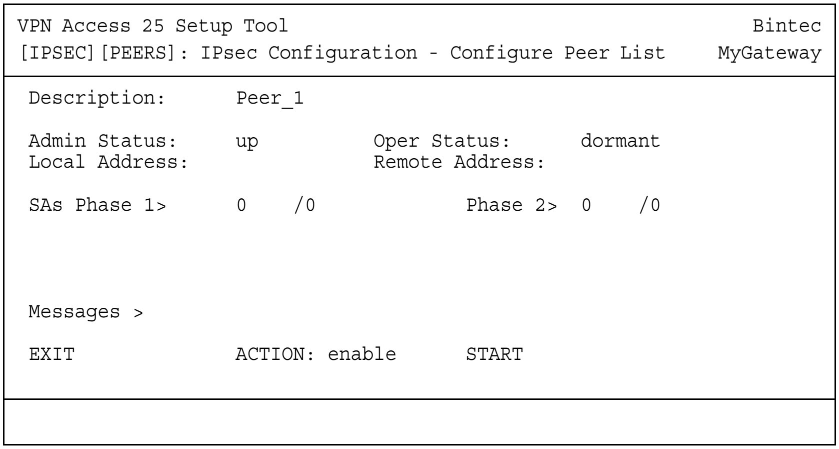
o Factory settings:
Wizard uses the factory default values.

Figure 2-2: HTML Wizard configuration choices

2.12 IPSec Peer Monitoring

The IPSec menus have been enhanced by detailed monitoring functions.

The monitoring menu is accessible by highlighting a peer in the peer list (***IPSec* → *Configure Peers***) an pressing "M" (must be a capital "M"). The monitoring menu looks as follows:



```
VPN Access 25 Setup Tool                                         Bintec
[IPSEC][PEERS]: IPsec Configuration - Configure Peer List     MyGateway

 Description:      Peer_1

 Admin Status:     up           Oper Status:      dormant
 Local Address:                 Remote Address:

 SAs Phase 1>      0    /0              Phase 2>  0    /0



 Messages >

 EXIT              ACTION: enable      START
```

The menu contains the following fields:

Field	Description
Description	Here the description of the monitored peer is displayed.
Admin Status	Here the ***Admin Status*** of the monitored peer is displayed.
Oper Status	Here the ***Oper Status*** of the monitored peer is displayed. This is the actual operational status of the peer.
Local Address	The local IP address of the IPSec tunnel is only displayed if it is actually available, i.e. if it is either statically configured or if the IPSec tunnel is already established.
Remote Address	The IP address of the remote peer is only displayed if it is actually available, i.e. if it is either statically configured or if the IPSec tunnel is already established.

Field	Description
SAs Phase 1	Here the number of Phase 1 SAs is displayed (in the form <*established*>/<*total*>). Highlighting ***PHASE 1*** an pressing enter allows access to a more detailed Phase 1 monitoring menu.
SAs Phase 2	Here the number of Phase 2 SAs is displayed (<*established*>/<*total*>). Highlighting ***PHASE 2*** an pressing enter allows access to a more detailed Phase 1 monitoring menu.
ACTION	Here you can perform a number of actions affecting the connection status of the peer. Available actions are: ■ *reset* - Sets the peers Admin Status to *down*, waits for the peers Oper Status to reach the state *down* and then resets the peers Admin Status to *up* again. ■ *enable* - Sets the peers Admin Status to *up.* ■ *disable* - Sets the peers Admin Status to *down*. ■ *set up* - Sets the peers Admin Status to *dialup*, which triggers the establishment of a Phase 1 SA for the tunnel.

Table 2-8: ***IPSEC → CONFIGURE PEERS → MONITORING MENU***

The ***PHASE 1>*** submenu link leads to the IKE SA monitoring list menu, which displays the IKE SAs for the peer currently monitored only. SAs for other peers may show up in the list as long as the remote ID is not known for those SAs yet. As soon as the remote ID is known, these SAs are deleted from this peer's view.

The ***PHASE 2>*** submenu link leads to the IPSec bundle list monitoring menu, which then displays only the bundles of the peer currently monitored.

The ***MESSAGES* >** submenu link leads to the message monitoring menu. It is initialized with a filter of "*peer {0}{<idx>}* ", where *<idx>* is the index of the peer currently monitored. Note that the space at the end of the filter is important, since otherwise all peers will match the filter. This means, that all messages regarding this peer and all messages for unknown peers (index *0*) are displayed. To suppress the messages for unknown peers, replace the filter with "*peer <idx>*".

