VPN Access 250, VPN Access 1000, X8500

Release Notes
System Software 7.8.7

Version 1.0

Goal and Purpose

This document describes the new features, changes and bugfixes in **System Software 7.8.7**.

Liability

This document has been put together with the greatest possible care. 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 contained in this document is subject to change without notice. You can find additional information and changes at www.funkwerk-ec.com.

As multiprotocol gateways, Bintec gateways set up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. Funkwerk Enterprise Communications GmbH accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks

Bintec and the Bintec logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

The company and product names mentioned are usually trademarks of the companies or manufacturers concerned.

Copyright

Guidelines and Standards

Bintec gateways comply with the following guidelines and standards:

R&TTE Directive 1999/5/EC

CE symbol for all EU states

You can find further information in the declarations of conformity under www.funkwerk-ec.com.

How to reach Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

Funkwerk Enterprise Communications
6 Avenue de la Grande Lande - CS 20102
33173 Gradignan cedex
France

Telephone: +33 (0)1 61 37 32 76
Fax: +33 (0)1 61 38 15 51
Internet: www.funkwerk-ec.com

1 Important Information

Please read the following information about System Software 7.8.7 carefully to avoid problems when updating or using the software.

1.1 Applicability

System Software 7.8.7 is available only for the following devices and cannot be used on other devices:

- **VPN Access 250**
- **VPN Access 1000**
- **X8500**.

1.2 Incompatibility

Configurations created or saved with **System Software 7.8.7** may be incompatible with some versions of our system software.

Take note, however, of the following indications regarding the update and the possibilities of a downgrade.

1.2.1 Preparation and update

To prepare and carry out an update to **System Software 7.8.7**, proceed as follows:

1. Backup the current boot configuration. Use one of the following possibilities:
   a) In the SNMP shell, enter `cmd=save path=boot.alt`. This backs up the current boot configuration in the Flash ROM of your gateway under the name "boot.alt".
   b) On a computer on your LAN, start a TFTP server and export the current

boot configuration using the ***CONFIGURATION MANAGEMENT*** menu of the Set-up tool. To do this, select:

- ***OPERATION*** = *put (FLASH -> TFTP)*
- ***TFTP SERVER IP ADDRESS*** = *<IP address of the TFTP servers on the LAN>*
- ***TFTP FILE NAME*** = *boot.alt*
- ***NAME IN FLASH*** = *boot*

2. Carry out the update to **System Software 7.8.7** as usual and reboot the gateway.
   The gateway will start with the new software, the existing boot-configuration will be used.

1.2.2 Downgrade

If you wish to carry out a downgrade, proceed as follows:

1. Replace the current boot configuration with the previous backup version. Use one of the following possibilities:
   a) In the SNMP shell, enter `cmd=move path=boot.alt pathnew=boot`. This overwrites the current boot configuration with the previous backup version. The configuration named "boot.alt" is thereby deleted from the flash ROM (if you want to keep this in the flash, use `cmd=copy` instead of `cmd=move`).
   b) On a computer on your LAN, start a TFTP server and import the current boot configuration using the ***CONFIGURATION MANAGEMENT*** menu of the Set-up tool. To do this, select:
   - ***OPERATION*** = get (TFTP -> FLASH)
   - ***TFTP SERVER IP ADDRESS*** = *<IP address of the TFTP servers on the LAN>*
   - ***TFTP FILE NAME*** = *boot.alt*
   - ***NAME IN FLASH*** = *boot*
2. Carry out the downgrade to the desired software version.
3. Reboot the gateway. The device will start with the previously backed up boot configuration and the old version of the system software.

2 New Functions

System Software 7.8.7 includes a number of new functions that significantly extend the performance compared with System Software 7.4.1:

2.1 New Discovery Protocol

System Software 7.8.7 includes the new Discovery protocol SNMP Multicast.

The Dime Manager uses this protocol to locate Funkwerk devices within the network.

2.2 Software update and file transfer extended

In **System Software 7.8.7** you can use HTTP(S) and web server authentication for a software update or for the transfer of configuration files.

The standard format is used for the URL encoding:

http[s]://[<User Name>:<Password>@] <Host> [:<Port>]/<Path>/<File>

tftp://<Server>/<File>

You can use this information in the command line when updating and transferring a configuration file and in the corresponding field on the system maintenance page under *http://<IP address of your gateway>/maint*.

Note

Please note that the URL in the command line must be divided into two parts (*hosturl* and *file*) to define the file format (see example below).

You can only use the full URL in the new file format for system maintenance.

Software update

The following shows examples for entries, if a software update is carried out with the *update* command:

update http://server:8080/download/R232bw_bl7802.sx6

update https://server/download/R232bw_bl7802.sx6

update http://user:secret@server/download/R232bw_bl7802.sx6.

Configuration

Configuration files can exist in two different formats: the old unencrypted format and the new CSV format (see **Release Notes Systemsoftware 7.5.1**).

Note

Note that you should only use the new CSV format, as the file used in this format is smaller, can be encrypted if necessary and guarantees better compatibility between the various system software versions.

If you want to transfer the configuration files to a web server, which has the HTTP extension WEBDAV (PUT method), you must enter the following:

cmd=put_all hosturl="http://<Server>/<Path>" file="<config>.cf" (for the old format).

cmd=put_all hosturl="http://<Server>/<Path>" file=:"<config>.cf" (for the new CSV format, if to be used unencrypted)

cmd=put_all hosturl="http://<Server>/<Path>" file="<pwd>:<config>.cf" (for the new CSV format, if the data is to be encrypted with a password)

(<config> means that you must enter the name of the desired configuration file here without brackets.)

If you want to download configuration files from a web server, you must enter the following:

cmd=get_all hosturl="http://<Server>/<Path>" file="<config>.cf" (recognises old and new formats automatically)

cmd=get_all hosturl="http://<Server>/<Path>" file="<pwd>:<config>.cf" (downloads an encrypted file).

2.3 Query the BOSS minimum version

In **System Software 7.8.7** you can query the minimum BOSS version required for the correct operation of specific hardware. If a minimum version is specified, you will need this version or a later version.

To do this, enter *show rev* in the SNMP shell.

The following output is displayed (example):

```
Logic     : V.1.0
Bootmon   : V.7.8.2
BOSS      : V.7.8.2 IPSec from 2008/12/12 00:00:00
            (minimal version: 7.8.2)
```

The last row indicates the minimum version required.

Alternatively, you can query the minimum version with the update command.

To do this, enter *update -i* in the SNMP shell:

The following output is displayed:

Flash-ROM management shell

```
Flash-Sh >
```

Enter *info -m*.

If a minimum version is defined in the flash, the following output is displayed (example):

BOSS minimal version 7.8.2.

If no minimum version is defined, the following output is displayed:

BOSS minimal version: none specified.

2.4 Simple Network Time Protocol Server

System Software 7.8.7 supports the SNTP server function.

Previously, time requests sent by a client to the gateway remained unanswered. With the SNTP server function, the gateway has an internal time server and can send an answer to such client requests (time settings and other options).

You can configure the SNTP server function in the Setup tool, in the ***System*** ➜ ***Time and Date*** menu, in the new ***Internal Time Server*** field:

Parameter	Value
Internal Time Server	Determines whether the internal time server is to be used and, if so, in which mode. The following options are available: ■ *disabled* (default value): Time requests from a client are not answered. This is the same behaviour as in previous software versions. ■ *enabled*: Time requests from a client will be answered with the current system time. This is given as GMT, without offset. ■ *depends on client mode*: Client-requests are answered if the system time is derived from an NTP server or is acquired over ISDN.

Table 2-1: Additional field in the ***System*** ➜ ***Time and Date*** menu

Note

Note that, for the SNTP server function, the MIB variable *biboAdmNTPServer* is used, (not the MIB variable *biboAdmTimeServer*).

2.5 ISDN Theft Protection

From System Software 7.8.7, you can use the ISDN theft protection function to prevent a thief who has stolen a gateway from gaining access to the gateway owner's LAN. (Without theft protection, he could dial into the LAN by ISDN if the *ShortHold* = *-1* field setting is true.)

All interfaces for which the theft protection is enabled are administratively set to "down" when the gateway boots (i.e. MIB variable *AdminStatus* = *down)*.

The gateway then calls itself by ISDN and checks its location. If the configured ISDN call numbers differ from the numbers dialled, the interfaces remain disabled.

If the numbers agree, the device assumes that it is at the original location and the interfaces are administratively set to "up"(*AdminStatus* = *up*).

To reduce cost, the function uses the ISDN D channel.

Note

Note that the ISDN theft protection function is not available for Ethernet interfaces.

You can configure the ISDN theft protection function in the Setup tool, in the ***SECURITY*** ➜ ***ISDN THEFT PROTECTION*** menu.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[SECURITY][ITP]: ISDN theft protection
                                Main Configuration            MyGateway


            ISDN theft protection       disabled
            Number of retries           3
            Timeout (sec)               5
            Dial Number
            Incoming Number
            Outgoing Number

            Interfaces >



            SAVE                         CANCEL
```

The menu contains the following fields:

Parameter	Value
ISDN theft protection	Determines the status of the theft protection. ■ *disabled* (default value): Theft protection is not active. ■ *enabled*: Theft protection is active.
Number of retries	Number of dial attempts made by the gateway to call itself by ISDN. Possible values: *1* .. *255*.
Timeout (sec)	The time in seconds that the gateway waits before trying again after an unsuccessful attempt to call itself. Possible values: *2* .. *20*.
Dial Number	Subscriber number to be called.
Incoming Number	Subscriber number to be compared with the current calling party number.
Outgoing Number	Own subscriber number, i.e. the number to be set as calling party number.

Table 2-2: Fields in the ***SECURITY*** ➜ ***ISDN THEFT PROTECTION*** menu

Under ***SECURITY*** ➜ ***ISDN THEFT PROTECTION*** ➜ ***INTERFACES*** the interfaces are shown to which the theft protection is applied. The menu contains values by way of example; before configuration, the list is empty.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[SECURITY][ITP][ITP INTERFACES]: ITP Interface List           MyGateway


            Status          StartIndex          StopIndex

            enabled         10001               10015
            enabled         10018               10018
            disabled        10016               10017




          ADD                 DELETE              EXIT
```

Under ***SECURITY*** ➜ ***ISDN THEFT PROTECTION*** ➜ ***INTERFACES*** ➜ ***ADD/EDIT*** you can configure the theft protection for individual interfaces or groups of interfaces.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[SECURITY][ITP][ITP INTERFACES][IFC-EDIT]:
                                ITP Interface Edit Menu       MyGateway


            Status                  enabled
            Start IfIndex           0
            Stop IfIndex            0




             SAVE                   CANCEL
```

The menu contains the following fields:

Parameter	Value
Status	Determines whether the theft protection is switched on or off. Possible values: ■ *enabled* (default value): Theft protection is active (switched on) for the interface or group of interfaces. ■ *disabled* (default value): Theft protection is not active (switched off) for the interface or group of interfaces.
Start IfIndex	Determines the first interface of a group. If ***START IFINDEX*** and ***STOP IFINDEX*** are the same, a single interface is configured for theft protection.
Stop IfIndex	Determines the last interface of a group. If ***STARTINDEX*** and ***STOPINDEX*** are the same, a single interface is configured for theft protection.

Table 2-3: Fields in the ***SECURITY*** ➜ ***ISDN THEFT PROTECTION*** ➜ ***INTERFACES*** ➜ ***ADD/EDIT*** menu

2.6 IP address ranges (pools)

With System Software 7.8.7 your gateway supports central administration for dynamic IP address ranges (pools). The DHCP and PPP subsystems can share dynamic IP address ranges.

Address ranges are configured in the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ ***ADD/EDIT*** menu. Here you can create new ranges or modify existing ranges.

The ranges that are available are not dependent on the number addresses contained for all users.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[IP][DYNAMIC][POOL][ADD]: Define Range of IP Addresses        MyGateway


    Identifier                          0
    Description
    IP Address
    Number of Consecutive Addresses     1
    Primary Domain Name Server
    Secondary Domain Name Server


            SAVE                              CANCEL
```

The menu contains the following fields:

Parameter	Value
Identifier	Unique whole number used to identify the address range. Possible values: 0 .. *999*.
Description	Description of the address range. Maximum number of characters: *20*.
IP Address	First IP address in the address range.
Number of Consecutive Addresses	Total number of IP addresses in the address range, including the first IP address (***IP ADDRESS***). Possible values: *1* .. *254*. Default value: *1*. In earlier software versions addresses were assigned to specific clients using address ranges with a unique IP address (***NUMBER OF CONSECUTIVE ADDRESSES*** = *1)*. In **System Software 7.8.7** you can assign individual IP addresses in the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***ASSIGNED IP ADDRESSES*** ➜ ***ADD/EDIT*** menu (see Page 98).
Primary Domain Name Server	Here you can enter the IP address of a global Domain Name Server. If no value is entered, the setting used is taken from ***IP*** ➜ ***STATIC SETTINGS*** , if the field ***DHCP ASSIGNMENT*** = *global* is set in the ***IP*** ➜ ***DNS*** menu. If ***DHCP ASSIGNMENT*** = *self* is set for the field, the IP address of the gateway is sent to the client. If ***DHCP ASSIGNMENT*** = *none* is set, there is no ***PRIMARY DOMAIN NAME SERVER*** and no ***SECONDARY DOMAIN NAME SERVER*** available.

Parameter	Value
Secondary Domain Name Server	Here you can enter the IP address of an alternative Domain Name Server. If no value is entered, the setting used is taken from ***IP ➜ STATIC SETTINGS*** , if the field ***DHCP ASSIGNMENT*** = *global* is set in the ***IP ➜ DNS*** menu. If ***DHCP ASSIGNMENT*** = *self* is set for the field, the IP address of the gateway is sent to the client. If ***DHCP ASSIGNMENT*** = *none* is set, there is no ***PRIMARY DOMAIN NAME SERVER*** and no ***SECONDARY DOMAIN NAME SERVER*** available.

Table 2-4: Fields in the ***IP ➜ IP ADDRESS POOLS ➜ POOLS ➜ ADD/EDIT*** menu

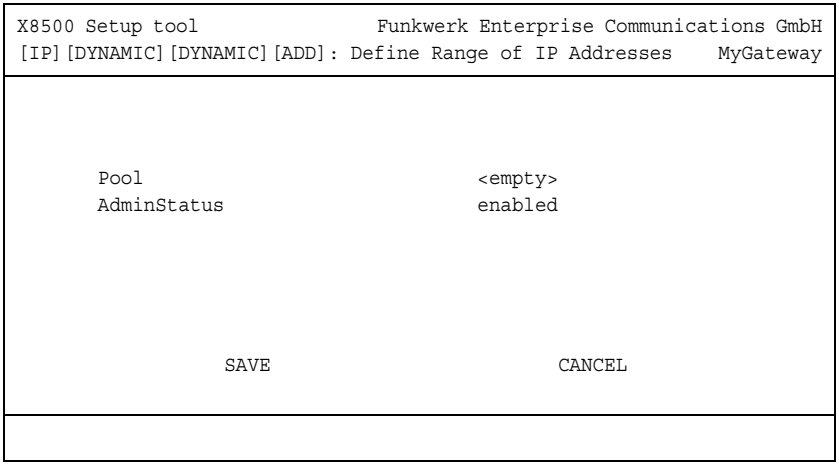
Once IP address ranges are configured, they can be allocated to the appropriate subsystem(s). You can choose whether, under ***IP ➜ IP ADDRESS POOLS ➜ DHCP ➜ ADD***, an IP address is allocated to the desired interface or, under ***IP ➜ IP ADDRESS POOLS ➜ IP ADDRESS POOL WAN (PPP) ➜ ADD***, an IP address is allocated to the PPP subsystem. IP addresses allocated to the PPP subsystem are assigned by the gateway as dynamic IP address server to WAN partners that dial up.

