



X8500

Software Configuration Guide



Installation and Configuration

Copyright © 2003 BinTec Communications AG, all rights reserved.

Version 1.3

Document #71000R

February 2003



Purpose This manual explains the installation and initial configuration of **X8500** with software release 6.2.1 or later. For up-to-the-minute information and instructions concerning the latest software release, you should always read our release notes, especially when carrying out a software update to a later release level. The latest release notes can always be found at www.bintec.net.

Liability While every effort has been made to ensure the accuracy of all information in this manual, BinTec Communications AG cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information, including changes and release notes for **X8500**, can be found at www.bintec.net.

As a multiprotocol router, **X8500** sets up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. BinTec Communications AG 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 BinTec Communications AG.

All other product names and trademarks mentioned are the property of the respective companies and manufacturers.

Copyright All rights are reserved. No part of this publication may be reproduced or transmitted in any form or by any means – graphic, electronic, or mechanical – including photocopying, recording in any medium, taping, or storage in information retrieval systems, without the prior written permission of BinTec Communications AG. Adaptation and especially translation of the document is inadmissible without the prior consent of BinTec Communications AG.

Guidelines and standards **X8500** complies with the following guidelines and standards:

- R&TTE Directive 1999/5/EC
- CE marking for all EU countries and Switzerland



You will find further information in the "Declarations of Conformity" at www.bintec.net.

How to reach BinTec

BinTec Communications AG
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 911 96 73 0

Fax: +49 911 688 07 25

Internet: www.bintec.de

BinTec Communications France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
France

Telephone: +33 5 57 35 63 00

Fax: +33 5 56 89 14 05

Internet: www.bintec.fr and
www.bintec.de/fr





	Table of Contents	5
1	Welcome!	11
	1.1 BinTec's X8500 CD	13
	1.2 Documentation from BinTec	14
	1.3 About this Manual	16
	1.3.1 Contents	16
	1.3.2 Meaning of Symbols	17
	1.3.3 Typographical Elements	18
2	General Safety Precautions	19
3	Getting Started	23
	3.1 Connection Methods	24
	3.1.1 Connecting Over the Serial Interface	25
	3.1.2 Connecting Over a LAN	27
	3.1.3 Connection Over ISDN	28
	3.2 Logging In	30
	3.3 Configuration Options	32
	3.4 Using the Setup Tool	33
	3.4.1 Menu Layout	34
	3.4.2 Menu Navigation	35
	3.4.3 Menu Commands	36
	3.4.4 Searching Lists	37
	3.4.5 Changing the Password	38
	3.4.6 Convention	39
	3.4.7 Menu Structure	40
	3.5 In Advance of Configuration	45
	3.5.1 Gathering Information	45

3.5.2	Checking the TCP/IP Protocol	46
3.5.3	Installing BRICKware Under Windows	49
4	Initial Configuration with Setup Tool	53
4.1	Basic Router Settings	55
4.1.1	Entering License(s)	56
4.1.2	Entering System Data	58
4.1.3	Configuring the LAN Interface	61
4.1.4	Configuring X8500 as DHCP Server	65
4.1.5	Setting Filters	68
4.2	Configuring WAN Interfaces	73
4.2.1	Configuring ISDN BRI interface	73
4.2.2	Broadband Internet Access (xDSL) with X8500	86
4.3	X8500 and the WAN	94
4.3.1	Entering a WAN Partner	94
4.3.2	Creating a Routing Entry	115
4.3.3	Activating Network Address Translation (NAT)	121
4.3.4	Examples	122
4.4	Saving the Configuration File	126
4.5	Configuring PCs in Your LAN	127
4.5.1	Configuring a PC	127
4.5.2	Remote CAPI Interface Configuration	130
4.5.3	Finding PCs on Your Partner's Network	131
4.6	Testing Your Configuration	134
5	Advanced Configuration with the Setup Tool	135
5.1	General WAN Settings	136
5.1.1	Dynamic IP Address Server	136
5.1.2	CAPI User Concept	138
5.1.3	General PPP Settings	142

5.1.4	X.31 TEI (Terminal Endpoint Identifier)	144
5.2	Settings Specific to WAN Partners	146
5.2.1	Delay After Connection Failure	146
5.2.2	Channel Bundling	147
5.2.3	Channel Bundling – Bandwidth On Demand (BOD)	149
5.2.4	Always On/Dynamic ISDN (AO/DI)	157
5.2.5	Application-Controlled Bandwidth Management (BOD)	165
5.2.6	Layer 1 Protocol (ISDN B-Channel)	171
5.2.7	IP Transit Network	173
5.2.8	Name Server	177
5.2.9	Routing Information Protocol (RIP)	180
5.2.10	Compression	183
5.2.11	Proxy ARP (Address Resolution Protocol)	185
5.2.12	Keepalive Monitoring	187
5.3	Basic IP Settings	193
5.3.1	System Time	193
5.3.2	Name Resolution in X8500 with DNS Proxy	197
5.3.3	Port Numbers	214
5.3.4	BOOTP Relay Agent	215
5.4	Quality of Service	218
5.4.1	Defining IP Filters	220
5.4.2	Classification and (TOS) Signaling	221
5.4.3	Activating the Classification	226
5.4.4	Defining QoS Bandwidth Management Policies	227
5.5	Bridging	239
5.6	Extra License Features	240
6	Configuration of Expansion Cards and Modules	241
6.1	WAN Interface Expansion Card for ISDN PRI and G.703	243

6.2	Expansion Card X8E-2BC	252
6.2.1	Communication Modules for ISDN BRI	252
6.2.2	Communication Module CM-PRI for ISDN PRI	255
6.2.3	Communication Module CM-100BT	256
6.2.4	Serial WAN Interfaces Communication Module CM-X21	257
6.3	Expansion Card X8E-DSP	262
6.4	Expansion Card for X.21/V.35	263
6.5	Resource Modules with Digital Modems	270
6.6	Resource Module for Encryption and Compression (XT-VPN)	280
6.7	Resource Module for X.21/V.35 (XT-2SYNC)	281
7	Configuration of Security Functions and Firewall	283
7.1	Activity Monitoring	284
7.1.1	Syslog Messages	284
7.1.2	Monitoring Functions in the Setup Tool	289
7.1.3	Credits Based Accounting System	293
7.1.4	Activity Monitor	296
7.2	Access Security	299
7.2.1	Logging In	299
7.2.2	Checking the Calling Party Number	300
7.2.3	Authentication of PPP Connections with PAP, CHAP or MS-CHAP	301
7.2.4	Callback	302
7.2.5	Closed User Group	304
7.2.6	Access to Remote CAPI	304
7.2.7	NAT (Network Address Translation)	304
7.2.8	Filters (Access Lists)	315
7.2.9	Local Filters	328
7.2.10	Back Route Verification	331
7.2.11	TAF Agent	332
7.2.12	Extended IP Routing (XIPR)	332

7.3	Line Tapping Security	338
7.3.1	Encryption	338
7.3.2	VPN (with extra license)	341
7.3.3	IPSec (with extra license)	341
7.4	Special Features	343
7.4.1	Start-up Procedure	343
7.4.2	Auto Logout	343
7.4.3	Prevention of Denial-of-Service Attacks	343
7.5	Checklist	345
8	Configuration Management and Flash Card	347
8.1	Administration of Configuration Files	348
8.2	Smart Media Flash Card	356
8.2.1	Formatting the Flash Card	356
8.2.2	File System and Directory Structures on the Flash Card	356
8.2.3	Behavior of X8500 with Flash Card in Boot Operation and Saving the Configuration	357
8.2.4	Configuration Management for the Flash Card	359
8.2.5	Command <code>fssh</code> in the SNMP Shell of X8500	363
8.3	Updating Software	368
8.3.1	BOOT Sequence	369
8.3.2	Updating BOOTmonitor	370
8.3.3	Update System Software	371
8.3.4	Updating Module Logic	373
9	Troubleshooting	375
9.1	Aids to Troubleshooting	376
9.1.1	Local SNMP Shell Commands	376
9.1.2	External Aids	377
9.2	Typical Errors and Procedure	379
9.2.1	System Errors	379

9.2.2	ISDN Connections	380
10	Important Commands	385
10.1	SNMP Shell Commands	386
10.2	BRICKtools for Unix Commands	393
11	General Safety Precautions in German	395
	Glossary	399
	Index	417

1 Welcome!

Congratulations on deciding to buy the **X8500** modular communications server from BinTec Communications AG – a remote access server solution for central corporations and for Internet Service Providers.



Figure 1-1: **X8500** - the central site router for professional applications

X8500 Feature List

- System card** The X8A-SYS system card is the control unit of **X8500**. With its Basic Rate Interface, the two Fast Ethernet ports and the serial console port, the system card provides for local and remote configuration, administration and monitoring of **X8500**.
- Expansion cards** Eight slots for expansion cards enable **X8500** to grow in line with your requirements. Thus a high degree of flexibility is assured.
- Resource modules** The expansion cards can also be equipped with powerful and scalable resource modules. This offers extremely high efficiency through high port or modem density.

Module carrier card The module carrier card can be fitted with BIANCA/BRICK-XL2 or BIANCA/BRICK-XM modules.

Hot Swap Any expansion card may be inserted into an unused slot while **X8500** is operating. Likewise, a PRI, G.703, DSP or SYNC expansion card can be replaced with a new one of the same type with the same licenses, as long as the new card has as many interfaces and as many modules as the old one.

Redundancy Two slots are provided for power supply units so you can set up a redundant power supply system with **X8500**.

RAS The flexible remote access server **X8500** can be used for WAN access, remote CAPI server or LAN router. **X8500** supports the TCP/IP and X.25 protocols and is also suitable for bridging other protocols based on the spanning tree method.

Remote CAPI Using BinTec's remote CAPI software, applications based on the widely used CAPI interface can be used network-wide. Thus the available ISDN connections can be used more effectively.

Security The features supplied include BinTec's well-tried security package SAFER-NET™. This package contains security technologies such as filters, Network Address Translation (NAT) and access passwords. The security functions protect **X8500** and the network connected to it against unauthorized access.

The future New technologies and developments are vital for BinTec Communications AG. **X8500**'s flexible platform with eight expansion slots and a powerful processor permits the immediate integration of new WAN/LAN technologies and features. This makes **X8500** a future-oriented and migration-capable device.

You can download BinTec's current software at www.bintec.net.

1.1 BinTec's X8500 CD

You will find all the programs you need for the installation, configuration and administration of **X8500** on your **X8500** CD.

BRICKware **BRICKware for Windows** contains Windows utility programs:

- **DIME Tools** are for monitoring and administration of your **X8500**.
- You gain access to **X8500** via the serial interface using the terminal program **Device at COM1** or **Device at COM2**.
- The **Configuration Manager** allows you to configure and administrate all BinTec routers in the network via a graphic interface. Here you can view and edit SNMP tables and variables.
- Remote CAPI Client:
The Remote CAPI Client allows you to use communications applications based on the standard CAPI interface.
- Token Authentication Firewall (TAF) program (optional):
This software package is required if you are using the Security Dynamics security system.
- The **Activity Monitor** enables you to monitor the utilization of **X8500** at a glance.

More detailed descriptions of all software programs can be found in our online document **BRICKware for Windows**.

What else? On the **X8500** CD, you will find a range of other useful directories in which you can find the following, for example:

- The documentation in electronic form (see also [chapter 1.2, page 14](#))
- A copy of the router software
- UNIX tools (administration)
- Adobe's Acrobat Reader

1.2 Documentation from BinTec

The following documentation is currently available:

- **Software Configuration Guide**
This manual.
- **Hardware Installation Guide**
Included with X8A-BOSS.
- Installation guide for the **X8500** expansion cards
Included with the expansion card(s) you purchase.
- Installation guide for the **X8500** power supply unit(s)
Included with X8A-PS.
- Installation guide for the **X8500** fan unit
Included with X85-FAN.
- Installation guide for rack-mounting **X8500**
Included with X85-RACK.
- Reference manuals (English, PDF/HTML)
 - **Software Reference** (PDF)
Online reference with detailed information on functions described here, a reference for the internal SNMP table structures and the operation of the SNMP shell.
 - **MIB Reference**
HTML document with short descriptions of SNMP tables and variables for **X8500**.
- **BRICKware for Windows** (English, PDF)
User's guide for Windows utility programs (**BRICKware**).
- **Release Notes** (PDF and/or printed)
Up-to-the-minute information and instructions concerning the latest software release, description of all changes undertaken since the previous release.

In the **Release Notes Firmware Logic and BOOTmonitor Update**, you will find instructions to help you upgrade BOOTmonitor and/or firmware logic, if applicable.

- **Release Notes** for the operation of routers in UK (English, PDF)
Instructions for the operation of BinTec routers in Great Britain.

You received this documentation together with **X8500**. The **Hardware Installation Guide** manual is provided in printed form. Your BinTec Companion CD also contains the complete documentation in electronic form (PDF, HTML). In addition to your Companion CD documentation, you can download all the latest documentation free of charge from our WWW server at www.bintec.net.

1.3 About this Manual

1.3.1 Contents

This manual is structured as follows:

Chapter	Contents
1: "Welcome!"	General introduction, scope of supply, information about this manual.
2: "General Safety Precautions"	General safety precautions in English.
3: "Getting Started"	Instructions on taking X8500 into operation.
4: "Initial Configuration with Setup Tool"	How to activate licenses, enter system data and configure basic router settings.
5: "Advanced Configuration with the Setup Tool"	How to configure advanced router settings.
6: "Configuration of Expansion Cards and Modules"	How to configure the expansion cards, communication modules and resource modules.
7: "Configuration of Security Functions and Firewall"	How to configure security functions and firewall.
8: "Configuration Management and Flash Card"	How to manage configuration files and SMFCs, and how to carry out software updates.
9: "Troubleshooting"	Important tips on fault clearance.
10: "Important Commands"	A brief overview of the most important commands of the SNMP shell and BRICKtools for Unix.
11: "General Safety Precautions in German"	General safety precautions in German.

Table 1-1: Short description of chapters

1.3.2 Meaning of Symbols

To help you locate and interpret information easily, this manual uses the following visual aids:






Symbol	Meaning
	Points out useful and relevant tips and tricks.
	Predicts potential pitfalls and explains how to avoid them.
	Brings to your attention general and important points.
	Explains additional background information.
	<p>Brings your attention to important safety precautions. Levels of danger are in accordance with ANSI:</p> <ul style="list-style-type: none"> ■ Caution (indicates possible danger that, if unheeded, could cause material damage) ■ Warning (indicates possible danger that, if unheeded, could cause bodily harm) ■ Danger (indicates danger that, if unheeded, could lead to serious bodily harm or death)

Table 1-2: List of visual aids

1.3.3 Typographical Elements

In order to help you find and interpret the information in this manual, the following typographical elements are used:

Typographical element	Meaning
➤	Here you are requested to do something.
■ — —	Lists including two levels.
MENU ➤ SUBMENU File ➤ Open	Indicates menus and submenus in the Setup Tool. Indicates menus and submenus under Windows.
Non-proportional (Courier), e.g. ping 192.168.1.254	■ Indicates commands (e.g. in the SNMP shell) that you must enter as shown. ■ Used to display the Setup Tool.
<IP address>	Indicates inputs in which you enter a value for the term shown in the brackets. Do not enter the pointed brackets.
<i>bold, italics, e.g.</i> <i>BigBoss</i>	Indicates example terms.
bold, e.g. ➤➤ MIB	Indicates terms that you can find in the glossary (for online texts, click the double arrow).
bold, e.g. biboAdmLoginTable, Windows Start menu	■ Indicates fields in the Setup Tool and MIB tables and variables. ■ Indicates keys/key combinations and Windows terms.
<i>italics, e.g.</i> <i>none</i>	Indicates values that can be entered or set in the Setup Tool or MIB variables.
Online:blue	Indicates links.

Table 1-3: Typographical elements

2 General Safety Precautions

General Safety Precautions in English

The following sections contain safety precautions you are strongly advised to heed when working with your equipment.

- Transport and storage**
- Only transport and store **X8500** in its original packaging or use other appropriate packaging to protect against knocking and shaking.
- Installation and operation**
- Read the information on the ambient conditions (see Technical Data) before installing and operating **X8500**.
 - Please comply with the general conditions applicable in your country when installing external ISDN basic rate accesses. In some cases, you may have to consult a technician who possesses the relevant approval. Obtain information about the special requirements of national regulations and make sure that your installation complies with these legal requirements.
 - Electrostatic charges may cause damage to the equipment. You should therefore wear a grounded wrist strap or touch a grounded surface before you touch sockets or extension cards of **X8500**. Only grip extension cards at the edges and do not touch components or conductor tracks.
 - Be sure to install the dummy front-panel sections in any unused slots to ensure that emissions causing electromagnetic interference are prevented.
 - Condensation may occur externally or internally if the equipment is moved from a colder room to a warmer room. When moving the equipment under such conditions, allow ample time for the equipment to reach room temperature and to dry out completely before operating. Observe the ambient conditions under Technical Data.
 - Never open the **X8500** power supply unit X8A-PS, as this can create a lethal danger through electric shock. Opening the **X8500** power supply unit invalidates the guarantee and the product liability.
 - Make sure that the connection requirements for the power supply unit are observed.

- Be sure to insert and fasten the **X8500** power supply unit properly before bringing **X8500** into operation. This ensures that the housing is reliably earthed.
 - Make sure to connect the power cord only to a power supply unit that has been properly inserted and fixed.
 - Make sure the local mains voltage is the same as the nominal voltages of the power supply unit. The **X8500** power supply unit X8A-PS may only be operated under the following conditions.
 - 100 - 240 V AC
 - 50/60 Hz
 - max. 3 A
 - Only connect the equipment to a safety mains socket that is grounded in accordance with the regulations (the equipment is equipped with a tested safety power cord).
 - Make sure the safety mains socket in the building is freely accessible.
 - Make sure you follow the correct cabling sequence, as described in the manual. Use only the cables supplied with the equipment or cables that meet the specifications in this manual. If you use other cables, BinTec Communications AG cannot accept liability for any damage occurring or for any adverse effects on operation. The equipment guarantee is invalidated in such cases.
 - Connect the equipment as described in the manual.
 - Arrange the cables so that they are not in the way and cannot be tripped over or damaged.
 - Do not connect, disconnect or touch the data lines during lightning storms.
 - Only connect terminals to **X8500** that meet the general safety requirements for telecommunications equipment. Terminals approved by CETECON (formerly BZT) meet these requirements. ISDN terminals connected to **X8500** must be approved for use with Euro ISDN (DSS1).
- Operation according to the regulations** ■ **X8500** establishes WAN connections depending on the system configuration. To avoid extra charges, you should carefully monitor the product.

- Ambient temperature should not exceed 40 °C. Avoid exposure to direct sunlight.
- Make sure no foreign objects (e.g. paper clips) or liquids get into the equipment (risk of electric shock, short-circuit). Make sure the equipment is sufficiently cooled.
- In an emergency (e.g. damaged housing or operating element, entry of liquid or foreign bodies), immediately disconnect the power supply and notify customer service.

Cleaning and repair

- Never use water to clean this equipment. Water spillage can result in serious danger for the user (e.g. electric shock) and cause considerable damage to the equipment.
- Never use scouring or abrasive alkaline cleaning agents on this equipment.

3 Getting Started

This chapter contains a description of the various connection and configuration methods for **X8500**.

It also contains installation instructions for the **BRICKware for Windows** software.



Caution!

As an ISDN multiprotocol router, **X8500** sets up ISDN connections in accordance with the system configuration. If your router is not configured correctly or completely, this can cause increased charges. The conditions that lead to setting up multiple connections depend heavily on the network in which your router is used.

To avoid unwanted charges, you should certainly monitor your product in operation:

- Use filters to reject certain data packets. Note that ISDN connections can be set up by broadcasts, especially in Windows networks. Further information on setting filters is contained in [chapter 7.2.8, page 315](#).
- Use the Credits Based Accounting System to define a maximum number/duration of ISDN connections or a maximum limit for charges within a certain time. This limits excessive charges in advance. See [chapter 7.1.3, page 293](#).
- See [chapter 9.2.2, page 380](#). This chapter lists most of the reasons for excessive charges.

This chapter tells you how to carry out the following tasks:

- How to access **X8500** ([chapter 3.1, page 24](#))
- How to log in to **X8500** ([chapter 3.2, page 30](#))
- Which methods of configuration are available to you ([chapter 3.3, page 32](#))
- How the ➤➤ **Setup Tool** is structured ([chapter 3.4, page 33](#))
- What to do before you start the configuration ([chapter 3.5, page 45](#))

3.1 Connection Methods

Before you can configure your **X8500**, you must connect **X8500**. There are various ways of doing this:

- Over the serial interface
- Over your >>> **LAN**
- Over an >>> **ISDN** connection

Diagram of connection methods:

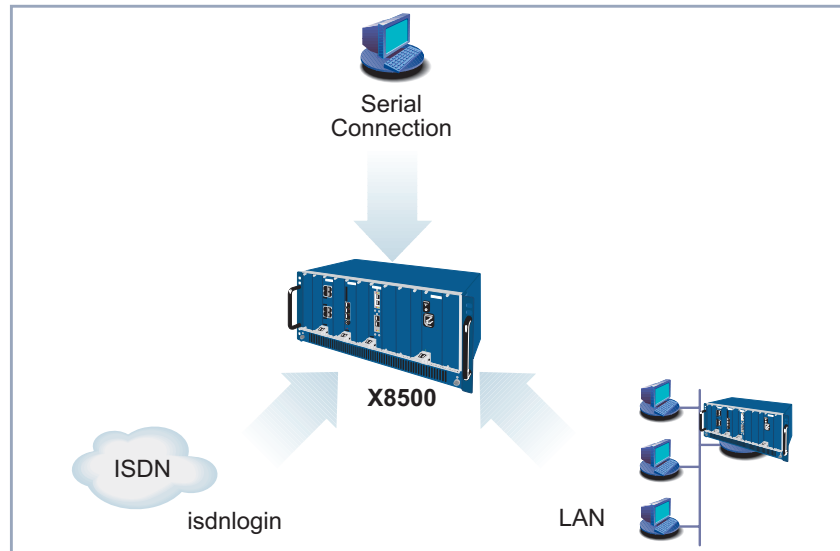


Figure 3-1: Possible connections to **X8500**

The various connection methods are presented below, so that you can choose the method most appropriate for your needs.

If you use the Configuration Manager (**BRICKware for Windows**) under Windows, you connect to **X8500** over the LAN.

3.1.1 Connecting Over the Serial Interface

Initial configuration Connecting over the serial interface is very suitable if you carry out an initial configuration on **X8500** before you have entered an IP address and netmask. To connect **X8500** to your computer over the serial interface, connect the serial interface of **X8500** to the serial interface of your computer.

Windows If you are using a Windows PC, you will need a terminal program, e.g. **HyperTerminal**, for the serial connection. How to install this assistant and **BRICKware for Windows** is described in [chapter 3.5.3, page 49](#).

To do Proceed as follows to access **X8500** over the serial interface:

- Click the Windows Start button and then **Programs** ➤ **BRICKware** ➤ **Device at COM1** (or **Device at COM2** if you use the COM2 port of your PC) to start **HyperTerminal**.
- Press **Return** (at least once) after the **HyperTerminal** window opens.
- A window with the login prompt appears. You are now in the SNMP shell of **X8500**.
- Continue with [chapter 3.2, page 30](#).



If the login prompt does not appear after pressing **Return** several times, the connection to **X8500** has not been set up successfully. Check the COM1 or COM2 settings on your PC.

- Click **File** ➤ **Properties**.
- Click **Configure....** in the **Connect to** tab.
The following settings are necessary:
 - Bits per second: 9600
 - Data bits: 8
 - Parity: none
 - Stop bits: 1
 - Flow control: none
- Enter the values and click **OK**.
- Set in the **Settings** tab:
 - Emulation: VT100
- Click **OK**.

The changes to the terminal program settings do not take effect until you disconnect the connection to **X8500** and set up the connection again.



You can also use any other terminal program that can be set to 9600 bps, 8N1 (8 data bits, no parity, 1 stop bit), software handshake (none) and VT100 emulation.

Unix If you are using a Unix PC, you will need a terminal program such as `cu` (under System V), `tip` (under BSD) or `minicom` (under Linux). The settings for these programs are the same as listed above.

Example of a command line for using `cu`: `cu -s 9600 -c/dev/ttyS1`

Example of a command line for using `tip`: `tip -9600 /dev/ttyS1`

3.1.2 Connecting Over a LAN



You can reach **X8500** from the LAN over the **telnet** service. Telnet is normally available on every PC. To be able to reach your **X8500** over the LAN, it must already have an **IP address** and **netmask**. If this is not the case and **X8500** has therefore not yet been configured, you have two options:

- If you are working with Windows, you can assign **X8500** an IP address before you start telnet. To do this, you will need the **DIME Tools**. If you have not yet installed **DIME Tools** with **BRICKware for Windows**, proceed as explained in [chapter 3.5.3, page 49](#).
- If you are not working with Windows, use an alternative connection method for initial configuration (over the serial interface or ISDN).

To do Proceed as follows to access **X8500** over the LAN interface:

- Connect **X8500** to the LAN.

Assigning IP addresses

To assign your **X8500** an IP address (if necessary) with the **DIME Tools**, proceed as follows:

- Click the Windows Start button and then **Programs** ➤ **BRICKware** ➤ **DIME Tools**.
If the **BootP** server is not started as standard, you must start it.
The BootP server window will appear after a short time if **X8500** is still unconfigured.
- Enter the name and IP address of your **X8500** under **Device Parameter**.
- Click **OK**.
- Close **DIME Tools**.

Running telnet

Now establish a connection to **X8500** with telnet:

Windows

- Click the Windows Start button and then **Run....**
- Type `telnet <IP address of X8500>`.
- Click **OK**.

A window with the login prompt appears. You are now in the SNMP shell of **X8500**. Continue with [chapter 3.2, page 30](#).

- Unix** ➤ Type `telnet <IP address of X8500>` into a terminal.
A window with the login prompt appears. You are now in the SNMP shell of **X8500**. Continue with [chapter 3.2, page 30](#).

3.1.3 Connection Over ISDN

Remote configuration Connection over ➤➤ **ISDN** with ➤➤ **ISDN login** is especially recommended if **X8500** is to be configured or administrated remotely (remote LAN in [figure 3-2, page 28](#)). This is possible even if **X8500** has not been initially configured, i.e. is still in the ex works state. A connection is then established by means of a router that is already configured or an ISDN card in the remote LAN, using a number of **X8500**'s ISDN connection in your own LAN (e.g. 1234).

It is thus possible for the administrator of a remote LAN to configure a **X8500** which is hundreds of kilometers away. The **X8500** your LAN merely has to be connected to an ISDN line and switched on.