2.13 New X.25 Features

Our X.25 implementation has been enhanced by a number of features such as the conversion of X.25 calls to TCP calls (X.25 to TCP Gateway) or sending X.25 data across TCP networks (XoT).

You can find information on the newly implemented features in the solution area of www.bintec.net.

Please note the change in license policy concerning X.25 described in “License Needed for X.25” on page 44.

3 Changes

The following changes have been made to enhance the functionality of your gateway:

3.1 IPSec Changes

3.1.1 License for IP Address Transfer via ISDN

The ability to transfer dynamically assigned IP addresses of IPSec peers using the ISDN B- or D-channel had to be removed from our system software in release 7.1.10. After careful investigation of the underlying patent issues, we are now able to offer this function again.

To enable the transfer of IP addresses in the ISDN B- or D-channel, you need to obtain a free license from the Service/Support section of our website at www.bintec.net. The licensing mechanism will soon be available, and it will work in the same way as the mechanism we use for issuing STAC/MPPC licenses. Please note that the license is free for you.

Information on how to install the license is available in the chapter "Licenses" of the **Bintec User's Guide**.

3.1.2 Filter in Messages Menu

The menu ***MONITORING AND DEBUGGING*** ➜ ***MESSAGES*** now offers the possibility to filter the displayed syslog messages. You can enter any string into the field ***FILTER***, and only such messages that contain the specified string are displayed in the message display area above. A wildcard (*) is implicitly assumed so that all messages that contain the specified string as a substring are displayed, too.

3.1.3 Wildcards and Empty Numbers in IPSec Callback

Before **System Software 7.1.12** it was not possible to enter wildcards for the ISDN number of an IPSec callback. Nor was it possible to leave ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***IPSEC CALLBACK***: ***INCOMING ISDN NUMBER*** completely empty.

3.2 License Needed for X.25

X.25 has been available without the need for a software license on gateways of the X-Generation Family. This has been changed, and as of **System Software**

7.1.12 a software license must be purchased and installed in order to make use of X.25.

Note

If you are updating from an older release to **System Software 7.1.12**, and have purchased the respective license, it is a good idea to install the license before you actually perform the update. This ensures that all X.25 functions will be available again immediately after the update.

3.3 Ping Daemon Available in All Products

With **System Software 7.1.12**, the Ping Daemon is available in all of our products that can be updated to this release.

Note

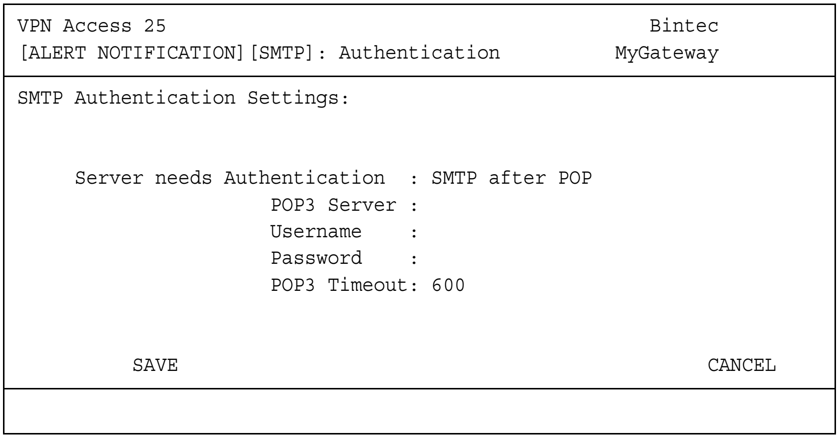
Note that the ping daemon is not identical with the ping command you can use from the SNMP shell. The ping daemon is configured through entries in the ***BIBOPINGTABLE*** and runs in the background only.

3.4 TAF Support Discontinued

Support for TAF (Token Authentication Firewall) is being discontinued as of **System Software 7.1.12**.

3.5 SMTP Authentication Support for Email Alert

Before **System Software 7.1.12** SMTP authentication was not supported by Email Alert. This has been changed and authentication can be configured in a newly created submenu (***MONITORING AND DEBUGGING*** ➜ ***EMAIL ALERT*** ➜ ***AUTHENTICATION SETTINGS***):



```
VPN Access 25                                                 Bintec
[ALERT NOTIFICATION][SMTP]: Authentication                 MyGateway

SMTP Authentication Settings:


     Server needs Authentication  : SMTP after POP
                      POP3 Server :
                      Username    :
                      Password    :
                      POP3 Timeout: 600


          SAVE                                                    CANCEL
```

The menu offers the following options:

Field	Value
Server needs Authentication	Here you choose the desired SMTP authentication. Available choices are: ■ *none* (default value) ■ *Enhanced SMTP* ■ *SMTP after POP.*
Username	For *Enhanced SMTP* authentication: this is the user name you use to directly login to the SMTP server. For *SMTP after POP* this is the user name you use to login to the POP3 server.
Password	For *Enhanced SMTP* authentication: this is the password you use to directly login to the SMTP server. For *SMTP after POP* this is the password you use to login to the POP3 server.