Note

Note that this only applies for WAN partners, for which, under ***WAN PARTNER ➜ ADD ➜ IP ➜ BASIC IP SETTINGS***, the ***IP TRANSIT NETWORK*** = *dynamic server* field setting is true.

In the ***IP ➜ IP ADDRESS POOLS ➜ IP ADDRESS POOL WAN (PPP)*** menu the IP address ranges are shown that are allocated to the PPP subsystem. If no IP address ranges have yet been allocated to this subsystem, the list is empty.

In the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***IP ADDRESS POOL WAN (PPP)*** ➜ ***ADD*** menu, you can allocate IP address ranges to the PPP subsystem.



The menu contains the following fields:

Parameter	Value
Pool	Select here the name of the address range that you have set up under ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ ***ADD/EDIT*** and wish to allocate to the PPP subsystem. If no IP address ranges are created yet, <empty> is displayed.

Parameter	Value
AdminStatus	Determines whether the IP address range is currently allocated to the PPP subsystem. Possible values: ■ *enabled* (default value): The IP address range is currently allocated to the PPP subsystem. ■ *disabled*: The IP address range is not currently allocated to the PPP subsystem.

Table 2-5: Fields in the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***IP ADDRESS POOL WAN (PPP)*** ➜ ***ADD*** menu

In the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***ASSIGNED IP ADDRESSES*** menu, you can see whether and how particular IP addresses are used.

The revision of the dynamic IP address ranges is reflected in the MIB tables as follows:

The MIB table ***IPDYNADDRTABLE*** has been replaced with two tables, the table ***IPDYNAADDRTABLE*** for dynamically generated entries, which are not saved in the configuration, and ***IPSTATADDRTABLE*** for manually generated entries, which are saved in the configuration. In the table ***IPDYNAADDRTABLE*** the MIB variable ***STATE*** has been expanded with the values *iprequest* and *ipreply*. In addition, the MIB table ***IPDYNADDRPOOLTABLE***, which contains all of the IP addresses that can be assigned dynamically, and the MIB table ***IPADDRTABLE*** are used in this context.

The MIB tables for the IP address ranges (WAN) have been revised too:

The MIB tables ***BIBOPPPIPASSIGNTABLE*** and ***BIBOPPPIPINUSETABLE*** are no longer in use; however, the ***BIBOPPPIPASSIGNTABLE*** table still currently exists. The entries in the ***BIBOPPPIPASSIGNTABLE*** table are converted to entries in the ***IPDYNADDRPOOLTABLE*** table and in the new ***BIBOPPPIPPOOLTABLE*** table.

2.7 Input/output link (pipe)

A pipe can be used to link the input of a second command with the output of the first command.

This is illustrated in the following example:

```
x8500:> echo test | cat
test
x8500:>
```

The `echo` command outputs the string `test`, which is used and output by the `cat` command as a default input.

Note

Remember that there must always be a space before and after the pipe character |.

Alternatively, there is a `pipe` command, which can be used as follows:

```
x8500:> pipe
Usage: pipe <cmd1> <cmd2>
Function: Execute two commands in a pipe (i.e. <cmd1> | <cmd2>)
```

2.8 Improved interface monitoring

In System Software 7.8.7 improvements have been made to interface monitoring and the recording and analysis of data that is sent and received. You can either use the trace command shown on the command line of your gateway or an appropriate program on your PC (bricktrace for UNIX or DimeTools for Windows).

The remote PC programs and the `trace` command allow you to log Ethernet, ISDN, ATM and WLAN interfaces and unencrypted data traffic in an IPSec tunnel, if this has been created as a virtual interface.

bricktrace, DimeTools

Remote programs on the PC have been upgraded with the following enhancements:

- For security reasons interfaces can only be logged with authentication (Admin password for the router).
- You can write the data in libpcap format so that it can be analysed with standard programs such as tcpdump, ethereal (new: wireshark) or ntop.
- A convenient IP session filter has been installed (options *-I* and *-B*).
- The internal trace connection (PC <-> gateway) is now filtered if the PC is logging the interface to which it is connected.

bricktrace

You can write a libpcap file with bricktrace data and, if required, start Ethereal simultaneously to display the data (Live Trace). Alternatively, you can save the data for subsequent analysis.
Further information on the features of bricktrace can be found in the help section using the command `-?` or in advanced help with `--help`.

Example:
`bricktrace --ethereal router-ip 1000`
starts the trace on LAN interface 1000 and automatically starts Ethereal simultaneously via a pipe.
`export TRACE_EXEC="wireshark -Sk -i"`
starts the wireshark program instead of the Ethereal program with the `--ethereal` option.

`bricktrace --pcap-file router 1000`
saves all data packets in a libpcap file. You can analyse this file at a later time.

If no interface number is specified, the program displays a list of the physical interfaces available for the gateway.

`-V 1..3`
Sets the version of the trace interface protocol;
for old devices: 1 or 2;
3 is the default value.

`--pwd=passwort`

Sets the password for the gateway (Version 3).

DimeTools With DimeTools you can save the data in a libpcap file and then open this file with the Ethereal program. A live trace cannot be performed via a pipe in Windows.

Note

Note that a live trace can only be performed via a pipe in Ethereal versions 0.10.12 and higher due to an error in the program.

trace The `trace` command has been upgraded with the following enhancements:

- A convenient IP session filter has been installed (options *-I* and *-B*).
- You can enter the interface number directly, e.g. `trace 1000` for the first LAN interface or `trace 100001` for the first IPSec interface.

IP-Session-Filter The `-I` and `-B` options (negated `-I !` and `-B !`) can be used to filter IP packets according to the fields *ip-source*, *ip-destination*, *protocol*, *src-port* and *dst-port*.

If you specify several filters without an option, the filters are linked with a logical And; the option `-o` links the filters with OR.

```
syntax:
       -I:         filter, unidirectional session
       -B:         filter, bidirectional session

usage: -I ip1:ip2:proto:port1:port2
       -B ip1:ip2:proto:port1:port2

   ip1:    source IP address
   ip2:    destination IP address
   proto:  protocol (1=ICMP, 6=TCP, 17=UDP, 50=ESP, 51=AH,
                     2=IGMP, 8=EGP, 46=RSVP)
   port1:  source port
   port 2: destination port

examples:
  -I 1.1.1.10               : all packets from 1.1.1.10
  -I !1.1.1.10              : no packets from 1.1.1.10
  -B !1.1.1.10              : no packets from and to 1.1.1.10
  -I :1.1.1.10              : all packets to 1.1.1.10
  -I 1.1.1.10:1.1.1.20      : all packets from 1.1.1.10 to 1.1.1.20
  -B 1.1.1.10:1.1.1.20     : all packets between 1.1.1.10 and 1.1.1.20
  -I ::6                    : all TCP packets
  -I ::6 -o -I ..17         : all TCP and UDP packets
  -I !::50                  : no ESP packets
  -I ::17::512              : all UDP packets to port 512
  -I 1.2.3.4::17::512       : all UDP packets from 1.2.3.4 to any
                              host/port 512
  -B ::6:1026:23           : all TCP packets between ports 1026 and 23
```

Press `-?` to obtain information for the `trace` command on IP session filters and `--help` for information for the bricktrace program.

2.9 Auto-completion with the tab key (Tab Completion)

System Software 7.8.7 supports auto-completion with the tab key (Tab Completion).

Entries on the SNMP shell of your device can now be completed automatically using the tab key. Simply enter the first few letters of a command and auto-complete the command by pressing the tab key.

The following entries can be completed:

- External commands (`ping`, `ifconfig` etc.)

- Local commands (`echo`, `sleep`, `halt` etc.)
- SNMP commands (tables, values)
- MIB groups

Auto-completion also offers a complete command (e. .g. if the tab character is not transmitted correctly due to the terminal settings), which can be used as follows:

`complete <required string>`.

Example: All commands that start with *l* are listed.

```
x8500:> complete l
l                    loop                 linkd
l2tpd                l2tp                 l2tpGlobals
l2tpSessionTable       l2tpTunnelProfileTable l2tpTunnelTable
localTcpAllowTable   localUdpAllowTable
x8500:>
```

2.10 New "grep" command

System Software 7.8.7 supports a basic grep command.

The grep command allows you to search for terms on the SNMP shell of your device. Lines that match the search term are output and all other terms are rejected. This can be linked with the output of all commands on the shell.

The following syntax is used:

```
x8500:> grep -h
Usage: grep [hvdie:] <pattern>
    -e <pattern>   specify multiple <pattern>
    -i             ignore case
    -v             invert match
    -d             debug
    -h             display help and exit
```

Example:

Find the process ID for the DynDNS Daemon using:

```
x8500:> ps -ef | grep ddnsd
```

Example:

Search for the process ID for ddnsd and bootpd using:

```
x8500:> ps -ef | grep -e ddnsd -e bootpd
```

Example:

To exclude NAT debug messages use:

```
x8500:> debug all | grep -v NAT
```

The grep command supports basic regular expressions. These can use the characters `* ? [ ] .`

Example:

```
x8500:> echo test | grep *t[ae]s?
```

`*` returns a match with any character string length.

`?` returns a match with any character.

`[ ]` corresponds to an OR operation, i.e. one of the specified characters must match.

2.11 Ping command extended

In System Software 7.8.7 the ping SNMP shell command has been extended with the options -t and -Q.

These new options allow you to explicitly set the TOS and TTS fields in ICMP packets.

ping -Q <tos>: Sets the specified TOS value.
(possible values<*tos*>: *0 - 15*.)

ping -t <ttl>: Sets the specified TTL value.

2.12 traceroute command extended

In System Software 7.8.7 the traceroute has been extended with the option -s.

The new option allows you to explicitly set the IP address used as the sender for a computer with several IP addresses.

traceroute -s <IP address>: Sets the specified IP address as the sender.

2.13 BOOTP relay

In System Software 7.8.7 your gateway supports the configuration of BOOTP relay servers not only for the system as a whole, but also for selected interfaces.

Global BOOTP relay server

The configuration of global BOOTP relay server has been moved from the ***IP*** ➜ ***STATIC SETTINGS*** menu to the ***IP*** ➜ ***BOOTP RELAY*** ➜ ***EDIT*** menu.

Specific BOOTP relay server

You can configure interface-specific BOOTP relay servers in the ***IP*** ➜ ***BOOTP RELAY*** ➜ ***ADD/EDIT*** menu.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[IP][BOOTP][ADD]: BOOTP Relay Interface Settings              MyGateway


    Interface                 en1-0
    Admin State               enabled
    Primary BOOTP Server
    Secondary BOOTP Server




           SAVE                              CANCEL
```

The menu contains the following fields:

Parameter	Value
Interface	Shows the interfaces for your device. Select an interface. If a BOOTP request is sent over the selected interface, this request is forwarded to the specified BOOTP relay server.
Admin State	Enables or disables the assignment between the interface and BOOTP relay server(s). Possible values: ■ *enabled* (default value): The assignment between the interface and BOOTP relay server(s) is enabled. ■ *disabled*: The assignment between the interface and BOOTP relay server(s) is disabled.
Primary BOOTP Server	Here you can enter the IP address of a server to which BOOTP or DHCP requests are forwarded.
Secondary BOOTP Server	Here you can enter the IP address of an alternative BOOTP or DHCP server.

Table 2-6: Fields in the ***IP*** ➜ ***BOOTP RELAY*** ➜ ***ADD/EDIT*** menu

2.14 PPPoE Passthrough

In System Software 7.8.7 you can create several PPPoE connections from the LAN directly in the Internet for an existing Internet connection using the PPPoE passthrough function over a DSL connection. Currently PPPoE passthrough can only be configured between two devices with an Ethernet interface. You are currently unable to use any filters, SIF, etc. for the PPPoE passthrough function.

The function is configured in the ***PPP*** menu and in the ***PPPP*** ➜ ***PPPoE PASSTHROUGH*** menu.

Select the interface specified for PPPoE connections from the ***PPPoE ETHERNET INTERFACE*** field in the ***PPP*** menu. (The menu contains example values.)

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[PPP]: PPP Profile Configuration                                MyGateway




      Authentication Protocol         CHAP + PAP + MS-CHAP
      Radius Server Authentication    inband

      PPP Link Quality Monitoring     no

      PPPoE Ethernet Interface        en1-1

      PPPoE Passthrough >




                 SAVE                            CANCEL
```

Configure the required Ethernet port pairs in the ***PPP*** ➜ ***PPPoE PASSTHROUGH*** menu. You can select one Ethernet port each for the PPPoE client and the PP-

PoE server (or the DSL "port" represented by *ethoa50-0* for device with a DSL connection). (The menu contains example values.)

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[PPP]: PPPoE Passthrough Configuration                        MyGateway

    Physical or virtual Ethernet Port attached to PPPoE Client(s)
    <x> en1-0              < > en1-4              < > en1-1
    < > en1-2

    Physical or virtual Ethernet Port attached to PPPoE Server
    < > en1-0              < > en1-4              <x> en1-1
    < > en1-2

                SAVE                           CANCEL
```

2.15 PPPoE Multilink

In System Software 7.8.7 you can connect several DSL connections from a provider over PPP as a static bundle in order to obtain more bandwidth. Each of these DSL connections should use a separate Ethernet connection for this. At the moment, many providers are still in the process of preparing the PPPoE Multilink function.

To configure PPPoE multilink you must first create a corresponding WAN partner. In the ***WAN Partner*** ➜ ***ADD*** ➜ ***Advanced Settings*** menu set ***Layer 1 Protocol*** = *PPP over Ethernet (PPPoE)* for this WAN partner. The PPPoE mul-

tilink is actually configured in the ***WAN PARTNER*** ➜ ***ADD*** ➜ ***ADVANCED SETTINGS*** ➜ ***EXTENDED INTERFACE SETTINGS*** menu. (The menu contains example values.)

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[WAN][ADD][ADVANCED][EXTIF]:
             Extended Interface Settings (WAN Partner Name)   MyGateway


      PPPoE Multilink          yes


      Ethernet Ports to use

      < > en1-0              < > en1-4             <x> en1-1
      <x> en1-2




                SAVE                          CANCEL
```

The menu contains the following fields:

Parameter	Value
PPPoE Multilink	Determines whether or not PPPoE multilink is used. Possible values: ■ *no* (default value): PPPoE multilink is not used. ■ *yes*: PPPoE multilink is used.
Ethernet Ports to use	Shows the Ethernet interfaces for your device. Different interfaces are available depending on your device and depending on whether or not and how the Ethernet switch is operated in split ports mode. Select the interface you wish to use for PPPoE multilink.

Table 2-7: Fields in the ***WAN Partner*** ➜ ***ADD*** ➜ ***Advanced Settings*** ➜ ***Extended Interface Settings*** menu

Note

For PPPoE Multilink, we recommend using your device's Ethernet switch in split ports mode and to use a separate Ethernet interface e.g. *en1-1*, *en1-2* for each PPPoE connection.

Note

If you also want to use an external modem for PPPoE Multilink, you must run your device's Ethernet switch in split ports mode.

Note

If you wish to use an external modem, then you must set the fields ***Queueing and Scheduling Algorithm*** = *priority queueing (PQ)* and ***Specify Traffic Shaping*** = *yes* in the ***QoS*** ➜ ***Interfaces and Policies*** ➜ ***EDIT*** ➜ ***QoS Scheduling and Shaping*** menu.

Note

If you wish to use an external modem, you must state the bandwidth of the upload connection.