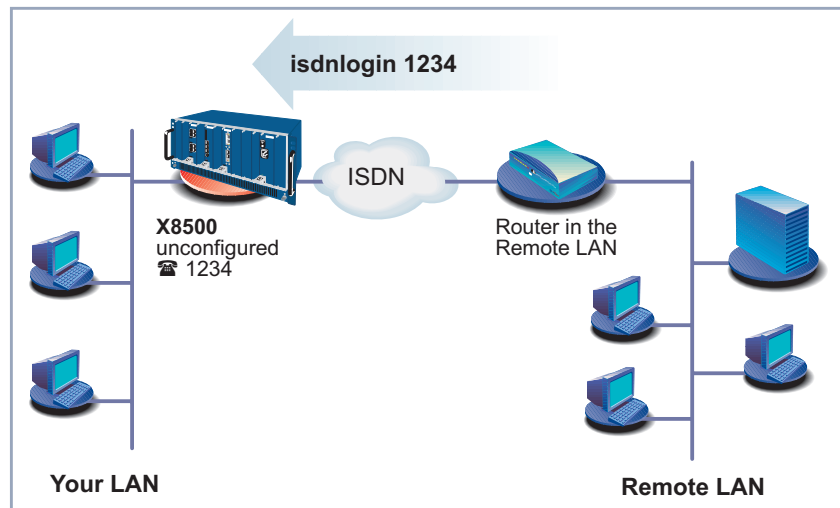


Figure 3-2: Connection over ISDN login for remote maintenance



Access over ISDN costs money. If **X8500** and the PC are in the same LAN, it is cheaper to access **X8500** over the LAN or the serial interface.

To do To reach **X8500** over ISDN login, proceed as follows:

- Connect **X8500** to the ISDN.
- Log in on your router in the remote LAN in the usual way.
- In the SNMP shell, type in `isdnlogin <number of the ISDN connection of X8500>`, e.g. `isdnlogin 1234`.

The login prompt will appear in the window. You are now in the SNMP shell of **X8500**. Continue with [chapter 3.2, page 30](#).

3.2 Logging In

Regardless of how you access **X8500**, the **SNMP shell** of **X8500** with the login prompt always appears first.

Ex works state In order to log in, you need to know an user name and a password. In its ex works state, **X8500** is provided with the following user names and passwords:

User name	Password	Permission
admin	bintec	Read and change system variables, save configurations, use the Setup Tool.
write	public	Write system variables (changes are lost when X8500 is turned off).
read	public	Read system variables.

Table 3-1: User names and passwords in ex works state

As you can see, it is only possible to change and save configurations when you log in with the user name `admin`.

Access information (user names and passwords) can only be changed if you log in with the user name `admin`. For security reasons, passwords are displayed only as asterisks. The user names appear in plain characters. The security concept of **X8500** enables you to read all configuration settings with the user name `read`, but not the access information. It is therefore impossible to log in with `read`, read the password of the `admin` user and subsequently log in with `admin` and make changes to the configuration.

To do This is how you log in:

- Type in your user name (e.g. `admin`) and press **Return**.
- Type in your password (e.g. `bintec`) and press **Return**.

Your router then issues an input prompt, e.g. `x8500 : >`. The login was successful.

**Caution!**

All BinTec routers are shipped with the same user names and passwords. As long as the passwords remain unchanged, the routers are not protected against unauthorized use. How to change the passwords is described in [chapter 3.4.5, page 38](#).

- Change the passwords to prevent unauthorized access to **X8500**.
- Remember your password!
If you forget your password, you will have to reset **X8500** to the ex work state and your configuration is lost!

Closing the SNMP shell To leave the SNMP shell after completing the configuration, enter `exit` and press **Return**.

3.3 Configuration Options

Before you set to work with the configuration, you must select a configuration method. For this reason, we would first like to give you an overview of the available options. This manual explains how to configure **X8500** by means of the Setup Tool.

Methods of Configuration Methods for configuring **X8500**:

- Setup Tool
- >> **SNMP** shell commands
- Configuration Manager
- Other SNMP managers

Setup Tool The Setup Tool is a menu-controlled tool for the configuration and administration of **X8500**. Configuration with the Setup Tool is much easier than configuration with SNMP commands, although not all settings can be made in the Setup Tool. This manual explains how to configure **X8500** using the Setup Tool. The Setup Tool is independent of the operating system of your PC. If a configuration step is only possible with the help of an SNMP command, the procedure for this is explained.

SNMP >> **SNMP** (Simple Network Management Protocol) is a >> **protocol** that defines how you can access the configuration settings. All configuration settings are stored in the >> **MIB** (Management Information Base) in the form of MIB tables and MIB variables. You can access these directly via the SNMP shell.

Configuration Manager and other SNMP Managers The Configuration Manager is a Windows-based SNMP manager provided by BinTec Communications AG. You can use its interface based on Windows Explorer to access all MIB tables and variables of **X8500**. You can also use other SNMP managers, such as SNM, HP OpenView or Transview to access and modify the MIB tables and variables. As more detailed knowledge of the structure and interrelations of router configuration is necessary, this method is suitable for more experienced users. Handling MIB tables and MIB variables is explained in the **Software Reference** and **MIB Reference**.

3.4 Using the Setup Tool

An introduction to using the Setup Tool is provided in this chapter. You can call up the Setup Tool once you have logged in to **X8500**:



To use the Setup Tool, you must log in with the user name `admin!` If you do not know the corresponding password, you cannot open the Setup Tool (see [chapter 3.2, page 30](#)).

► Type `setup` behind the input prompt and hit **Return**.

The main menu of the Setup Tool opens:

```

X8500 Setup Tool                                     BinTec Communications AG
                                                    MyX8500
-----
Licenses          System
Slot Card (State) Interfaces/Resource[Unit]
1:
2:
3:
4:
SYS: X8A-SYS      (R)  ETH[1]  ETH[2]  BRI[4]
5:  X8E-4PRI     (R)  PRI[0]  PRI[1]  PRI[2]  PRI[3]  MOD[4]  MOD[5]
6:  X8E-2BC     (R)  CM-100BT:ETH[0]  CM-2BRI:BRI[2]  BRI[3]
7:
8:

WAN Partner
IP      PPP      MODEM  CREDITS    CAPI    QoS
Configuration Manager
Monitoring and Debugging
Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items.<Return> to
enter

```

In our example, **X8500** is equipped with the system card (X8A-SYS), with the expansion card X8E-4PRI with two modem modules, and with a carrier card (X8E-2BC) with the communication modules CM-100BT and CM-2BRI.

3.4.1 Menu Layout

Every Setup Tool menu consists of three parts:

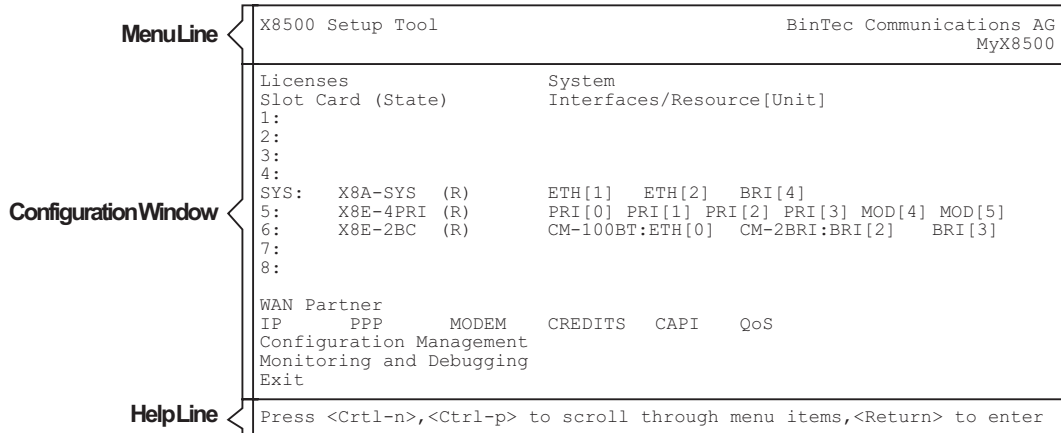


Figure 3-3: Setup Tool menu layout with example components

- The menu line contains a navigation aid to show you where in the Setup Tool menu system you currently are. The system name of **X8500** is also displayed. This is especially helpful if you are using several BinTec routers with different system names.
- The configuration window is where the actual entries are made and the respective settings are displayed. The field in which the cursor is currently located is also highlighted.
- The help line tells you how to move around in the menu currently displayed or which entries you can change.

The Setup Tool is easy to use. After a few minutes, you will have no problem finding your way around. Nevertheless, we would first like to point out a few things you should be aware of when using the **X8500** Setup Tool.

3.4.2 Menu Navigation

You can use the following keys or key combinations to navigate the various menus in the Setup Tool:

Key combination	Meaning
Tabulator	To move to the next item in a menu.
Return	To open a submenu or activate a menu command (e.g. SAVE).
up or down (arrow keys)	To move forwards or backwards between menu fields (functions with VT 100 emulation when using a terminal program).
left or right (arrow keys)	To scroll backwards or forwards in the same field to reveal a list of possible entries (functions with VT 100 emulation when using a terminal program).
Esc Esc	Esc twice in succession: To return to the previous menu. Cancels any changes made.
Space	To toggle the delete flag for list entries that are to be deleted. The tagged entries are marked with <i>D</i> . Pressing Space again removes the tag marking.
Ctrl - l	To redraw the screen.
Ctrl - n	To move to the next item in a menu.
Ctrl - p	To move to the previous item in a menu.
Ctrl - f	To scroll forward a page in a long list. An "=" sign at the bottom right indicates the end of the list or a "v" indicates more to come.
Ctrl - b	To scroll back a page in a long list. An "=" sign at the top right indicates the start of the list or a "^" indicates more to come.
Ctrl - c	Leave the Setup Tool.

Table 3-2: Navigation in the Setup Tool

3.4.3 Menu Commands

When you start moving around in the Setup Tool, you will notice that some menus have special command options, such as **DELETE**, **SAVE** and **CANCEL**. There are a few slight differences between these commands that you should be aware of.

Menu Command	Meaning
ADD	To create or add an item to a list. A submenu appears for entering the desired settings.
CANCEL	To discard all changes made in the current menu.
DELETE	To delete all entries tagged with the Space bar for deletion from a list. These changes become effective immediately.
OK	To confirm the changes in the current menu. These changes do not become effective until SAVE is hit in the next menu.
SAVE	All variables set in the current menu and all its submenus are saved to memory. These changes become effective immediately.
EXIT	To leave the current menu and return to the previous menu. Any entries made are lost.

Table 3-3: Buttons in the Setup Tool



Leave the Setup Tool with **Save as boot configuration and exit** to save the configuration to the flash memory.

3.4.4 Searching Lists

Some Setup Tool menus contain lists of items, e.g. the **WAN PARTNER** menu, which lists all ►► **WAN partners** currently configured:

```

X8500 Setup Tool                               BinTec Communications AG
[WAN]: WAN Partners                             MyX8500

Current WAN Partner Configuration

  Partnername          Protocol          State
  -----
  BigBoss              ppp            dormant
  T_ONLINE             ppp            dormant
  Partner1             ppp            dormant
  Partner2             ppp            dormant
  PROVIDER             ppp            dormant
  ^
  |
  =

ADD          DELETE          EXIT

Press<Ctrl-n>,<Ctrl-p>to scroll,<Space>tag/untag DELETE,<Return>to edit
Search: p

```

These lists are in alphabetical order according to the contents of the first field. An incremental search function is provided, which is very useful for searching for an item in long lists.

Proceed as follows:

- Enter the first letter of the item you are looking for, with the cursor located on any item in the list. Entries can be made in upper or lower case.
- As long as the search is active, you can enter more characters to refine the search.
- The **Backspace** or **Delete** key can be used to edit the search string. The cursor automatically jumps to the first match it finds in the list.

The characters entered for the search are displayed in the help line at the bottom of the menu.

Do not enter invisible characters, such as **Tabulator** or **Space**, as they stop the search and could lead to a function being executed.



If the search does not work, make sure that the cursor is located in a list field. The search cannot run if the cursor is located in a command field, e.g. **ADD** or **DELETE**.

Example: In the **WAN PARTNER** menu shown above, the entries provide the following search results:

Entry	Cursor moves to entry
p OR P	Partner1
pr, Pr, pR, PR	PROVIDER
p a r t n e r 2	Partner1 , on entering 2 to Partner2

Table 3-4: Search results

3.4.5 Changing the Password

The procedure described below for changing the password applies to all **X8500** passwords: the access passwords for the user names `admin`, `read` and `write`, the RADIUS password, the PPP password, the provider password and the CAPI user passwords.

Any character may be used for entering a password. Passwords are only displayed as asterisks, even during password changes. The number of asterisks is the same as the number of characters in the password.



To start the **X8500** Setup Tool in a mode in which the passwords are visible and can be changed by being entered only once, you must enter the command `setup -p`. This option only exists if you have logged in on **X8500** under the user name `admin`.

To do To change a password, proceed as follows:

- Select the password field in the appropriate menu and enter the new password. The field changes to the change mode and the message `Change Password` appears in the help line.



In the password field, the **Backspace** key always deletes the complete entry and not just one character.

- Now press **Return**, **Tabulator** or a **Cursor key** to confirm. The field changes to the confirm mode and `Confirm Password` is displayed in the help line.
- Now enter the new password again and confirm by pressing **Return**, **Tabulator** or a **Cursor key**.
If both entries match, the password is changed. The new password is saved on leaving the menu with the **SAVE** button. If you leave the menu by pressing **CANCEL** or **Esc Esc**, the password change is not saved.
If the two passwords you entered were not the same, the field is reset to the old password and "Password doesn't match, try again." is displayed in the help line.

3.4.6 Convention

Convention The following convention is used in this manual:

- Example: "Go to **IP** ➤ **ROUTING**":
Explanation: Tag the **IP** menu in the main menu of the Setup Tool and press **Return**. Tag the **ROUTING** submenu there and press **Return**.
- Example: "Go to **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** ➤ **ADD** ➤ **ADVANCED SETTINGS**":
Explanation: Tag the **WAN PARTNER** menu in the main menu of the Setup Tool and press **Return**. Tag the **ADD** button there and press **Return**. Tag the **WAN NUMBERS** submenu and press **Return**. Tag the **ADD** button there and press **Return**. Now tag the **ADVANCED SETTINGS** submenu and press **Return**.
- Example: "Go to **WAN PARTNER** ➤ **EDIT** ➤ **WAN NUMBERS**":
Explanation: Tag the **WAN PARTNER** menu in the main menu of the Setup Tool and press **Return**. Select an existing entry there and press **Return**. Now tag the **WAN NUMBERS** submenu and press **Return**.

3.4.7 Menu Structure

The main menu of the Setup Tool looks like this:

```

X8500 Setup Tool                                     BinTec Communications AG
                                                    MyX8500

Licenses      System
Slot Card (State)  Interfaces/Resource[Unit]
1:
2:
3:
4:
SYS: X8A-SYS (R)   ETH[1]  ETH[2]  BRI[4]
5:  X8E-4PRI (R)   PRI[0]  PRI[1]  PRI[2]  PRI[3]  MOD[4]  MOD[5]
6:  X8E-2BC (R)   CM-100BT:ETH[0]  CM-2BRI:BRI[2]  BRI[3]
7:
8:

WAN Partner
IP      PPP      MODEM      CREDITS      CAPI      QoS
Configuration Manager
Monitoring and Debugging
Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items.<Return> to enter

```

In our example, **X8500** is equipped with the system card (X8A-SYS), with the PRI expansion card X8E-4PRI with two modem modules, and with a carrier card (X8E-2BC) with the communication modules CM-100BT and CM-2BRI.

The menu structure of the Setup Tool looks like this:

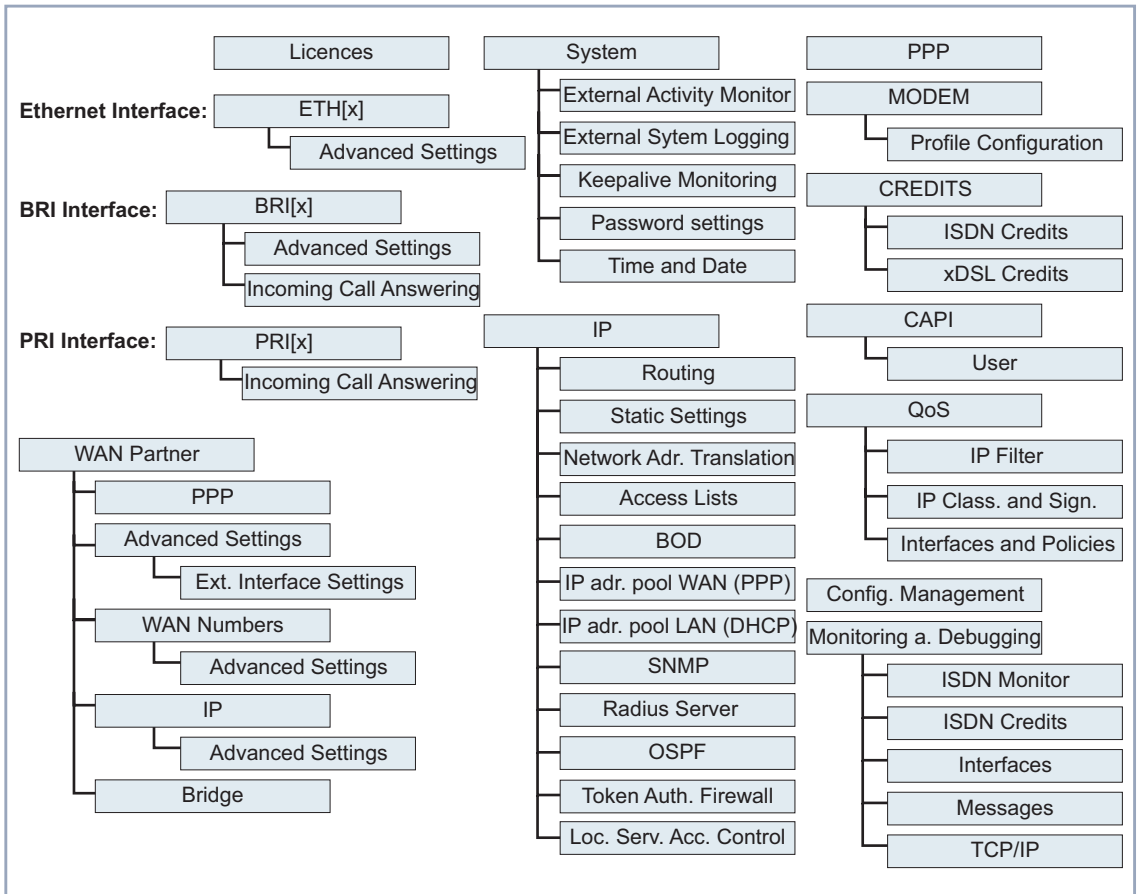


Figure 3-4: Setup Tool basic menu structure

The menus of the Setup Tool available on **X8500** in our example are illustrated in [figure 3-4, page 41](#). Depending on your expansion card setup, your Setup Tool main menu may differ from the example. BRI interfaces will be displayed as BRI[x], PRI interfaces as PRI[x], and Ethernet interfaces as ETH[x], where "x" accounts for the corresponding port on your expansion card or communication module. When you activate further licenses, **X8500** detects this and displays the corresponding menus (for entering license, see [chapter 4.1.1, page 56](#)).

Summary To help you find your bearings during configuration, the menus of the example in [figure 3-4, page 41](#) are briefly explained below:

Menu	Function
LICENSES	This menu is for entering the license information and activating licenses.
SYSTEM	In this menu, you enter the basic system settings of X8500 , e.g. system name and passwords.
ETH[x]	This menu is for configuring the ➤➤ LAN interface of X8500 . Here you enter data such as the IP address and netmask of X8500 .
BRI[x], PRI[x]	This menu is for configuring an ISDN interface of X8500 . Here you enter data such as the type of ISDN connection to which X8500 is connected. The submenus BRI[x] ▶ INCOMING CALL ANSWERING and PRI[x] ▶ INCOMING CALL ANSWERING is for assigning the available ISDN numbers to the desired services (e.g. PPP routing, ➤➤ CAPI , ➤➤ ISDN Login).
WAN PARTNER	Here you define all your WAN partners, e.g. your ➤➤ Internet Service Provider (➤➤ ISP). All the WAN partners entered are displayed in a list that includes the name of partner, protocol used and current status of each.

Menu	Function
IP	<p>Here you enter the settings for the >>> IP protocol. This menu consists of several submenus:</p> <p>IP ▶ ROUTING includes X8500's IP routing table. Here you enter routes to your partners (e.g. default routes, network routes), which ensure that your X8500 sends all the >>> data packets to the correct addresses.</p> <p>IP ▶ STATIC SETTINGS is for entering important settings, e.g. the domain name of X8500, the IP addresses of additional >>> servers (e.g. Domain Name Server) and system time specifications.</p> <p>IP ▶ NETWORK ADDRESS TRANSLATION is for configuring the interfaces to the partners for which you want to use the Network Address Translation function (>>> NAT).</p> <p>IP ▶ ACCESS LISTS is for defining >>> filters to allow or deny access from or to the different hosts in the connected networks. You can thus prevent your X8500 from establishing unintended connections to the ISDN.</p> <p>IP ▶ BANDWIDTH ON DEMAND (BOD) is for defining filters for the Bandwidth on Demand and AO/DI (Always On/Dynamic ISDN) functions.</p> <p>IP ▶ IP ADDRESS POOL WAN (PPP) is for setting up a pool of IP addresses that your X8500 as a dynamic IP address server can assign to WAN partners, who can then dial in.</p> <p>IP ▶ IP ADDRESS POOL LAN (DHCP) is for configuring X8500 as a >>> DHCP server. As a DHCP server, X8500 assigns the IP addresses to the hosts in the LAN dynamically.</p> <p>IP ▶ SNMP is for changing the basic >>> SNMP settings.</p> <p>IP ▶ RADIUS SERVER is for configuring RADIUS servers.</p> <p>IP ▶ DNS is for defining the procedure for name resolution in X8500.</p> <p>IP ▶ LOCAL SERVICES ACCESS CONTROL is for controlling access to the local UDP and TCP services in X8500.</p>
PPP	<p>Includes generally valid >>> PPP settings, e.g. authentication protocol, that do not just refer to particular WAN partners. With these settings, the router can perform an authentication procedure for incoming calls, even if the calling line number cannot be identified (e.g. because the call is made from an analog line that does not transfer the calling line number).</p>

Menu	Function
MODEM	In this menu, you define modem profiles. Modem Profile 1 is the default modem profile which is automatically used for modem connections.
CREDITS	Here you administrate X8500 's Credits Based Accounting System.
CAPI	Includes the settings for BinTec's CAPI user concept. You can use this to assign user names and passwords to users of the X8500 's CAPI applications. This makes sure that only authorized users can receive incoming calls and make outgoing calls via CAPI.
QoS	This menu is for configuring Quality of Service.
CONFIGURATION MANAGEMENT	Here you can administrate X8500 's configuration files. You can save them either locally on X8500 or on your PC, for example.
MONITORING AND DEBUGGING	Includes submenus that enable you to locate problems in your network and monitor activities, e.g. at X8500 's WAN interface.
EXIT	Quit the Setup Tool with EXIT . You save the configuration file in the flash memory with EXIT ➤ Save as boot configuration and exit . This file is loaded on restarting X8500 . Leave the Setup Tool without saving the configuration in the flash memory with EXIT ➤ Exit without saving .

Table 3-5: Setup Tool menus

3.5 In Advance of Configuration

We recommend the following procedure for initial configuration of **X8500**:

- Prepare your configuration as described in [chapter 3.5.1, page 45](#).
- Check the TCP/IP Protocol as described in [chapter 3.5.2, page 46](#).
- Install the **BRICKware** as described in [chapter 3.5.3, page 49](#).
- Connect **X8500** as explained in the **Hardware Installation Guide**.

3.5.1 Gathering Information

Router settings Before you start to configure your **X8500**, make sure you have the following information about your ISDN connection and your network environment. Write down the relevant values in the table below so that you can quickly find the necessary information while you are performing the configuration. Examples are shown below:

Access data	Example	Your value
ISDN extensions	<i>10, 11, 12</i>	
IP address of X8500	<i>192.168.1.254</i>	
Netmask of X8500	<i>255.255.255.0</i>	

- ISDN extensions: The extension numbers of your ISDN connection.
- IP address and netmask of **X8500**: If you are installing a new network, simply use the example values given.

Internet access For access to the Internet via your Internet Service Provider (ISP), you will need access information that should be provided by your ISP.

Access data	Example	Your value
Provider name	<i>GoInternet</i>	
Dial-in number	<i>1234567</i>	
User account	<i>MyName</i>	
Password	<i>TopSecret</i>	

Corporate network connection (LAN-LAN) For connection to a corporate network or another WAN partner, you must know the following information about the opposite terminal.

Access data	Example	Your value
Partner's name	<i>BigBoss</i>	
Dial-in number	<i>0911987654321</i>	
Local name	<i>LittleIndian</i>	
Password	<i>Secret</i>	
Partner's network address(es)	<i>10.1.1.0</i>	
Partner's netmask(s)	<i>255.255.255.0</i>	

Agree on the data with your WAN partner: You must both use the same password; your entry for "local name" and your partner's entry for "partner's name" must be identical; your entry for "partner's name" and your partner's entry for "local name" must also be identical.

3.5.2 Checking the TCP/IP Protocol

To check if the TCP/IP protocol is already installed on your PC, or to install it now, proceed as follows:

- Unix** ➤ Make sure the TCP/IP protocol is installed before you start the configuration.

- Windows 95/98**
- Click the Windows Start button and then **Settings** ➤ **Control Panel**.
 - Double click **Network**.
 - Look for **TCP/IP** in the list of network components.
 - If you can't find the entry, install the TCP/IP protocol as explained below.
- Windows NT**
- Click the Windows Start button and then **Settings** ➤ **Control Panel**.
 - Double click **Network**.
 - Select the **Protocols** tab and look for **TCP/IP Protocol** in the list of network components.
 - If you can't find the entry, install the TCP/IP protocol as explained below.
- Windows 2000**
- Click the Windows Start button and then **Settings** ➤ **Network and DCN Connections**.
 - Double click **LAN Connection**.
 - Click the **General** tab and then **Properties**. Look for **Internet Protocol (TCP/IP)** in the list of network components.
 - If you can't find the entry, install the TCP/IP protocol as explained below.
- Windows ME**
- Click the Windows Start button and then **Settings** ➤ **Control Panel**. View all the control panel options.
 - Double click **Network**.
 - Look for the entry **TCP/IP** in the **Configuration** tab.
 - If you can't find this entry, install the TCP/IP protocol as described below.
- Windows XP Professional**
- As soon as an Ethernet card is plugged into your PC, Windows XP detects this and automatically installs the TCP/IP protocol. Should problems still occur, consult the **Help and Support Center** or the **Network Setup Wizard** of Windows XP.