Field	Value
POP3 Server	Here you enter the domain name of the POP3 server that will leverage the authentication to the SMTP server.
POP3 Timeout	Here you enter a timeout after which the authentication is considered invalid and is repeated. Possible values are *60* to *3600* seconds, default is *600*.

Table 3-1: ***MONITORING AND DEBUGGING* ➔ *EMAIL ALERT* ➔ *AUTHENTICATION SETTINGS***

3.6 LOCAL Interface Enabled for OSPF and Routing

Routes bound to the LOCAL interface were not considered for routing, nor were they distributed by OSPF. This has been changed, and the local interface is now available for route definition as well as for OSPF.

3.7 SDSL Firmware as Discrete File

Up to now, the SDSL logic needed to connect an **X2400** gateway to an SDSL network was part of the system software for all **X2000** Family gateways. This has been changed, and like the ADSL logic the SDSL logic is now available as a discrete logic file which can be handled independently of the system software proper.

With the SDSL logic removed from the system software, it is now possible to update it independently from the system software and avoid risks like, e.g. incompatible configurations that may arise with an update of the system software. Moreover, the change saves valuable space in the Flash ROM of **X2300** Family gateways, since there the SDSL logic is not required. With the growing scope of features supported by our software, this warrants the possibility of future upgrades for **X2300** family gateways.

Note that after updating an **X2400** gateway to **System Software 7.1.12**, your gateway will lack the SDSL logic if you do not install it. In this state, SDSL connections are not possible. Installing the necessary SDSL logic is described in a "How to..." which you can find in the same ZIP file as **System Software 7.1.12** and which is also available for download from the same location as **System Software 7.1.12**.

3.8 Configurable Timeout for HTML Wizard Sessions

Up to now a HTML Wizard session timed out after a comparatively short time of inactivity. **System Software 7.1.12** introduces a configurable inactivity timer.

By calling the HTML Wizard with the URL http://<gateway IP address>/wizard?inactivity=<timeout in seconds> you can now configure the inactivity timeout according to your needs.

3.9 HTML Wizard NAT Settings

Up to now, the HTML Wizard created internet WAN Partners with the silent deny option for network address translation (NAT) disabled. This has been changed.

The Wizard now creates an internet WAN Partner with silent deny enabled, since this offers additional protection against attacks from the Internet.

3.10 SSHD Monitoring Added

The SSHD monitoring menu was missing from ***MONITORING AND DEBUGGING***. It has been added in order to unify access to monitoring options.

3.11 Default Setting for Classification and Signalling

The default value suggested in ***QoS* ➜ *IP Classification and Signalling* ➜ *ADD*** has been changed from *classify & set TOS M* to *classify (keep TOS) M* since that is the setting most often used.

3.12 Latency Reduced for PPP Dial Out Failures

Before **System Software 7.1.12**, a PPP interface was not set into a "blocked" state immediately after ***biboPPPMaxRetries*** +1 subsequent dialout attempt failures. Furthermore, there was a short delay caused by the retry timer started after each attempt.

The behavior has been changed to minimize the latency of blocking an interface. This will enhance the responsiveness to conditions that require rerouting the data traffic via a backup interface.

3.13 DOVB 64 kbps Supported

DOVB 64 kbps can now be choosen as ***Layer 1 Protocol*** when configuring a WAN Partner.

4 Solved Problems

The following problems that could occur with earlier versions of our system software have been solved in System Software 7.1.12:

- "HTML Wizard - Various Improvements" on page 52
- "IPSec - Various Improvements" on page 53
- "BRRP - Various Improvements" on page 54
- "VLAN - Various Improvements" on page 55
- "DHCP - Various Improvements" on page 56
- "QoS - Stack Trace with WFQ" on page 57
- "Setup Tool - PPP Blocktime Takes Undesirable Values" on page 57
- "Setup Tool - Organization of QoS Menu" on page 57
- "Setup Tool - Misplaced Description in Load Balancing Menu" on page 58
- "LCP - Two-Phase Negotiation Leads to Wrong Encapsulation" on page 58
- "Setup Tool - Typo Corrected" on page 58
- "QoS - Problems with X8E-SYNC" on page 59
- "SNMP - Read Community Deleted" on page 59
- "Load Balancing - Wrong Session Count on IPSec Interfaces" on page 59
- "RIP - TOS Tagging not Possible" on page 59
- "PPP - Obsolete Entries in pppSessionTable" on page 60
- "X8500 - PCI Error" on page 60
- "PPP - Connection Reject" on page 60
- "IP Filters - Port Specification Imprecise" on page 61
- "ARP - Wrong ARP Tell" on page 61