2.16 VLAN and Bridging

VLANs allow you to separate individual network segments, e.g. individual departments of a company. In the new *VLAN* menu System Software 7.8.7 supports the configuration of VLANs on interfaces for which bridging mode is configured.

You can display all the VLANs already configured, edit your settings and create new VLANs.

Administration

In the ***VLAN*** ➜ ***ADMINISTRATION*** menu you can view a list of the created bridge groups. (The list contains example values. The list is empty if no bridge groups are created.)

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[VLAN] [ADMINISTRATION]                                      MyGateway


  Bridge Group Name   Status    Non Mgmt Frames    Mgmt VID
  ──────────────────────────────────────────────────────────

    br0               enable       forward           1
    br1               disable      drop              2
    br2               disable      forward           1




                              EXIT
```

In the ***VLAN*** ➜ ***ADMINISTRATION*** ➜ ***EDIT*** menu you can make general settings for a VLAN. The options must be configured separately for each bridge group.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[VLAN][ADMINISTRATION][EDIT]: br0                                MyGateway


        Bridge Group Name   br0

        Admin Status        disable

        Management VID      Management
        Non Mgmt Frames     forward



           SAVE                          CANCEL
```

The menu contains the following fields:

Parameter	Value
Bridge Group Name	Shows the selected bridge group.
Admin Status	Enables or disables the VLAN for the selected bridge group. Possible values: ■ *disable* (default value): The VLAN is disabled. ■ *enable*: The VLAN is enabled.
Management VID	Management VLAN ID. Enter the VLAN ID of the VLAN in which your device is to operate.

Parameter	Value
Non Mgmt Frames	Determines whether or not frames that are not marked with the management VLAN ID are forwarded or rejected. Possible values: ■ *forward* (default value): The frames are forwarded. ■ *drop*: The frames are rejected.

Table 2-8: Fields in the ***VLAN*** ➜ ***ADMINISTRATION*** ➜ ***EDIT*** menu

VLAN In the ***VLAN*** ➜ ***VLAN*** menu you can view which VLANs are created and which ***VLAN NAME*** is assigned to which ***VLAN ID***. (The list contains example values.)

```
X8500 Setup tool                    Funkwerk Enterprise Communications GmbH
[VLAN][VLANS]                                                      MyGateway


   VLAN Name                                  VLAN ID
   ____________________________________________

   Management                                    1
   Support                                       2




   ADD          MEMBERS          DELETE          EXIT
```

In the ***VLAN*** ➜ ***VLAN*** ➜ ***ADD*** menu you can create new assignments. The VLAN is created with the name *Management* and the ID *1* by default:

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[VLAN][VLANS][ADD]: VLAN ID                                    MyGateway


        VLAN Name           Management

        VLAN ID             1



          SAVE                          CANCEL
```

The ***VLAN*** ➜ ***VLAN*** ➜ ***ADD*** submenu contains the following fields:

Parameter	Value
VLAN Name	Enter a name for the VLAN here. Maximum number of characters: 32.
VLAN ID	VLAN Identifier Enter a unique whole number that identifies the VLAN. Possible values: *1* .. *4094*. Default value: *1*.

Table 2-9: Fields in the ***VLAN*** ➜ ***VLAN*** ➜ ***ADD/EDIT*** menu

In the ***VLAN*** ➜ ***VLAN*** ➜ **Members** menu you can see which VLANs are assigned to which interfaces and which frames are sent over the respective interface. (The list contains example values.) The **Members** button appears if the

INTERFACE MODE = *Bridging* field is set in the ***ETHERNET SWITCH*** ➜ ***FAST ETHERNET/EN1-X*** ➜ ***EDIT*** menu.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[VLAN] [VLANS] [MEMBER]                                        MyGateway


   VLAN ID     Port Name     Egress Rule
   ____________________________________

     1          en1-0         untagged
     1          en1-2         untagged
     1          en1-3         untagged
     2          en1-2         untagged
     2          en1-3         tagged




   ADD                DELETE              EXIT
```

The ***VLAN*** ➜ ***VLAN*** ➜ **Members** ➜ **ADD** menu contains the following fields:

Parameter	Value
VLAN ID	VLAN Identifier Shows the names of the VLANs created in the ***VLAN*** ➜ ***VLAN*** ➜ ***ADD*** menu. You can choose a VLAN.
Port Name	Here you can view all of the interfaces for which bridging has been configured (see menu ***ETHERNET SWITCH*** ➜ ***FAST ETHERNET/EN1-X*** ➜ ***ADD/EDIT***). Select the interface you wish to assign to the VLAN, i.e. to become a member of the chosen VLAN.
Egress Rule	Determines whether the frames with VLAN information or the frames without VLAN information are forwarded to the selected interface. Possible values: ■ *untagged* (default value): The frames without VLAN information are forwarded. ■ *tagged*: The frames with VLAN information are forwarded.

Table 2-10: Fields in the ***VLAN*** ➜ ***VLAN*** ➜ ***MEMBERS*** ➜ ***ADD*** menu

PVID In the ***VLAN → PVID*** menu you can view and determine rules for receiving frames on the VLAN interface. (The list contains example values.)

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[VLAN] [PVIDS]                                                MyGateway


 Port Name      PVID   Untagged Frames   Non Member Frames
 ____________________________________________________________

 en1-0           1       forward           forward
 en1-2           2       drop              drop
 en1-3           1       forward           forward




              MEMBERS            EXIT
```

The ***VLAN*** ➜ ***PVID*** ➜ ***EDIT*** menu contains the following fields:

Parameter	Value
Port Name	Shows the port for which you are editing the rules.
PVID	Port VLAN Identifier Assign the selected port a PVID.
Untagged Frames	Defines how to handle frames that contain no VLAN information. Possible values: ■ *forward* (default value): The frames without VLAN information are forwarded. ■ *drop*: The frames without VLAN information are rejected.
Non Member Frames	Determines whether or not frames whose VLAN information does not match the chosen port are forwarded or rejected. Possible values: ■ *forward* (default value): The frames are forwarded. ■ *drop*: The frames are rejected.

Table 2-11: Fields in the ***VLAN*** ➜ ***PVID*** ➜ ***EDIT*** menu

In the ***VLAN*** ➜ ***PVID*** ➜ **Members** menu you can see which VLANs are assigned to which interfaces and which frames are sent over the respective interface. The information is the same as in the ***VLAN*** ➜ ***VLAN*** ➜ **Members** menu.

2.17 Multicast

In the new *IP* ➜ *MULTICAST* menu System Software 7.8.7 supports message transmission in TCP/IP networks to a group of recipients. Whereas *FORWARDING* simply forwards the data, IGMP and PIM only send data to specific hosts and thus prevent unnecessary data traffic.

In multicast mode the data is sent to a type of "virtual address", to the so-called multicast group. For, IPv4 the IP addresses 224.0.0.0 to 239.255.255.255 are reserved for multicast groups in the class D network.

Interested recipients can register with any number of multicast groups. Hosts, in this context also referred to as sources, that broadcast an Internet radio station, send their packets to the respective multicast groups. The packets are forwarded to the recipients based on the registrations for the multicast group.

IGMP (Internet Group Management Protocol) manages the multicast groups in local networks and regulates the exchange of member information for these groups using queries and reports. The latest version of IGMP is version 3, which is downward compatible with versions 1 and 2.

By comparison, PIM (Protocol Independent Multicast) is a multicast routing protocol. With PIM the distribution of information is regulated via a central point, which is known as the rendezvous point. Data packets are initially routed here before being made available to other recipient routers.

Multicast routing protocols differentiates between sparse mode and dense mode. In dense mode, all packets are forwarded and only packets to groups that have been explicitly cancelled are rejected. In sparse mode, packets are only forward to groups if they have been ordered.

MSDP (Multicast Source Discovery Protocol) is mainly used in **System Software 7.8.7** to connect several PIM domains and to operate inter-domain routing.

In the ***IP*** ➜ ***MULTICAST*** menu you can disable or enable the multicast function.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST]: Multicast Configuration                          MyGateway


          Status                    enabled

          Interfaces >

          Forwarding >
          IGMP >
          PIM >
          MSDP >




          SAVE                              CANCEL
```

The ***IP*** ➜ ***MULTICAST*** menu provides access to the following submenus:

- ***INTERFACES***
- ***FORWARDING***
- ***IGMP***
- ***PIM***
- ***MSDP***.

Interfaces In the ***IP*** ➜ ***MULTICAST*** ➜ ***INTERFACES*** menu you can view the active multicast interfaces and their usage.

Forwarding In the ***IP*** ➜ ***MULTICAST*** ➜ ***FORWARDING*** ➜ ***ADD/EDIT*** menu you can set up a one-off forward for packets to a multicast group.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][FORWARDING]: Add/Edit Rule                          MyGateway


  Group Address
  Status                        active


  Source Interface              none
  Destination Interface         none


            SAVE                              CANCEL
```

The ***IP*** ➜ ***MULTICAST*** ➜ ***FORWARDING*** ➜ ***ADD/EDIT*** menu contains the following fields:

Parameter	Value
Group Address	IP address of the group for which this entry applies. The address must be in the range 224.0.0.0 - 239.255.255.255. The address 224.0.0.0 allows you to specify all multicast packets.
Status	Activates or deactivates the entry. Possible values: ■ *active* (default value): The entry is active, the data packets are forwarded. ■ *inactive*: The entry is not active and is not taken into account.
Source Interface	Interface at which the data packets are received. ***SOURCE INTERFACE*** and ***DESTINATION INTERFACE*** must be different interfaces.
Destination Interface	Interface at which the data packets are forwarded. ***SOURCE INTERFACE*** and ***DESTINATION INTERFACE*** must be different interfaces.

Table 2-12: Fields in the ***IP*** ➜ ***MULTICAST*** ➜ ***FORWARDING*** ➜ ***ADD/EDIT*** menu

Note

Ensure that your settings under ***FORWARDING*** do not overlap with interfaces that are simultaneously configured for IGMP or PIM. Packets for groups that are configured under ***FORWARDING*** are forwarded if they have been explicitly cancelled by IGMP or PIM to the interfaces.

IGMP

In the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** menu, define whether or not IGMP is enabled. You can specify whether IGMP only operates in version 3 or whether compatibility mode is used. Compatibility mode automatically adjusts the IGMP version

that is used on this interface. As a result, hosts with version 2 or version can also be operated on the respective interface alongside hosts with version 3. In addition, you can define the interface on which IGMP is used.

The menu contains example values.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][IGMP]: IGMP Configuration                          MyGateway


Status        auto                      Advanced >
Mode          compat

Interface     Status              Mode
-------------------------------------------------------------------------
en1-0         active              routing









SAVE      ADD      DELETE      EXIT
```

The ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** menu contains the following fields:

Parameter	Value
Status	Defines whether or not IGMP is used. Possible values: ■ *auto* (default value): IGMP is switched on. IGMP will create host-mode interfaces when requested by applications. ■ *down*: IGMP is switched off. ■ *up*: IGMP is switched on.

Parameter	Value
Mode	Determines in which mode IGMP is used. Possible values: ■ *compat*: IGMP is used in compatibility mode, i.e. hosts that work with version 1, 2 or 3 are included. If several versions are available in a network, the version with the lowest version number (the oldest version) is chosen as the common default. ■ *v3only*: Only IGMP version 3 is used, i.e. only V3 hosts are included.

Table 2-13: Fields in the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** menu

In the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADD/EDIT*** menu you can define the interfaces on which IGMP is used.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][IGMP][INTERFACE]: Configure IGMP Interface        MyGateway



Interface                           en1-0
Status                              active
Mode                                routing

Query Interval (s)                  125
Max Response Time (ms)              10000
Robustness                          2
Last Member Query Interval (ms)     1000
StateLimit (msg/s)                  0

ProxyIfIndex                        none



SAVE                          CANCEL
```

The ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADD/EDIT*** menu contains the following fields:

Parameter	Value
Interface	Select the interface over which IGMP queries are sent and responses are accepted. To do this, select the interface behind which the multicast recipient is concealed.
Status	Activates or deactivates IGMP on the selected interface. Possible values: ■ *active* (default value): The entry is active, IGMP is used on the selected interface. ■ *inactive*: The entry is not active, IGMP is not used on the selected interface.
Mode	Select whether the interface defined here operates in host mode and in routing mode or in host mode only. Possible values: ■ *routing* (default value): the interface operates in routing mode and in host mode. ■ *host-only*: the interface operates in host mode only.
Query Interval	Enter the interval in seconds in which IGMP queries are to be sent. Possible values: *0* .. *600*. Default value: *125*.

Parameter	Value
Max Response Time (ms)	For the sending of queries, enter the interval in milliseconds within which hosts must respond. The hosts randomly select a time delay from this interval before sending the response. This spreads the load in networks with several hosts, improving performance. Possible values: *0* .. *25500*. Default value: *10000*.
Robustness	Select the multiplier for controlling the timer values. A higher value can e.g. compensate for packet loss in a network susceptible to loss. If the value is too high, however, the time between logging off and stopping of the data traffic can be increased (leave latency). Possible values: Whole numbers *2* .. *8*. Default value: *2*.
Last Member Query Interval (ms)	Waiting time in milliseconds for a response to a query to a group. If you shorten the interval, it will be more quickly detected that the last member has left a group so that no more packets for this group should be forwarded to this interface.
StateLimit	Defines the maximum number of queries or reports per second for the selected interface.
ProxyIfIndex	Here you can decide whether your device is to forward the hosts' IGMP messages on this interface via another proxy interface. If you want the hosts' IGMP messages to be forwarded, select the interface for your device that is used as the IGMP proxy. In general, IGMP must also be active on this interface.

Table 2-14: Fields in the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADD/EDIT*** menu

The ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** menu allows you to access the submenu

- ***ADVANCED***.

The ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** menu contains the following fields:

Parameter	Value
Max Groups	Defines the maximum number of total possible groups both internally and in reports. Default value: *64*.
Max Sources	Defines the maximum number of sources that are specified in version 3 reports and the maximum number of internally managed sources per group. Default value: *64*.
StateLimit	Defines the maximum permitted total number of incoming queries and reports per second. Default value: *0*.

Table 2-15: Fields in the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** menu

The ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** menu provides access to the following submenus:

- ***STATIC GROUPS***
- ***MONITOR***
- ***ACL***.

You can create static groups in the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** ➜ ***STATIC GROUPS*** menu. Packets to these groups are always forwarded on the respective interface, even if a specific group has not been ordered explicitly. The menu contains the following fields:

Parameter	Value
Group Address	IP address of the static group. Here you can enter an IP multicast address.

Parameter	Value
Interface	Interface at which the data is forwarded to the group. IGMP must be active on this interface.
Status	Determines whether or not the static group is active. Possible values: ■ *active* (default value): The static group is active. ■ *inactive*: The static group is not active.

Table 2-16: Fields in the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP***➜ ***ADVANCED*** ➜ ***STATIC GROUPS*** menu

In the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** ➜ ***MONITOR*** menu you can monitor certain IGMP parameters that refer to an interface. The menu contains the following fields:

Parameter	Value
Interface	Shows the interface on which IGMP is active.
Compat Version	Shows the IGMP version currently being used.
Querier	Shows the router that is acting as the querier and is sending queries.
V1 ExpiryTime(s)	If a V1 host exists in your network, IGMP is operated in compatibility mode with version 1. If no V1 host responds within the interval ***V1 EXPIRYTIME(S)***, the system switches to V2 or V3.
ExpiryTime(s)	Shows the validity period of the querier if your gateway is not currently acting as the querier. The value *0* shows that your gateway is the querier.

Parameter	Value
V2 ExpiryTime(s)	If a V2 host exists in your network, IGMP is operated in compatibility mode with version 2. If no V2 host responds within the interval ***V2 EXPIRYTIME(S)***, the system switches to V3.
Joins	Shows the number of group registrations received (joins) on the respective interface.
Wrong Queries	Shows the number of incorrect queries received on the respective interface.
Group	Shows the number and IP addresses of the groups.

Table 2-17: Fields in the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** ➜ ***MONITOR*** menu

In the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** ➜ ***MONITOR*** ➜ ***GROUP*** menu you can monitor certain IGMP parameters that refer to a group.

The menu contains the following fields:

Parameter	Value
Group	Shows the IGMP group.
LastReporter	Shows the last host to send a report for this group.
Mode	Shows the IGMP filter mode. Possible values: ■ EXCLUDE: Packets from the specified sources are excluded from the transmission. ■ INCLUDE: Packets from the specified sources are included for the transmission.
V1HostExpiryTime(s)	Shows the length of the group membership if a host has registered for the group with IGMP version 1.
ExpiryTime(s)	Shows the length of group membership.
V2HostExpiryTime(s)	Shows the length of the group membership if a host has registered for the group with IGMP version 2.
included / excluded Source	Shows the IP addresses of the sources that are permitted for or excluded from data transmission depending on the value of the ***MODE*** field.

Table 2-18: Fields in the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** ➜ ***MONITOR*** ➜ ***GROUP*** menu

You can accept and reject reports and packets from specific hosts using rules from the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** ➜ ***ACL*** menu. You can also modify the order of the rules or delete rules.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][IGMP]: ACL Configuration                            MyGateway


Press 'u' to move ACL up or press 'd' to move ACL down.

Pos    Interface   Sender          Group           Type      Action

  0    en1-0       192.168.0.1/24  224.0.0.0/4     traffic   deny
  1    any         0.0.0.0/0       224.1.2.3/32    traffic   deny




    ADD                DELETE             SAVE                CANCEL
```