Installing the TCP/IP Protocol

- Windows 95/98**
- Click **Add** in the **Network** dialog box.
 - Select **Protocol** in the list of network components and click **Add**.

- Select **Microsoft** as manufacturer and **TCP/IP** as network protocol and click **OK**.
 - If you are in an existing network, you may have to make other settings at this point. Ask your system administrator.
 - If you are setting up a new network, click **OK**.
 - Follow the on-screen instructions and restart your PC when you have finished.
- Windows NT**
- Click the **Protocols** tab in the **Network** dialog box. Click **Add**.
 - Select **TCP/IP protocol** from the list of network protocols. Click **OK**.
 - If setting up a new network, click **Yes** to answer the question.
 - In an existing network, ask your system administrator.
 - Follow the on-screen instructions and restart your PC when you have finished.
- Windows 2000**
- Click the Windows Start button and then **Settings** ➤ **Network and DCN Connections**.
 - Double click **LAN Connection**.
 - Click the **General** tab and then **Properties**.
 - Select the **General** tab and click **Install**.
 - Select **Protocol** in the list of network components and click **Add**.
 - Select **Internet Protocol (TCP/IP)** as network protocol and click **OK**.
 - If you are in an existing network, you may have to make other settings at this point. Ask your system administrator.
 - If you are setting up a new network, click **OK** and **Close**.
 - Follow the on-screen instructions and restart your PC when you have finished.
- Windows ME**
- Click the Windows Start button and then **Settings** ➤ **Control Panel**. View all the control panel options.
 - Double click **Network**.
The **Network** window opens.

- Click **Add** in the **Configuration** tab.
The **Select Network Component Type** window opens.
 - Tag the **Protocol** entry and click **Add**.
 - Tag the network protocol **TCP/IP** in the **Select Network Protocol** window and click **OK**.
 - Click **OK** in the **Network** window.
 - Tag the network protocol **TCP/IP** in the **Select Network Protocol** window and click **OK**.
- Finally** ➤ Repeat the installation for all PCs on the network if you wish to use the LAN-LAN connection, Internet access or communications applications over **X8500**.

3.5.3 Installing BRICKware Under Windows

BRICKware for Windows is BinTec's Windows software. The **DIME Tools**, part of the **BRICKware**, contain mainly assistants for configuration, maintenance and diagnosis of **X8500**. The **DIME Tools** comprise the following:

- TFTP Server
- Time Server
- Syslog Daemon
- CAPI and ISDN Tracer

A detailed description of **BRICKware for Windows** and all its components can be found in the online documentation **BRICKware for Windows**.

BRICKware also contains configuration programs for Remote CAPI, which you may need on the PCs in your LAN.

Proceed as follows to install **BRICKware**:

- Close all Windows programs on your PC.
- Place your BinTec Companion CD in the CD-ROM drive of your PC.
The start window appears automatically after a short time.

- If the Start window does not open automatically, click your CD-ROM drive in Windows Explorer and double-click **setup.exe**. (Or click **Settings** ➤ **Control Panel**. First click **Software** and then **Install**. Follow the instructions on the screen.)
- Select the desired language in the Start window or leave the default setting.
- Select **BRICKware**.
The configuration assistant is activated.

If the version of **BRICKware** saved on your PC is older than version 5.2.1, you will be asked to deinstall this so that you can install the current version of **BRICKware**.

If the version is later than version 5.2.1, you can carry out an update on your **BRICKware**.

If you already have the current version of **BRICKware** installed on your PC, you can select from various installation possibilities during a new installation.

Deinstalling If you are requested to deinstall **BRICKware**, follow the instructions on the screen to remove the program from your PC. The win.ini file is saved on your PC before deinstallation.

A window informs you as soon as **BRICKware** is deinstalled and you can now install the new software.

New installation Proceed as follows to install **BRICKware**:

- Confirm the welcome window by clicking **Next**.
- Enter the directory in which **BRICKware** is to be installed or accept the default directory.
- Click **Next**.
- Select your equipment.
- Click **Next**.
- Select the software components you wish to install.
- Click **Next**.
A list of the components selected for the installation appears.

- To install these components, click **Next**.

The files are copied. A window appears after a short time telling you that the installation of **BRICKware** is completed.

Update If you have a later version of **BRICKware** than 5.2.1, you can carry out an update.

- Follow the instructions on the screen.

The existing **BRICKware** files on your PC are replaced with the new files. A window appears after a short time telling you that the **BRICKware** update is completed. Click **Finish** to end the update operation.

Current BRICKware already available If a current version of **BRICKware** is already saved on your PC, you can change the existing installation, restore a defective part of the program or remove **BRICKware** from your PC during a new installation.

- Follow the instructions on the screen.

The files are copied or removed from your PC. A window appears after a short time telling you that the maintenance operations are completed. Click **Finish** to end the maintenance operation.

4 Initial Configuration with Setup Tool

This chapter tells you how to carry out the initial configuration of your **X8500** using the Setup Tool.

Here a diagram of a typical scenario with **X8500**:

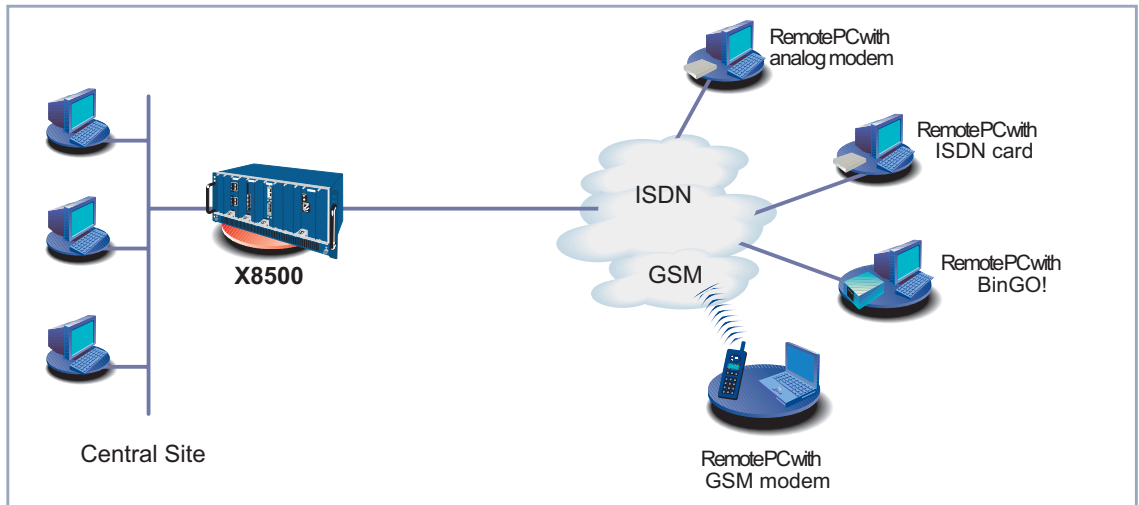


Figure 4-1: Example scenario for **X8500**

This chapter is broken down as follows:

- Basic router settings ([chapter 4.1, page 55](#))
This chapter describes the steps you must always carry out for taking **X8500** into operation, irrespective of the environment or applications for which you use **X8500**.
- Configuring the WAN interfaces ([chapter 4.2, page 73](#))
Description of how to configure a WAN interface of **X8500**, including the distribution of incoming calls to subsystems and users ("[Incoming Call Answering](#)", [page 77](#)).
- **X8500** and the WAN ([chapter 4.3, page 94](#))
 - Configuring WAN Partners ([chapter 4.3.1, page 94](#))

- Creating a routing entry ([chapter 4.3.2, page 115](#))
- Activating NAT ([chapter 4.3.3, page 121](#))
- Example configurations ([chapter 4.3.4, page 122](#))
- Saving the configuration ([chapter 4.4, page 126](#))
- What to do in your Windows network ([chapter 4.5, page 127](#))
- Testing your configuration ([chapter 4.6, page 134](#))

4.1 Basic Router Settings

The configuration of the basic router settings concerns only your **X8500** and your local network. You will find examples of names, **IP addresses**, extensions, etc. If you are setting up a new Local Area Network (LAN) together with **X8500** and have not been assigned any IP addresses (e.g. from the system administrator at your head office), simply use the IP addresses given as examples.

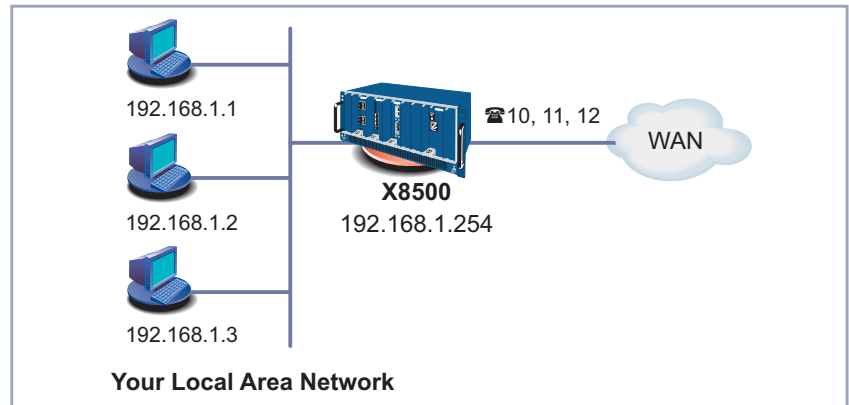


Figure 4-2: Basic router settings – **X8500** in the LAN

The following steps are necessary:

- Entering a license where required ([chapter 4.1.1, page 56](#))
- Entering system data (e.g. passwords) ([chapter 4.1.2, page 58](#))
- Configuring the LAN interface ([chapter 4.1.3, page 61](#))
- Configuring **X8500** as a DHCP server (optional) ([chapter 4.1.4, page 65](#))
- Setting NetBIOS filters (optional) ([chapter 4.1.5, page 68](#))

The work to be done on your network and PCs can be found in [chapter 4.5.1, page 127](#).

4.1.1 Entering License(s)

License This chapter describes, how you activate the functions of the software and hardware licenses you may have purchased.

License data The license data include the Software License ID or the hardware serial number of your equipment, a PIN and a license serial number. You received the last two items with your license. For online licensing at www.bintec.net, you enter the above license data and receive a key. You then enter this key together with your license serial number in the Setup Tool to activate the functions of your license in your router.

Entering License To enter your license, proceed as follows:

- Log in to **X8500** with the user name `admin`, as described in [chapter 3.2, page 30](#).
- Open the Setup Tool with `setup`.
- Go to **LICENSES**.

All subsystems and licenses already enabled are listed under **Available Licenses**:

X8500 Setup Tool		BinTec Communications AG	
[LICENSE]: Licenses		MyX8500	
Available Licenses:			
IP (builtin), OSPF, STAC, CAPI, BRIDGE			
Software License ID: JSH7D0WAAC2A9GJ1KE3H2A75HJZ			
Serialnumber	Used for	Description	State
builtin	feature mask 295	composite	ok
X8APRI04	Slot 5	PRIMARY RATE	ok
ADD	DELETE	EXIT	
Press<Ctrl-n>,<Ctrl-p>to scroll,<Space>tag/untagDELETE,<Return>to edit			

The field **Software License ID** displays the serial number which you need to enter to enable any software licenses. In the case of **X8500** it displays the serial number of internal Smart Media Flash Card.

Ex works state The following licenses are available on **X8500** in the ex works state:

Subsystems	Meaning
IP	IP routing
STAC	➤➤ STAC ➤➤ data compression
CAPI	➤➤ Remote CAPI interface makes communications applications possible on your PC, e.g. sending and receiving faxes.
BRIDGE	Bridging
OSPF	Open Shortest Path First

Table 4-1: Licensed subsystems in ex works state

Subsystems obtainable with license The following subsystems are available on **X8500** with appropriate licenses:

Subsystems	Meaning
TAF	Token Authentication Firewall
TUNNELING	Virtual Private Networking (VPN, PPTP)
FRAME RELAY	Frame Relay
IPSec	Internet Protocol Security
X25	X.25

Table 4-2: Subsystems with license

To do To enter your license, proceed as follows:

- Add a new entry with **ADD**.
Another menu window opens.
- Enter **Serialnumber** (the license serial number you received on buying the license) and **Key** (received during online licensing).
- Confirm with **SAVE**.
The entries are temporarily saved and activated. You have returned to the **LICENSES** menu. The subsystems activated by your license data are now listed. The license entered is displayed with the state *ok*.



If *not ok* is displayed as status:

- Enter the license data again.
- Check your hardware serial number.

If the license state is displayed as *not_supported*, you have entered a license for a subsystem your router does not support. You will not be able to make use of the functionality associated with the license.

Disabling license Proceed as follows to disable a license:

- Go to **LICENSES**.
- Tag the desired license with the **Space** bar.
The tagged entry is marked with **D**.
- Confirm with **DELETE**.

The license is deactivated. You can reactivate this license any time by entering the valid **Key** and **Serialnumber** (license serial number for this license).



It is possible that the licenses provided ex works are accidentally deleted. Proceed as follows to reactivate the deleted licenses:

- Go to **LICENSES** ➤ **ADD**.
- Enter the **Mask** 65535.
- Leave all other fields empty.
- Confirm with **Return**.

The licenses of the ex works state are reactivated.

4.1.2 Entering System Data

System name, ... Now you should enter the basic system data for your **X8500**.

- Go to **SYSTEM**.

The following menu opens:

X8500 Setup Tool		BinTec Communications AG
[SYSTEM]: Change System Parameters		MyX8500
System Name	MyX8500	
Local PPP ID (default)	BigBoss	
Location	3rd floor	
Contact	admin@BigBoss.com	
Syslog Output on Serial Console	no	
Message Level for the Syslog Table	info	
Maximum Number of Syslog Entries	20	
External Activity Monitor>		
External System Logging>		
Keepalive Monitoring>		
Password Settings>		
Time and Date>		
SAVE		CANCEL
Enter string, max. length = 34 chars		

The following parts of the menu are relevant for this configuration step:

Field	Meaning
System Name	Defines the system name of X8500 , is also used as PPP host name. Appears as input prompt when logging in to X8500 . If no system name is set, a warning appears on logging in with the user name <code>admin</code> .
Local PPP ID	This entry is necessary for identification of X8500 , if PPP authentication (e.g. PAP or CHAP) is carried out that is not specific to a partner (see chapter 5.1.3, page 142).
Location	Indicates where X8500 is located (optional).
Contact	States the contact person responsible (optional). Enter, for example, the e-mail address of your system administrator.

Table 4-3: **SYSTEM**

Passwords Enter the passwords for **X8500** in the submenu **SYSTEM ► PASSWORD SETTINGS**:

Field	Meaning
admin Login Password/SNMP Community	Password for user name admin.
read Login Password/SNMP Community	Password for user name read.
write Login Password/SNMP Community	Password for user name write.
HTTP Server Password	Password for http status page of X8500 .
Activity Monitor Password	Password for Activity Monitor .

Table 4-4: **SYSTEM ► PASSWORD SETTINGS**



Caution!

All BinTec routers are shipped with the same user names and passwords. As long as the password remains unchanged, they are not protected against unauthorized use. How to change the passwords is described in [chapter 3.4.5, page 38](#).

- Change the passwords to prevent unauthorized access to **X8500**.
- Remember your password!
If you forget your password, you will have to reset **X8500** to the ex works state and your configuration is lost!

The permission rights of the possible user names and passwords can be found in [chapter 3.2, page 30](#).

To do Proceed as follows to enter the relevant system data and passwords:

- Enter **System Name** of **X8500**, e.g. **MyX8500**.
- Enter the **Local PPP ID**.
The entry can be the same as the **System Name**.

- Enter your **Location**, e.g. *Europe*.
- Enter **Contact**, e.g. *SysAdmin*.
- Go to **SYSTEM** ➤ **PASSWORD SETTINGS**.
- Enter **admin Login Password/SNMP Community**.
- Enter **read Login Password/SNMP Community**.
- Enter **write Login Password/SNMP Community**.
- Enter **HTTP Server Password**.
- Enter **Activity Monitor Password**.
- Confirm with **SAVE**.
- Confirm with **SAVE**.

You have returned to the main menu and the entries are temporarily saved and activated.

Advanced configuration The menu **SYSTEM** ➤ **EXTERNAL ACTIVITY MONITOR** contains the settings necessary for monitoring **X8500** with the BinTec Windows tool **Activity Monitor** (see [chapter 7.1.4, page 296](#) and **BRICKware for Windows**).

The menu **SYSTEM** ➤ **EXTERNAL SYSTEM LOGGING** contains the settings for syslog messages (see [chapter 7.1.1, page 284](#)).

The menu **SYSTEM** ➤ **KEEPALIVE MONITORING** contains the settings for the keep-alive monitoring function (see [chapter 5.2.12, page 187](#)).

The menu **SYSTEM** ➤ **TIME AND DATE** contains the settings for manually entering time and date in **X8500** (see [chapter 5.3.1, page 193](#)).

4.1.3 Configuring the LAN Interface

This chapter describes how to configure the LAN interface (10/100 Base-T Ethernet) of **X8500**. The LAN interface is the physical interface to the local network. Since the menus for all Ethernet interfaces are identical, in the following they are referred to as **ETH[x]**. In the menu **ETH[X]** described below, enter the address where your router can be reached in the LAN. As long as your router does not have this entry, it cannot be recognized by other hosts in the network.

Example subnets If your **X8500** is connected to a LAN that consists of two subnets, you should enter a **Second Local IP Number** and a **Second Local Netmask** for it for the second subnet. This is explained in the following example:

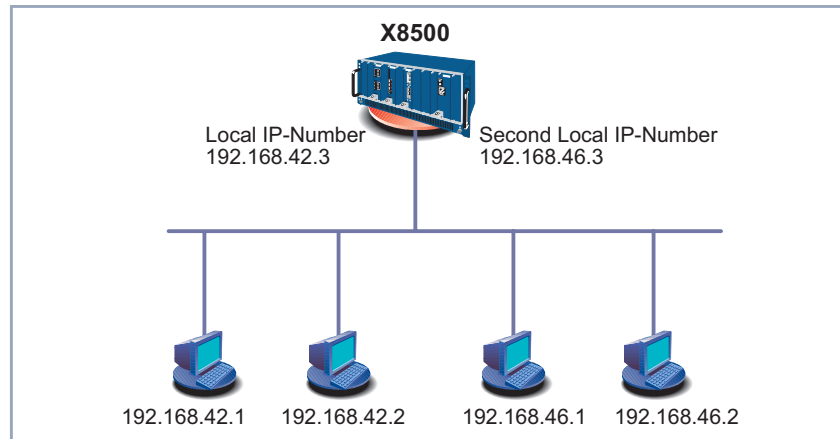


Figure 4-3: **X8500** with two different local IP addresses

The first subnet has two hosts with the **IP addresses** 192.168.42.1 and 192.168.42.2 and the second subnet has two hosts with the IP addresses 192.168.46.1 and 192.168.46.2. To be able to exchange data packets with the first subnet, **X8500** uses the IP address 192.168.42.3, for example, and 192.168.46.3 for the second subnet. The **netmasks** for both subnets must also be indicated.

- IP address, netmask, Encapsulation** ➤ Go to an Ethernet interface of your system card, e.g. **ETH[1]**.

The following menu opens:

X8500 Setup Tool		BinTec Communications AG
[SLOT 0 UNIT 1 ETHERNET]: Configure Ethernet Interface		MyX8500
IP-Configuration		Manual
Local IP Number		192.168.1.254
Local Netmask		255.255.255.0
Second Local IP Number		
Second Local Netmask		
Encapsulation		Ethernet II
Mode		Auto
Bridging		disabled
Advanced Settings>		
SAVE		CANCEL
Enter IP address (a.b.c.d or resolvable host name)		

Entries are possible in this menu for IP configuration and **bridging**. This chapter explains only the configuration of the **IP**. Retain the preset values under **Bridging**.

The following parts of the menu are relevant for this configuration step:

Field	Meaning
IP-Configuration	Possible values: <ul style="list-style-type: none"> ■ <i>Manual</i>: default value. IP address and netmask must be entered. ■ <i>DHCP</i>: X8500 gets IP address from DHCP server.
Local IP Number	IP address of X8500 in the LAN.
Local Netmask	Netmask of the network in which X8500 with Local IP Number is located.
DHCP MAC Address	Only for IP-Configuration DHCP . MAC address of corresponding Ethernet interface.

Field	Meaning
Second Local IP Number	Second IP address of X8500 in the LAN.
Second Local Netmask	Netmask of the network in which X8500 with Second Local IP Number is located.
Encapsulation	<p>Defines the kind of header added to the IP packets that run over this LAN interface. Possible values:</p> <ul style="list-style-type: none"> ■ <i>Ethernet II</i> (conforms to IEEE 802.3) ■ <i>Ethernet SNAP</i> <p>You can generally retain the default value <i>Ethernet II</i>. The first LAN interface of the system card in the system card slot is called en0-1 for <i>Ethernet II</i> and en0-1-snap for <i>Ethernet SNAP</i>.</p>
Mode	<p>Defines the mode in which the LAN interface is operated. Possible values:</p> <ul style="list-style-type: none"> ■ <i>Auto</i> (default value) Automatic detection of the LAN parameters is activated and the LAN interface is operated in the appropriate mode. ■ <i>10 MBit Half Duplex</i> ■ <i>10 MBit Full Duplex</i> ■ <i>100 MBit Half Duplex</i> ■ <i>100 MBit Full Duplex</i> <p>You should normally leave the default value at <i>Auto</i>.</p>

Table 4-5: **ETH[x]**

To do Proceed as follows to configure **X8500**'s LAN interface:

- Select *Manual* for **IP-Configuration**.

- Enter **Local IP Number** of **X8500**, e.g. **192.168.1.254**.
- Enter **Local Netmask**, e.g. **255.255.255.0**.
- If applicable, enter **Second Local IP Number** and **Second Local Netmask**.
- Select **Encapsulation**, e.g. **Ethernet II**.
- Select **Mode**, e.g. **Auto**.
- Confirm with **SAVE**.
You have returned to the main menu. The entries are temporarily saved and activated.

Advanced configuration Information about bridging can be found in the **Software Reference**.

The menu **ETH[x] ➤ ADVANCED SETTINGS** contains settings for the Routing Information Protocol RIP (see [chapter 5.2.9, page 180](#)), IP Accounting, Proxy ARP (see [chapter 5.2.11, page 185](#)) and Back Route Verification (see [chapter 7.2.10, page 331](#)).

4.1.4 Configuring X8500 as DHCP Server

IP addresses in the LAN Each PC in your ➤➤ **LAN** and **X8500** requires its own IP address. If you configure **X8500** as a ➤➤ **DHCP** (Dynamic Host Configuration Protocol) server, **X8500** automatically assigns ➤➤ **IP addresses** from a defined IP address pool to requesting PCs in the LAN. A PC sends out an address request and in turn receives its IP address assigned by **X8500**. You do not need to assign fixed IP addresses to PCs, which reduces the amount of configuration work in your network. To do this, you set up a pool of IP addresses, from which **X8500** assigns IP addresses to hosts in the LAN for a defined period of time. A DHCP server also transfers the addresses of the Domain Name Server entered statically or by PPP negotiation (➤➤ **DNS**), ➤➤ **NetBIOS** name server (WINS) and standard ➤➤ **gateway**.

Configuring DHCP server Proceed as follows if you want to configure **X8500** as DHCP server:

- Go to **IP ➤ IP ADDRESS POOL LAN (DHCP) ➤ ADD**.

The following menu opens:

X8500 Setup Tool		BinTec Communications AG
[IP][DHCP][ADD]: Add Range of IP Addresses		MyX8500
Interface	en0-1	
IP Address	192.168.1.1	
Number of Consecutive Addresses	8	
Lease Time (Minutes)	120	
MAC Address		
Gateway		
NetBT Node Type	not specified	
	SAVE	CANCEL
Use <Space> to select		

The menu contains the following fields:

Field	Meaning
Interface	An interface to which the next address pool is assigned. When an address request is received over Interface , one of the addresses in the address pool is assigned.
IP Address	First IP address in the address pool.
Number of Consecutive Addresses	Total number of IP addresses in the address pool, including the first IP address (IP Address).
Lease Time (Minutes)	Specifies the length of time an address from the pool can be assigned to a host. After the Lease Time (Minutes) expires, the address can be assigned elsewhere.
MAC Address	(optional) Only for Number of Consecutive Addresses = 1 : IP Address is only assigned to the device with MAC Address .

Field	Meaning
Gateway	Defines which IP address is assigned to the DHCP client as gateway. If no IP address is entered here, the IP address of X8500 is also given.
NetBT Node Type	Defines how and in what order the assignment of NetBIOS names to IP addresses is attempted for the hosts of an address pool. You can accept the default value <i>not specified</i> . A detailed description of this function is given in the Software Reference .

Table 4-6: **IP ► IP ADDRESS POOL LAN (DHCP) ► ADD**

To do Make the following entries to configure **X8500** as a DHCP server:

- Select **Interface**, e.g. **en0-1**.
- Enter **IP Address**, e.g. **192.168.1.1**.
- Enter **Number of Consecutive Addresses**, e.g. **8**.
- Enter **Lease Time (Minutes)**, e.g. **120**.
- Enter **MAC Address**, if applicable.
- Enter **Gateway**, if applicable.
- Select **NetBT Node Type**, e.g. **not specified**.
- Confirm with **SAVE**.

You have returned to **IP ► IP ADDRESS POOL LAN (DHCP)**, where the IP address pools are listed. The entries are temporarily saved and you have defined an address pool with eight IP addresses: 192.168.1.1 to 192.168.1.8.



You can also create several entries to define an IP address pool of unconnected address ranges, e.g. **192.168.1.20 - 192.168.1.29** and **192.168.1.35 - 192.168.1.40**, and so on. Simply follow the procedure described above again.

4.1.5 Setting Filters

NetBIOS filters If you are working with Windows in your local network, you should set **NetBIOS** filters to save costs. This prevents establishing connections from the network to your Internet Service Provider (**ISP**), e.g. in order to forward WINS requests from PCs in your network. This means that **X8500** asks your **ISP** which **host name** can be assigned an IP address. These connections are unnecessary because the **ISP** cannot resolve WINS names.

A more detailed explanation of **filters** and security features can be found in [chapter 7.2.8, page 315](#).