4.1 HTML Wizard - Various Improvements

4.1.1 Misleading Error Message

ID 3360

When configuring Internet access with Internet Service Provider = T-Online (applicable to use in Germany only), you were asked for your "Anschlusskennung". If you did not confirm your entry correctly, an error message is displayed that your "password" has not been confirmed correctly, even though the "Anschlusskennung" is not a password.

This problem has been solved.

4.1.2 CLID Configuration

(ID n/a)

When activating CLID (Calling Line Identification) in a LAN-LAN connection, the field for specifying the WAN partner’s MSN was initially blank. The configuration could be saved, however, resulting in a disfunctional CLID configuration.

The behavior has been changed so that the HTML Wizard assumes the previously configured WAN Partner Number, omitting any initial "0". Users can change that setting, but the configuration can no longer be saved without a CLID number.

4.1.3 Useless Option Removed

When configuring a DSL WAN partner with the T-Online preset, users could choose between a PPPoE and a PPTP connection. This choice is unnecessary, since T-Online does not currently offer DSL over PPTP connections.

This problem has been solved.

4.2 IPSec - Various Improvements

4.2.1 QoS Classification Fails

ID 3401

The high priority classification of a QoS configuration failed if hardware acceleration was used.

This problem has been solved.

4.2.2 Dead IPSec Peers

ID 3469

If neither an IP address nor IPSec Callback was configured for an interface peer, no tunnel was actually established. The value of ***IPSECPEEROPERSTATUS*** never changed from *dormant* to *up*.

This problem has been solved.

4.2.3 IPSec Callback Cannot be Disabled

(ID 3528)

If ISDN callback has been configured for a peer, it is impossible to disable it again using the Setup Tool. Similarly, the Setup Tool IPSec Wizard sets a peer's callback settings to *passive* if *both* has been selected in the respective submenu.

This problem has been solved.

4.2.4 Hardware Encryption too Slow

ID n/a

The overall performance of hardware supported encryption on VPN Access 100 has been optimized.

4.2.5 IPSec Debug Output Crashed Gateway

(ID n/a)

If IPSec debug output was enabled or IPSec cache or traffic list entries were dumped, the gateway rebooted.

This problem has been solved.

4.3 BRRP - Various Improvements

ID n/a

Fine tuning the BRRP implementation has resulted in a significant enhancement of performance and ease of use:

- The configuration of tasks for synchronous operation of multiple virtual routers has been simplified.
- Differing internal states between the virtual routers connected by task definitions are avoided.
- BRRP now uses its own syslog subject ("BRRP").

4.4 VLAN - Various Improvements

4.4.1 Setup Tool - Deleting Interface Does not Clear Route Table

ID 2720

Creating a virtual interface in the Setup Tool also created a network route within the ***IPROUTETABLE***. Deleting a virtual interface (again in the Setup Tool) cleared e.g. the ***IFTABLE*** again, but did not delete the respective route entry.

This problem has been solved.

4.4.2 Setup Tool - Virtual Interface IP Addresses Deleted

ID 2908 and 3397

Confirming the configuration of an Ethernet interface with ***SAVE*** deleted the IP addresses of all virtual interfaces that have been configured for that Ethernet interface.

This problem has been solved.

4.4.3 Setup Tool - VLAN Configuration for Physical Interface Cannot be Saved

ID 2909

The configuration window for a physical Ethernet interface offered the options *VLAN* for the field IP-Configuration and accordingly the specification of a ***VLAN ID***. If an Ethernet interface was configured in this way, however, the settings were lost upon confirming the configuration with ***SAVE***.

If the same configuration parameters were passed to the MIB on the SNMP shell, the router panicked and rebooted.

This problem has been solved.

4.4.4 Setup Tool - MAC Address not saved

ID 2910

If you specified a MAC address during Ethernet configuration, the MAC address seemed to be saved when confirming with ***SAVE*** (upon re-entering the MAC address was still visible). It was, however, never saved to the MIB so that after quitting the Setup Tool and then re-entering the respective menu, the MAC address was gone and the ***IFTABLE*** did not show any newly configured MAC address.