You can create rules in the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** ➜ ***ACL*** ➜ ***ADD*** menu.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][IGMP]: Add/Edit ACL Rule                            MyGateway



   Interface                          en1-0
   Sender Address                     192.168.0.1
   Sender Netmask                     255.255.255.0
   Group Address                      224.0.0.0
   Group Netmask                      240.0.0.0

   Type                               traffic

   Action                             deny



   SAVE              CANCEL
```

The menu contains the following fields:

Parameter	Value
Interface	Interface for which a rules is created.
Sender Address	IP address of the sender. This is the host sending the IGMP messages for the *report* type. For *traffic* entries this equates to the multicast source.
Sender Netmask	Netmask of the sender.
Group Address	IP address of the multicast group.
Group Netmask	Netmask of the multicast group.

Parameter	Value
Type	Distinguishes between the types of packets. Possible values: ■ *traffic*: Multicast packets ■ *report*: IGMP messages
Action	Defines how the data is handled. Possible values: ■ *deny*: Data is rejected. ■ *accept*: Data is accepted.

Fields in the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** ➜ ***ADVANCED*** ➜ ***ACL*** ➜ ***EDIT*** menu

PIM In the ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** menu you can disable or enable the PIM function.

Note

Please note that you require a valid licence to use the PIM function.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][PIM]: PIM Configuration                            MyGateway


              Status                    enabled


              Interfaces >
              Rendezvous Points >

              AnycastRP >



              SAVE                                    EXIT
```

The ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** menu provides access to the following submenus:

- ***INTERFACES***
- ***RENDEZVOUS POINTS***
- ***ANYCASTRP***.

In the ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** ➜ ***INTERFACES*** ➜ ***ADD/EDIT*** menu you can define the interfaces on which PIM is used.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][PIM][INTERFACE]: Configure PIM Interface          MyGateway



Interface            en1-0
Status               active
Mode                 Sparse
Stub Interface       disabled

Role   Router


Hello Interval (s)             30          Propagation Delay (s)    1
Triggered Hello Delay (s)      5           Override Interval (s)    3
Hello HoldTime (s)             180         DR Priority              1
JoinPrune Interval (s)   30
JoinPrune HoldTime (s)   180



SAVE                          CANCEL
```

The ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** ➜ ***INTERFACES*** ➜ ***ADD/EDIT*** menu contains the following fields:

Parameter	Value
Interface	Choose the interface used for PIM, i.e. over which multicast routing is operated.
Status	Activates or deactivates the entry. Possible values: ■ *active* (default value): PIM is active on this interface. ■ *inactive*: PIM is not active on this interface.
Mode	Mode to be used for PIM. ■ *Sparse Mode* (default value): PIM is used in sparse mode. ■ *Dense Mode*: Not available.
Stub Interface	Determines whether or not the interface is used for PIM data packets. This parameter allows you to use an interface for IGMP, for example, whilst preventing (fake) PIM messages. Possible values: ■ *disabled*: The interface is disabled for PIM data packets. ■ *enabled*: The interface is enabled for PIM data packets.
Role	Defines which role the gateway is assigned. Possible values: ■ *Routers*: The gateway acts as a router. ■ *RP*: The gateway acts as a rendezvous point.

Parameter	Value
Hello Interval (s)	Defines the interval (in seconds) at which PIM Hello messages are sent over this interface. The value *0* means that no PIM Hello messages are sent on this interface. Possible values: *0* .. *18000*.
Triggered Hello Delay (s)	Defines the maximum waiting time until a PIM Hello message is sent after a system boot or after a reboot of a neighbour. The value *0* means that PIM Hello messages are always sent straight away. Possible values: *0* .. *60*.
Hello HoldTime (s)	Defines the value of the holdtime field in a PIM Hello message. This indicates how long a PIM route is available. As soon as the ***HELLO HOLDTIME (S)*** has expired and no other Hello messages have been received, the PIM route will be classed as unavailable. Possible values: *0* .. *65535*.
JoinPrune Interval (s)	Defines the frequency at which the PIM Join/Prune messages are sent on the interface. The value *0* means that no periodic PIM Join/Prune messages are sent on this interface. Possible values: *0* .. *18000*.
JoinPrune HoldTime (s)	Defines the value entered in the holdtime field of a PIM Join/Prune message. This is the time for which a recipient must maintain the Join/Prune state. Possible values: *0* .. *65535*.

Parameter	Value
Propagation Delay (s)	Defines the value entered in the Propagation Delay field. This field is part of the LAN Prune Delay option in the PIM Hello messages, which are sent on this interface. Propagation Delay and Override Interval represent the so-called LAN-Prune-Delay settings. These result in a delay in processing prune messages for upstream routers. If the ***PROPAGATION DELAY (S)*** is too short, the transfer of multicast packets may be cancelled before a downstream router has sent a prune override message. Possible values: *0* .. *32*.
Override Interval (s)	Defines the value that the gateway enters in the Override_Interval field for the LAN Prune Delay option. ***OVERRIDE INTERVAL (S)*** defines the maximum time a downstream router can wait until sending a prune override message.
DR Priority	Defines the value of the designated router priority entered in the DR Priority option. The higher the value, the greater the probability that the corresponding router will be used as the designated router.

Table 2-19: Fields in the ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** ➜ ***INTERFACES*** ➜ ***ADD/EDIT*** menu

In the ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** ➜ ***RENDEZVOUS POINTS*** ➜ ***ADD/EDIT*** menu you can define which rendezvous point is responsible for which groups.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][PIM][RP]: Configure RP                              MyGateway


      Group Range           All Groups


      RP Address
      Precedence            0



       SAVE                           CANCEL
```

The menu contains the following fields:

Parameter	Value
Group Range	Here you can specify all groups or a multicast network segment.
Group Address	Only for ***GROUP RANGE*** = *Specify*. IP address of the multicast network segment.
Group Prefix Length	Only for ***GROUP RANGE*** = *Specify*. The netmask length of the multicast network segment. 224.0.0.0/4 indicates the entire multicast class D segment. Possible values: *4* .. *32*.
RP Address	IP address of the rendezvous point

Parameter	Value
Precedence	Priority You can enter whole numbers.

Fields in the ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** ➜ ***RENDEZVOUS POINTS*** ➜ ***ADD/EDIT*** menu

In the ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** ➜ ***ANYCASTRP*** menu you can join two or more PIM domains and distribute the load between these. You can use two gateways as a backup for one another.

```
X8500 Setup tool                Funkwerk Enterprise Communications GmbH
[IP][MCAST][PIM]: AnycastRP Configuration                       MyGateway


      AnycastRP Address          1.1.1.1
      Local RP Address           192.168.0.1
      Remote RP Address          192.168.1.2
      Via                        MSDP



      SAVE            CANCEL
```

The menu contains the following fields:

Parameter	Value
AnycastRP Address	Virtual RP address.
Local RP Address	Local RP address.
Remote RP Address	IP address of the RP peer.

Parameter	Value
Via	Defines how the PIM domains are joined. Possible values: ■ MSDP ■ PIM Register.

Fields in the ***IP*** ➜ ***MULTICAST*** ➜ ***PIM*** ➜ ***ANYCASTRP*** menu

Note

Please note that an additional virtual address configuration is required for AnycastRP.

MSDP MSDP (Multicast Source Discovery Protocol) allows you to join several domains using PIM. Each domain uses its own rendezvous point. In the ***IP*** ➜ ***MULTICAST*** ➜ ***MSDP*** menu you can disable or enable the MSDP function or create a detailed configuration.

The ***IP*** ➜ ***MULTICAST*** ➜ ***MSDP*** ➜ ***ADD/EDIT*** menu contains the following fields:

Parameter	Value
Remote Address	IP address of the peer.
Local address	Local IP address.
Status	Activates or deactivates the entry. Possible values: ■ *active* (default value): The entry is active. ■ *inactive*: The entry is not active.
Retry Interval (s)	Interval in seconds until the next connection attempt if a previous attempt has failed. Default value: *30*.
Holdtime (s)	Interval in seconds until a peer is classed as inactive and is disconnected. Default value: *75*.
KeepAlive (s)	Interval in seconds within which a KeepAlive message must be sent. Default value: *60*.

Table 2-20: Fields in the ***IP*** ➜ ***MULTICAST*** ➜ ***MSDP*** ➜ ***ADD/EDIT*** menu

2.18 Stateful Inspection Firewall - Simplified configuration

The configuration of the bintec Stateful Inspection Firewall has been simplified. You can now group together interfaces, services and addresses. The internal use of alias names has also been improved.

Groups are configured in the respective submenu in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** menu.

Interface Groups

You can group together interfaces in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT INTERFACE GROUPS*** ➜ ***ADD/EDIT*** menu. The menu consists of the following fields:

Parameter	Value
Alias	Here you enter a name for the interface group you want to configure.
Interface Alias 1 -10	Shows the alias names of the interfaces for your device. You can choose the desired alias names and group together up to ten interfaces.

Table 2-21: New fields in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT INTERFACE GROUPS*** ➜ ***ADD/EDIT*** menu

Service Groups

You can group together services in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES GROUPS*** ➜ ***ADD/EDIT*** menu. The menu consists of the following fields:

Parameter	Value
Alias	Here you enter a name for the service group you want to configure.
Service Alias 1 - 10	Shows the alias names of the services configured on your device. You can choose the desired services and group together up to ten services.

Table 2-22: New fields in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT INTERFACE GROUPS*** ➜ ***ADD/EDIT*** menu

Address Groups

You can group together address aliases in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESS GROUPS*** ➜ ***ADD/EDIT*** menu. The menu consists of the following fields:

Parameter	Value
Alias	Here you can enter a name for the address alias group you want to configure.

Parameter	Value
Interface Alias 1 - 10	Shows the alias names of the interfaces for which an alias has been configured for an IP address or an IP address range on your device. You can choose the desired alias names and group together up to ten aliases.

Table 2-23: New fields in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESS GROUPS*** ➜ ***ADD/EDIT*** menu

2.19 QoS classification included in the Stateful Inspection Firewall

In System Software 7.8.7IP QoS classification has been included in the configuration of the Stateful Inspection Firewall.

This allows you to use SIF internal session handling for packet classification as required for QoS policies.

An important advantage is easier QoS configuration:

- An individual IP packet filter no longer has to be configured.
- Packet direction and destination port can be ignored.
- Cross-relationships no longer have to be configured separately in dependent sessions, e.g. PPTP/GRE, H232/RTP, FTP...).
- QoS classification is now carried out for all traffic flows that are not blocked by the SIF.

The configuration is carried out in the ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ **ADD/EDIT** menu:

```
X8500 Setup Tool                Funkwerk Enterprise Communications GmbH
[SECURITY][STATEFUL INSPECTION][ADD]                            MyGateway

   Source              <-- Addresses   select     Addresses       -->
   Destination         <-- Addresses   select     Addresses       -->
   Edit Addresses >

   Service           <-- Services      select      Services        -->
   Edit Services >

   Action                      accept


   QoS Priority   default (no special IP QoS handling)


                  SAVE                           CANCEL
```

The menu contains the following fields for QoS classification:

Field	Meaning
QoS Priority	Select the priority with which the data specified by the filter is handled on the send side. Possible values: ■ *default (no special IP QoS handling)* (default value): No priority. ■ *low latency (highest priority)*: Low Latency Transmission (LTT), i.e. handling of data with the lowest possible latency, e. g. default mode for VoIP data (unless otherwise defined, e.g. in the ***VoIP*** menu). ■ *high* ■ *medium* ■ *low.*

Field	Meaning
QoS Class ID	Only for ***QoS Priority*** = *high*, *medium* or *low*. Defines the QoS packet class. Possible values: *1* (default value) to *255*.

Table 2-24: ***Security*** ➜ ***Stateful Inspection*** ➜ ***Edit Filters*** ➜ ***ADD/Edit***

Note

Note that the rules required for classifying data must be defined for each interface as normal in the ***QoS*** ➜ ***Interfaces and Policies*** menu.

2.20 QoS - Layer 2 support

System Software 7.8.7 supports layer 2 prioritisation in accordance with IEEE 802.1p.

The required parameters are in the ***Security*** ➜ ***Access Lists*** ➜ ***Filters*** ➜ ***ADD/EDIT***, ***QoS*** ➜ ***IP Filters*** ➜ ***ADD/EDIT*** and ***QoS*** ➜ ***IP Classification and Signaling*** ➜ ***ADD/EDIT*** ➜ ***Signaling (TOS/DSCP - Level 2)*** menus.

2.21 New DynDNS provider selfHOST and NO-IP

System Software 7.8.7 provides the DynDNS provider selfHOST and NO-IP.

2.22 ISDN login supports ISDN subaddresses

In System Software 7.8.7 `isdnlogin` supports own ISDN subaddresses as well as dialled ISDN subaddresses.

2.23 RADIUS - Simultaneous use of several switched lines and MLPPP

In System Software 7.8.7 you can use several switched lines with the same ID and the same password together with channel bundling (MLPPP) under RADIUS.

2.24 VoIP traffic between PBXs

In System Software 7.8.7, you can set the value *always* in the *MODE* field in the *VOIP* ➜ *DYNAMIC BANDWIDTH CONTROL* ➜ *ADD* menu to optimise VoIP traffic between two PBXs.

2.25 ISAKMP Configuration Method (IKE Config Mode)

System Software 7.8.7 now offers the ISAKMP Configuration Method (IKE Config Mode for short) that allows you to connect a mobile PC workstation (Secure IPSec Client) to the head office over VPN. The IP address and, if required, other data such as the domain and server parameters for DNS and WINS are sent to the client by the VPN gateway on request. This method allows an IP address to be dynamically assigned from the internal address range of the head office.