To do To prevent these unnecessary connections, proceed as follows:



When configuring filters, make sure not to lock out yourself.

- Use the serial interface or ISDN login on **X8500** for filter configuration.
- If you still access **X8500** over your LAN (e.g. telnet), before starting filter configuration select in the menu **IP** ➤ **ACCESS LISTS** ➤ **INTERFACES** ➤ **EDIT: First rule = none**.
- Go to **IP** ➤ **ACCESS LISTS** ➤ **FILTER** ➤ **ADD**.

The following menu window opens:

X8500 Setup Tool		BinTec Communications AG	
[IP][ACCESS][FILTER][ADD]: Configure IP Access Filter		MyX8500	
Description	wrong_dns		
Index	1		
Protocol	udp		
Source Address			
Source Mask			
Source Port	specify		
Specify Port	137		
Destination Address			
Destination Mask			
Destination Port	specify		
Specify Port	53		
Type of Service (TOS)	00000000	TOS Mask	00000000
SAVE		CANCEL	
Enter string, max. length = 48 chars			

Filter for WINS requests Make the following entries to define a filter for WINS requests:

- Enter **Description:** *wrong_dns*.
- Select **Protocol:** *udp*.
- Select **Source Port:** *specify*.
- Enter **Specify Port:** *137*.
- Select **Destination Port:** *specify*.
- Enter **Specify Port:** *53*.
- Confirm with **SAVE**.

You have returned to **IP** ➤ **ACCESS LISTS** ➤ **FILTER** and the entries are temporarily saved.

Now define a second filter as follows:

- Go to **IP** ➤ **ACCESS LISTS** ➤ **FILTER** ➤ **ADD**.
- Enter **Description:** *all*.
- Select **Protocol:** *any*.
- Select **Source Port:** *any*.
- Select **Destination Port:** *any*.
- Confirm with **SAVE**.

You have returned to menu **IP** ➤ **ACCESS LISTS** ➤ **FILTER**. The entries are temporarily saved and both filters are now listed.

Filter rules To define rules for these filters, proceed as follows:

- Go to **IP** ➤ **ACCESS LISTS** ➤ **RULES** ➤ **ADD**.

The following menu window opens:

X8500 Setup Tool		BinTec Communications AG	
[IP][ACCESS][RULE][ADD]: Configure IP Access Rules		MyX8500	
Action	deny M		
Filter	wrong_dns (1)		
SAVE		CANCEL	
Use <Space> to select			

First rule Make the following entries to define a rule:

- Select **Action:** *deny M*.
- Select **Filter:** *wrong_dns (1)*.
- Confirm with **SAVE**.

You have returned to **IP** ➤ **ACCESS LISTS** ➤ **RULES**, and the entries are temporarily saved.

Second rule Now define a second rule as follows:

- Go to **IP** ➤ **ACCESS LISTS** ➤ **RULES** ➤ **ADD**.
- Select **Insert Behind Rule:** *RI 1 FI 1 (wrong_dns)*.
- Select **Action:** *allow M*.
- Select **Filter:** *all (2)*.
- Confirm with **SAVE**.

You have returned to **IP** ➤ **ACCESS LISTS** ➤ **RULES**.

The entries have been saved and listed:

```

X8500 Setup Tool                               BinTec Communications AG
[IP][ACCESS][RULE]: Configure IP Access Rules   MyX8500

Abbreviations:  RI (Rule Index)    M (Action if filter matches)
                 FI (Filter Index) !M (Action if filter does not match)
                 NRI (Next Rule Index)

RI  FI      NRI    Action      Filter      Conditions
1   1        2     deny M     wrong_dns   udp, sp 137, dp 53
2   2        0     allow M    all

      ADD              DELETE          REORG          EXIT

Press<Ctrl-n>,<Ctrl-p>to scroll,<Space>tag/untagDELETE,<Return>to edit

```

Assign interfaces Proceed as follows:

➤ Go to **IP** ➤ **ACCESS LISTS** ➤ **INTERFACES**.

The following menu window opens:

```

X8500 Setup Tool                               BinTec Communications AG
[IP][ACCESS][INTERFACES]: Configure First Rule   MyX8500

Configure first rules for interfaces

Interface    First Rule      First Filter
en0-1        1                1 (wrong_dns)
en0-1-snap   1                1 (wrong_dns)

EXIT

Press <Ctrl-n>,<Ctrl-p> to scroll, <Return> to edit/select

```

➤ Select the LAN interface of **X8500** (**en0-1** or **en0-1-snap**) and confirm with **Return**.

➤ Select **First Rule: RI 1 FI 1 (wrong_dns)**.

➤ Leave the set values for all other fields.

➤ Confirm with **SAVE**.

These entries ensure that all data traffic that passes from source ➤➤ **port 137** to destination port 53 will be discarded. This means that no unnecessary connections will be established to resolve WINS names.

- Leave **IP** ➤ **ACCESS LISTS** ➤ **INTERFACES** with **EXIT**.
- Leave **IP** ➤ **ACCESS LISTS** with **EXIT**.
- Leave **IP** with **EXIT**.

You have returned to the main menu. The configuration of the basic router settings is complete. The entries are temporarily saved and activated.



Leave the Setup Tool with **Save as boot configuration and exit** to save the configuration to the flash memory.

4.2 Configuring WAN Interfaces

This chapter describes the configuration of the following WAN interfaces of **X8500**:

- ISDN BRI interface (see [chapter 4.2.1, page 73](#))
- You can also configure the second LAN interface of the system card or any other LAN interface of **X8500** as an interface to the WAN by providing a connection to xDSL, using PPP-over-Ethernet or PPTP ([chapter 4.2.2, page 86](#))

Installing expansion cards enables additional interfaces to be used on **X8500** (see [chapter 6, page 241](#)).

4.2.1 Configuring ISDN BRI interface

You can use the ISDN BRI interface of **X8500** for both dialup and leased lines (see "[Leased Line](#)", [page 84](#)) over ISDN.

Configuring the ISDN BRI interface consists of the following:

- Entering the settings of your ISDN connection:
Here you set the most important parameters of your ISDN connection.
- Configuring Incoming Call Answering:
Here you tell **X8500** how to react to calls coming in from the WAN.

Dialup line Firstly, enter the settings for your ISDN connection.

- Go to the BRI interface of your system card, e.g. **BRI[4]**.

In this example, the menu of the BRI interface of the system card is shown (SLOT 0 UNIT 4 ISDN BRI) The following menu opens:

```

X8500 Setup Tool                               BinTec Communications AG
[SLOT 0 UNIT 4 ISDN BRI]: Configure ISDN Basic Rate Interface MyX8500

Result of Autoconfiguration: Euro ISDN, point-to-multipoint
ISDN Switch Type                    autodetect on bootup

D-Channel                            dialup
B-Channel 1                          dialup
B-Channel 2                          dialup

Incoming Call Answering>
Advanced Settings>

                                SAVE                                CANCEL

Use <Space> to select

```

Since the menus of all BRI interfaces are identical, in the following they will be referred to as **BRI[x]**.

The menu **BRI[x]** contains the following fields:

Field	Meaning
Result of Autoconfiguration	Status of ISDN autoconfiguration. Automatic ▶▶ D-channel detection runs until a setting is found or until the ISDN protocol is entered manually under ISDN switch type.
ISDN Switch Type	Defines the ISDN ▶▶ protocol supplied by your ISDN provider. The following parameters are possible: <ul style="list-style-type: none"> ■ <i>autodetect on bootup</i>: automatic D-channel detection (default setting) ■ <i>Euro ISDN point to multipoint</i>: Euro ISDN for point-to-multipoint ■ <i>Euro ISDN point to point</i>: Euro ISDN for point-to-point

Field	Meaning
Continuation of ISDN Switch Type	<ul style="list-style-type: none"> ■ <i>1TR6 point to multipoint</i> ■ <i>1TR6 point to point</i> ■ <i>National ISDN 1 AT&T NI1, EWSD NI1</i> ■ <i>AT&T 5ESS Custom ISDN point to multipoint</i> ■ <i>AT&T 5ESS Custom ISDN point to point</i> ■ <i>National ISDN 1 Northern Telecom DMS100</i> ■ <i>Japan NTT INS64</i> ■ <i>none</i> ■ <i>leased line B1 channel (64S): leased line over B-channel 1</i> ■ <i>leased line B1+B2 channel (64S2): leased line over both B-channels</i> ■ <i>leased line D+B1+B2 channel (TS02): leased line over D-channel and both B-channels</i> ■ <i>leased line B1+B2 different endpoints (digital 64S with dual connection): leased line to two different endpoints</i> <p>Note: Tested only for Euro ISDN.</p>
D-Channel	<p>D-channel configuration. The selection can only be changed if ISDN Switch Type = <i>leased line D+B1+B2 (TS02)</i>. Possible values:</p> <ul style="list-style-type: none"> ■ <i>leased dte</i> (default value) ■ <i>leased dce</i>

Field	Meaning
B-Channel 1	Configuration of first B-channel . Possible values: <ul style="list-style-type: none"> ■ <i>dialup</i> (default setting) ■ <i>not used</i> ■ <i>leased dte</i> ■ <i>leased dce</i>
B-Channel 2	Configuration of second B-channel. Possible values: <ul style="list-style-type: none"> ■ <i>dialup</i> (default setting) ■ <i>not used</i> ■ <i>leased dte</i> ■ <i>leased dce</i>

Table 4-7: **BRI[x]**

To do Make the following entries:

- Select **ISDN Switch Type**: *autodetect on bootup*.

This setting enables **X8500** to use its automatic D-channel detection. As long as the D-channel detection is running, *running* appears next to **Result of Autoconfiguration**. Once the setting has been found, it is displayed, e.g. *Euro ISDN, point-to-multipoint*.



If the ISDN protocol is not detected, it can be entered manually under **ISDN Switch Type**. The automatic D-channel detection is then switched off.

An incorrectly set ISDN protocol prevents ISDN connections being established!



In most cases, you can accept the preset values for **D-Channel**, **B-Channel 1** and **B-Channel 2**.

If you use an ISDN leased line and have requested a special service from your service provider, it may be necessary to set the local side of the leased line at this point (DTE or DCE). You must then ensure that the far end has set the opposite value. You must also set **D-channel**, **B-channel 1** and **B-channel 2** to the same values, if you have selected *leased line D+B1+B2 channel (TS02)* under **ISDN Switch Type**.

➤ Confirm with **SAVE**.

You have returned to the main menu. The entries are temporarily saved and activated.

Incoming Call Answering

If you use the ISDN BRI interface or ISDN PRI interface for dialup connections, you must now tell **X8500** its own numbers for this interface (these settings are not possible for leased lines). **X8500** distributes the incoming calls to the appropriate internal services according to the settings in the following menus.

X8500 supports the following services:

■ PPP (Routing):

The ➤➤ **PPP** service is **X8500**'s general routing service. This connects incoming data calls from WAN partners' dialup connections to your ➤➤ **LAN**. This enables partners outside your own local network to access hosts within your LAN. This subsystem also enables outgoing data calls to be made to WAN partners outside your local network.



This PPP routing is also used for X.25 connections.

■ ISDN Login:

The ➤➤ **ISDN Login** service allows incoming data calls access to the ➤➤ **SNMP shell** of your **X8500**. This is how **X8500** is remotely configured and administrated.

■ CAPI:

The **▶▶ CAPI** service allows connection of incoming and outgoing data and voice calls to communication applications on hosts in the LAN that access the **▶▶ Remote-CAPI** interface of **X8500**. This enables, for example, hosts connected to **X8500** to receive and send faxes.

To be able to use CAPI applications on hosts in the LAN, you must carry out the Remote CAPI configuration on the individual hosts (see [chapter 4.5, page 127](#)) in addition to assigning the extension numbers as described in this chapter.

Following a diagram of call distribution:

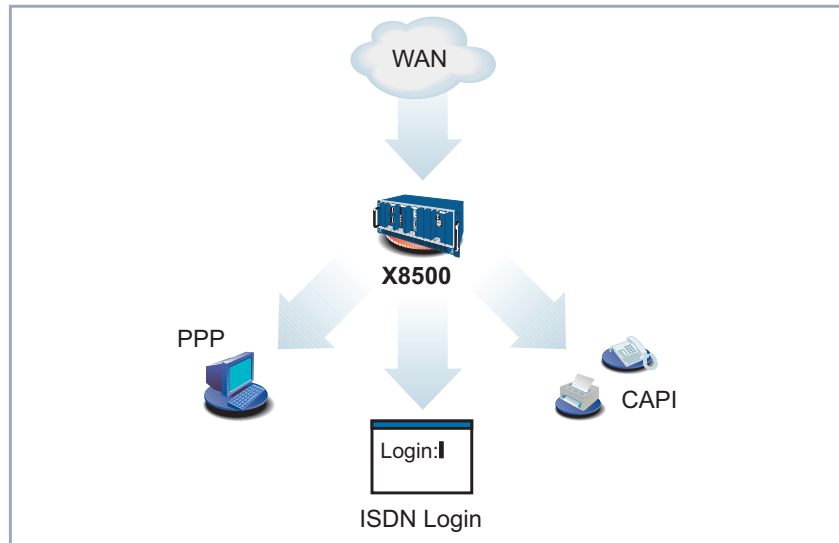


Figure 4-4: Distribution of incoming calls

When a call is received, **X8500** first checks the Called Party Number (CPN) and the type of call (data or voice call). The CPN is the extension the partner has dialed to reach **X8500**. Then the call is forwarded to the corresponding service (see [figure 4-4, page 78](#)).

If your ISDN connection has more than three extensions, a practical allocation could look as follows:

Called party number	Data services	Voice services
10	PPP (routing)	
11	CAPI	CAPI
12	ISDN Login	

Table 4-8: Assignment of extensions to services



If no entry is specified in the following menu, every incoming ISDN call is accepted by the ISDN Login service. To avoid this, be sure to make the necessary entries here.

As soon as you have made one or more entries in this menu, the matching incoming calls are distributed to the corresponding services.



In the unconfigured ex works state, a user with the user name "default" and no password is already entered for the CAPI subsystem. All calls to the CAPI are offered to all CAPI applications in the LAN.

To distribute incoming calls for the CAPI subsystem to defined users with passwords, you should use BinTec's User Concept (see [chapter 5.1.2, page 138](#)). You should then delete the user "default" without password.



All incoming calls that do not match an entry are passed on to the CAPI service.

Configuring Incoming Call Answering



Now set the entries for Incoming Call Answering:

The settings of Incoming Call Answering for ISDN BRI interfaces correspond to the settings of Incoming Call Answering for ISDN PRI interfaces.

➤ Go to, e.g., **BRI[4]** ➤ **INCOMING CALL ANSWERING**.

The following menu opens:

X8500 Setup Tool		BinTec Communications AG	
[SLOT 0 UNIT 4 ISDN BRI][INCOMING]: Incoming Call Answering		MyX8500	
Item	Number	Mode	Username
CAPI 1.1 EAZ 1 Mapping	11	right to left	
CAPI 1.1 EAZ 1 Mapping	11	right to left	
ISDN Login	12	right to left	
PPP (routing)	10	right to left	
ADD	DELETE	EXIT	
Press<Ctrl-n>,<Ctrl-p>to scroll,<Space>tag/untagDELETE,<Return>to edit			

This menu lists the previously completed assignment of services to extension numbers.

To make entries in the list, proceed as follows:

- Use **ADD** to add a new entry or select an existing entry.
- Confirm with **Return** to change the entry.

Another menu window opens:

X8500 Setup Tool		BinTec Communications AG	
[SLOT 0 UNIT 4 ISDN BRI][INCOMING][ADD]: Incoming Calls		MyX8500	
Item	PPP (routing)		
Number	10		
Mode	right to left		
Bearer	data		
SAVE	CANCEL		
Use <Space> to select			

The menu **BRI[x] ► INCOMING CALL ANSWERING ► ADD** resp. **PRI[x] ► INCOMING CALL ANSWERING ► ADD** contains the following fields:

Field	Meaning
Item	Service which shall accept a call to the Number below. Possible values: see table 4-10, page 83 .
Number	Phone number under which the service (Item) entered above can be reached.
Mode	Mode in which X8500 compares the digits of Number with the called party number of the incoming call: <ul style="list-style-type: none"> ■ <i>right to left</i> (default value) ■ <i>left to right (DDI)</i>: Always select if X8500 is connected to a point-to-point connection.
CAPI Username	(only for Item = <i>CAPI 1.1 EAZ 0...9 Mapping</i> and for Item = <i>CAPI 2.0</i>) CAPI user name. Only necessary if you want to use the CAPI user concept (see chapter 5.1.2, page 138).
Bearer	Type of incoming call. Possible values: <ul style="list-style-type: none"> ■ <i>data</i>: data call ■ <i>voice</i>: voice call (modem, voice, analog fax) ■ <i>any</i>: both data and voice calls

Table 4-9: **BRI[x] ► INCOMING CALL ANSWERING ► ADD, PRI [x] ► INCOMING CALL ANSWERING ► ADD**

The **Item** field includes the following selection:

Possible Values	Meaning
<i>PPP (routing)</i>	Default setting for ►► PPP routing. Also applicable for the PPP connections below.

Possible Values	Meaning
<i>ISDN Login</i>	Enables logging in with ➤➤ isdnlogin .
<i>PPP 64k</i>	Enables 64 kbps PPP data connections.
<i>PPP 56k</i>	Enables 56 kbps PPP data connections.
<i>PPP Modem</i>	(Only available if PRI expansion card or CM-PRI and resource module with digital modems is installed) Assigns incoming analog calls to the PPP routing service. The digital modem on the resource module that accepts this call uses the settings for Modem Profile 1, which were selected in the menu MODEM ▶ PROFILE CONFIGURATION ▶ PROFILE 1 .
<i>PPP DOVB</i>	Data Transmission Over Voice Bearer - useful in the USA, for example, where voice connections are sometimes cheaper than data connections.
<i>PPP V.110 (1200...38400)</i>	Enables PPP connections with V.110 at bit rates of 1200 bps, 2400 bps, ..., 38400 bps.
<i>PPP V.120</i>	Enables incoming PPP connections with V.120.
<i>Pots</i>	Not available with X8500 .
<i>PPP Modem Profile 1...8</i>	(Only available if PRI expansion card or CM-PRI and resource module with digital modems is installed) Assigns incoming analog calls to the PPP routing service. The digital modem on the resource module that accepts this call uses the settings for Modem Profile 1... 8, which were selected in the menu MODEM ▶ PROFILE CONFIGURATION ▶ PROFILE 1...8 .
<i>CAPI 1.1 EAZ 0...9 Mapping</i>	Enables connections with Remote CAPI applications. Required for CAPI 1.1 applications only.

Possible Values	Meaning
<i>X.25 PAD</i>	Enables data connections with X.25 PAD.
<i>CAPI 2.0</i>	Enables connections with Remote CAPI applications. Only for CAPI 2.0 applications.

Table 4-10: **Item**

Make sure you enter the right number under **Number**, i.e. the number that actually arrives at **X8500**! For example, if **X8500** is connected to a **PABX**, only the PABX extension number arrives at **X8500**.

If you are not sure which number arrives at **X8500**, proceed as follows:

- Call **X8500** with a conventional telephone using one of its extension numbers.
- Go to **MONITORING AND DEBUGGING** ➤ **ISDN MONITOR**.
You can now see the incoming call in the menu.
- Place the cursor on the call and enter **d** (for details).
Under **Local Number**, you can see the part of the number that arrives at **X8500**.
- Type in this part of the number in **BRI[x]** ➤ **INCOMING CALL ANSWERING** ➤ **ADD** resp. **PRI[x]** ➤ **INCOMING CALL ANSWERING** ➤ **ADD** under **Number**.



If you use a communication application on your PC that is based on Remote CAPI 1.1 (current version: Remote CAPI 2.0), **X8500** must translate the **MSNs** (= **Number**, multidigit) of the incoming call to **EAZs** (single digit) (CAPI 1.1 can only detect single-digit numbers). This is why the CAPI entry under **Item** is not simply called "CAPI" but "CAPI 1.1 EAZ x Mapping". When using CAPI 1.1, you must therefore make sure you assign each CAPI application the corresponding EAZ(s) by "mapping". For example select for **Number** = 1234 the entry **Item** = **CAPI 1.1 EAZ 0 Mapping** and for **Number** = 5678 the entry **Item** = **CAPI 1.1 EAZ 1 Mapping**.

With CAPI 2.0, the MSN is evaluated directly, so "conversion" to EAZ is not necessary. You should certainly try to change your PC system to CAPI 2.0 so that you can also use new features.

Assign extensions numbers to services

Make the following entries:

- Select the **Item**, e.g. *PPP (routing)*.
- Enter the **Number**, e.g. *10*.
- Select the **Mode**, e.g. *right to left*.
- Select the **Bearer**, e.g. *data*.
- Confirm with **SAVE**.

You have returned to the menu **BRI[4]** ➤ **INCOMING CALL ANSWERING**. The entries are temporarily saved and displayed in the list.

You have now assigned one of your extensions (*10*) to a possible service (*PPP (routing)*). If a data call is received by called party number 10, it is therefore forwarded to the PPP (routing) service. If the PPP (routing) service initiates an outgoing data call, then 30 is assigned as calling party number.

- Repeat these steps until you have assigned all desired services to one of the available **Numbers**.

This concludes the configuration of Incoming Call Answering. **X8500** now distributes the incoming calls to the internal services.

Advanced Configuration

BRI[x] ➤ **ADVANCED SETTINGS** contains settings for X.31 TEI (see [chapter 5.1.4, page 144](#)).

If you use a leased line, you can implement a backup solution using the Bandwidth on Demand feature (see [chapter 5.2.3, page 149](#)). If you use this facility, a dialup connection is set up to the connection partner if the leased line fails.

Leased Line

You can also use ISDN BRI and ISDN PRI interfaces of **X8500** for leased lines.

To configure the ISDN interface for use with a leased line you will need to set the ISDN Switch Type manually:

- Go to the appropriate interface, e.g. **BRI[4]**.

- Scroll through the entries in **ISDN Switch Type** and select the appropriate type of leased line.

Upon exiting this field the cursor will jump to the first channel used.



In most cases, you can accept the preset values for **D-Channel**, **B-Channel 1** and **B-Channel 2**.

If you use an ISDN leased line and have requested a special service from your service provider, it may be necessary to set the local side of the leased line at this point (DTE or DCE). You must then ensure that the far end has set the opposite value.

Example of settings for leased line:

```

X8500 Setup Tool                               BinTec Communications AG
[SLOT 0 UNIT 4 ISDN BRI]: Configure ISDN Basic Rate Interface MyX8500

Result of autoconfiguration: autoconfiguration disabled
ISDN Switch Type             leased line B1 channel (64S)

D-Channel                    not used
B-Channel 1                  leased dte
B-Channel 2                  not used

Incoming Call Answering>
Advanced Settings>

                                SAVE                CANCEL

Use <Space> to select

```

- Confirm with **SAVE**.

You have returned to the main menu. The entries are temporarily saved and activated.



A WAN partner interface is created automatically for leased lines. The field **State** in the menu **WAN PARTNER** should show *up*.

- Edit the previously created entry for a leased line in the **WAN PARTNER** menu and enter the necessary parameters.

4.2.2 Broadband Internet Access (xDSL) with X8500

BinTec Communications AG's **X8500** offers the PPP-over-Ethernet and PPTP protocols. These protocols are required, for example, for connecting terminals to the Internet over the xDSL connection to achieve increased bandwidth.



If you use the xDSL connection of a provider other than Deutsche Telekom, ask the provider about any special features of your xDSL connection that need to be considered.

Example 1: Deutsche Telekom

Scenario for following example configuration:

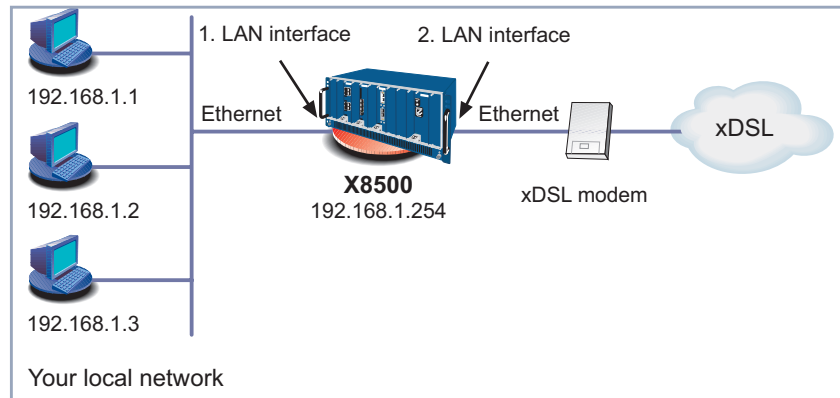


Figure 4-5: Example scenario

The LAN connection is handled over one Ethernet interface of **X8500**. The xDSL modem is connected to a second Ethernet interfaces of **X8500**.



If you receive a special cable from Deutsche Telekom AG or another provider for connecting the xDSL modem, please use only this cable.

Configuring the IP address

Proceed as follows to define the IP address of **X8500**:

- Go to, e.g., **ETH[2]**.

- Enter your IP address in the **Local IP Number** field, e.g. **192.168.1.254**.
- Enter your netmask in the **Local Netmask** field, e.g. **255.255.255.0**. This address should be the default gateway for the hosts in your LAN.
- Confirm with **SAVE**.

General PPP settings The general PPP settings are configured in the **PPP** menu:

Here you must configure an interface on which PPP-over-Ethernet is to run. You can leave all the other settings at the default value.

- Go to **PPP**.

The following field is relevant:

Field	Meaning
PPPoE Ethernet Interface	Defines the interface used for xDSL.

Table 4-11: **PPP**

Proceed as follows to define the necessary PPP settings:

- Select your **PPPoE Ethernet Interface**, e.g. **en0-2** (second LAN interface in [figure 4-5, page 86](#)).
- Confirm with **SAVE**.

WAN partner settings To configure a PPP-over-Ethernet partner, proceed exactly as for configuration of a WAN partner.



When configuring the WAN partner, make sure that Van Jacobson Header Compression is not activated in the menu **WAN PARTNER** ➤ **ADD** ➤ **IP** ➤ **ADVANCED SETTINGS**. The Bridging and Bandwidth on Demand functions can not be used either.

- Go to **WAN PARTNER** ➤ **ADD**.

The following fields are relevant:

Field	Meaning
Partner Name	Enter a name for uniquely identifying the PPP-over-Ethernet partner.
Encapsulation	Encapsulation defines how the data packets are packed for transfer to the WAN partner. PPP-over-Ethernet: Only <i>PPP</i> should be selected here.