This problem has been solved.

4.4.5 Setup Tool - Panic after VLAN Configuration

ID 3392

After performing a VLAN configuration, the gateway occasionally panicked and rebooted.

This problem has been solved.

4.5 DHCP - Various Improvements

Our DHCP implementation has undergone thorough maintenance, resulting in better performance and error avoidance. Additionally, the following problem has been solved:

4.5.1 Stacktrace after Failed IP Address Check

ID 2586 and 2824

Before the DHCP server assigns an IP address lease to a client, it checks whether this IP address is already used by another host by means of a ping. If there was an answer to the ping, i.e. if the check failed, a stacktrace was caused. The same situation could be caused by enforcing a DHCP renew from the host side.

4.6 QoS - Stack Trace with WFQ

(ID n/a)

Using WFQ (Weighted Fair Queuing) in a QoS configuration, sporadically resulted in stack traces.

This problem has been solved.

4.7 Setup Tool - PPP Blocktime Takes Undesirable Values

ID 2987

The SNMP shell as well as the Setup Tool allowed assigning very low and even negative values to the variable ***BIBOPPPBLOCKTIME***. Negative values have the effect of a very long blocktime (depending of the value entered), and very small values (e.g. < 5 sec.) may lead to problems if callback is enabled.

This has been changed: the problematic values can no longer be entered.

4.8 Setup Tool - Organization of QoS Menu

ID 3001

The layout of the menu ***QOS*** ➜ ***IP CLASSIFICATION AND SIGNALLING*** has been changed to provide a better overview of the filters already configured. Formerly, some of the filter parameters eventually were not visible.

4.9 Setup Tool - Misplaced Description in Load Balancing Menu

ID 3176

In the list view of the menu ***BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)* ➜ *IP LOAD BALANCING OVER MULTIPLE INTERFACES***, entries in the column ***DESCRIPTION*** are unintentionally indented.

This problem has been solved.

4.10 LCP - Two-Phase Negotiation Leads to Wrong Encapsulation

ID 3303

Channel bundling could fail (no data were transferred) if the remote side used a two phase authentication procedure in which the remote endpoints provide different options for Address Field Compression during LCP (Link Control Protocol) negotiation.

This problem has been solved.

4.11 Setup Tool - Typo Corrected

ID 3405

In the menu ***WAN PARTNER* ➜ *ADVANCED SETTINGS*** the was a typo in the available options for the parameter ***CALLBACK***.

This problem has been solved.

4.12 QoS - Problems with X8E-SYNC

(ID 3412)

When handling a high amount of traffic, a QoS configuration for priority queues with a bandwidth restriction was not working properly.

This problem has been solved.

4.13 SNMP - Read Community Deleted

ID 3474

Every login attempt for an account defined in ***biboAdmLoginTable*** caused the ***biboAdmReadCommunity*** to be changed to the empty string, i.e. the Read Community was deleted.

This problem has been solved.

4.14 Load Balancing - Wrong Session Count on IPSec Interfaces

(ID 3487)

Using the IP Load Balancing feature for IPSec interfaces could result in a wrong session count (as shown by ***ipLoadBIfTable***: ***ActAssignedSessions***).

This problem has been solved.

4.15 RIP - TOS Tagging not Possible

(ID 3491)

TOS signalling was not possible for locally generated RIP packets.

This problem has been solved.

4.16 PPP - Obsolete Entries in pppSessionTable

(ID 3515)

After disconnecting an incoming PPP call with inband authentication, the respective entry in the ***PPPSESSIONTABLE*** was not deleted. This could lead to a memory leak.

This problem has been solved.

4.17 X8500 - PCI Error

(ID 3562)

With X8A-SYS-VPN a PCI error message was displayed during booting if an X8E-2SYNC module was present. With an X8A-SYS board the gateway rebooted during the boot process.

This problem has been solved.

4.18 PPP - Connection Reject

(ID 3582)

An LCP Protocol-Reject was caused by an uncompressed Address Protocol header in the CHAP or PAP Authentication Response sent by the Bintec gateway. This was not RFC compliant.

This problem has been solved.

4.19 IP Filters - Port Specification Imprecise

(ID 3601)

In a number of contexts where IP filters are employed, ports could be specified for protocols other than TCP or UDP although the ports are considered for these protocols only. There was no hint that filter entries with protocol *any* and *any port* specified match for TCP or UDP packets only.

This problem has been solved: The port respective fields are now hidden for all protocols that do not support port specification.

4.20 ARP - Wrong ARP Tell

(ID 3671)

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

This problem has been solved.