IKE Config Mode can be operated by extending the IPSec configuration. Data is transmitted from the gateway to the client in IPSec according to IKE (Phase 1) and is therefore protected by encryption.

Note

Note that IKE Config Mode is only available for IPSec peers with a virtual interface.

Proceed as follows to use IKE Config Mode.

1. Create at least one IP address range. To do this, select the Setup Tool menu options ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ **ADD**. Enter a unique integer ***IDENTIFIER*** and a name for the IP address range in the ***DESCRIPTION*** field. Enter the first address of the IP address range in the ***IP ADDRESS*** field and the number of IP addresses the range contains in the ***NUMBER OF CONSECUTIVE ADDRESSES*** field. Add the remaining settings as desired. Save the created IP address range with **SAVE**. Select **ADD** to create additional IP address ranges.
   The created IP address ranges are available.
2. Select IKE Config Mode and assign your chosen IP address range. To do this, select the Setup Tool menu options ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND*** and select ***IP TRANSIT NETWORK*** = *IKE Config Server Mode*. Select the desired IP address range in the ***IP ADDRESS POOL*** field, complete the settings as desired and save the settings with **Save**.

IKE Config Mode configuration is complete and an IPSec client can now dial into the gateway.

2.26 SSH Client

In System Software 7.8.7 the SSH (Secure Shell) Client function is available. This allows you to set up a secure connection from your gateway to a remote computer or to a second gateway and, for example, to output the command line of the remote computer on your gateway or to check the configuration of the second gateway.

To dial into a remote computer or a second gateway, enter the command line *ssh <User Name Gateway>@<IP address of the remote computer or IP address of the second gateway>*.

2.27 IGMP Host for local applications

System Software 7.8.7 supports IGMP for local multicast applications; i.e. local applications (e.g. Access Point Discovery Daemon) log in to specific

multicast groups using IGMP reports and so can receive multicast packets. This may be necessary for switches that use IGMP snooping.

For this mode you do not need to manually enable IGMP for each application on the corresponding interface, you can simply use the automated function provided: As soon as a host opens a local application using multicast, IGMP is automatically enabled on the corresponding interface, and the IGMP interface is operated in host mode.

By default, this automated function is set to ***Status*** = *auto* in the Setup Tool menu ***IP*** ➜ ***Multicast*** ➜ ***IGMP***.

If the IGMP status is enabled (***IGMP Status*** = *up)*, you must manually configure the respective interfaces for IGMP host. If an interface is operated in "Host only mode" (***IP*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ **ADD** with ***Mode*** = *host-only*), applications will only receive packets on this interface. Routing must be allowed (***IP*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ **ADD** with ***Mode*** = *routing*) to manage IGMP statuses for other systems on this interface and to route incoming packets there.

In the ***IP*** ➜ ***Multicast*** ➜ ***Interfaces*** menu you can view the interfaces on which IGMP has been enabled either by the automated function or manually in the ***IP*** ➜ ***Multicast*** ➜ ***IGMP*** menu.

2.28 STunnel support

System Software 7.8.7 supports STunnel. You can transport unsecure TCP data securely via an SSL tunnel, without needing a VPN. Each SSL tunnel can contain up to five TCP connections, e.g. for HTTP where several TCP connections are normally set up.

You can configure SSL tunnels in the Setup Tool menu ***Security*** ➜ ***SSL Tunnel***.

The ***SECURITY*** ➜ ***SSL TUNNEL*** menu contains the following fields:

Parameter	Value
SSL Tunnel	Here you can enable and disable the function. Possible values: ■ *down* (default value): The function is disabled. ■ *up*: The function is enabled. ■
TCP Keepalive Retries	If no data is currently being exchanged on the TCP connection, you can specify how often a TCP packet is sent for test purposes to establish whether or not the partner is maintaining the current TCP session. The fields ***TCP KEEPALIVE RETRIES*** and ***TCP KEEPALIVE TIMEOUT (SEC)*** determine how often and at what interval a TCP packet is sent for test purposes. Possible values are *0* to *255*. The default value is *3*.
TCP Keepalive Timeout (sec)	If no data is currently being exchanged on the TCP connection, you can specify the number of seconds after which a TCP packet is sent to establish whether or not the partner is maintaining the current TCP session. The fields ***TCP KEEPALIVE RETRIES*** and ***TCP KEEPALIVE TIMEOUT (SEC)*** determine how often and at what interval a TCP packet is sent for test purposes. Possible values are *0* to *65535*. The default value is *5*.

Table 2-25: Fields in the ***SECURITY*** ➜ ***SSL TUNNEL*** menu

In the ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** menu you can view the tunnels that have already been created. In the ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** menu you can create new tunnels.

The ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** menu contains the following fields:

Parameter	Value
Admin status	Here you can enable and disable the tunnel. Possible values: ■ *down* (default value): The tunnel is disabled. ■ *up*: The tunnel is enabled.
Description	Enter a description that uniquely defines the tunnel.
External IP	IP address of remote terminal ■ *client*: IP address to which the client connects. ■ *server*: If an IP address is specified, a connection can only be established to a client with this IP address. If no IP address is specified, a connection can be established to any client.
External port	External port used according to the setting in the ***EXTERNAL MODE*** field.

Parameter	Value
External mode	Indicates whether the tunnel is set up at the specified ***EXTERNAL PORT*** or listens at the ***EXTERNAL PORT*** because the tunnel is being set up from the remote terminal. Possible values: ■ *client*: The tunnel is set up at the ***EXTERNAL PORT***. ■ *server*: The tunnel listens at the ***EXTERNAL PORT***.
Internal IP	IP address of the gateway The default value is *127.0.0.1*.
Internal port	Internal port used according to the setting in the ***INTERNAL MODE*** field.
Internal mode	Indicates whether the tunnel is set up from the specified ***INTERNAL PORT*** or listens at the ***INTERNAL PORT*** because the tunnel is being set up from the remote terminal. Possible values: ■ *client*: The tunnel is set up from the ***INTERNAL PORT***. ■ *server*: The tunnel listens at the ***INTERNAL PORT***.
Certificate	Enter the certificate to be used for authentication.
CA Certificate	Enter the CA (Certificate Authority) certificate to be used for authentication.

Table 2-26: Fields in the ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** menu

The ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** ➜ ***(ADVANCED) TIMER SETTINGS*** menu contains the following fields:

Parameter	Value
Retry timeout (s)	Defines the time in seconds after which another attempt should be made to set up the tunnel if the connection setup fails. Possible values are *0* to *3600*. The default value is *60*.
Maximum retries	Defines the maximum number of attempts that should be made to set up the tunnel if the connection setup fails. Possible values are *-1* to *50*. A value of *-1* means that several attempts are made to create a tunnel without restricting the number of attempts. The default value is *3*.
Reopen delay (s)	Defines the delay after which a dropped tunnel is reopened if the connection setup is successful. Possible values are *-1* to *315360000*. A value of *-1* means that the tunnel is reopened immediately. The default value is *0*.
Short hold	Defines the idle time in seconds. Possible values are *-1* to *3600*. A value of *-1-* means that the connection is always maintained, i.e. is never cleared.

Table 2-27: Fields in the ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** ➜ ***(ADVANCED) TIMER SETTINGS*** menu

2.29 VLAN prioritization

If in **System Software 7.8.7** data is received with VLAN prioritization according to IEEE 802, this data is accepted and processed further.

2.30 Checking the MAC address

To reduce the risk of spoofing attacks, an additional check has been added for the MAC address if the variable ***AllowedPeers*** = *dhcpclients* is set in the MIB table ***ipExtIfTable***.

2.31 DNS - Bailiwick Checking

In **System Software 7.8.7** Bailiwick Checking has been added, i.e. no unqueried supplied entries (Additional Resource Records) can be infiltrated in DNS replies.

2.32 Leased Line - Bundle

The new field ***Bundle Number*** has been added to the Setup Tool menu ***PRI2-x*** for the setting ***ISDN Switch Type*** = *leased line, 1 Hyperchannel (G.703 + G.704)* and ***ISDN Switch Type*** = *leased line, G.703 (unstructured, no G.704)* to allow leased line interfaces to be combined into a bundle. ***Bundle Number*** = *0* indicates that no bundle is created. A ***Bundle Number*** between 1 and 255 assigns the respective interface to a bundle with the indicated number.

2.33 OSPF

The new field ***Perform Demand procedures*** has been added to the Setup Tool menu ***IP*** ➜ ***Routing Protocols*** ➜ ***OSPF*** ➜ ***Interfaces*** ➜ **Edit** with the values

yes (default value) and *no*. The new field maps the MIB variable ***IFDEMAND*** in the MIB table ***OSPFIFTABLE*** in the Setup Tool.

2.34 HTTPS added

The option *https (tcp)* has been added to the ***SERVICE*** field in the Setup Tool menu ***SECURITY*** ➜ ***LOCAL SERVICES*** ➜ ***ACCESS CONTROL*** ➜ **ADD**.

2.35 New option for monitoring interfaces

The new option *set interface dialup* has been added to the ***OPERATION*** field in the Setup Tool menu ***MONITORING AND DEBUGGING*** ➜ ***INTERFACES*** ➜ **EXTENDED**.

2.36 Bandwidth on Demand (BoD) extended

In **System Software 7.8.7** you can automatically reduce the number of unused links / B channels for incoming connections in the MIB table ***PPPEXTIFTABLE*** using the MIB variable ***BODMODE*** = *bod-reduce-incoming*.

This is useful, for example, if Windows clients have been configured for Multilink PPP dialin, but the gateway is configured without Multilink PPP and without channel bundling.

2.37 DHCP - New MIB variable SendRepliesToRelay

The variable ***SENDREPLIESTORELAY*** has been added to the MIB table ***IPDHCPPOOLTABLE*** for sending DHCP replies from the internal DHCP server to the DHCP relay when required.

2.38 IPSec - Extended Authentication (XAuth) available

System Software 7.8.7 now offers Extended Authentication for IPSec (XAuth), an additional authentication method for IPSec tunnel users.

The gateway can take on two different roles when using XAuth as it can act as a server or as a client:

- As a server the gateway requires a proof of authorisation.
- As a client the gateway provides proof of authorisation.

In server mode multiple users can obtain authentication via XAuth, e.g. users of Apple iPhones. Authorisation is verified either on the basis of a list or via a Radius Server. If using a one time password (OTP), the password check can be carried out by a token server (e.g. SecOVID from Kobil), which is installed behind the Radius Server.

If a company's headquarters is connected to several branches via IPSec, several peers can be configured. A specific user can then use the IPSec tunnel over various peers depending on the assignment of various XAuth profiles. This is useful, for example, if an employee works alternately in different branches, if each peer represents a branch and if the employee wishes to have on-site access to the tunnel.

XAuth is carried out once IPSec IKE (Phase 1) has been completed successfully and before IKE (Phase 2) begins.

If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.

XAuth Server

If you wish to configure your gateway as a XAuth server, you can allow authentication via a Radius Server or locally.

XAuth Server with authentication via RADIUS

If you wish to use a Radius Server, you must configure this for XAuth.

1. To do this, select ***IP*** ➜ ***REMOTE AUTHENTICATION (RADIUS/TACACS+)*** ➜ ***RADIUS AUTHENTICATION AND ACCOUNTING*** ➜ **ADD** in the Setup Tool menu.
2. Select ***PROTOCOL*** = eXtended *AUTHentication*.

3. Enter the required group name for the Radius Server in the ***GROUP DESCRIPTION NEW*** field.
4. Change and add the remaining settings for the Radius Server as desired and save the settings with **SAVE**.
   The Radius Server for XAuth is created.

Create a corresponding profile.

1. To do this, select ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND** ➜ ***PEER SPECIFIC SETTINGS*** ➜ ***XAUTH PROFILE*** ➜ **edit** ➜ **ADD**.
2. Enter a unique integer ***INDEX***.
3. Enter a ***DESCRIPTION*** for the XAuth profile.
4. Select ***ROLE*** = *server*.
5. Select ***MODE*** = *radius*, select the desired RADIUS server group in the ***AAASERVERGROUP*** field and save the settings with **SAVE**.
   The profile is created with Radius Server.

Create an IPSec Peer for XAuth.

1. To do this, select ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND**.
2. Enter a ***DESCRIPTION*** for the peer.
3. Click **Peer specific Settings**.
4. Select the desired profile in the ***XAUTH PROFILE*** field.
5. Change and add the remaining settings for the IPSec peer as desired and save the settings with **SAVE**.
   The IPSec Peer is created.

XAuth Server with local authentication

If you wish to obtain authentication locally via group assignment, you can define an XAuth profile with the respective user group.

1. To do this, select ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND** ➜ ***PEER SPECIFIC SETTINGS*** ➜ ***XAUTH PROFILE*** ➜ **edit** ➜ **ADD**.
2. Enter a unique integer ***INDEX***.
3. Enter a ***DESCRIPTION*** for the XAuth profile.
4. Select ***ROLE*** = *server*.
5. Select ***MODE*** = *local*.
6. Enter an integer value in the ***USERLISTGROUPID*** field.

7. Select ***VIEW USERLIST***.
   You view the user list with the entered ***USERLISTGROUPID***.
8. Add further users by using the **ADD** button and define ***NAME*** and ***PASSWORD*** for each.
9. Save each user wirh **SAVE**.
   The XAuth profile is added with the defined user group.

Create an IPSec Peer for XAuth.

1. To do this, select ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND**.
2. Enter a ***DESCRIPTION*** for the peer.
3. Select **Peer specific Settings**.
4. Select the desired profile in the ***XAUTH PROFILE*** field.
5. Change and add the remaining settings for the IPSec peer as desired and select **Save**.
   The IPSec Peer is created.

XAuth Client

If you wish to configure your gateway as a XAuth Client proceed as follows:

Create a profile for XAuth in client mode.

1. To do this, select ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND** ➜ ***PEER SPECIFIC SETTINGS*** ➜ ***XAUTH PROFILE*** ➜ **edit** ➜ **ADD**.
2. Enter a unique integer ***INDEX***.
3. Enter a ***DESCRIPTION*** for the XAuth profile.
4. Select ***ROLE*** = *client*.
5. Enter the required user name in the ***NAME*** field.
6. Enter the password for the user and save the settings with **SAVE**.
   The profile is created.

Create an IPSec Peer for XAuth.

1. To do this, select ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND**.
2. Enter a ***DESCRIPTION*** for the peer.
3. Select **Peer specific Settings**.
4. Select the desired profile in the ***XAUTH PROFILE*** field.

5. Change and add the remaining settings for the IPSec peer as desired and save the settings with **SAVE**.
   The IPSec Peer is created.

2.39 IPSec - Dynamic Bandwidth Control available

In System Software 7.8.7 you can also select IPSec interfaces in the *INTERFACE* field in the *VOIP* ➜ *DYNAMIC BANDWIDTH CONTROL* ➜ *ADD* menu.

2.40 IPSec - Start mode for IPSec peers

System Software 7.8.7 supports a new start mode for IPSec peers.

To ensure that a tunnel is enabled as soon as the gateway is activated, a new parameter has been introduced for peer configuration. The ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** ➜ ***PEER SPECIFIC SETTINGS*** menu now allows you to choose between ***START MODE*** *Always Up* and ***START MODE*** *On demand*. If you choose ***START MODE*** *Always Up*, the gateway tries to establish a tunnel as soon as the boot up process is complete.

2.41 IPSec - Dynamic Peer and IKE Config Mode

In **System Software 7.8.7** "Dynamic Peer Mode" can be used together with IKE Config Mode.

2.42 IPSec - Dynamic Peer and XAUTH

In **System Software 7.8.7** "Dynamic Peer Mode" can be used together with XAUTH.