Table 4-12: **WAN PARTNER** ➔ **ADD**

- Enter your WAN partner's name for PPP-over-Ethernet under **Partner Name**, e.g. *t-online*.
- Select **Encapsulation**: *PPP*.
- Go to **WAN PARTNER** ➔ **ADD** ➔ *PPP*.

WAN partner PPP settings

The following fields are relevant:

Field	Meaning
Partner PPP ID	ID of WAN partner. Remains empty.
Local PPP ID	Your T-Online user ID. Comprises the following elements: <user account><T-Online number>#<co-user number>@t-online.de user account = the 12-digit user account (example: <i>000460004256</i>) T-Online number = telephone number (example: <i>091169386</i>) co-user number = 4-digit co-user number (example: <i>0001</i>) The T-Online number and the co-user number must be separated by # if the T-Online number has less than 12 digits.

Field	Meaning
PPP Password	Your T-Online password.
Keepalives	Activates keepalive packets. The activated Keepalive function checks the interface status. This permits faster detection and signaling if the connection to the provider fails (for example, if the LAN cable is accidentally disconnected).

Table 4-13: **WAN PARTNER** ► **ADD** ► **PPP**

- Do not enter a **Partner PPP ID**.
- Enter the **Local PPP ID**,
e.g. **000460004256091169386#0001@t-online.de**.
- Enter the **PPP Password**.
- Select **Keepalives**: *on*.
- Confirm with **OK**.

Advanced settings ► Go to **WAN PARTNER** ► **ADD** ► **ADVANCED SETTINGS**.

The following field is relevant:

Field	Meaning
Layer 1 Protocol	Here you can define the Layer 1 Protocol of the ISDN B-channel that X8500 is to use for connections to the WAN partner. <i>PPP over Ethernet (PPPoE)</i> must be selected here for access to T-DSL.

Table 4-14: **WAN PARTNER** ► **ADD** ► **ADVANCED SETTINGS**

- Select **Layer 1 Protocol**: *PPP over Ethernet (PPPoE)*.
- Confirm with **OK**.

IP settings ► Go to **WAN PARTNER** ► **ADD** ► **IP**.

The following field is relevant:

Field	Meaning
IP Transit Network	Defines whether X8500 uses a transit network to the WAN partner. The IP address is assigned dynamically if <i>dynamic client</i> is selected.

Table 4-15: **WAN PARTNER** ➤ **ADD** ➤ **IP**

- Select **IP Transit Network**: *dynamic client*.
- Confirm with **SAVE** and **EXIT** until you have returned to the main menu.
- Go to **IP** ➤ **ROUTING** ➤ **ADD**.

Creating a default route

The following field is relevant:

Field	Meaning
Partner / Interface	Your PPPoE partner.

Table 4-16: **IP** ➤ **ROUTING** ➤ **ADD**

- Select **Route Type**: *Default route*.
- Select **Partner / Interface**, e.g. *t-online*.
- Confirm with **SAVE**.

Activating Network Address Translation (NAT)

You can use NAT to ensure the following:

- No more accesses can be made to your network from the Internet
- Connections to the Internet appear only under a single dynamically assigned IP address
- Go to **IP** ➤ **NETWORK ADDRESS TRANSLATION**.
- Select the WAN interface on which you want to activate NAT, e.g. *t-online*, and confirm with **Return**.

Another menu window opens.

The following field is relevant:

Field	Meaning
Network Address Translation	Here you can activate Network Address Translation (NAT) for your WAN partner. This conceals your whole network to the outside world with just one IP address.

Table 4-17: **IP** ➔ **NAT**

- Select **Network Address Translation**: *on*.
- Leave **Silent Deny**: *no*.
- Confirm with **SAVE**.

The WAN interface for xDSL is configured.

Example 2: Telekom Austria (high-speed Internet access)

Telekom Austria offers a high-speed access to the Internet (A-Online Speed), which is available in Austria. Proceed as follows:

Configuring WAN partners

- Go to **WAN PARTNER** ➔ **ADD**.
- Enter your **Partner Name** (= provider name): *Telekom_Austria*.
- Select **Encapsulation**: *PPP*.
- Select **Compression**: *none*.
- Select **Encryption**: *none*.

Selecting PPP authentication

- Select **PPP** and confirm with **Return**.
- Select **Authentication**: *CHAP*.
- Do not enter a **Partner PPP ID**. This field remains empty.
- Enter **Local PPP ID** (= your user name), e.g. *3909987000*.
- Type in **PPP Password**.
- Deactivate **Keepalives**: *off*.
- Deactivate **Link Quality Monitoring**: *off*.

- Confirm with **OK**.
- You have returned to the menu **WAN PARTNER** ➤ **ADD**.

Setting short hold

- Select **Advanced Settings** and press **Return**.
- Select **Callback**: *no*.
- Enter **Static Short Hold (sec)**, e.g. **90**. (If you use a flat-rate connection, you can enter **Static Short Hold (sec)** -1.)
- Enter **Idle for Dynamic Short Hold (%)**: *0*.
- Enter **Delay after Connection Failure (sec)**, e.g. **300**.
- Select **Layer 1 Protocol**: *PPP over PPTP*.
- Leave out **Extended Interface Settings**.
- Confirm with **OK**.
- You have returned to the menu **WAN PARTNER** ➤ **ADD**.

Carrying out IP configuration

- Select **IP** and press **Return**.
- Enter **VPN Partner's IP Address** : *10.0.0.138*.
- Select **via IP Interface**: e.g. **en0-2** (second LAN interface in [figure 4-5, page 86](#)).
- Enter **local IP Address**: *10.0.0.140*.
- Leave out **Advanced Settings**.
- Confirm with **SAVE**.
- You have returned to the menu **WAN PARTNER** ➤ **ADD**.

- Confirm with **SAVE**.
- Leave **WAN PARTNER** with **EXIT**.

Creating routing entry

- Go to **IP** ➤ **ROUTING**.
- Add a new entry with **ADD**.
- Select **Route Type**: *Default route*.
- Select **Network**: *WAN without transit network*.
- Select **Partner / Interface**: *Telekom_Austria*.
- Enter **Metric**, e.g. **1**.

- Confirm with **SAVE**.
- Leave **IP** ➤ **ROUTING** with **EXIT**.
You have returned to the **IP** menu.

Activating NAT

- Go to **IP** ➤ **NETWORK ADDRESS TRANSLATION**.
- Select Telekom_Austria as IP interface and press **Return**.
- Select **Network Address Translation: on**.
- Leave **Silent Deny: no**.
- Confirm with **SAVE**.
- Leave **IP** ➤ **NETWORK ADDRESS TRANSLATION** with **EXIT**.
- Leave **IP** with **EXIT**.
You have returned to the main menu. The configuration of the high-speed access is complete.

4.3 X8500 and the WAN

To enable **X8500** to make connections to networks or hosts outside your LAN, you must configure the partners you want to connect to as WAN partners on your **X8500**. This applies to outgoing connections (**X8500** dials out to a WAN partner), as well as for incoming connections (a WAN partner dials the number of your **X8500**) and leased lines and G.703.

Consequently, if you want to access the Internet, you must set up your Internet Service Provider (▶▶ **ISP**) as a WAN partner. If you wish to establish a LAN-LAN connection, e.g. between your LAN (head office) and the LAN of a branch office (corporate network connection), you have to configure the LAN of your branch office as a WAN partner.

If you set up one or more leased lines or G.703, a WAN partner for each leased line and G.703 connection is already created automatically in the WAN Partner menu. Edit this entry to suit your requirements.

General proceeding Configuring a WAN partner generally involves the following steps:

- Entering a WAN partner ([chapter 4.3.1, page 94](#)):
 - Defining a ▶▶ **protocol** (encapsulation)
 - Entering extension(s)
 - Defining ▶▶ **PPP** settings for authentication
 - Defining ▶▶ **short hold**
 - Carrying out IP configuration
- Creating routing entry ([chapter 4.3.2, page 115](#))
- Activating Network Address Translation (▶▶ **NAT**) (optional, [chapter 4.3.3, page 121](#))

Examples You can find a number of frequently required configuration examples in [chapter 4.3.4, page 122](#).

4.3.1 Entering a WAN Partner

Here you are going to configure access to your WAN partners, e.g. your Internet Service Provider (ISP). Before you get down to it, you should collect the neces-

sary access information that you received from your ISP or system administrator (see [chapter 3.5.1, page 45](#)). The terms used may vary slightly from provider to provider.

Configuring WAN partners

To enter a WAN partner, proceed as follows:

➤ Go to **WAN PARTNER**.

The following menu window opens:

X8500 Setup Tool		BinTec Communications AG
[WAN]: WAN Partners		MyX8500
Current WAN Partner Configuration		
Partnername	Protocol	State
T-Online	ppp	dormant
ADD	DELETE	EXIT
Press<Ctrl-n>, <Ctrl-p>to scroll, <Space>tag/untagDELETE, <Return>to edit		

This is where all WAN partners currently configured are listed with the corresponding **Partnername**, **Protocol** ([table 4-19, page 99](#)) and **State** ([table 4-18, page 96](#)).



A WAN partner interface is created automatically for leased lines and G.703 connections. Edit the previously created entry for a leased line in the **WAN PARTNER** menu and enter the necessary parameters.

State can have the following values:

Possible Values	Meaning
<i>up</i>	connected
<i>dormant</i>	not connected (dialup connection)

Possible Values	Meaning
<i>blocked</i>	not connected (an error occurred on establishing a connection, a renewed attempt is only possible after a specified number of seconds)
<i>down</i>	set to <i>down</i> by administration (deactivated); for leased lines: not connected.

Table 4-18: **State**

To make an entry in the list, proceed as follows:

- Use **ADD** to add a new entry or select an existing entry. Confirm with **Return** to change the entry.

Another menu window opens:

X8500 Setup Tool	BinTec Communications AG
[WAN][ADD]: Configure WAN Partner	MyX8500
Partner Name	T-Online
Encapsulation	PPP
Encryption	none
Compression	none
Calling Line Identification	no
PPP >	
Advanced settings >	
WAN Numbers >	
Weekly Schedule >	
IP >	
Bridge >	
SAVE	CANCEL
Enter string, max length = 25 chars	

The menu contains the following fields:

Field	Meaning
Partner Name	Enter a name for uniquely identifying the WAN partner.

Field	Meaning
Encapsulation	<p>➤➤ Encapsulation. Defines how the</p> <p>➤➤ data packets are packed for transfer to the WAN partner. Possible values:</p> <ul style="list-style-type: none"> ■ <i>PPP</i> ■ <i>Multi-Protocol LAPB Framing</i> ■ <i>Multi-Protocol HDLC Framing</i> ■ <i>Async PPP over X.75</i> ■ <i>Async PPP over X.75/T.70/BTX</i> ■ <i>Async PPP over V.120 (HSCSD)</i> ■ <i>X.25_PPP</i> ■ <i>X.25</i> ■ <i>HDLC Framing (IP only)</i> ■ <i>LAPB Framing (IP only)</i> ■ <i>X31 B-Channel</i> ■ <i>X.25 No Signalling</i> ■ <i>X.25 PAD</i> ■ <i>X.25 No Configuration</i> ■ <i>Frame Relay</i> ■ <i>X.25 No Configuration, No Signalling</i>

Field	Meaning
Encryption	<p>Defines the type of encryption that should be used for data traffic to the WAN partner. Can only be used if STAC compression is not activated for the connection. Possible values:</p> <ul style="list-style-type: none"> ■ <i>MPPE 40</i>: MPPE version 1 with 40-bit key ■ <i>MPPE 56</i>: MPPE version 1 with 56-bit key ■ <i>MPPE 128</i>: MPPE version 1 with 128-bit key ■ <i>MPPE V2 40</i>: MPPE version 2 with 40-bit key ■ <i>MPPE V2 56</i>: MPPE version 2 with 56-bit key ■ <i>MPPE V2 128</i>: MPPE version 2 with 128-bit key ■ <i>DES 56</i>: DES with 56-bit key (only available if VPN license is activated) ■ <i>DES3 168</i>: Triple DES with 168-bit key (only available if VPN license is activated) ■ <i>Blowfish 56</i>: Blowfish with 56-bit key (only available if VPN license is activated) ■ <i>Blowfish 168</i>: Blowfish with 168-bit key (only available if VPN license is activated) ■ <i>none</i>: no encryption <p>These values are only available if <i>PPP</i>, <i>Async PPP over X.75</i>, <i>Async PPP over X.75/T.70/BTX</i>, <i>X.25_PPP</i> or <i>Async PPP over V.120 (HSCSD)</i> has been selected under Encapsulation.</p>

Field	Meaning
Compression	<p>Defines the type of compression that should be used for data traffic to the WAN partner. Possible values:</p> <ul style="list-style-type: none"> ■ <i>STAC</i> ■ <i>MS-STAC</i> ■ <i>none</i> <p>These values are only available if <i>PPP</i>, <i>Async PPP over X.75</i>, <i>Async PPP over X.75/T.70/BTX</i>, <i>X.25_PPP</i> or <i>Async PPP over V.120 (HSCSD)</i> has been selected under Encapsulation, and <i>none</i> has been selected under Encryption.</p>
Calling Line Identification	<p>Indicates whether calls from this WAN partner should be identified by means of the calling party number (▶▶ CLID). The value of this field is dependent on Direction in the submenu WAN NUMBERS and cannot be set here.</p>

Table 4-19: **WAN PARTNER** ▶ **ADD**

Specifying Protocol

To do Make the following entries:

- ▶ Type in **Partner Name**, e.g. *BigBoss*.
- ▶ Select **Encapsulation**, e.g. *PPP*.
- ▶ Select **Compression**, e.g. *none*, if applicable.
- ▶ Select **Encryption**, e.g. *none*, if applicable.

Entering Extensions

Proceed as follows to enter the extensions of your WAN partners:

- ▶ Go to submenu **WAN PARTNER** ▶ **ADD** ▶ **WAN NUMBERS**.

Entering Extension Numbers

This is where the currently entered extensions of the WAN partners are listed:

```

X8500 Setup Tool                               BinTec Communications AG
[WAN][ADD][WAN Numbers]: WAN Numbers (BigBoss)   MyX8500

WAN Numbers for this partner:

      WAN Number      Direction
      0911987654321   outgoing

ADD                DELETE                EXIT

Press<Ctrl-n>,<Ctrl-p>to scroll,<Space>tag/untagDELETE,<Return>to edit

```

To make an entry in the list, proceed as follows:

- Use **ADD** to add a new entry or select an existing entry. Confirm with **Return** to change the entry.

Another menu window opens:

```

X8500 Setup Tool                               BinTec Communications AG
[WAN][ADD][WAN NUMBERS][ADD]:Add or Change WAN Numb.(BigBoss) MyX8500

Number                0911987654321
Direction             outgoing

Advanced settings >

ISDN Ports to use:
  System <X> BRI[4]
  Slot 3 <X> PRI[0] <X> PRI[1] <X> PRI[2] <X> PRI[3]
  Slot 6 <X> BRI[2] <X> BRI[3]

                SAVE                Cancel

Enter string, max length = 40 chars

```

The menu contains the following fields:

Field	Meaning
Number	Extension of WAN partner.

Field	Meaning
Direction	Defines whether Number should be used for incoming or outgoing calls or for both.
ISDN Ports to use	Defines the ISDN ports to use.

Table 4-20: **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** ➤ **ADD**

The **Direction** field contains the following selection options:

Possible Values	Meaning
<i>outgoing</i>	For outgoing calls, where you dial your WAN partner.
<i>both (CLID)</i>	For incoming and outgoing calls.
<i>incoming (CLID)</i>	For incoming calls, where your WAN partner dials in to your X8500 .

Table 4-21: **Direction**

When **X8500** is connected to a PABX system for which a "0" prefix is necessary for external line access, this "0" must be considered when entering the access number.

Wildcards When entering the **Number**, you can either enter the extension digit for digit or you can replace single numbers or groups of numbers with wildcards. **Number** can therefore equal various extensions.

You can use the following wildcards, which have different effects for incoming and outgoing calls:

Wildcard	Meaning		Example		
	Incoming calls	Outgoing calls	Number	X8500 accepts incoming calls, e.g. with:	Outgoing calls, i.e. X8500 sets up a connection to the WAN partner with:
*	Matches a group of none or more digits.	Is ignored.	123*	123, 1234, 123789	123
?	Matches exactly one digit.	Is replaced by 0.	123?	1234, 1238, 1231	1230
[a-b]	Defines a range of matching digits.	The first digit of the specified range is used.	123[5-9]	1235, 1237, 1239	1235
[^a-b]	Defines a range of excluded digits.	The first digit after the specified range is used.	123[^0-5]	1236, 1238, 1239	1236
{ab}	Optional sequence to match.	Sequence is used.	{00}1234	001234 and 1234	001234

Table 4-22: Wildcards for incoming and outgoing calls



If the calling party number of an incoming call matches both a WAN partner's **Number** with wildcards and a WAN partner's **Number** without wildcards, the entry without wildcards is always used.

To do Make the following entries:

- Enter the **Number**, e.g. **0911987654321**.
- Select the **Direction**, e.g. **outgoing**.

- Confirm with **SAVE**.
The entries are saved and listed.
- Leave **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** with **EXIT**.

Defining PPP Settings for Authentication

Now enter the ➤➤ **PPP** settings of your WAN partner. These are used to authenticate your connection partner.

When a call is received, the Calling Party Number is always sent over the ISDN ➤➤ **D-channel**. This number enables **X8500** to identify the caller (➤➤ **CLID**), provided the caller is entered as a WAN partner. After identification with CLID, the router can additionally carry out ➤➤ **PPP authentication** with the WAN partner before it accepts the call. The router needs the necessary data for this, which you should enter here. First establish the type of authentication process that should be performed, then enter a mutual password and two user names. You receive this information, for example, from your Internet Service Provider (ISP) or the system administrator at your head office. The call is only accepted if the data entered in **X8500** matches the caller's data.

If you authenticate WAN partners over a RADIUS server, please see the relevant instructions in the **Software Reference**.

Configure PPP authentication for your WAN partner

To set the PPP authentication for the WAN partner, proceed as follows:

- Go to **WAN PARTNER** ➤ **ADD** ➤ **PPP**.

The following menu opens:

X8500 Setup Tool	BinTec Communications AG
[WAN][ADD][PPP]: PPP Settings (BigBoss)	MyX8500
Authentication	CHAP + PAP
Partner PPP ID	BigBoss
Local PPP ID	LittleIndian
PPP Password	Secret
Keepalives	off
Link Quality Monitoring	off
OK	CANCEL
Use <Space> to select	

The menu contains the following fields:

Field	Meaning
Authentication	Authentication protocol
Partner PPP ID	ID of WAN partner.
Local PPP ID	X8500's ID.
PPP Password	Password.
Keepalives	Activates Keepalive packets for checking if the distant PPP terminal is reachable. Possible values: <input type="checkbox"/> <i>off</i> <input type="checkbox"/> <i>on</i>
Link Quality Monitoring	Activates PPP Link Quality Monitoring as per RFC 1989. Possible values: <input type="checkbox"/> <i>off</i> <input type="checkbox"/> <i>on</i> Only necessary in exceptional cases, e.g. with Nokia Communicator.

Table 4-23: **WAN PARTNER** ➤ **ADD** ➤ **PPP**

The **Authentication** field contains the following selection options:

Possible Values	Meaning
<i>PAP</i>	Only run ►► PAP (PPP Password Authentication Protocol); the password is transferred uncoded.
<i>CHAP</i>	Only run ►► CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); the password is transferred coded.
<i>none</i>	Run no PPP authentication protocol.
<i>MS-CHAP</i>	Only run MS-CHAP (MS Challenge Handshake Authentication Protocol).
<i>CHAP + PAP + MS-CHAP</i>	Primarily run CHAP, on denial, the authentication protocol required by the WAN partner.
<i>MS-CHAP V2</i>	Run MS-CHAP version 2 only.
<i>CHAP + PAP</i>	Run primarily CHAP, otherwise PAP.

Table 4-24: **Authentication**

To do Make the following entries:

- Select **Authentication**, e.g. **CHAP**.
- Enter **Partner PPP ID**, e.g. **BigBoss**.
- Enter **Local PPP ID**, e.g. **LittleIndian**.



How to enter the passwords is described in [chapter 3.4.5, page 38](#).

- Enter **PPP Password**, e.g. **Secret**.
- Select **Keepalives**, e.g. **off**.
- Select **Link Quality Monitoring**, e.g. **off**.

➤ Confirm with **OK**.

You have returned to **WAN PARTNER** ➤ **ADD**.



In some cases, the caller cannot be identified with ➤➤ **CLID**, although entered as a WAN partner. In this case, your **X8500** does not know which authentication protocol was set for this WAN partner. To enable the call to still be accepted, **X8500** falls back on general settings in the PPP, which you can change as necessary ([chapter 5.1.3, page 142](#)).

Defining Short Hold

Now set short hold so that **X8500** terminates the ISDN connection when there is no further data exchange. The short hold setting can be either static or dynamic and tells **X8500** the duration of the idle time, after which it is to clear the ISDN connection.

Static The static ➤➤ **short hold** setting determines how much time should pass between sending the last ➤➤ **data packet** and clearing the ISDN connection. Enter a fixed period of time in seconds.

Dynamic With the dynamic short hold setting, no fixed period of time is specified and the length of an ISDN charging unit is considered instead. Dynamic short hold is based on AOCD (advice of charge during the call).

When setting dynamic short hold, you specify how much time should pass after the last exchange of data before the connection is cleared. You enter a percentage based on the last charging unit. The value of **Idle Timer for Dynamic Short Hold** can therefore change, just as the length of the charging unit changes (according to the time of day, weekend, weekday, etc.). If you enter 50%, for example, **Idle Timer for Dynamic Short Hold** is 60 seconds if the preceding charging unit was 120 seconds, and 300 seconds if the preceding charging unit was 600 seconds. The connection is cleared on expiry of the **Idle Timer for Dynamic Short Hold** and shortly before the next charging unit starts.

Diagram of short hold:

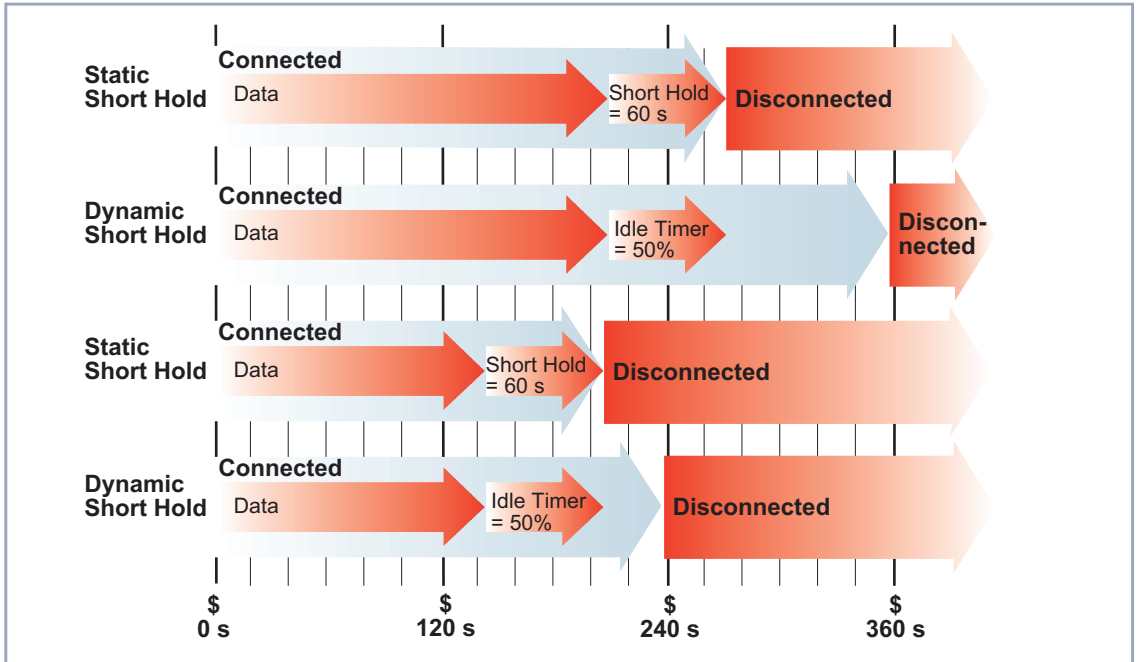


Figure 4-6: Dynamic and static short hold



Please note: You can only use dynamic short hold if you receive charging information during the connection (AOCD). Ask your telephone company.



If you use dynamic short hold, you must also set static short hold so that you do not get a permanent ►► **dialup connection** if AOCD (advice of charge during the call) fails.

You should make sure static short hold comes into operation later than dynamic short hold. If not, **X8500** always clears the connection based on static short hold and never gives dynamic short hold a chance to disconnect. In this case, enter a value for **Static Short Hold (sec)** that is a little more than the expected maximum dynamic idle time.

In Germany, only Deutsche Telekom currently supports call charging information.

Proceed as follows:

► Go to **WAN PARTNER** ► **ADD** ► **ADVANCED SETTINGS**.

The following menu window opens:

X8500 Setup Tool		BinTec Communications AG
[WAN][ADD][ADVANCED]: Advanced Settings (BigBoss)		MyX8500
Callback	no	
Static Short Hold (sec)	20	
Idle for Dynamic Short Hold (%)	0	
Delay after Connection Failure (sec)	300	
Layer 1 Protocol	ISDN 64 kbps	
Channel Bundling	no	
Extended Interface Settings (optional) >		
Special Interface Types	none	
OK		CANCEL
Use <Space> to select		

The following parts of the menu are relevant for this configuration step:

Field	Meaning
Static Short Hold (sec)	Idle time in seconds for static short hold. Example values for trunk connections: <i>60</i> , only effective if charging pulses are transmitted during the connection (AOCD), <i>20</i> otherwise.
Idle for Dynamic Short Hold (%)	Idle time in percent for dynamic short hold. Only effective if charging pulses are transmitted during the connection (AOCD).

Table 4-25: **WAN PARTNER** ► **ADD** ► **ADVANCED SETTINGS**

To do Make the following entries:

- Enter **Static Short Hold (sec)**, e.g. **20**.
- Enter **Idle for Dynamic Short Hold (%)**, e.g. **0**.
- Confirm with **OK**.

You have returned to **WAN PARTNER** ► **ADD**.



Tips on entering **Idle for Dynamic Short Hold %**:

- For interactive connections (e.g. ►► **telnet**), specify a high value (e.g. **80...90**) to avoid clearing connections during short phases without data exchange.
- For Internet connections (e.g. WWW, http, etc.), specify a medium to high value (e.g. **50...80**) to avoid clearing connections while waiting.
- For data connections (e.g. ►► **ftp**), specify a low value (e.g. **10...40**) to avoid the unnecessary continuation of a connection after data has been transferred.