3 Changes

The following changes have been made in System Software 7.8.7 to improve performance and usability:

3.1 Configuration file format changed

The file format of the configuration file has been expanded to allow encryption and to ensure compatibility when restoring the configuration on the gateway in various system software versions.

The new format is a CSV format, which can be read and modified easily. In addition, you can view the corresponding file clearly using Microsoft Excel for example.

The administrator can store encrypted backup files for the configuration. When the configuration is sent by e-mail (e.g for support purposes) confidential configuration data can be protected fully if required.

In the ***CONFIGURATION MANAGEMENT*** menu, you can transfer or retrieve files to or from the TFTP host as normal using the *put* and *get* commands.

If you want to transfer a configuration file to a TFTP host using the *put* command, you can choose whether the configuration file is saved encrypted or without encryption or whether the old format is used. As a configuration file in the old format can only be reloaded on to the device with the same software version, we do not recommend that you use the old format.

When selecting the *get* command, the system can automatically recognise the file format. If the file is encrypted, the password must be entered on import.

In the ***CONFIGURATION MANAGEMENT*** menu, the options in the ***TFTP FILE NAME*** field have been expanded to include the new file format.

Field	Meaning
TFTP File Name	Only for ***OPERATION*** = *put (FLASH -> TFTP)*. *get (TFTP -> FLASH)*, *state (MEMORY -> TFTP)*. Name of the configuration file on the TFTP server. The file name format allows you to determine which format will be used for the configuration file. Possible formats: ■ *config.cf*: Previous format V0, unencrypted. For *config* you can enter any name. ■ *pwd:config.cf*: New format V1, encrypted. For *pwd* you can enter any password, for *config* you can enter any name. ■ *:config.cf*: New format V1, unencrypted. For *config* you can enter any name.

The *cf_convert.exe* program allows you to convert configuration files in the format V1 to V0 format and vice versa. You can also decrypt encrypted files using this program by entering the password, if known. The program can be found at www.funkwerk-ec.com

The basic use of this program *cf_convert.exe* is as follows:

```
cf_convert

usage: cf_convert [-options]  infile [outfile]

   infile:  input filename (or "stdin")
   outfile: output filename (or "stdout" or none)

Options:
        -p <pwd>:     decryption password
        -o <version>: 0 or 1: output format version
        -v:           increment verbosity

Examples:
  cf_convert -p passwd router.cf router.csv: decrypt file
  cat infile | cf_convert -p passwd stdin | ..: usage within pipe
```

3.2 DHCP implementation expanded

The DHCP implementation has been restructured and expanded following the new implementation of the IP address ranges (pools) (see Page 22).

DHCP The ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** menu replaces the ***IP*** ➜ ***IP ADDRESS POOL LAN (DHCP)*** menu.

The ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT*** menu consists of the following fields:

Parameter	Value
Interface	Interface to which an address range is to be assigned. When a DHCP request is received over ***INTERFACE***, one of the addresses in the address range is assigned. You can choose an interface here.
Pool	Displays the name of the IP address range defined in the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** menu The relevant name is stated in the ***DESCRIPTION*** field. You can choose an address range here.
Assignment Mode	Determines which clients are to be served from the address range. Possible values: ■ *local* (default value): Clients in the local network are assigned addresses from the address range. ■ *relay*: Clients that send requests via a relay server are assigned addresses from the address range. ■ *local/relay*: Clients from the local network and clients that send requests via a relay server are assigned addresses from the address range.
Lease Time (minutes)	Defines the maximum length of time an address from the address range is assigned to a host. Possible values: *1* .. *300*. Default value: *120*.

Parameter	Value
Gateway	Defines which IP address is transferred to the DHCP client as gateway. If no IP address is entered here, the IP address defined in the ***INTERFACE*** field is transferred.
First TFTP Server	Standard TFTP server, via which IP telephones receive the configuration. If the field ***FIRST TFTP SERVER*** = *0.0.0.0*, the value of the ***SECOND TFTP SERVER*** field is used. If the fields ***FIRST TFTP SERVER*** = *0.0.0.0* and ***SECOND TFTP SERVER*** = *0.0.0.0*, no TFTP server is available.
Second TFTP Server	Alternative TFTP server, via which IP telephones receive the configuration. If the field ***SECOND TFTP SERVER*** = *0.0.0.0*, the value of the ***FIRST TFTP SERVER*** field is used. If the fields ***FIRST TFTP SERVER*** = *0.0.0.0* and ***SECOND TFTP SERVER*** = *0.0.0.0*, no TFTP server is available.
Radius Accounting	Logs the IP address assignment and use of the IP addresses using a RADIUS server. Possible values: ■ *disabled* (default value): IP address assignment and use is not recorded. ■ *enabled*: IP address assignment and use is recorded.
Radius Group Id	Specifies the groups from which the RADIUS server must originate. Possible values: *1 .. 999999*.

Parameter	Value
Alive Check	Checks whether the clients that have been assigned an IP address from the IP address range can still be reached. Possible values: ■ *enabled*: Checks the reachability of the clients. ■ *disabled*: Does not check the reachability of the clients. Default value: dis*abled*.
Alive Test Period (seconds, 0=disabled)	Specifies the time (in seconds) after which the system checks whether the clients that have been assigned an IP address from the IP address range can still be reached. Possible values: *0* .. *65535*. Default value: *0*. If the value here is *0*, no alive test is carried out.
Admin State	Enables or disables the assignment of the IP address range to the chosen interface. Possible values: ■ *enabled* (default value): The assignment between the IP address range and the interface is enabled. ■ *disabled*: The assignment between the IP address range and the interface is disabled.

Table 3-1: New fields in the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT*** menu

IP Address Pool WAN (PPP)

The ***IP*** ➜ ***IP ADDRESS POOL WAN (PPP)*** menu has been moved to ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***IP ADDRESS POOL WAN (PPP)*** .

Assigned IP Addresses

The ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***ASSIGNED IP ADDRESSES*** menu displays a list of the reserved IP addresses with additional information.

Parameter	Value
IP Address	Shows the reserved IP address.
User Type	For ***ENTRY TYPE*** = *dynamic*. Shows the subsystem that created the entry. For ***ENTRY TYPE*** = *manual*. Shows the subsystem that assigns the IP address. Possible values: ■ *DHCP* (default value) DHCP subsystem. ■ *other*: Other subsystem. ■ *none*: The entry cannot be reserved.
Type	Entry Type Shows the IP address assignment. Possible values: ■ *dynamic*: The IP address has been assigned dynamically. The entry has been created automatically by the system. ■ *manual* (default value): The IP address has been assigned manually by the administrator. Manual entries are saved in the configuration file.

Parameter	Value
PhysAddr	Physical Address For ***ENTRY TYPE*** = *dynamic*. Shows the MAC address of the client. For ***ENTRY TYPE*** = *manual* and ***USER TYPE*** = *DHCP*. Shows the physical address, which must match the address in the DHCP request. The address is shown if it has been configured and requested.
Host Name	For ***ENTRY TYPE*** = *dynamic*. Shows a host name , if this is contained in the address request. For ***ENTRY TYPE*** = *manual* and ***USER TYPE*** = *DHCP*. Shows the host names of the client, if a host name has been configured.

Parameter	Value
State	State This information is used for support purposes. Possible values: ■ *in*: init: initial value. ■ *ch*: checking: Checks the use of an IP address (this is one of several temporary states). ■ *aw*: awrequest: Checks the use of an IP address (this is one of several temporary states). ■ *rc*: requestcheck: Checks the use of an IP address (this is one of several temporary states). ■ *cx*: checkexpired: Checks the use of an IP address (this is one of several temporary states). ■ *fo*: foreign: The IP address is being used by another system. ■ *ow*: own: The IP address is being used by the router. ■ *re*: reserved: The IP address is reserved for a specific client. ■ *al*: allocated: The IP address is currently assigned to a client.

Table 3-2: New fields in the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***ASSIGNED IP ADDRESSES*** menu

The ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***ASSIGNED IP ADDRESSES*** ➜ ***ADD/EDIT*** menu is used to assign IP addresses or to modify existing entries.

In the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***ASSIGNED IP ADDRESSES*** menu, you can see whether and how particular IP addresses are used.

In this menu you can easily change the type of assignment for an IP address. For example , you assign an IP address that is assigned to a client over DHCP to this client. To do this, select the desired entry in the list using the **space bar**. Press *s* to assign the current IP address. Similarly, you can also release assigned addresses for DHCP. To do this, select the list entry and press *f*.

In previous software versions you could assign individual IP addresses manually, implicitly in the ***IP*** ➜ ***IP ADDRESS POOL LAN (DHCP)*** menu.

The ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***ASSIGNED IP ADDRESSES*** ➜ ***ADD/EDIT*** menu contains the following fields:

Parameter	Value
IP Address	Reserved IP Address. Here you can enter all IP addresses contained in the address ranges defined in the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** menu.
User Type	Using the IP address. Possible values: ■ *DHCP* (default value) The IP address is being used for DHCP. ■ *other*: The IP address is being used for another subsystem. ■ *none*: The IP address is not being used.
Entry Type	Assigning the IP address. Possible values: ■ *dynamic*: The IP address is assigned dynamically. You can release existing entries, which have a manually assigned IP address, for dynamic IP address assignment. ■ *manual* (default value): The IP address is reserved manually for a specific client. These manual entries are saved in the configuration file.

Parameter	Value
Client Identifier	Only for ***USER TYPE*** = *DHCP*. Identifies the client. For ***ENTRY TYPE*** = *manual*. If you enter a value here, the ***PHYSICAL ADDRESS*** field is ignored. You can also use the ***PHYSICAL ADDRESS*** field as an alternative to the ***CLIENT IDENTIFIER*** field. For ***ENTRY TYPE*** = *dynamic*. ***CLIENT IDENTIFIER*** has been sent by the DHCP Client. Possible values: hexadecimal numbers. Maximum number of characters: 20.
Physical Address	Only for ***USER TYPE*** = *DHCP*. For ***ENTRY TYPE*** = *manual*. You can enter the physical address of the client here. This must match the address in the DHCP request. You can use the ***PHYSICAL ADDRESS*** field as an alternative to the ***CLIENT IDENTIFIER*** field. For ***ENTRY TYPE*** = *dynamic*. Client's MAC address.
Host Name	Only for ***USER TYPE*** = *DHCP*. Client's host name. For ***ENTRY TYPE*** = *manual*. Here you can enter a host name for the client that is sent with the answer to an address request. For ***ENTRY TYPE*** = *dynamic*. Host name contained in an address request.

Parameter	Value
Use Default Parameters	If there is a group of optional parameters, you can either use the default values or define the parameters individually. To do this, the parameters are either hidden or shown. ■ *yes* (default value): Hides the optional parameters. The default values are used. ■ *no*: Shows the optional parameters. You can define the parameters.
LeaseTime	For ***USE DEFAULT PARAMETERS*** = *no*. Defines the length of time an address from the address range is reserved for a host. Default value: *-1*. The default value adopts the value entered in the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** menu.
Gateway	For ***USE DEFAULT PARAMETERS*** = *no*. Defines which IP address is transferred to the client as gateway. Default value: *255.255.255.255*. The default value adopts the entry from the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT*** menu. The value *0.0.0.0* transmits the address of the next gateway, i.e. either the IP address of the interface of the IP address of the relay server.

Parameter	Value
Primary DNS	For ***USE DEFAULT PARAMETERS*** = *no*. Here you can enter the IP address of a global Domain Name Server. If a value is entered in the ***PRIMARY DOMAIN NAME SERVER*** field or in the ***SECONDARY DOMAIN NAME SERVER*** field, the corresponding entries in the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ ***ADD/EDIT*** menu are ignored. Default value: *255.255.255.255*. The default value adopts the corresponding entry from the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ ***ADD/EDIT*** menu. If the fields ***PRIMARY DOMAIN NAME SERVER*** = *0.0.0.0* and ***SECONDARY DOMAIN NAME SERVER*** = *0.0.0.0*, the value set for ***IP*** ➜ ***STATIC SETTINGS*** is used, if in the ***IP*** ➜ ***DNS*** menu the field ***DHCP ASSIGNMENT*** = *global* is set.
Secondary DNS	For ***USE DEFAULT PARAMETERS*** = *no*. Here you can enter the IP address of an alternative Domain Name Server. If a value is entered in the ***PRIMARY DOMAIN NAME SERVER*** field or in the ***SECONDARY DOMAIN NAME SERVER*** field, the corresponding entries in the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ ***ADD/EDIT*** menu are ignored. Default value: *255.255.255.255*. The default value adopts the corresponding entry from the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***POOLS*** ➜ ***ADD/EDIT*** menu. If the fields ***PRIMARY DOMAIN NAME SERVER*** = *0.0.0.0* and ***SECONDARY DOMAIN NAME SERVER*** = *0.0.0.0*, the value set for ***IP*** ➜ ***STATIC SETTINGS*** is used, if in the ***IP*** ➜ ***DNS*** menu the field ***DHCP ASSIGNMENT*** = *global* is set.

Parameter	Value
Primary TFTP Server	For ***USE DEFAULT PARAMETERS*** = *no*. Here you can enter the IP address for a standard TFTP server via which the IP telephones obtain their IP addresses and configuration. Default value: *255.255.255.255*. The default value adopts the entry from the ***IP ➜ IP ADDRESS POOLS ➜ DHCP ➜ ADD/EDIT*** menu. If a value (not 255.255.255.255) is entered in the ***PRIMARY TFTP SERVER*** field or in the ***SECONDARY TFTP SERVER*** field, the corresponding values in the ***IP ➜ IP ADDRESS POOLS ➜ DHCP ➜ ADD/EDIT*** menu are ignored.
Secondary TFTP Server	For ***USE DEFAULT PARAMETERS*** = *no*. Here you can enter the IP address for an alternative TFTP server via which the IP telephones obtain their IP addresses and configuration. Default value: *255.255.255.255*. The default value adopts the entry from the ***IP ➜ IP ADDRESS POOLS ➜ DHCP ➜ ADD/EDIT*** menu. If a value (not 255.255.255.255) is entered in the ***PRIMARY TFTP SERVER*** field or in the ***SECONDARY TFTP SERVER*** field, the corresponding values in the ***IP ➜ IP ADDRESS POOLS ➜ DHCP ➜ ADD/EDIT*** menu are ignored.

Parameter	Value
Alive Test Period	For ***USE DEFAULT PARAMETERS*** = *no*. Specifies the time (in seconds) after which the system checks whether the clients that have been assigned an IP address can still be reached. If a client can no longer be reached, the IP address can be assigned elsewhere. Possible values: *0* .. *65535*. Default value: *-1*. The default value adopts the value from the ***ALIVE TEST PERIOD*** field in the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT*** menu. If ***ALIVE INTERVAL*** = *0*, no test is carried out.
Radius Accounting	For ***USE DEFAULT PARAMETERS*** = *no*. Logs the IP address assignment and use of the IP addresses using a RADIUS server. Possible values: ■ *default* (default value): Adopts the value from the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT*** menu. ■ *enabled*: IP address assignment and use is recorded. ■ *disabled*: IP address assignment and use is not recorded.
Radius Group Id	For ***USE DEFAULT PARAMETERS*** = *no*. Specifies the groups from which the RADIUS server must originate. Default value: *-1*. The default value adopts the value from the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***DHCP*** ➜ ***ADD/EDIT*** menu.