You will find a more detailed explanation about static and dynamic short hold in the **Software Reference**.

Carrying out IP Configuration

The IP configuration of your WAN partner consists in entering the **IP address** and **netmask** of your partner.

Proceed as follows:

➤ Go to **WAN PARTNER** ➤ **ADD** ➤ **IP**.

The following menu opens:

X8500 Setup Tool	BinTec Communications AG
[WAN][ADD][IP]: IP Configuration (BigBoss)	MyX8500
IP Transit Network	no
local IP Address	
Partner's LAN IP Address	10.1.1.0
Partner's LAN Netmask	255.255.255.0
Advanced settings >	
SAVE	CANCEL
Use <Space> to select	

The menu contains the following fields:

Field	Meaning
IP Transit Network	<p>Defines whether X8500 sets up a transit network to the WAN partner. Possible values:</p> <ul style="list-style-type: none"> ■ <i>yes</i>: Transit network is used. ■ <i>dynamic client</i>: X8500 receives the IP address dynamically. ■ <i>dynamic server</i>: X8500 allocates IP addresses to dial-in clients. ■ <i>no</i>: No transit network is used.

Field	Meaning
local IP Address	Only for the value <i>no</i> for IP Transit Network . IP address of X8500 . You do not normally need to make an entry here, unless you wish to configure a transit network for one of your WAN partners (see chapter 5.2.7, page 173).
local WAN IP Address	Only for the value <i>yes</i> for IP Transit Network . WAN IP address of X8500 in the transit network.
Partner's WAN IP Address	Only for the value <i>yes</i> for IP Transit Network . WAN IP address of WAN partner in the transit network.
Partner's LAN IP Address	Only for the value <i>yes</i> or <i>no</i> for IP Transit Network . WAN partner's LAN IP address.
Partner's LAN Netmask	Only for the value <i>yes</i> or <i>no</i> for IP Transit Network . Your WAN partner's LAN netmask. If you make no entry, X8500 enters a default netmask for the net class used under Partner's LAN IP Address .
Default Route	Only for the value <i>dynamic client</i> for IP Transit Network . Possible values: ■ <i>yes</i> : Route to this WAN partner is defined as default route. ■ <i>no</i> : Route to this WAN partner is not defined as default route.

Field	Meaning
Enable NAT	<p>Only for the value <i>dynamic client</i> for IP Transit Network.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>yes</i>: NAT is activated for this WAN partner. <input type="checkbox"/> <i>no</i>: NAT is deactivated for this WAN partner. <p>This setting is equivalent to activating NAT in the menu IP ➤ NETWORK ADDRESS TRANSLATION ➤ EDIT.</p>

Table 4-26: **WAN PARTNER** ➤ **ADD** ➤ **IP**

The submenu **WAN PARTNER** ➤ **ADD** ➤ **IP** ➤ **ADVANCED SETTINGS** contains the following fields:

Field	Meaning
RIP Send	Enables RIP packets to be sent via the interface to the WAN partner and LAN interface. For possible values, see table 5-28, page 182 .
RIP Receive	Enables RIP packets to be received via the interface to the WAN partner and LAN interface. For possible values, see table 5-28, page 182 .
Van Jacobson Header Compression	<p>Reduces the size of TCP/IP packets.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>on</i>: VJHC enabled. <input type="checkbox"/> <i>off</i>: VJHC disabled.

Field	Meaning
Dynamic Name Server Negotiation	In the event of dynamic name server negotiation, defines whether X8500 receives IP addresses for Primary Domain Name Server , Secondary Domain Name Server , Primary WINS and Secondary WINS from the WAN partner or sends them to the WAN partner. For possible values, see table 5-47, page 211 .
IP Accounting	For saving accounting messages for TCP, UDP and ICMP sessions. Possible values: <ul style="list-style-type: none"> ■ <i>on</i>: IP accounting activated. ■ <i>off</i>: IP accounting deactivated. For further information, see also chapter 7.1.1, page 284 .
Back Route Verify	If Back Route Verification is activated at a WAN partner, only those data packets are transported via the interface to the WAN partner that would be routed over the same interface on the back route. Possible values: <ul style="list-style-type: none"> ■ <i>on</i>: Back Route Verification activated for this WAN partner. ■ <i>off</i>: Back Route Verification is not activated for this WAN partner. For further information, see chapter 7.2.10, page 331 .

Field	Meaning
Route Announce	Possible values: <ul style="list-style-type: none"> ■ <i>up or dormant</i>: Routes are propagated if the status is up or dormant. ■ <i>always</i>: Routes are propagated independent of the operational status. ■ <i>up only</i>: Routes are only propagated if the operational status of the interface is up.
Proxy ARP	Enables X8500 to answer ARP requests from its own LAN and from hosts of defined WAN partners (see chapter 5.2.11, page 185). For possible values, see table 5-33, page 186 .

Table 4-27: **WAN PARTNER** ➤ **ADD** ➤ **IP** ➤ **ADVANCED SETTINGS**

To do Make the following entries (normally sufficient for a corporate network connection):

- Select **IP Transit Network**, e.g. *no*.
- Enter **Partner's LAN IP Address**, e.g. *10.1.1.0*.
- Enter **Partner's LAN Netmask**, e.g. *255.255.255.0*.
- Confirm with **SAVE**.
- Confirm with **SAVE** again.

You have returned to **WAN PARTNER** and your entries are temporarily saved and activated.

See chapter [chapter 4.3.4, page 122](#) for example settings in the submenu **WAN PARTNER** ➤ **ADD** ➤ **IP** ➤ **ADVANCED SETTINGS**.



If you are setting up access to the Internet, you do not normally know the IP address of your Internet Service Provider (ISP). Either your **X8500** is assigned its **Local ISDN IP Address** dynamically (for the duration of the connection) or statically by the ISP. In such a case, make the following settings in **WAN PARTNER ► ADD ► IP**:

IP address is assigned dynamically:

- Select **IP Transit Network**: *dynamic client*.

IP address is assigned statically:

- Select **IP Transit Network**: yes.
Local ISDN IP Address: **X8500**'s static IP address you get from your ISP (often termed your gateway or router address).
Partner's ISDN IP Address: Partner's IP address (if known) or else **X8500**'s static IP address you get from your ISP.
No entries for **Partner's LAN IP Address** and **Partner's LAN Netmask**.

You will find information about the transit network in [chapter 5.2.7, page 173](#).



To be able to use the Domain Name Server of the ISP while connected, make the following settings in **WAN PARTNER ► ADD ► IP ► ADVANCED SETTINGS**:

- Select **Dynamic Name Server Negotiation**: *client (receive)*.

This setting is only necessary if you have not entered fixed IP addresses for DNS on the PCs of your network.

4.3.2 Creating a Routing Entry

A routing entry is created automatically in the routing table of your **X8500** for every WAN partner. You can edit existing routing entries and add new ones. For the connection to your Internet Service Provider, you should always configure a default route.

All IP routes entered are listed in the menu **IP ► ROUTING**:

X8500 Setup Tool		BinTec Communications AG					
[IP][ROUTING]: IP Routing		MyX8500					
The flags are: U (Up), D (Dormant), B (Blocked),							
G (Gateway Route), I (Interface Route)							
S (Subnet Route), H (Host Route), E (Extended Route)							
Destination	Gateway	Mask	Flags	Met	Interface	Pro	
192.168.1.1	192.168.1.254	255.255.255.0	US	0	en0-1	loc	
10.1.1.0		255.255.255.0	DI	0	BigBoss	mgmt	
default		0.0.0.0	DI	0	GoInternet	mgmt	
ADD		ADDEXT		DELETE		EXIT	
Press<Ctrl-n>,<Ctrl-p>to scroll,<Space>tag/untagDELETE,<Return>to edit							

Flags shows the current status (Up, Dormant, Blocked) and the type of route (Gateway Route, Interface Route, Subnet Route, Host Route, Extended Route). The protocol with which **X8500** has "learned" the routing entry is displayed under **Pro**.

Creating routing entry To define a route, proceed as follows:

- Go to **IP ► ROUTING**.
- Use **ADD** to add a new entry or select an existing entry. Confirm with **Return** to change the entry.



To create extended IP routing entries, confirm with the **ADDEXT** button to open the relevant menu. In this case, see [chapter 7.2.12, page 332](#).

The following menu window opens:

X8500 Setup Tool		BinTec Communications AG
[IP][ROUTING][ADD]: IP Routing		MyX8500
Route Type	Network route	
Network	WAN without transit network	
Destination IP Address	10.1.1.0	
Netmask	255.255.255.0	
Partner / Interface	BigBoss	
Metric	1	
SAVE		CANCEL
Use <Space> to select		

The menu contains the following fields:

Field	Meaning
Route Type	Type of route. Possible values: <ul style="list-style-type: none"> ■ <i>Host route</i>: Route to a single host ■ <i>Network route</i>: Route to a network ■ <i>Default route</i>: Is only used if no other suitable route is available.
Network	Defines the type of connection (LAN, WAN), see table 4-29, page 118 .
Destination IP Address	Only for Route Type <i>Host route</i> or <i>Network route</i> . IP address of the destination host or LAN.
Netmask	Netmask of the partner LAN (Only possible for Route Type = <i>Network route</i> . If no entry is made, the router uses a default netmask).
Partner / Interface	WAN partner (only possible for Network = <i>WAN without transit network</i>).

Field	Meaning
Gateway IP Address	Only for Network LAN or <i>WAN with transit network</i> . IP address of the host to which X8500 should forward the IP packets.
Metric	The lower the value, the higher the priority of the route (possible values 0...15).

Table 4-28: **IP** ➤ **ROUTING** ➤ **ADD**

The **Network** field contains the following selection options:

Possible Values	Meaning
<i>LAN</i>	Route to a destination host or LAN that can be reached via X8500 's LAN interface.
<i>WAN without transit network</i>	Route to a destination host or destination LAN that can be reached via a WAN partner without considering a transit network.
<i>WAN with transit network</i>	Route to a destination host or destination LAN that can be reached via a WAN partner only with transit network.
<i>Refuse</i>	X8500 discards data packets using this route and sends the sender a message saying the destination of the packet is unreachable.
<i>Ignore</i>	X8500 discards data packets using this route without sending a status message.

Table 4-29: **Network**



You can only configure one default route on your **X8500**. If you set up access to the Internet, you must therefore configure the route to your Internet Service Provider (ISP) as a default route.

If you configure a corporate network connection, only enter the route to the head office as a default route if you do not configure Internet access over **X8500**.

If you configure both Internet access and a corporate network connection, enter a default route to the ISP and a network route to the head office.

Default route To define a default route, proceed as follows:

- Select **Route Type**: *Default route*.
- Select **Network**: *WAN without transit network*.
- Select **Partner / Interface**: e.g. *GoInternet*.
- Enter **Metric**, e.g. *1*.
- Confirm with **SAVE**.

You have returned to **IP** ➤ **ROUTING**. The entries are temporarily saved and activated. The newly entered or modified route is listed.



The corporate network can consist of several LANs with different network IP addresses and netmasks (➤➤ **subnets**). That is, if you do not enter your head office access as a default route (e.g. because you have already set up your Internet access as a default route), then you must make a separate routing entry for each network you want to reach at the head office.

Diagram of corporate network with several LANs:

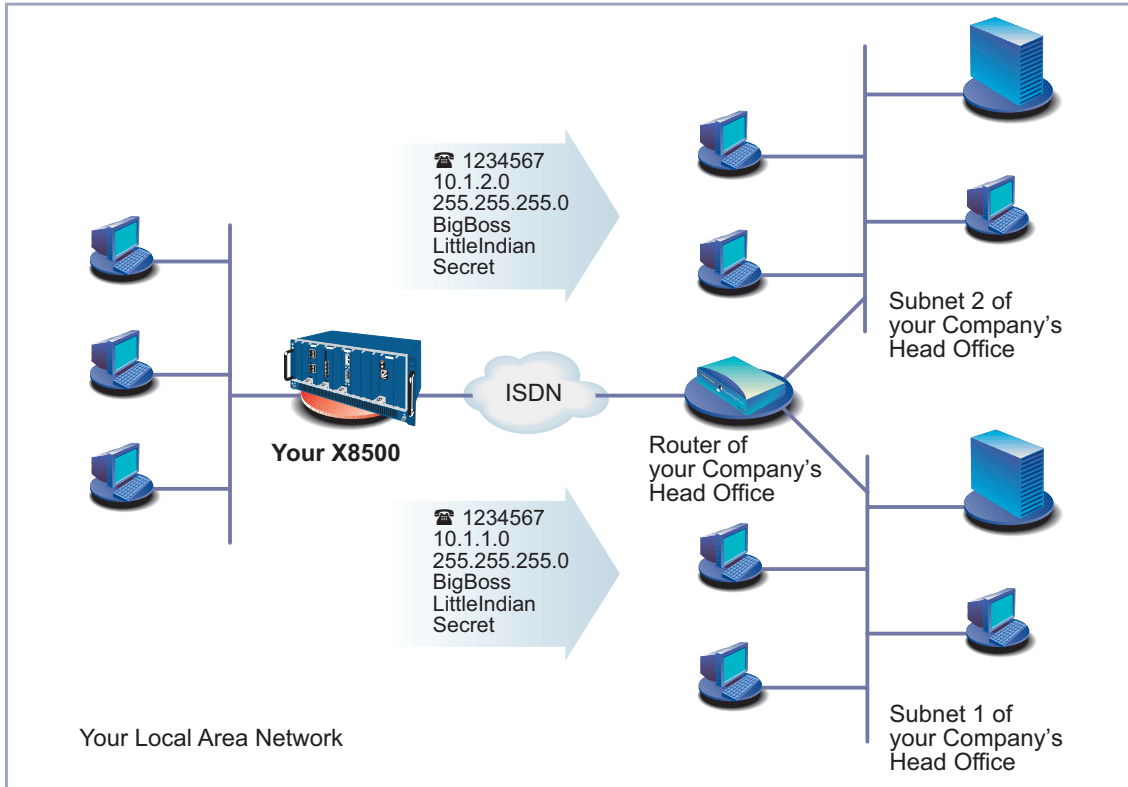


Figure 4-7: Corporate network with several connected LANs

Network route Proceed as follows to establish a network route, e.g. for a corporate network connection (without a default route):

- Select **Route Type**: *Network route*.
- Select **Network**: *WAN without transit network*.
- Enter **Destination IP Address**, e.g. **10.1.2.0**.
- Enter **Netmask**, e.g. **255.255.255.0**.
- Enter **Partner / Interface**, e.g. **BigBoss**.
- Enter **Metric**, e.g. **1**.

- Confirm with **SAVE**.
You have returned to **IP** ➤ **ROUTING**. The entries have temporarily been saved and activated. The newly entered or modified route is listed.
- Repeat these steps if you have to enter several routes.

4.3.3 Activating Network Address Translation (NAT)

Here you can activate Network Address Translation (➤➤ **NAT**) for your WAN partner. This conceals your whole network from the outside world with just one IP address. You should certainly do this for your connection to the Internet Service Provider (ISP).

More information about Network Address Translation (NAT) can be found in [chapter 7.2.7, page 304](#).

Activating NAT Proceed as follows to activate NAT:

- Go to **IP** ➤ **NETWORK ADDRESS TRANSLATION**.

The following menu opens:

```

X8500 Setup Tool                               BinTec Communications AG
[IP][NAT]: NAT Configuration                    MyX8500

Select IP Interface to be configured for NAT

Name           Nat      Static mappings      Static mappings
                off      from OUTSIDE        from INSIDE
GoInternet     off      0                    0
BigBoss        off      0                    0
en0-1          off      0                    0
en0-1-snap     off      0                    0
en0-2          off      0                    0
en0-2-snap     off      0                    0

EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select

```

- Mark the interface or the WAN partner for which you want to activate NAT (e.g. **GoInternet**) and confirm with **Return**.

Another menu window opens:

X8500 Setup Tool		BinTec Communications AG	
[IP][NAT][CONFIG]: NAT Configuration (GoInternet)		MyX8500	
Network Address Translation	on		
Silent Deny	no		
Enter configuration for sessions:	requested from OUTSIDE		
	requested from INSIDE		
SAVE		CANCEL	
Use <Space> to select			

To do Make the following entries:

- Select **Network Address Translation**: *on*.
- Leave **Silent Deny** *no*.
- Confirm with **SAVE**.

Network Address Translation is activated for the selected interface or WAN partner.

- Leave **IP** ➤ **NETWORK ADDRESS TRANSLATION** with **EXIT**.
- Leave **IP** with **EXIT**.

You have returned to the main menu.

Only outgoing sessions are allowed initially if NAT is activated. To allow certain connections from outside to hosts within the LAN, these must be explicitly defined and admitted. How to do this is described in [chapter 7.2.7, page 304](#).

4.3.4 Examples

The WAN partner settings for some example configurations are shown below:

- ["Internet Access Over T-Online", page 123](#)
- ["Internet Access Over Compuserve", page 124](#)



How to enter the passwords is described in [chapter 3.4.5, page 38](#).

Internet Access Over T-Online

T-Online The following settings are necessary:

- In **WAN PARTNER** ► **ADD**:
Partner Name: *T_ONLINE*
Encapsulation: *PPP*
Compression: *none*
Encryption: *none*
- In **WAN PARTNER** ► **ADD** ► **WAN NUMBERS** ► **ADD**:
Number (= dial-in number): e.g. *0191011*
Direction: *outgoing*
- In **WAN PARTNER** ► **ADD** ► **PPP**:
Authentication: *CHAP + PAP*
Local PPP ID (= user account + T-Online number + joint user account): e.g.
123456789012081512345678#0001
PPP Password: e.g. *mycat*
Keepalives: *off*
Link Quality Monitoring: *off*
- In **WAN PARTNER** ► **ADD** ► **ADVANCED SETTINGS**:
Callback: *no*
Static Short Hold (sec): e.g. *60*
Idle for Dynamic Short Hold (%): e.g. *0*
Delay after Connection Failure (sec): e.g. *300*
Channel Bundling: *no*
Layer 1 Protocol: *ISDN 64 kbps*
Special Interface Types: *none*
- In **WAN PARTNER** ► **ADD** ► **IP**:
IP Transit Network: *dynamic client*

- In **WAN PARTNER** ➤ **ADD** ➤ **IP** ➤ **ADVANCED SETTINGS**:
 - RIP Send:** *none*
 - RIP Receive:** *none*
 - Van Jacobson Header Compression:** *off*
 - Dynamic Name Server Negotiation:** *client (receive)*
 - IP Accounting:** *off*
 - Back Route Verify:** *off*
 - Route Announce:** *up or dormant*
 - Proxy Arp:** *off*
- In **IP** ➤ **ROUTING** ➤ **ADD**:
 - Route Type:** *Default route*
 - Network:** *WAN without transit network*
 - Partner / Interface:** *T-Online*
 - Metric:** e.g. *1*.
- In **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **T_Online** ➤ **Return**:
 - Network Address Translation:** *on*
 - Silent Deny:** *no*

Internet Access Over Compuserve

Compuserve The following settings are necessary:

- In **WAN PARTNER** ➤ **ADD**:
 - Partner Name:** *COMPUSERVE*
 - Encapsulation:** *Async PPP over X.75*
 - Compression:** *none*
 - Encryption:** *none*
- In **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** ➤ **ADD**:
 - Number** (= dial-in number): e.g. *010880191919*
 - Direction:** *outgoing*
- In **WAN PARTNER** ➤ **ADD** ➤ **PPP**:
 - Authentication:** *none*
 - Keepalives:** *off*
 - Link Quality Monitoring:** *off*

- In **WAN PARTNER** ► **ADD** ► **ADVANCED SETTINGS**:
 - Callback**: *no*
 - Static Short Hold (sec)**: e.g. **120**
 - Idle for Dynamic Short Hold (%)**: e.g. **0**
 - Delay after Connection Failure (sec)**: e.g. **300**
 - Channel Bundling**: *no*
 - Layer 1 Protocol**: *ISDN 64 kbps*
 - Special Interface Types**: *none*

- In **WAN PARTNER** ► **ADD** ► **ADVANCED SETTINGS** ► **COMPUSERVE LOGIN**:
 - Provider**: Compuserve Network
 - Host**: CIS
 - User ID** (= your user name)
 - Password** (= your password)

- In **WAN PARTNER** ► **ADD** ► **IP**:
 - IP Transit Network**: *dynamic client*

- In **WAN PARTNER** ► **ADD** ► **IP** ► **ADVANCED SETTINGS**:
 - RIP Send**: *none*
 - RIP Receive**: *none*
 - Van Jacobson Header Compression**: *off*
 - Dynamic Name Server Negotiation**: *client (receive)*
 - IP Accounting**: *off*
 - Back Route Verify**: *off*
 - Route Announce**: *up or dormant*
 - Proxy Arp**: *off*

- In **IP** ► **ROUTING** ► **ADD**:
 - Route Type**: *Default route*
 - Network**: *WAN without transit network*
 - Partner / Interface**: *COMPUSERVE*
 - Metric**: e.g. **1**

- In **IP** ► **NETWORK ADDRESS TRANSLATION** ► **COMPUSERVE** ► **Return**:
 - Network Address Translation**: *on*
 - Silent Deny**: *no*

4.4 Saving the Configuration File

After creating a working configuration on your **X8500**, make sure you save it:

- From the Setup Tool main menu, select **Exit** and confirm with **Return**.

Another menu window opens:

X8500 Setup Tool	BinTec Communications AG
[EXIT]: Exit Setup	MyX8500
Back to Main Menu	
Save as boot configuration and exit	
Exit without saving	

You have three alternatives:

- Select **Back to Main Menu** to return to the Setup Tool main menu.
- Select **Save as boot configuration and exit** to save the configuration data as "boot" file in the flash memory.

The SNMP shell of **X8500** opens with the command prompt. All the changes you have just made with the Setup Tool are saved in the flash. The configuration file you have just saved will be loaded the next time you start your **X8500**.

- Select **Exit without saving** to quit the Setup Tool without saving your changes in the flash.

The SNMP shell of **X8500** opens with the command prompt. All settings or changes you have made with the Setup Tool will be lost when you turn off your **X8500**.

4.5 Configuring PCs in Your LAN

Additional configuration is necessary on the individual PCs in your LAN to connect them to **X8500**.

- Remote CAPI configuration
Configuration of the CAPI interface on the PCs enables you to use communication applications such as FAX software.
- Settings for data connections
You may have to make various settings on your PCs in the LAN to permit data transmission over **X8500**.

4.5.1 Configuring a PC

To ensure that your network and its external data connection work properly, you may have to make additional settings on your PCs:

- If you have not configured **X8500** as a DHCP server and the PCs do not yet have any IP addresses, you will have to define (as per the next chapter) the IP addresses now and show the PCs "the way out" (gateway, DNS).
- If you have configured a connection to a corporate network, you will certainly want to reach PCs from the partner LAN (e.g. head office) via Windows. To do this, you must proceed as described in ["Finding PCs on Your Partner's Network"](#), page 131.

Telling the PC the IP Address, Gateway and DNS

If you have not configured **X8500** as a DHCP server and your PCs do not yet have any IP addresses, you must now tell the PCs at which IP address they can be reached. You must also tell the PCs the way out, e.g. how to get to the Internet.

A TCP/IP protocol must be installed before the following configuration work can be carried out (see [chapter 3.5.2, page 46](#)).

Proceed as follows:

- Click the Windows Start button and then **Settings** ➤ **Control Panel**.
 - Double click **Network**.
- Windows 95/98**
- Click **TCP/IP** ➤ **Properties**.
 - Enter a unique IP address for your PC and the netmask in the **IP Address** tab, e.g. **192.168.1.1** and **255.255.255.0**.
 - Enter **X8500**'s IP address, e.g. **192.168.1.254**, in the **Gateway** tab. Click **Add**.
 - If you do not have your own DNS server, enter **X8500**'s IP address in the **DNS Configuration** tab under **DNS Server Search Order**, e.g. **192.168.1.254**.
- Windows NT**
- Select the **Protocols** tab. Click **TCP/IP Protocol** ➤ **Properties**.
 - Click **Specify IP Address** in the **IP Address** tab and set the IP address, netmask and default gateway, e.g. **192.168.1.254**, **255.255.255.0** and **192.168.1.1**. Enter the IP address of **X8500** as default gateway.
 - Click **Add** in the **DNS** tab under **DNS Server Search Order** and enter **X8500**'s IP address, e.g. **192.168.1.254**.
- Windows 2000**
- Click the Windows Start button and then **Settings** ➤ **Network and DCN Connections**.
 - Double click **LAN Connection**.
 - Click the **General** tab and then **Properties**.
 - Select the **Internet Protocol (TCP/IP)** in the **General** tab. Click **Properties**.
 - Activate the **Use next IP address** option in the **General** tab. Specify the IP address, netmask and standard gateway, e.g. **192.168.1.254**, **255.255.255.0** and **192.168.1.1**. Enter the IP address of **X8500** as default gateway.
 - If you do not have your own DNS, enter the IP address of **X8500** as DNS address. Activate the **Use next DNS server addresses** option.
 - Enter the address, e.g. **192.168.1.254** and click **OK**.
 - Close the open windows with **OK** and **Close**.

- Windows ME**
- Click the Windows Start button and then **Settings** ➤ **Control Panel**. View all the control panel options.
 - Double click **Network**.
The **Network** window opens.
 - Tag the **TCP/IP** entry for your Ethernet card in the **Configuration** tab and click **Properties**.
 - Click the option button **Specify IP Address** in the **IP Address** tab of the **TCP/IP Properties** window.
 - Enter the IP address and netmask, e.g. **192.168.1.1** and **255.255.255.0**.
 - Enter the IP address of your router in the **Gateway** tab under **New Gateway**, e.g. **192.168.1.254**. Click **Add**.
 - If you do not have your own DNS, enter your router's IP address in the **DNS Configuration** tab under **DNS Server Search Order**. Click **Add**.
 - Click **OK**.
 - Click **OK** in the **Network** window.
- Windows XP Professional**
("Traditional Start menu")
- Click the Windows Start button and then **Settings** ➤ **Control Panel** ➤ **Network Connections** ➤ **LAN Connections**.
 - In the **LAN Connection Status** window in the **General** tab, click **Properties**.
 - In the **LAN Connection Properties** window in the **General** tab, tag the **Internet Protocol (TCP/IP)** entry and click **Properties**.
 - Click the option button for **Use Next IP Address**.
 - Enter the IP address, netmask and default gateway, e.g. **192.168.1.1**, **255.255.255.0** and **192.168.1.254**. Enter the IP address of your router as default gateway.
 - If you do not have your own DNS server, enter the IP address of your router as DNS server address under **Preferred DNS Server**.
- Finally**
- Confirm all entries and restart your PC (not necessary for Windows 2000 and Windows XP).
 - Repeat the installation for all the PCs in your network.