Table 3-3: New fields in the ***IP*** ➜ ***IP ADDRESS POOLS*** ➜ ***ASSIGNED IP ADDRESSES*** ➜ ***ADD/EDIT*** menu

3.3 DNS - Local Name Server

In addition to global name servers, you can now define local name servers via which specific entries should be resolved. Local name servers are configured in the ***IP*** ➜ ***DNS*** ➜ ***FORWARDED DOMAINS*** ➜ ***ADD/EDIT*** menu.

The ***IP*** ➜ ***DNS*** ➜ ***FORWARDED DOMAINS*** ➜ ***ADD/EDIT*** menu contains the following additional fields:

Parameter	Value
Forward to	Defines where a host name is sent for name resolution. Possible values: ■ *Interface* (default value): Defines the WAN partner to which a connection is to be set up for name resolution. ■ *Name server*: Defines which specific name server is to be used for name resolution.
Primary	Only for ***FORWARD TO*** *name servers*. IP address of a Domain Name Server via which the specific entry is to be resolved.
Secondary	Only for ***FORWARD TO*** *name servers*. IP address of an alternative Domain Name Server.

Table 3-4: New fields in the ***IP*** ➜ ***DNS*** ➜ ***FORWARDED DOMAINS*** ➜ ***ADD/EDIT*** menu

3.4 DNS with two IP addresses

Some SIP providers use an infrastructure with optimised load balancing to guarantee high availability for their users.

When a gateway sends a DNS request to one of these providers, two IP addresses will be returned. In **System Software 7.8.7** both IP addresses are now

sent by the gateway rather than only one as in previous versions. Both addresses can be determined using the `nslookup` command, for example, in Windows XP.

3.5 DNS Query IDs generated randomly

In **System Software 7.8.7** the DNS Query IDs are generated randomly for security reasons.

3.6 MIB-Variable DNSNegotiation changed

System Software 7.8.7 has changed the ***DNSNEGOTIATION*** MIB-variable in the ***BIBOPPPDNS*** MIB table.

In the ***DNSNEGOTIATION*** MIB-variable, *enabled* and *dynamic_client* are no longer used to request or convert a WINS address. If a WINS address is requested, this is done using the *dynamic_client_with_wins* value.

3.7 MGCP Proxy Support terminated

Support for the MGCP Proxy is to be stopped from **System Software 7.8.7**.

3.8 Behaviour of ISDN interface with active NAT changed

System Software 7.8.7 has changed the behaviour of ISDN interfaces with active NAT during TCP sessions.

Until now all NAT entries were deleted if the state of the ISDN interface changed from *down* to *up*.

Now the system checks whether the IP address has remained the same. If this is the case, the NAT entries are kept.

3.9 Application Level Gateway changed

System Software 7.8.7 has changed the Application Level Gateways for use based on session rather than terminal.

The ***VoIP*** ➜ ***Application Level Gateway*** ➜ ***MGCP Terminal configuration*** and ***VoIP*** ➜ ***Application Level Gateway*** ➜ ***SIP Terminal configuration*** menus have therefore been removed.

3.10 Spanning Tree Algorithm removed

System Software 7.8.7 has removed the Spanning Tree Algorithm from the bridging function.

3.11 Possible number of NAT sessions increased

Until now the number of NAT ports for each protocol (TCP, UDP, ICMP) was limited to 4,000.

In **System Software 7.8.7** each global pool can increase dynamically in increments of 500 up to a maximum number of 32,500.

3.12 IPSec description changed

(ID 3208)

In the ***IPSec*** ➜ ***Configure Peers*** ➜ ***ADD/EDIT*** ➜ ***Peer specific Settings*** menu *p2* has been renamed *Peer No. 2*.

3.13 Ping function expanded

In **System Software 7.8.7** the Don't Fragment Flag can be set in outgoing IP packets. To do this, enter the *ping -M <IP Address>*.

3.14 Default value for number of NAT ports increased

The default value for the number of NAT ports in global pools has been increased from 4000 to 32767.

3.15 NAT pass-through added

In **System Software 7.8.7** you can now use the new MIB table ***ipNatExcludeTable*** to work off part of the data traffic from NAT, i.e. configure NAT pass-through.

3.16 UDP port numbers generated randomly

In **System Software 7.8.7** numbers are assigned randomly in the range 1024 to 60000 to UDP ports for local services. Previously, these were assigned in ascending order starting at 1024.

3.17 Processing of blank IP addresses changed

Previously *0.0.0.0* was displayed automatically when the IP address was blank. If an MIB table returns a blank IP address, this is displayed immediately as blank.

The system checks whether or not an IP address has to be entered. A message window appears if applicable.

3.18 Interface description changed

The description of the *Call-by-Call (dialin only)* option has been changed to the *Multiuser (dialin only)* option in the ***SPECIAL INTERFACE TYPES*** field of the Setup Tool menu ***WAN PARTNER*** ➜ **ADD/EDIT** ➜ ***ADVANCED SETTINGS*** .

3.19 Configuration Management expanded

The ***OPERATION*** field in the Setup Tool menu ***CONFIGURATION MANAGEMENT*** has been expanded with the options *get-all (TFTP -> FLASH)* and *put-all (FLASH -> TFTP)*.

3.20 Improved configuration change

The implementation of the IP and DHCP configuration for changing an interface from routing to bridging and vice versa has been improved to obtain consistent configurations.

3.21 MIB tables for AUX port reorganised

Due to the new Serial over IP function and in order to improve clarity to new MIB tables ***AUXCONFIGTABLE*** and ***AUXSTATTABLE*** have been created for the AUX port and the table ***TTYPROFILETABLE*** has been deleted. The ***TTYIFTABLE*** table now contains the new MIB variable ***CURRENTMODE***, the ***MODE*** variable has been supplemented with the value *soip*; some of the entries in this table have been moved to the table ***AUXSTATTABLE*** or table ***AUXCONFIGTABLE***.

3.22 RADIUS Server group configuration simplified

The MIB variable ***GROUPDESCR*** has been added to the MIB table ***RADIUSSERVERTABLE*** to make it easier to reach a group of RADIUS servers that have been grouped together with the ***GROUPID*** variable.

4 Problems Solved

The following problems have been solved in System Software 7.8.7:

4.1 IP - Memory loss

(ID 4832)

Incorrect deletion of sessions resulted in a loss of memory and a gateway reboot.

This problem has been solved.

4.2 Setup tool crash

(ID 8020)

The setup tool crashed when calling up the ***System*** ➜ ***Schedule & Monitor*** ➜ ***Keepalive Monitoring (Hosts & Ifc)*** menu.

The problem has been solved.

4.3 Stacktrace with specific value for encapsulation

(ID 7819)

In the MIB table ***biboPPPTable*** the obsolete value ***Encapsulation*** = *x25_ppp* caused a stacktrace. The other following obsolete values existed:

x31_bchan, *x75btx_ppp*, *x25_nosig*, *x25_ppp_op*t, *x25_pad*, *x25_noconfig*, *x25_noconfig_nosig* and *ipoa*.

The problem has been solved, the obsolete values have been removed.

4.4 Stacktrace for triggered RIP messages

(ID n/a)

Sending triggered RIP messages caused a stacktrace.

The problem has been solved.

4.5 Problems with the system after 194 days

(ID 7309)

After 194 days users logged in to the system, but could not execute any commands or load the setup tool.

The problem has been solved.

4.6 Email alert problems

(ID n/a)

Unintentional entries in the MIB table ***ipSifExpectTable***, not visible with SNMP, resulting in poor IP performance in some cases.

The problem has been solved.

4.7 Email alert not fully disabled

(ID 3240)

userAlertAdminStatus = *disable* did not fully disable the email alert.

The problem has been solved.

4.8 Only numbers for called party number

(ID 786)

Only numbers could be entered for a called party number.

The problem has been solved; other alphanumerical characters can now be entered.

4.9 Bootconfig - Encapsulation value not saved

(ID 7675)

If the value *HDLC Framing (only IP)* was selected in the ***WAN PARTNER*** ➜ **ADD** menu in the ***ENCAPSULATION*** field, this value was not saved in the boot configuration, but was set for ***ENCAPSULATION*** after saving the value *PPP*.

The problem has been solved.

4.10 HTTP - Incorrect system information

(ID 8345)

Incorrect information about S2M interfaces displayed in the system information on the respective HTTP page.

The problem has been solved.

4.11 MS-CHAP authentication error between Windows clients and router

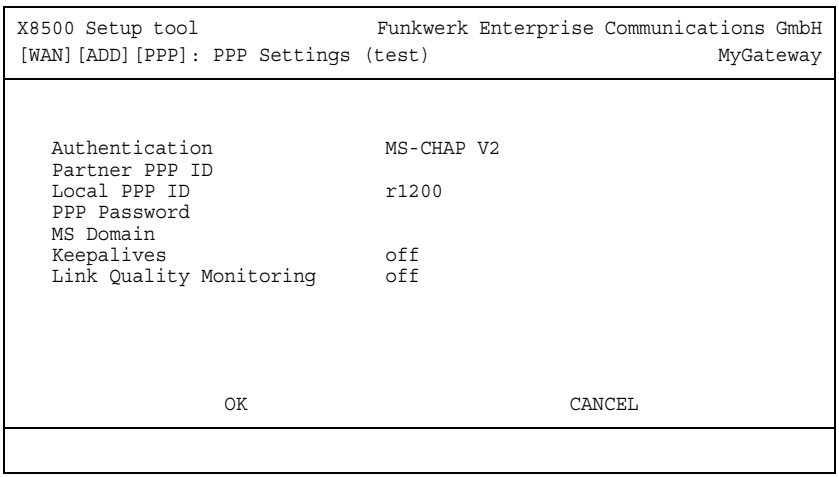
(ID 2318)

The authentication negotiation between Windows clients and the route failed over PPP or PPTP connections, if the login name was used with the domain names, e.g. DEVELOPMENT\Developer.

The problem has been solved.

In MS-CHAP V1 the full identification name (domain name and login name) is used for authentication.

In MS-CHAP V2 only the login name is used for authentication. The domain name is checked separately. To do this, enter the domain name, if any, in the new ***MS DOMAIN*** field. The field is only displayed if ***AUTHENTICATION*** = *MS-CHAP*, *MS-CHAP V2* or *CHAP* + *PAP* + *MS-CHAP*.



4.12 RADIUS - Incorrect use of MS-CHAPv2 instead of MS-CHAPv1

(ID 7016)

During authentication via a RADIUS server with *MS-CHAP V1*, *MS-CHAP V2* was mistakenly used for callback instead.

The problem has been solved.

4.13 RADIUS - Reload with two servers failed

(ID 6873)

If working with two RADIUS servers, one configured with reload interval (MIB-variable ***RELOADINTERVAL*** in the MIB table ***RADIUSSERVERTABLE***) and the other configured without reload interval, no reload is carried out when changing from the server with reload interval to the server without reload interval.

The problem has been solved.

4.14 RIP - Next Hop information not sent

(ID 4165)

Next Hop information not sent in route announces (RFC 2453).

The problem has been solved.

4.15 RIP - Incorrect metric 0 in triggered updates

(ID 7542)

Triggered update packets contained routes with the incorrect metric value *0*.

The problem has been solved.

4.16 RIP source IP address incorrect

(ID 10378)

RIP packets with the source IP address 0.0.0.0. were sent via WAN interfaces.

The problem has been solved.

4.17 DNS - Name resolution failed

(ID 6916)

Name resolution on the device may suddenly stop functioning after a few days.

The problem has been solved.

4.18 DNS request failed

(ID n/a)

The first DNS request sent to the system stops the system.

The problem has been solved.

4.19 CAPI - Unintentional system reboot

(ID 7257)

Once a connection was established with the message ".. Outgoing call established" the device unintentionally rebooted.

The problem has been solved.

4.20 CAPI - Incorrect version number

(ID 4965)

The version numbers 1.1 and 2.0 have been specified for CAPI. However, the device only supports CAPI 2.0.

The problem has been solved.

4.21 NAT policies deleted incorrectly

(ID n/a)

NAT policies may be deleted, even if the IP address has not changed. This was reported on PPP connections with dynamic client, but could also happen on other connections.

The problem has been solved.

4.22 PPP - Incomplete CLID test

(ID 6528 - Only for devices with ISDN)

An incomplete CLID test resulted in calls being accepted even if the calling partner number was incorrect.

The problem has been solved.

4.23 PPP - Multi-user entries not observed

(ID 5650)

When deciding whether or not an incoming call is accepted, multi-user entries in ***BIBOPPPTABLE*** were not observed.

The problem has been solved.

4.24 PPP - Use of several switched lines failed

(ID 8411)

If several switched lines were configured for a PPP interface and the first line was not available, the other numbers were not used.

The problem has been solved.

4.25 PPP - Authentication of leased lines failed

(ID 7536)

Authentication failed for PPP leased lines.

The problem has been solved.

4.26 PPP - Unintentional system reboot

(ID n/a)

The device unintentionally rebooted when establishing the connection.

The problem has been solved.

4.27 Multilink PPP - Data packet order incorrect

(ID 8428)

With multilink PPP, small data packets were not transported in the correct order.

The problem has been solved.

4.28 PPPoE and Ethernet interfaces - Problems with external DSL modems

(ID 9225)

If the MIB-variable ***MaxTxRate*** in the ***qosIfTable*** table was changed and in the ***ifTable*** table the variable ***OperStatus*** = *up*, the MIB-variable ***Speed*** in the ***ifTable*** MIB table was not adjusted for PPPoE and Ethernet interfaces. This led to latency problems in scenarios with external DSL modems.

The problem has been solved.

4.29 PPPoE problems

(ID 10668)

Problems sometimes occurred when establishing a PPPoE session if the provider's BRAS was not operating according to RFC 2516.

The problem has been solved.

4.30 PPPoE Passthrough - Interfaces not displayed correctly

(ID 10106)

The bridge group interfaces were not displayed in the ***PHYSICAL OR VIRTUAL ETHERNET PORT ATTACHED TO PPPOE CLIENT(S)*** area in the Setup Tool menu ***PPP ➜ PPPOE PASSTHROUGH***.

The problem has been solved.

4.31 Multilink PPPoE - Panic

(ID 8512)

A panic occurred if the load exceeded 10 Mbps on multilink connections with two or more PPPoE links.

The problem has been solved.

4.32 PPTP - Incorrect value in the via IP Interface field

(ID 3105)

If in the ***PPTP ➜ ADD ➜ IP ➜ BASIC IP-SETTINGS*** menu the fields ***PPTP VPN PARTNER'S IP ADDRESS***, ***VIA IP INTERFACE***, ***REMOTE IP ADDRESS*** and ***REMOTE NETMASK*** were selected and this menu was called up again after saving this configuration, the value ***AUTO*** was mistakenly displayed for the ***VIA IP INTERFACE*** field.

In addition, the host route to ***PPTP VPN PARTNER'S IP ADDRESS*** was duplicated when resetting the ***VIA IP INTERFACE*** field after saving.

The problems have been solved.

4.33 PPTP connection setup failed

(ID 10379)

The PPTP connection setup sometimes failed if it had been initiated externally and if IP load balancing was used.

The problem has been solved.

4.34 PPTP connection setup failed

(ID 2787)

The PPTP connection setup sometimes failed if it had been initiated externally, if the gateway was a tunnel endpoint and if PPTP passthrough was activated.

The problem has been solved.

4.35 MPPE for X.21 leased line connections failed

(ID 7767)

MPPE could not be used as encryption for leased line connections over X.21.

The problem has been solved.

4.36 BRRP - Configuration of virtual router not correct

(ID 8262)

In the ***BRRP*** ➜ ***CONFIGURATION*** ➜ ***ADD*** menu, after setting or changing the ***VIRTUAL ROUTER ID*** field, the ***VIRTUAL INTERFACE***, ***MASTER IP ADDRESS*** and ***MAC ADDRESS*** fields were reset to their default values.