4.5.2 Remote CAPI Interface Configuration

Enter **X8500** as CAPI server in the Remote CAPI configuration program.

The **X8500** CAPI server provides the following facilities:

- Operating communications applications on every PC in the network
- Simultaneous ISDN access over communications applications from several PCs

To enable CAPI applications on all PCs in the network, you must configure the Remote CAPI interface on all PCs.

Installing the CAPI Configuration Program

- To do**
- Insert the BinTec ISDN Companion CD in the CD-ROM drive and wait for setup to start. If the Start window does not open automatically, click your CD-ROM drive in Windows Explorer and double-click **setup.exe**.
 - Select **BRICKware** in the window and continue with the setup until you reach router selection.
 - Select **X8500** and click **Next**.
 - Select **Remote CAPI Client** in the component selection window.
 - Follow the instructions on the screen.
 - Click **OK**.

The installation is completed and the Remote CAPI configuration window appears automatically at the end of the installation.

Configuring the Remote CAPI

Proceed as follows:

- Enter **X8500**'s IP address, e.g. **192.168.1.254** in the **Remote CAPI** tab.
- Enter the user name and password as configured on **X8500**. The rights for these users you set here must correspond with your settings on **X8500**.
- Click **Use these values**.

The "Remote CAPI is ready" message appears after a short time.



If an error message appears after clicking **Use these values**, make sure that:

- **X8500's** IP address is correct.
 - You have entered a valid user name.
 - The right port number is entered, 2662 for **Remote CAPI**. The port number must match the port number configured on **X8500**.
 - Your PC has been configured as a DHCP client and perhaps does not yet have an IP address.
- If no error message appears, click **OK**.
- Repeat the Remote CAPI installation on all PCs in the network on which you want to use communications applications.



You can find a more detailed description of the Remote CAPI configuration in **BRICKware for Windows**. A description of the Multibrick CAPI for Windows NT is also included there, which allows you to define several BRICKs as CAPI servers in the network.

4.5.3 Finding PCs on Your Partner's Network

You have now set everything on your **X8500** to connect to your partner's network. Let us suppose, for example, that you now want to establish contact between your PC and the Windows **BossPC** in your partner's network.



There are a few things you should know first. Every PC in your LAN or in your partner's network requires a unique address, the IP address. In addition to the use of IP addresses, an alternative means of addressing PCs that developed in the past was by computer or host names (e.g. **BossPC**). PCs, however, only understand IP addresses and not names. It is therefore necessary for the names to be translated (resolved) into their corresponding IP addresses. Typical examples of such name resolution are DNS or WINS servers. As you normally do not want to set up your own DNS server in a small network, there is an alternative way of resolving the name **BossPC** into an IP address: the LMHOSTS file. LMHOSTS files must, however, be maintained separately on each PC in your LAN.



We recommend using the DNS Proxy function of **X8500** for name resolution, which can replace the administration of HOSTS files. This is explained in [chapter 5.3.2, page 197](#).

In the LMHOSTS file, IP addresses are arranged with their computer names in tabular form. If, for example, you are looking for **BossPC**, a PC located in your partner's network (e.g. head office), your PC asks its LMHOSTS file for the corresponding IP address and in this way is able to find the PC.



Caution!

The following configuration can lead to increased connections and thus higher telephone bills. The conditions that cause connections to be established are largely dependent on the respective network configuration. In particular, you should note that if you connect a network drive, regular requests will increase the number of connections made.

➤ To avoid unintentional charges, it is essential that you monitor your **X8500**.



You can only use the following process if you have not configured extensive NetBIOS filtering. Otherwise certain Windows functions cannot be used, e.g. network drive connections.

If you require access to the partner network for several PCs in your network, you must save the assignment of IP address to name on each of these PCs.

You should also ensure that:

- you and your WAN partner are in the same domain or work group.
- you receive the necessary permission from the WAN partner to access PCs in your partner's network.

Tell your PC the IP address of **BossPC** as follows by editing the LMHOSTS text file:

- Click the Windows Start button and then **Find** ▶ **Files and Folders...**
- Type in `lmhosts.*`.
- Click **Find now**.
- Open the file found with a text editor.

- Type in the IP address of the PC in the partner network, followed by a tab or space, followed by the name of the PC, e.g. **10.1.1.1 BossPC**. Save and close the file under the name "lmhosts".
- Repeat the same procedure for each PC in the partner network that you want to reach over Windows.
- Click the Windows Start button and then **Find ▶ Computer....**
- Type in the name of the PC, e.g. **BossPC**, and click **Find now**. The name of the PC appears after a moment.

DNS configuration

- Register your router as DNS server ([chapter 4.5.1, page 127](#)) on each of your PCs.
- Set your router as DNS Proxy ([chapter 5.3.2, page 197](#)).

Creating a shortcut on the desktop

- To avoid having to look for the PC every time you restart, right-click the PC icon in the computer window and click **Create Shortcut**. You are then asked if you want the shortcut to be placed on the desktop.
- Click **Yes**.
Now you can connect to the **BossPC** on your partner's network at any time.

Network drive mapping

Alternatively, you could establish a network drive connection:

- Open Windows Explorer, click **Tools**, then **Map network drive**.
- Specify the drive and enter the path, e.g. **\\BossPC**.
- Click **Reconnect at logon**.
- Click **OK**.

4.6 Testing Your Configuration



Caution!

Incorrect configuration of the devices in your LAN may result in unintended connections and increased charges! Monitor your **X8500** and make sure that the system does not establish unwanted ISDN connections (and charges).

- To avoid unnecessary charges, check whether the filters you set are sufficient for your needs. If not, you can configure filters with the Setup Tool ([chapter 7.2.8, page 315](#)).
- Watch the LEDs on your **X8500**, use the monitor function of the Setup Tool (cf. [chapter 7.1, page 284](#)) or check your settings with an SNMP Management Tool.

Testing the LAN connection

Test the connection to your **X8500**:

- In the start menu of your PC, click **Run** and enter `ping`, followed by a space and the IP address of **X8500**, e.g. `ping 192.168.1.254`. If the configuration is correct, a window opens to indicate "Reply from 192.168.1.254...".

Testing Internet access

- Test the Internet access by entering www.bintec.net in the Internet browser.

If the configuration is correct, BinTec's start page opens. BinTec's Internet site offers you the latest news, updates and documentation.

5 Advanced Configuration with the Setup Tool

This chapter contains more **X8500** configuration options for the advanced user. The following configuration steps are described:

- General ►► **WAN** Settings ([chapter 5.1, page 136](#))
- Settings Specific to WAN Partners ([chapter 5.2, page 146](#))
- Basic ►► **IP** Settings ([chapter 5.3, page 193](#))
- Quality of Service ([chapter 5.4, page 218](#))
- Bridging ([chapter 5.5, page 239](#))
- Extra License Functions ([chapter 5.6, page 240](#))



Use the Credits Based Accounting System (see [chapter 7.1.3, page 293](#)). This enables you to set a limit for connections to **X8500** to prevent unnecessary charges accumulating as a result of mistakes made during configuration.

5.1 General WAN Settings

This chapter describes:

- **X8500** as dynamic IP Address >> **server** ([chapter 5.1.1, page 136](#))
- CAPI User Concept ([chapter 5.1.2, page 138](#))
- General >> **PPP** settings ([chapter 5.1.3, page 142](#))
- Setting of X.31 TEI value ([chapter 5.1.4, page 144](#))

These settings are not linked to certain WAN partners, but concern all WAN connections.

5.1.1 Dynamic IP Address Server

IP address pools **X8500** can operate as a dynamic IP address server for PPP connections. You can use this function by providing one or more pools of >> **IP addresses**. These IP addresses can be assigned to dial-in WAN partners for the duration of the connection.



Any host routes entered always have priority over IP addresses from the address pools. That is, when an incoming call has been authenticated, **X8500** first checks whether a host route is entered in the routing table for this caller. If not, **X8500** can assign an IP address from an address pool (if available).



If address pools have more than one IP address, you cannot specify which WAN partner receives which address. The addresses are initially assigned in order. If a new dial-in takes place within an interval of one hour, an attempt is made to assign the same IP address assigned to this partner the last time.

Configuration is made in:

- **IP** ▶ **IP ADDRESS POOL WAN (PPP)**
- **WAN PARTNER** ▶ **EDIT** ▶ **IP**
- **WAN PARTNER** ▶ **EDIT** ▶ **IP** ▶ **ADVANCED SETTINGS**

Fields of the menu **IP ► IP ADDRESS POOL WAN (PPP) ► ADD**:

Field	Meaning
Pool ID	Unique number for identifying the address pool. A pool may comprise a number of address ranges.
IP Address	First IP address in the address pool.
Number of Consecutive Addresses	Total number of IP addresses in the address pool, including the first IP address (IP Address).

Table 5-1: **IP ► IP ADDRESS POOL WAN (PPP) ► ADD**

Menu **WAN PARTNER ► EDIT ► IP**:

Field	Meaning
IP Transit Network	Defines whether a transit network is to be used between X8500 and the WAN partner. You must select <i>dynamic server</i> here if you assign an address pool.

Table 5-2: **WAN PARTNER ► EDIT ► IP**

Relevant field of the menu **WAN PARTNER ► EDIT ► IP ► ADVANCED SETTINGS**:

Field	Meaning
IP Address Pool	Pool ID of the address pool assigned to the WAN partner.

Table 5-3: **WAN PARTNER ► EDIT ► IP ► ADVANCED SETTINGS**

To do Proceed as follows:

- Go to **IP ► IP ADDRESS POOL WAN (PPP) ► ADD**.
- Enter **Pool ID**.
- Enter **IP Address**.

- Enter **Number of Consecutive Addresses**.
- Confirm with **SAVE**.
- Go to **WAN PARTNER** ➤ **EDIT** ➤ **IP** to assign an address pool to a WAN partner.
- Select **IP Transit Network**: *dynamic server*.
- Go to **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**.
- Enter **IP Address Pool**: *Pool ID*.
- Confirm with **OK**.
- Confirm with **SAVE** until you have returned to the main menu.

The settings are temporarily saved and activated. **X8500** is set up as dynamic IP address server.

5.1.2 CAPI User Concept

User name and password The CAPI user concept is used to check access to the ➤➤ **CAPI** service. This ensures that only users entered with a user name and password can use **X8500**'s CAPI services.

Example This means, for example, that an incoming fax for the user *Winnetou* is only passed to *Winnetou* and not to a user such as *Old Shatterhand*, who is located in the same LAN. If the CAPI user concept is not used (see "[Incoming Call Answering](#)", page 77), all incoming calls passed to the CAPI service are offered to all CAPI applications in the LAN. The first user to respond receives the call.

Configuration is made in:

- **CAPI** ➤ **USER**
- **PRI[x]** ➤ **INCOMING CALL ANSWERING** and **BRI[x]** ➤ **INCOMING CALL ANSWERING**

Following the fields of the menu **CAPI ► USER ► ADD**:

Field	Meaning
Name	User name for which access to the CAPI service is to be allowed or denied (maximum 16 characters).
Password	Password with which the user Name has to identify to gain access to the CAPI service.
CAPI	Determines whether access to the CAPI service is allowed or denied for the user Name . Possible values: <ul style="list-style-type: none"> ■ <i>enabled</i>: access to CAPI allowed ■ <i>disabled</i>: access to CAPI denied

Table 5-4: **CAPI ► USER ► ADD**

Following the fields of the menu **PRI[x] ► INCOMING CALL ANSWERING ► ADD** and **BRI[x] ► INCOMING CALL ANSWERING ► ADD**:

Field	Meaning
Item	Service which is to accept a call to the Number below.
Number	Phone number under which the service (Item) entered above can be reached.
Mode	Mode in which X8500 compares the digits of Number with the called party number of the incoming call: <ul style="list-style-type: none"> ■ <i>right to left</i>: default mode. ■ <i>left to right (DDI)</i>: always select this mode if X8500 is connected to a point-to-point ISDN access (system access).

Field	Meaning
CAPI Username	Corresponds to Name in CAPI ➤ USER . User to whom an incoming call to the CAPI service under Number is to be passed.
Bearer	Type of incoming call. Possible values: <ul style="list-style-type: none"> ■ <i>data</i>: data call ■ <i>voice</i>: voice call (modem, voice, analog fax) ■ <i>any</i>: both data and voice calls

Table 5-5: **BRI[x]** ➤ **INCOMING CALL ANSWERING** ➤ **ADD** or **PRI [x]** ➤ **INCOMING CALL ANSWERING** ➤ **ADD**



When on starting **X8500** in **CAPI** ➤ **USER** there is no entry, automatically a standard entry is created without password (with **Name** = *default* and **CAPI** = *enabled*).

To do Proceed as follows:

- Go to **CAPI** ➤ **USER**.
- Select an existing entry and confirm it with **Return** or add a new entry with **ADD**.
- Enter **Name**.
- Enter your **Password**.



How to enter the passwords in the Setup Tool is described in [chapter 3.4.5, page 38](#).

- Select **CAPI**.
- Confirm with **SAVE**.
- Repeat these steps for every user in the LAN.

- Go to **BRI[x]** ➤ **INCOMING CALL ANSWERING** resp. **PRI[x]** ➤ **INCOMING CALL ANSWERING**.

Make an entry here for every user in the LAN who has access to the CAPI service.

- Select an existing entry and confirm it with **Return** or add a new entry with **ADD**.
- Select **Item**, z. B. **CAPI 2.0**.



If you use a communication application on your PC that is based on Remote CAPI 1.1 (current version: Remote CAPI 2.0), **X8500** must translate the ➤➤ **MSNs** (= **Number**, multidigit) of the incoming call to ➤➤ **EAZs** (single digit) (CAPI 1.1 can only detect single-digit numbers). This is why the CAPI entry under **Item** is not simply called "CAPI" but "CAPI 1.1 EAZ x Mapping". When using CAPI 1.1, you must therefore make sure you assign each CAPI application the corresponding EAZ(s) by "mapping". For example select for **Number** = 1234 the entry **Item** = *CAPI 1.1 EAZ 0 Mapping* and for **Number** = 5678 the entry **Item** = *CAPI 1.1 EAZ 1 Mapping*.

With CAPI 2.0, the MSN is evaluated directly, so "conversion" to EAZ is not necessary. You should certainly try to change your PC system to CAPI 2.0 so that you can also use new features.

- Enter **Number**.
- Select **Mode**.
- Enter **CAPI Username**.
- Select **Bearer**.
- Confirm with **SAVE**.
- Repeat these steps as often as necessary until you have created an entry for every user.



When you carry out remote CAPI configuration on the hosts, you must enter the user name and password for each user corresponding to the entries in **X8500**.

5.1.3 General PPP Settings

Authentication You must enter the >> **PPP** settings for each WAN partner, e.g. the settings needed for authentication of connection partners with >> **CHAP** or >> **PAP** (see [chapter 4.3, page 94](#)). If a call is received, **X8500** then recognizes the calling WAN partner from the calling party number with the aid of >> **CLID** (Calling Line Identification) and therefore knows what authentication negotiations it has agreed with this partner. The call is accepted if the authentication is correct.

CLID In the following cases, it is not possible to identify an incoming call via CLID:

- The call is made over an analog line (the caller dials into your router via a >> **modem**)
- The caller suppresses the CLID facility

In both cases, **X8500** receives no calling line number. The caller therefore cannot be identified by CLID, even if the caller is entered as a WAN partner. **X8500** does not know which >> **PPP authentication** protocol to use to identify the incoming call.

General PPP settings In order to answer the call in spite of the identification problem, **X8500** executes the defined general PPP authentication protocol with the caller. This protocol does not refer to a certain WAN partner. If the data (password, partner PPP ID) obtained by executing the authentication protocol are the same as the data of an entered WAN partner, **X8500** accepts the incoming call.

The general PPP settings are configured in **PPP**.

Field	Meaning
Authentication Protocol	<p>Defines the PPP authentication protocol offered to the caller first. Possible values:</p> <ul style="list-style-type: none"> ■ <i>PAP</i>: PAP only ■ <i>CHAP</i>: CHAP only ■ <i>CHAP + PAP</i>: first CHAP, then PAP ■ <i>MS-CHAP</i>: MS-CHAP only ■ <i>CHAP + PAP + MS-CHAP</i>: First CHAP, if denied then the protocol required by the caller. ■ <i>MS-CHAP V2</i>: MS-CHAP, version 2 only ■ <i>none</i>: no PPP authentication
Radius Server Authentication	<p>Settings for RADIUS server authentication in case you use authentication via RADIUS. Possible values:</p> <ul style="list-style-type: none"> ■ <i>inband</i> (default value): Only inband RADIUS requests (PAP,CHAP) are sent to the specified RADIUS server. ■ <i>Calling Line Identification (CLID)</i>: Only outband requests are sent to the RADIUS server. ■ <i>CLID + inband</i>: Both requests are sent to the RADIUS server (first outband request, then inband request if necessary). ■ <i>none</i>: No requests are sent. <p>For further information on RADIUS, see Software Reference.</p>

Field	Meaning
PPP Link Quality Monitoring	<p>Defines whether Link Quality Monitoring is executed for PPP connections. Possible values:</p> <ul style="list-style-type: none"> ■ <i>no</i>: is not executed. ■ <i>yes</i>: The connection statistics are stored in the ➤➤ MIB table biboPPPLQMTTable.
PPPoE Ethernet Interface	<p>Defines the interface used by PPP-over-Ethernet for using an xDSL connection (see chapter 4.2.2, page 86).</p>
PPPoE Server Mode	<p>For PPPoE connections.</p> <p>Enables X8500 to connect PPPoE clients over this Ethernet interface.</p> <p>Default value: <i>disabled</i>.</p>

Table 5-6: **PPP**

To do Proceed as follows to define the relevant fields for general PPP settings:

- Go to **PPP**.
- Select **Authentication Protocol**, e.g. **CHAP + PAP + MS-CHAP**.
- Select **PPP Link Quality Monitoring**, e.g. **no**.
- Confirm with **SAVE**.

The entries are temporarily saved and activated. The PPP settings are configured.

5.1.4 X.31 TEI (Terminal Endpoint Identifier)

The menu **BRI[x] ➤ ADVANCED SETTINGS** contains settings for X.31 TEI (X.25 in the D-channel). You only need to make changes here if you want to use the X.31 TEI value for CAPI applications.

The menu contains the following fields:

Field	Meaning
X.31 TEI Value	X.31 TEI is detected automatically in ISDN auto-configuration and this value set to <i>specify</i> . If autoconfiguration has not detected TEI, you can set <i>specify</i> manually.
Specify TEI Value	The value for X.31 TEI assigned by the exchange. This value is detected automatically by ISDN auto-configuration, but can also be entered manually.
X.31 TEI Service	<p>Here you select the service for which you want to use X.31 TEI. Possible values:</p> <ul style="list-style-type: none"> ■ <i>Capi</i> ■ <i>Capi Default</i> ■ <i>Packet Switch</i> <p><i>Capi</i> and <i>Capi Default</i> are for using X.31 TEI for CAPI applications. For <i>Capi</i>, the TEI value set in the CAPI application is used. For <i>Capi Default</i>, the value of the CAPI application is ignored and the default value set here is always used.</p> <p>Set to <i>Packet Switch</i> if you want to use X.31 TEI for the X.25 router.</p>

Table 5-7: **BRI[x]** ► **ADVANCED SETTINGS**

5.2 Settings Specific to WAN Partners

Specific functions for **➤➤ WAN partners** make it possible to define the characteristics for connections to WAN partners individually. Carry out the configuration steps described separately for each WAN partner.

- Delay after Connection Failure ([chapter 5.2.1, page 146](#))
- Channel Bundling ([chapter 5.2.2, page 147](#))
- Channel Bundling – Bandwidth on Demand (BOD) ([chapter 5.2.3, page 149](#))
- Always On/Dynamic ISDN (AO/DI) ([chapter 5.2.4, page 157](#))
- Application-Controlled Bandwidth Management ([chapter 5.2.5, page 165](#))
- Layer 1 Protocol (ISDN B-Channel) ([chapter 5.2.6, page 171](#))
- IP Transit Network ([chapter 5.2.7, page 173](#))
- Name Server ([chapter 5.2.8, page 177](#))
- **➤➤ RIP** (Routing Information Protocol) ([chapter 5.2.9, page 180](#))
- Compression: **➤➤ VJHC**, **➤➤ STAC**, MS-STAC ([chapter 5.2.10, page 183](#))
- **➤➤ Proxy ARP** (Address Resolution Protocol) ([chapter 5.2.11, page 185](#))
- Keepalive Monitoring ([chapter 5.2.12, page 187](#))

The configuration steps necessary in each case are explained in detail below.

5.2.1 Delay After Connection Failure

This function enables you to set the period of time **X8500** is to wait after an unsuccessful attempt to set up a call.

This is configured in **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**:

Field	Meaning
Delay after Connection Failure (sec)	Block timer. Indicates the waiting time in seconds before X8500 tries again after an attempt to establish a connection has failed.

Table 5-8: **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**

To do Proceed as follows:

- Go to **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**.
 - Enter **Delay after Connection Failure (sec)**.
 - Confirm with **OK**.
 - Confirm with **SAVE**.
- The waiting time is set.

5.2.2 Channel Bundling

X8500 supports dynamic and static ►► **channel bundling** for dialup connections. Only one B-channel is initially opened when a connection is established.

Dynamic Dynamic channel bundling means that **X8500** connects other ►► **ISDN** B-channels to increase the throughput for connections to the WAN partner, if this is required, e.g. for large amounts of data. If the amount of data traffic drops, the additional ►► **B-channels** are closed again.

Static In static channel bundling, you specify right from the start how many B-channels **X8500** uses for connections to the WAN partner, regardless of the amount of data transferred.

The configuration is made in **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**:

Field	Meaning
Channel Bundling	Defines whether and which type of channel bundling is to be used for connections to the WAN partner.

Field	Meaning
Total Number of Channels	For dynamic channel bundling: Defines the maximum number of B-channels that may be opened. For static channel bundling: Defines the number of B channels that are open during the complete connection.

Table 5-9: **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**

The **Channel Bundling** field contains the following selection options:

Possible values	Meaning
<i>no</i>	No channel bundling, only one B-channel is ever available for connections.
<i>dynamic</i>	Dynamic channel bundling.
<i>static</i>	Static channel bundling.

Table 5-10: **Channel bundling**

To do Proceed as follows:

- Go to **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**.
- Select the desired value for **Channel Bundling**.
- Enter **Total Number of Channels**.
- Confirm with **OK**.
- Confirm with **SAVE**.

The entries are temporarily saved and activated.

Refer to Bandwidth on Demand (BOD) function, see [chapter 5.2.3, page 149](#).

5.2.3 Channel Bundling – Bandwidth On Demand (BOD)

Bandwidth management, subsequently called BOD (Bandwidth on Demand), offers advance configuration options for dialup connections compared with the basic configuration of channel bundling (see [chapter 5.2.2, page 147](#)). BOD permits dynamic bundling of leased lines with dialup lines to cope with large amounts of data. You have the following options:

- BOD for leased lines, i.e. dynamic connection of one or more dialup connection(s) to the existing leased line, if required.
- BOD for dialup connections, i.e. dynamic connection of one or more dialup connection(s) to the existing dialup connection, if required.
- Backup for leased lines, i.e. establishing a dialup connection when the leased line to the partner fails. To enable this, more than one additional channel must be allowed in the configuration (**Maximum Number of Dialup Channels** > 1).

Switching B-channels in and out

The use of the B-channels is controlled by the data throughput or by application-controlled bandwidth management (Bandwidth On Demand).

First B-channels can be added as soon as the bandwidth is no longer sufficient for data transmission. A B-channel is added if the current data utilization of the relevant interface to the connection partner is 90 % or more of the maximum permissible utilization for at least five seconds. The percentage utilization of the bundle assuming a B-channel is dropped is calculated from the measured utilization. A B-channel is dropped if the calculated value stays below 80 % of the maximum permissible utilization of the remaining channels for 10 seconds.

Second the application-controlled addition of B-channels for **X8500** via filters and rules can be configured in a similar way to access lists for IP packets. You will find a description of the configuration in [chapter 5.2.5, page 165](#).

Both throughput-controlled and application-controlled bandwidth management can use the Bandwidth Allocation Control Protocol (BACP/BAP to RFC 2125) for agreeing with the remote terminal on the circumstances under which B-channels are to be added or dropped. In this case, the use of BACP/BAP is agreed during the initial connection setup.

Static or dynamic short hold (see ["Defining Short Hold", page 106](#)) may also cause an additional B-channel to be dropped. If static short hold has been configured, this always has the highest priority. If dynamic short hold has been configured, the calculated value mentioned above must also apply.

X8500 also supports the AO/DI (Always On/Dynamic ISDN) function for using the ISDN D-channel for data transmission (see [chapter 5.2.4, page 157](#)).

Authentication PPP authentication is not required from the connection partner for establishing a leased line. Authentication is, however, necessary for any dialup connections switched in.

Configuration is made in:

- **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS (OPTIONAL)**
- **WAN PARTNER** ► **EDIT** ► **WAN NUMBERS** ► **ADD** (menu description in [chapter 4.3, page 94](#))
- **WAN PARTNER** ► **EDIT** ► **PPP** (menu description in [chapter 4.3, page 94](#))



The fields described below appear only for dialup connections if **Channel Bundling** = *dynamic* has previously been selected in the menu **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**.

The menu **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS (OPTIONAL)** contains the following fields:

Field	Meaning
Mode	Defines which mode is used for BOD. Possible values: see table 5-12, page 156 .

Field	Meaning
Line Utilization Weighting	<p>Defines how the line utilization is calculated. Possible values:</p> <ul style="list-style-type: none"> ■ <i>equal</i>: All the measured values of throughput in Line Utilization Sample (sec) are weighted equally for the calculation (default value). ■ <i>proportional</i>: The last measured values of throughput are weighted more heavily for the calculation, i.e. the calculation is most heavily influenced by the last measured values in Line Utilization Sample (sec).
Line Utilization Sample (sec)	<p>Time interval in seconds. Throughput measurements in Line Utilization Sample (sec) are included in the calculation of the line utilization. Possible values: 5 to 300 (default value: 5).</p>
Gear Up Threshold	<p>Utilization threshold at which another B-channel is added for a connection. Default value: 90.</p>
Gear Down Threshold	<p>B-channels are dropped until the remaining channels have at least the percentage utilization degree remaining here. Default value: 80.</p>
D-Channel Queue Length	<p>(only if Layer 1 Protocol = AO/DI in the menu WAN PARTNER ► EDIT ► ADVANCED SETTINGS)</p> <p>Threshold value for the number of bytes accumulated in the D-channel at which the system is to change to the B-Channel Mode (see chapter 5.2.4, page 157).</p> <p>Possible values: 0 to 20000 (default value: 7500).</p>

Field	Meaning
Maximum Number of Dialup Channels	Maximum permitted number of channels that are opened for dialup connections. The value is only displayed here; it is set under Total Number of Channels in the menu WAN PARTNER ► EDIT ► ADVANCED SETTINGS .