The problem has been solved.

4.37 BRRP - Incorrect IP address

(ID 10112)

In the Setup Tool menu ***BRRP*** ➜ ***MONITORING*** the IP address of the physical interface was displayed by mistake instead of the IP address of the virtual interface.

The problem has been solved.

4.38 Inconsistent layer 2 mode

(ID 1737)

The value of the layer 2 mode for leased lines was mistakenly taken from MIB table ***PPP*** and not from the tables ***ISDNCHTABLE*** or ***X21IFTABLE***.

The problem has been solved.

4.39 SIF and NAT - Extended passive FTP connections blocked

(ID 7197)

Although an allow rule was created for FTP connections, the SIF blocked the data connections for an extended passive FTP connection.

The problem has been solved.

4.40 SIF - Unintentional filtering

(ID n/a)

Local data traffic was blocked by the SIF even though local filtering was disabled. This also occurred when the SIF was deactivated completely if deny rules existed in the SIF configuration.

The problem has been solved.

4.41 SIF - Default entries not loaded

(ID n/a)

The default entries for ***ipSifAliasServiceTable*** and ***ipSifAliasAddressTable*** were not loaded if several configurations were stored on the gateway.

The problem has been solved.

4.42 SIF - Unintentional blocking of data traffic

(ID n/a)

Data traffic blocked by unstable or inconsistent entries in the MIB tables ***ipSifAliasAddressTable*** and ***ipSifAliasTable***.

The problem has been solved.

4.43 SIF - Removing a service group causes a stacktrace

(ID 7751)

When configuring a stateful inspection firewall, removing a service group causes a stacktrace.

The problem has been solved.

4.44 SIF did not work correctly with interface groups

(ID 8934)

If a stateful inspection firewall was configured together with interface groups, the filters did not work correctly.

The problem has been solved.

4.45 SIF - Unexpected MIB table entries

(ID 6194)

Unexpected table entries appeared in MIB table ***ipSifAliasAddressTable***.

The problem has been solved.

4.46 SIF - System crash when registering with a provider

(ID 6016)

System crash when attempting to register with a provider with an incorrect IP address.

The problem has been solved.

4.47 SIF - Memory problems in many sessions

(ID 9221)

As the number of sessions was unlimited with a SIF, the system crashed when there was a large number of sessions due to memory problems.

The problem has been solved.

4.48 SIF - Second put command failed

(ID 8542)

When sending two consecutive put commands over TFTP with a SIF, the second put command failed.

The problem has been solved.

4.49 SIF - Source port test not working

(ID n/a)

The test for the MIB-variable ***SOURCEPORT*** in the MIB table ***IPSIFALIASSERVICETABLE*** failed.

The problem has been solved.

4.50 SIF - Address aliases accidentally deleted

(ID 7689)

Address aliases accidentally deleted during PPP inband authentication for a SIF.

The problem has been solved.

4.51 SIF - Stacktrace during Configuration

(ID 11405)

Upon configuring the SIF services, a stacktrace occurred and the Setup was terminated.

The problem has been solved.

4.52 SIF - Incorrect port range

(ID n/a)

Values from *0* to *65535* could be entered by mistake in the ***RANGE*** field in the the Setup Tool menu ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES*** ➜ **ADD/EDIT**.

The problem has been solved; the possible values have been changed to *1 - 65536*.

4.53 IPSec - Unintentional reboot

(ID 8395)

The device rebooted when host routes, e.g. for logging in externally, were entered in an IPSec Peer with traffic lists.

The problem has been solved.

4.54 IPSec - Panic

(ID 7218)

The message "improper state 5" was output on the console. This resulted in a panic.

The problem has been solved.

4.55 IPSec - Panic

(ID 10155)

A panic occurred if a subject name was entered using an incorrect notation for certificate enrolment over SCEP.

The problem has been solved.

4.56 IPSec - Panic without reboot

(ID 10024)

If an IPSec peer with traffic listen entry or a traffic list entry was deleted, a panic without reboot occurred.

The problem has been solved.

4.57 IPSec - Incorrect value of LifeSeconds MIB-variables

(ID 7825)

If the value 65535 of MIB-variable ***LIFESECONDS*** in the ***IKEPROFILETABLE*** MIB table was overwritten, an incorrect value was used.

The problem has been solved.

4.58 IPSec - Incorrect name resolution for IPSec peers

(ID 5754)

Incorrect IP addresses assigned during name resolution for peers with several host names.

The problem has been solved.

4.59 IPSec - RADIUS reload failed

(ID 5379)

If a RADIUS reload of IPSec peers was carried out frequently, the reload failed after a certain gateway time.

The problem has been solved.

4.60 IPSec - Dynamic peer not working

(ID n/a)

Configuration not working if a dynamic peer was configured on a virtual interface. A peer based on traffic lists was working.

The problem has been solved.

4.61 IPSec - No automatic CRL import via event scheduler

(ID n/a)

Unable to import CRLS via the event scheduler as the import could not be confirmed via the scheduler.

The problem has been solved.

4.62 IPSec - No RIP

(ID 7486)

RIP not working via an IPSec tunnel.

The problem has been solved.

4.63 IPSec - Phase 2 not initiated

(ID 3432)

Phase 2 not initiated if the interface of the source route was down.

The problem has been solved.

4.64 IPSec - Phase 2 negotiation not working

(ID 7284)

Phase 2 negotiation not working after silent disconnect.

The problem has been solved.

4.65 IPSec - Phase -2 negotiation failed

(ID 10877)

A false netmask was tried for phase-2 negotiation under certain conditions and the negotiation failed accordingly.

The problem has been solved.

4.66 IPSec phase-2 bundles do not transmit local network

(ID 11409)

Local network not transmitted with IPSec phase-2 bundles, if no local IP address was configured on the router.

The problem has been solved.

4.67 IPSec - Interface reset not possible

(ID 3232)

Unable to reset an IPSec interface in the ***MONITORING AND DEBUGGING*** ➜ ***INTERFACES*** ➜ ***<INTERFACE>*** ➜ **EXTENDED** menu with the ***OPERATION*** > *reset* setting.

The problem has been solved.

4.68 IPSec - DELETE button mistakenly displayed

(ID 7895)

A **Delete** button was mistakenly displayed in the ***IPSEC*** ➜ ***IKE (PHASE 1) DEFAULTS*** ➜ ***<EDIT>*** ➜ **ADD** ➜ ***VIEW PROPOSALS*** menu. However, no entries can be deleted in this menu.

The problem has been solved.

4.69 IPSec - Setting option missing for Twofish key length

(ID n/a)

When configuring an IKE or IPSec proposal there is no option to specify a key length for using Twofish.

In **System Software 7.8.7** 128, 192 and 256 bit length keys can be used. After updating the software, the IPSec configuration is not adjusted automatically, as new proposals have to be created. In a new configuration, this support function is enabled automatically.

4.70 IPSec - Tunnel setup

(ID 9004)

If an IPSec tunnel was setup using a packet generated locally by the gateway, the phase 2 of the tunnel was setup with the IP address of the source interface and a 32 bit netmask, instead of with the values of the corresponding subnet (e.g. 192.168.1.254/32 instead of 192.168.1.0/24). This caused errors in the tunnel setup, particularly with open source IPSec solutions.

This problem has been solved

4.71 IPSec - Irrelevant menus displayed

(ID 10077)

In the Setup Tool the menus for Pre and Post IPSec Rules were displayed even if the configuration was purely interface-based. A configuration in this menu could have unexpected results.

The problem has been solved.

4.72 IPSec - Incorrect input mask for Block Time field

(ID 11840)

A value of up to four digits could be entered in the ***Block Time*** field in the setup tool menu ***IPSec*** ➜ ***IKE (Phase 1)*** ➜ **Edit** ➜ **ADD**, although the value range for this field *-1* to *86400*.

The problem has been solved.

4.73 IPSec - Duplicate OSPF interfaces

(ID 9171)

OSPF interface were duplicated after a RADIUS reload in IPSec with RADIUS.

The problem has been solved.

4.74 IPSec / OSPF - Unwanted OSPF update

(ID 10371)

An unwanted OSPF update was triggered during an IPSec tunnel to renegotiate the key. This interrupted the tunnel depending on the configuration.

The problem has been solved.

4.75 OSPF - Authentication Type

(ID 2843)

OSPF not working if ***AUTHENTICATION TYPE*** = *md5*.

The problem has been solved.

4.76 OSPF

(ID 7724)

If OSPF was active on interface *1000*, only one LAN route was propagated via interface *1400* on interface *1000*.

The problem has been solved.

4.77 DynVPN callback via voice call failed

(ID 7578)

When attempting to initialise a DynVPN via a voice call, the message "Requested L1 resources not available" was returned.

The problem has been solved.

4.78 X.25 connection failed

(ID 7960)

No connection could be established between a CISCO device and a bintec device via the X.21 interfaces.

The problem has been solved.

4.79 X.25 - LLC reconnection failed

(ID 3881)

Reconnection failed when attempting to re-establish an interrupted LLC connection.

The problem has been solved.

4.80 SNMP - MIB search operations failed

(ID 4767)

Search operations within MIB accounts failed.

The problem has been solved.

4.81 SNMP Shell - Faulty input/output link (pipe)

(ID n/a)

Processes sometimes froze when using a pipe.

The problem has been solved.

4.82 SNMP shell - Problems with Signal Interrupt

(ID n/a)

When sending a SIGINT (Signal Interrupt; e.g. with the key combination **Ctrl** + **c** or by entering *kill*) to the SNMP shell whilst displaying the prompt, the prompt sometimes changed and it was impossible to display the previously shown table.

The problem has been solved.

4.83 SNMP shell - ifoperstatus shown incorrectly

(ID 4751)

Interfaces with extended routes were shown with an incorrect status through `ifoperstatus`.

The problem has been solved.

4.84 SNMP Shell - Command not Executed Properly

(ID 11448)

Command execution on the shell malfunctioned if the batch included a command which the shell interprets as an external command.

The problem has been solved.

4.85 Dynamic Bandwidth Control

(ID 7699)

The bandwidth calculation of the data packet sizes for the Dynamic Bandwidth Control function did not work for ipoa interfaces.

The problem has been solved.

4.86 ICMP_TIMESTAMP Messages - Format changed

(ID n/a)

Due to an error in the firmware of some competitors, the format of ICMP_TIMESTAMP and ICMP_TIMESTAMP_REPLY Messages was expanded.

Funkwerk devices can now handle expanded ICMP_TIMESTAMP and ICMP_TIMESTAMP_REPLY Messages.

4.87 QoS - Value not set for field direction

(ID 3656)

In the ***QoS*** ➜ ***IP Classification and Signalling*** ➜ ***ADD/EDIT*** menu, the value selected in the ***Direction*** field was not saved with **SAVE** and did not appear in the list of classification and signalling rules.

The problem has been solved.

4.88 QoS - High Priority Queue without Effect

(ID 11304)

In combination with certain SIF rules it could occur that a high priority queue was not handled properly.

The problem has been solved.

4.89 QoS - Counter overrun

(ID n/a)

Due to the high data rates of modern interfaces, the octet counter often overran when using QoS.

The problem has been solved; 64 bit counters are now used.

4.90 IP Load Balancing - Display of port ranges incomplete

(ID 8370)

If the ***DISTRIBUTION POLICY*** = *service/source-based routing* field is set in the ***IP ➜ BANDWIDTH MANAGEMENT (TDRC / LOAD BALANCING / BOD) ➜ IP LOAD BALANCING OVER MULTIPLE INTERFACES ➜*** **ADD/EDIT** menu and a value was selected for the ***INTERFACE*** field, in the ***IP ROUTING LIST*** submenu for example the ***SERVICE*** = *client_1* field was set, only the first value of the relevant port range was displayed.

The problem has been solved, the complete port ranges are displayed.

4.91 VoIP - Registration failed with 1and1

(ID 5621)

Registration with the provider failed with the VoIP telephone snom 190.

The problem has been solved.

4.92 Syslog messages with following zeros

(ID 8146)

Syslog messages were sent with following zeros.

The problem has been solved.

4.93 Syslog messages - Values not output

(ID 10305)

In syslog messages values were not output in 64 bit format; "u" was displayed instead.

The problem has been solved; the values are output correctly.

4.94 Inconsistent MIB-variables

(ID 7839)

Inconsistent MIB-variables occurred if a configuration was loaded via tftp get.

The problem has been solved.

4.95 IGMP - Cache Entries not Removed

(ID 11356)

Cache entries of the IGMP proxy are not properly removed.

The problem has been solved.

4.96 Ethernet - MAC Address Ignored

(ID 11245)

If an Ethernet interface was changed from "DHCP" to "Manual", a specified MAC address was ignored, and the MAC address of the Ethernet chip was used instead.

The problem has been solved.

4.97 Stacktrace for routing over L2TP or bridging over L2TP

(ID 10619)

For routing over L2TP or bridging over L2TP, high data rates could cause a panic followed by a stacktrace.

The problem has been solved.

4.98 Number of Telnet sessions unlimited

(ID 1882)

If several incoming Telnet sessions were opened simultaneously, the gateway stopped responding.

The problem has been solved; the number of Telnet sessions is now limited, the default value is *10*.

4.99 Cert - No support for negative indices

(ID 11285)

The `cert` tool on the SNMP shell did not support any certificates with a negative index and without description. However, certain certificates are saved in this format, but could not be deleted manually.

The problem has been solved.

4.100 Name server responses not accepted

(ID n/a)

"Manke" DNS requests were not accepted by mistake and were rejected with the error message "Bailiwick check failed for <xxx>.com". The domain association was miscalculated internally when validating a top level record.

The problem has been solved.

4.101 Compatibility issues with converters

(ID 10878)

Problems occurred with some G.703 converters on X.21 interfaces.

The problems have been solved.

4.102 Problems displaying an IP address

(ID 10833)

If the IP address has been changed and not saved in the ***LOCAL IP NUMBER*** field in the ***ETHERNET*** ➜ **EDIT** menu in the Setup Tool in bridging mode, the current IP address can be seen in the first ***LOCAL IP NUMBER*** field and the new IP address entered in the second ***LOCAL IP NUMBER*** field by scrolling.

The problem has been solved.

4.103 Missing field mode

(ID 9296)

The ***MODE*** field was not displayed for the settings ***ROUTE TYPE*** = *Default route* and ***NETWORK*** = *LAN* in the Setup Tool menu ***IP*** ➜ ***ROUTING*** ➜ ***ADDEXT***.

The problem has been solved.

4.104 Deleting two TDRC entries triggers a stacktrace

(ID 6464)

If two entries were created for a T-DSL interface in the Setup Tool menu ***IP*** ➜ ***BANDWIDTH MANAGEMENT (TDRC / LOAD BALANCING / BOD)*** ➜ ***TCP DOWNLOAD RATE CONTROL (TDRC)*** ➜ **ADD**, one with ***OPTIMIZE DOWNLOAD RATE VIA TCP ACK PRIORISATION*** = *yes* and the other with ***OPTIMIZE DOWNLOAD RATE VIA TCP ACK PRIORISATION*** = *no* and ***TDRC MODE*** = *static (fixed maximum rate for TCP download)*, both entries were selected and deleted, the message "Exception: 0x1c00 Data breakpoint Debug" appeared followed by a stacktrace without reboot.

The problem has been solved.

4.105 Entries deleted

(ID 10105)

If an entry had been made for ***IPEXTRTTABLE*** on the SNMP shell, this was deleted the next time the corresponding interface is changed in the Setup Tool menu ***BASIC IP SETTINGS***.

The problem has been solved.