Table 5-11: **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS (OPTIONAL)**

The **Mode** field includes the following selection options:

Possible values	Meaning
<i>Bandwidth On Demand Disabled</i>	Deactivates BOD, no additional channels are opened (default value).
<i>Bandwidth On Demand Enabled</i>	(For dialup connections only) Activates BOD, additional channels can be opened. The connection partner who initiated the connection opens the additional channels.
<i>BAP, Active Mode</i>	(Bandwidth Allocation Protocol) Necessary for the AO/DI (Always On/Dynamic ISDN) function, see table 5-17, page 164 .
<i>BAP, Passive Mode</i>	BAP behaves as follows in Passive Mode: <ul style="list-style-type: none"> ■ Call Request: one of the two communication partners wants to add a B-channel; is accepted if applicable. ■ Callback Request: the remote terminal is requested to add a B-channel; is initiated if applicable. ■ Link Drop Request: one communication partner wants to drop a B-channel; dropping is initiated or accepted if applicable.

Possible values	Meaning
<i>BAP, Active and Passive Mode</i>	<p>BAP behaves as follows in Active and Passive Mode:</p> <ul style="list-style-type: none">■ Call Request: one of the two communication partners wants to add a B-channel; is initiated or accepted if applicable.■ Callback Request: is not used.■ Link Drop Request: one communication partner wants to drop a B-channel; dropping is initiated or accepted if applicable.
<i>BAP, Client Active Mode</i>	<p>BAP behaves as follows in Client Active Mode: The partner who sets up the initial call is in <i>Active Mode</i> (see <i>BAP, Active Mode</i>) and the partner who accepts the initial call is in <i>Passive Mode</i> (see <i>BAP, Passive Mode</i>).</p>

Possible values	Meaning
<i>BAP, Dialup Client Mode</i>	<p>(For dialup connections only)</p> <p>In this scenario the client is the active partner, control and responsibility (cost for channel bundling) lie with him. It is expected that the central side accepts all requests which agree with the WAN partner configuration of the central side router.</p> <p>BAP behaves as follows in Dialup Client Mode:</p> <ul style="list-style-type: none"> ■ Call Request: the client wants to add a B-channel; is initiated if applicable. ■ Callback Request: the remote terminal (server) is requested to add a B-channel (initiated); the remote terminal then sends a callback request. ■ Link Drop Request: one communication partner wants to drop a B-channel; dropping is initiated if applicable. <p>If the ISP distributes incoming calls to more than one router, this setting ensures channel bundling for clients.</p> <p>The system administrator of the ISP should refer to Release Notes 6.2.1.</p>

Possible values	Meaning
<i>BAP, Dialup Server Mode</i>	<p>(For dialup connections only)</p> <p>In this scenario the client is the active partner, control and responsibility (cost for channel bundling) lie with him. It is expected that the central side accepts all requests which agree with the WAN partner configuration of the central side router.</p> <p>BAP behaves as follows in Dialup Server Mode:</p> <ul style="list-style-type: none"> ■ Call Request: the client wants to add a B-channel; is accepted if applicable. ■ Callback Request: the remote terminal (server) is requested to add a B-channel; the remote terminal then sends a callback request; is accepted if applicable. ■ Link Drop Request: one communication partner wants to drop a B-channel; dropping is accepted if applicable. <p>If the ISP distributes incoming calls to more than one router, with this setting the ISP ensures channel bundling for the client.</p> <p>The system administrator of the ISP should refer to Release Notes 6.2.1.</p>
<i>Backup</i>	<p>(For leased lines only)</p> <p>Backup connection is activated if the leased line fails. The backup connection is cleared when the leased line is available again.</p> <p>BOD is also available for this mode, if a value > 1 is used for Maximum Number of Dialup Channels.</p>

Possible values	Meaning
<i>Bandwidth On Demand Active</i>	(For leased lines only) Enables BOD and defines the active partner. Only one of the connection partners should be configured as active partner. The active partner initiates switching in and out additional B-channels on demand.
<i>Bandwidth On Demand Passive</i>	(For leased lines only) Enables BOD and defines the passive partner. The passive partner does not initiate switching in and out additional channels.

Table 5-12: **Mode**

To do Proceed as follows:

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS** ➤ **EXTENDED INTERFACE SETTINGS (OPTIONAL)**.
- Select the desired value for **Mode** and **Line Utilization Weighting**.
- Enter the desired value for **Line Utilization Sample (sec)**.
- Confirm with **SAVE**.
- Confirm with **OK**.
- Go to **WAN PARTNER** ➤ **EDIT** ➤ **WAN NUMBERS** ➤ **ADD**.
- Enter **Number**.
- Select **Direction**.



Select **Direction** = *outgoing* if you have set **Mode** = *Bandwidth On Demand Active*.

Select **Direction** = *incoming (CLID)*, if you have set **Mode** = *Bandwidth On Demand Passive*.

- Confirm with **SAVE**.
- Go to **WAN PARTNER** ➤ **EDIT** ➤ **PPP**.
- Select **Authentication**.

- Enter **Partner PPP ID**, **Local PPP ID** and **PPP Password**, if applicable.
 - Confirm with **OK**.
 - Confirm with **SAVE**.
- The settings are temporarily saved and activated.

5.2.4 Always On/Dynamic ISDN (AO/DI)

Always On/Dynamic ISDN (AO/DI) uses the existing ISDN infrastructure to configure a special service for the user without hardware changes: AO/DI is a permanently available (always on) but nevertheless low-cost connection from the end customer to the service provider. Only Deutsche Telekom provided this feature at the time this manual was printed.

Short Description AO/DI uses X.25 data packet transmission in the D-channel (X.31) to set up a PPP connection (PPP over X.25). 9600 bps are available for data transmission in the D-channel (D-channel Mode). If more bandwidth is needed, one or more B-channels are dynamically added (Dynamic ISDN). Data transmission in this case is only in the B-channel or B-channels (B-channel Mode).

AO/DI offers the following advantages:

- An additional, independent communication channels
- Permanent connection to the Internet at low-cost
- Transparent bandwidth control
- In D-Channel Mode
 - high reliability and guaranteed throughput times
 - volume-oriented charges independent of distance
- Time-dependent connection charges in B-Channel Mode only for bandwidth-intensive applications

How Does AO/DI Work?

AO/DI is implemented in **X8500** via a special PPP interface. As soon as the interface is configured and ready for operation, the initial PPP connection is set up via X.31 (X.25 in the D-channel). This involves carrying out authentication of

the PPP connection partner and assigning a dynamic IP address and DNS addresses, if applicable (AO/DI Client Mode).

As the D-channel connection is normally no longer ended after connection set-up, it represents a permanently available (always on) connection to the provider.

As soon as the bandwidth of the D-channel is no longer adequate for data transmission, B-channels are added and data transmission takes place exclusively in the B-channels (Dynamic ISDN). This is implemented in **X8500** by an advanced configuration option in the IP subsystem. An interface is assigned filters, rules and rule chains as for the IP access lists (see [chapter 7.2.8, page 315](#)). These rules can be used to determine whether additional B-channels are to be set up for certain protocols, ports or IP addresses, or whether data transfer is to take place exclusively in the D-channel.

How is AO/DI Configured?

The following steps are necessary for configuring **X8500** for AO/DI:

- Carry out X.31 configuration, i.e. reserve the **TEI Value** for X.25 (Packet Switch, see "[X.31 configuration](#)", [page 159](#))
- Carry out X.25 configuration (see "[X.25 configuration](#)", [page 159](#)):
 - Link configuration for Datex-P
 - Call routing
- Configure AO/DI partner as WAN partner (see "[Configuring AO/DI partner as WAN partner](#)", [page 161](#)):
 - Select PPP parameters
 - Define the PPP interface as AO/DI interface
 - Enter X.25 destination address for initial connection setup
 - Check throughput-controlled bandwidth management (dynamic B-channel bundling)
 - Check application-controlled bandwidth management

You will find all the necessary steps below for configuring **X8500** for AO/DI.

X.31 configuration Proceed as follows to assign X.31 to X.25:

- Go to **BRI[x]** ➤ **ADVANCED SETTINGS** (the menu is described in chapter 5.1.4, page 144).
- Select **X.31 TEI Value**: *specify*.



The default setting for **X.31 TEI Value** should be *specify*. If this is not the case, the X.31 service has not been detected by autoconfiguration and this service is probably not supported (contact your telephone provider).

- Enter **Specify TEI Value**, e.g. **1** (ask your provider for a valid value).
- Select **X.31 TEI Service**: *Packet Switch*.
- Confirm with **SAVE**.
You have returned to the **BRI[x]** menu.
- Confirm with **SAVE**.
You have returned to the main menu. The main menu now contains the X.25 menu, which you need for the following configuration steps. For information about the X.25 parameters, see the **Software Reference** at www.bintec.net.

X.25 configuration



Please note the following when carrying out X.25 configuration:

- Some of the X.25 parameters must be adapted to the X.25 network connected. For Datex-P, the **Window size/Packetsize Neg.** field must be deactivated.
- For **X8500**, the X.25 software is designed as an X.25 switch. This switch must be appropriately configured for AO/DI.

Proceed as follows to make the preset link settings for X.25 configuration for Datex-P:

- Go to **X.25** ➤ **LINK CONFIGURATION**.
- Select the interface for which you want to configure X.25, e.g. **x31d2-0-1**.

The following parts of the menu are relevant for this configuration step:

Field	Meaning
L3 Packet Size	Permissible size of data packets for this connection on the third layer of the OSI model.
Windowsize/Packetsize Neg.	Negotiation of the size of Windowsize and Packetsize with the remote terminal. There is only one meaningful setting for Datex-P: <i>never</i> , i.e. negotiation is deactivated.
Highest Two-Way-Channel (HTC)	Defines the highest number of virtual channels that can be added. Possible values: <i>0 to 4095</i> ; default value: <i>2</i> .

Table 5-13: X.25 ► LINK CONFIGURATION ► EDIT

- Select **L3 Packet Size max**: *256*.
- Select **Windowsize/Packetsize Neg.**: *never*.
- Enter **Highest Two-Way-Channel (HTC)**: *1*.
- Confirm with **SAVE**.
- Leave **X.25 ► LINK CONFIGURATION** with **Exit**.

Proceed as follows to make the preset routing settings for X.25 configuration:

- Go to **X.25 ► ROUTING ► ADD**.

The following parts of the menu are relevant for this configuration step:

Field	Meaning
Source Link	Source interface of data packets.
Destination Link	Destination interface of data packets.
Destination X.25 Address	X.25 destination address.

Table 5-14: X.25 ► ROUTING ► ADD

- Select **Source Link**: *local*.

- Select **Destination Link**, e.g. *x31d2-0-1*.
 - Enter **Destination X.25 Address**, e.g. *019011*.
 - Confirm with **SAVE**.
 - Leave **X.25** ➤ **ROUTING** ➤ **ADD** with **Exit**.
 - Leave **X.25** ➤ **ROUTING** with **Exit**.
- You have returned to the main menu.

Configuring AO/DI partner as WAN partner

To define an AO/DI-capable PPP interface, proceed as follows:

- Go to **WAN PARTNER** ➤ **ADD**.
- Enter **Partner Name**, e.g. *AODI partner*.
- Select **Encapsulation**: *PPP*.

Proceed as follows to make the PPP settings:

- Go to **WAN PARTNER** ➤ **ADD** ➤ **PPP**.
- Select **Authentication**, e.g. *CHAP*.
- Leave out **Partner PPP ID**.
- Enter **Local PPP ID**, e.g. *bintec_router*.
- Enter **PPP Password** twice, e.g. *secret*.

An asterisk appears on the screen as a place marker for each letter you enter for the password.

- Confirm with **OK**.

To activate AO/DI on the PPP interface and enter the X.25 address, proceed as follows:

- Go to **WAN PARTNER** ➤ **ADD** ➤ **ADVANCED SETTINGS**.

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

Field	Meaning
Layer 1 Protocol	Defines which Layer 1 Protocol X8500 is to use. There is only one meaningful setting for AO/DI: <i>AO/DI</i> .

Field	Meaning
Channel Bundling	Defines whether or which type of channel bundling is to be used for connections to the WAN partner (see chapter 5.2.2, page 147). If <i>AO/DI</i> is selected under Layer 1 Protocol , <i>dynamic</i> is set automatically for Channel Bundling .
Total Number of Channels	Defines the maximum number of B-channels that may be opened for dynamic channel bundling. Possible values: 0 to 9999; default value: 1.
Remote X.25 Address	X.25 destination address. Appears only if <i>AO/DI</i> is selected under Layer 1 Protocol .

Table 5-15: **WAN PARTNER** ➤ **ADD** ➤ **ADVANCED SETTINGS**

- Select **Layer 1 Protocol**: *AO/DI*.
- Enter **Total Number of Channels**, e.g. **1**.
- Enter **Remote X.25 Address**, e.g. **019011**.

Proceed as follows to configure BACP/BAP for the "AO/DI client" access (control of Bandwidth On Demand):

- Go to **WAN PARTNER** ➤ **ADD** ➤ **ADVANCED SETTINGS** ➤ **EXTENDED INTERFACE SETTINGS (OPTIONAL)**.

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

Field	Meaning
Mode	Defines which mode is used for BOD. Only the <i>BAP</i> , <i>Active Mode</i> setting is used for an AO/DI client.
Line Utilization Weighting	Weighting within the interval considered for adding and dropping B-channels.
Line Utilization Sample (sec)	Length of the interval over which the mean of the measured throughput data is taken and weighted with Line Utilization Weighting .

Field	Meaning
Gear Up Threshold	Utilization threshold at which another B-channel is added for a connection. Default value: 90.
Gear Down Threshold	B-channels are dropped until the remaining channels have at least the percentage utilization degree remaining here. Default value: 80.
D-Channel Queue Length	Threshold value for the number of bytes accumulated in the D-channel at which the system is to change to the B-Channel Mode. Possible values: 0 to 20000 (default value: 7500).
Maximum Number of Dialup Channels	Maximum number of channels that may be opened. The value is defined in the Total Number of Channels field under WAN PARTNER ► ADD ► ADVANCED SETTINGS .

Table 5-16: **WAN PARTNER ► ADD ► ADVANCED SETTINGS ► EXTENDED INTERFACE SETTINGS (OPTIONAL)**

The following selection option in the **Mode** field is relevant for AO/DI:

Possible values	Meaning
<i>BAP, Active Mode</i>	<p>The Bandwidth Allocation Protocol (BAP) knows three different options for negotiating a bandwidth change. It behaves as follows in <i>Active Mode</i>:</p> <ul style="list-style-type: none"> ■ Call Request: one of the two communication partners wants to add a B-channel; adding the channel is initiated if applicable, but not accepted. ■ Callback Request: the remote terminal is requested to add a B-channel; adding the channel is not initiated but accepted if applicable. ■ Link Drop Request: one communication partner wants to drop a B-channel; dropping is initiated but not accepted.

Table 5-17: **Mode** = *BAP, Active Mode*

- Select **Mode**: *BAP, Active Mode*.
- Use the preset values for the other fields of this menu.
- Confirm with **SAVE**.
- Confirm with **OK**.

To enter the necessary ISDN extensions for adding B-channels, proceed as follows:

- Go to **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** ➤ **ADD**.
- Enter the **Number**, e.g. **0911123456**.
- Select **Direction**: *outgoing*.
- Confirm with **SAVE**.
- Leave **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** ➤ **ADD** with **Exit**.

For dynamic assignment of the IP address by the service provider, proceed as follows:

- Go to **WAN PARTNER** ➤ **ADD** ➤ **IP**.
- Select **IP Transit Network**: *dynamic client*.
- Confirm with **SAVE**.
- Confirm with **SAVE**.
- Leave **WAN PARTNER** with **Exit**.

You have returned to the main menu.

5.2.5 Application-Controlled Bandwidth Management (BOD)

Filters and rules Application-controlled bandwidth management is configured by filters and rules in a similar way to Access Lists for IP packets (see [chapter 7.2.8, page 315](#)). First filters are defined in order to determine which IP packets (and thus applications) are to be filtered. Rules determine what to do with data packets filtered out. If several rules are defined, they can be interlinked using a rule chain.

Defining BOD filters Proceed as follows to define suitable filters:



Filter entries are shared with access lists ([chapter 7.2.8, page 315](#)) and QoS filters ([chapter 5.4.1, page 220](#)).

- Go to **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **FILTER** ➤ **ADD**.
- Enter **Description**, e.g. *mail_smtp_out*.
- Select **Protocol**, e.g. *tcp*.
- Enter **Destination Address**, e.g. *172.16.8.15*.
- Enter **Destination Mask**, e.g. *255.255.255.255*.
- Select **Destination Port**: e.g. *specify*.
- Enter **Specify Port**, e.g. *25* (port for SMTP).

- Confirm with **SAVE**.
A list of all the previously defined filters appears.
- Leave **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **FILTER** with **Exit**.

Defining BOD rules A rule for BOD is defined in a similar way to a rule for IP packets (see [chapter 7.2.8, page 315](#)). Different rules normally refer to different filters and can be interlinked to form a rule chain. Each rule results in an action. The direction of the data packets for which it is to apply can also be stated for each rule, i.e. for sent or received data packets.

Proceed as follows to define a rule for BOD:

- Go to **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **RULES FOR BOD** ➤ **ADD**.

In addition to the already familiar fields for definition of conventional rules (see [chapter 7.2.8, page 315](#)), the menu contains the following fields:

Field	Meaning
Action	Defines the action to be taken for a filtered data packet.
Direction	Direction of data packets to which the rule is to be applied. Possible values: <ul style="list-style-type: none"> ■ <i>incoming</i>: incoming data packets ■ <i>outgoing</i>: outgoing data packets ■ <i>both</i>: incoming and outgoing data packets
Number of Channels	Number of B-channels that are to be used for this service.
Filter	Filter used.

Table 5-18: **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **RULES FOR BOD** ➤ **ADD**

The **Action** field, which indicates how a filtered data packet is to be handled, contains the following selection options:

Possible values	Meaning
<i>invoke M</i>	B-channels are added if the rule matches.

Possible values	Meaning
<i>invoke !M</i>	B-channels are added if the rule does not match.
<i>deny M</i>	B-channels are not added if the rule matches.
<i>deny !M</i>	B-channels are not added if the rule does not match.
<i>ignore</i>	The rule is ignored or it is omitted if part of a rule chain.

Table 5-19: Action

- Select **Action**, e.g. *invoke M*.
 - Select **Direction**, e.g. *outgoing*.
 - Select **Number of Channels**, e.g. *1*.
 - Select **Filter**, e.g. *mail_smtp_out*.
 - Confirm with **SAVE**.
 - Leave **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **RULES FOR BOD** with **Exit**.
 - Leave **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** with **Exit**.
- You have returned to the main menu.

To apply a rule to an interface, proceed as follows:

- Go to **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **CONFIGURE INTERFACES FOR BOD**.
- Select the interface to which you wish to apply a rule and press **Return**.
- Select the rule you wish to apply to this interface, e.g. *mail_smtp_out*.
- Confirm with **SAVE**.
- Leave **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **CONFIGURE INTERFACES FOR BOD** ➤ **EDIT** with **Exit**.
- Leave **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **CONFIGURE INTERFACES FOR BOD** with **Exit**.

- Leave **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** with **Exit**.
You have returned to the main menu.
- Leave the **IP** menu with **Exit**.
You have returned to the main menu.

Configuration Examples for Application-Controlled Bandwidth Management (Bandwidth on Demand)

Two configuration examples are described below:

- Additional bandwidth for HTTP connections
- Restricting mail reception to D-channel

Additional bandwidth for HTTP connections

The following example shows a special configuration of **X8500** for connection setup of the PC with the IP address 172.16.77.11 (TCP port 80) to the Internet. The system should always change to B-Channel Mode with one B-channel when an HTTP connection is set up to the Internet.

Proceed as follows to define the relevant filter for BOD:

- Go to **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **FILTER** ➤ **ADD**.
- Enter **Description**: *hostxy_http_out*.
- Select **Protocol**: *tcp*.
- Select **Connection State** *any*.
- Enter **Source Address**: *172.16.77.11*.
- Enter **Source Mask**: *255.255.255.255*.
- Select **Destination Port**: *specify*.
- Enter **Specify Port**: *80*.
- Confirm with **SAVE**.

A list of all the previously defined filters appears.

- Leave **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **FILTER** with **Exit**.

Proceed as follows to define a rule for BOD:

- Go to **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **RULES FOR BOD** ➤ **ADD**.

- Select **Action**: *invoke M*.
 - Select **Direction**: *outgoing*.
 - Select **Number of Channels**: *1*.
 - Select **Filter**: *hostxy_http_out (1)*.
 - Confirm with **SAVE**.
 - Leave **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **RULES FOR BOD** with **Exit**.
- Defining interfaces**
- Go to **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **CONFIGURE INTERFACES FOR BOD**.
 - Select the appropriate interface and confirm with **Return**.
You are now in the menu **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **CONFIGURE INTERFACES FOR BOD** ➤ **EDIT**.
 - Select the rule *R1 1 FI 1 (hostxy_http_out)*.
 - Confirm with **SAVE**.
 - Leave the menu **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **CONFIGURE INTERFACES FOR BOD** with **EXIT**.
 - Leave the menu **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** with **EXIT**.
 - Leave the menu **IP** with **EXIT**.
You have returned to the main menu. The settings are temporarily saved and activated.

Restricting mail reception to D-channel

In the following configuration example, mail reception is restricted to the D-channel and there is no change to B-Channel Mode. The inquiry about whether new mails have been received does not cause a change to B-Channel Mode either.

Proceed as follows to define the relevant filter for BOD:

- Go to **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **FILTER** ➤ **ADD**.
- Enter **Description**: *mail_pop3_in*.
- Select **Protocol**: *tcp*.
- Select **Connection State** *any*.
- Enter **Destination Address**: *172.16.8.15*.

- Enter **Destination Mask**: *255.255.255.255*.
- Select **Destination Port**: *specify*.
- Enter **Specify Port**: *110*.
- Confirm with **SAVE**.
A list of all the previously defined filters appears.
- Leave **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **FILTER** with **Exit**.

Proceed as follows to define a rule for BOD:

- Go to **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **RULES FOR BOD** ➤ **ADD**.
- Select **Action**: *deny M*.
- Select **Direction**: *incoming*.
- Select **Filter**: *mail_pop3_in (2)*.
- Confirm with **SAVE**.
- Leave **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **RULES FOR BOD** with **Exit**.

Defining interfaces

- Go to **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **CONFIGURE INTERFACES FOR BOD**.
- Select the appropriate interface and confirm with **Return**.
You are now in the menu **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **CONFIGURE INTERFACES FOR BOD** ➤ **EDIT**.
- Select the rule *RI 2 FI 2 (mail_pop3_in)*.
- Confirm with **SAVE**.
- Leave the menu **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **CONFIGURE INTERFACES FOR BOD** with **EXIT**.
- Leave the menu **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** with **EXIT**.
- Leave the menu **IP** with **EXIT**.

You have returned to the main menu. The settings are temporarily saved and activated.

5.2.6 Layer 1 Protocol (ISDN B-Channel)

ISDN B-channel You can define the Layer 1 Protocol of the ISDN **B-channel** that **X8500** is to use for connections to the WAN partner. The default setting is the protocol for 64-kbps ISDN data connections, which is the default value of the B-channel. Only change the setting if expressly required.

This is configured in **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**:

Field	Meaning
Layer 1 Protocol	Defines which Layer 1 Protocol X8500 is to use. This setting applies only to outgoing calls to the WAN partner and to incoming calls from the WAN partner, if they have been identified from the calling party number.

Table 5-20: **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**



For incoming calls that cannot be identified from the calling party number, **X8500** uses the settings under **Item** in menu **BRI[x]** ► **INCOMING CALL ANSWERING** resp. **PRI[x]** ► **INCOMING CALL ANSWERING** as the Layer 1 Protocol (see "[Incoming Call Answering](#)", page 77).

Layer 1 Protocol contains the following selection options:

Possible values	Meaning
<i>ISDN 64 kbps</i>	For 64-kbps ISDN data connections. This is the default value.
<i>ISDN 56 kbps</i>	For 56-kbps ISDN data connections.

Possible values	Meaning
<i>Modem</i>	(Only available if expansion card and resource module with digital modems are installed.) Assigns incoming analog calls to the PPP routing service. The digital modem on the resource module that accepts this call uses the settings for Modem Profile 1, which were selected in the menu MODEM ► PROFILE CONFIGURATION ► PROFILE 1 .
<i>DOVB</i>	Data transmission Over Voice Bearer - useful in the USA, for example, where voice connections are sometimes cheaper than data connections.
<i>V.110 (1200 ... 38400)</i>	For GSM connections with V.110 at bit rates of 1200 bps, 2400 bps,..., 38400 bps.
<i>Modem Profile 1 ... 8</i>	(Only available if expansion card and resource module with digital modems are installed.) Assigns incoming analog calls to the PPP routing service. The digital modem on the resource module that accepts this call uses the settings for Modem Profile1... 8, which were selected in the menu MODEM ► PROFILE CONFIGURATION ► PROFILE 1...8 .
<i>PPTP PNS</i>	For VPN interface.
<i>PPP over Ethernet (PPPoE)</i>	For connections to xDSL (see chapter 4.2.2, page 86).
<i>AO/DI</i>	For using Always On/Dynamic ISDN (AO/DI, see chapter 5.2.4, page 157).
<i>PPP over PPTP</i>	For connections with xDSL, e.g. in Austria, see " Example 2: Telekom Austria (high-speed Internet access) ", page 91.

Table 5-21: Layer 1 Protocol



Most of the entries for **Layer 1 Protocol** correspond to the entries for **Item** in **BRI[x] ► INCOMING CALL ANSWERING** resp. **PRI[x] ► INCOMING CALL ANSWERING** (see "[Incoming Call Answering](#)", page 77).

To do Proceed as follows:

- Go to **WAN PARTNER ► EDIT ► ADVANCED SETTINGS**.
- Select **Layer 1 Protocol**.
- Confirm with **OK**.
- Confirm with **SAVE**.

The protocol you chose is configured.

5.2.7 IP Transit Network

When you enter a WAN partner in **X8500**, there are various options for indicating the IP address of the partner network:

- You enter the ►► **IP address** and ►► **netmask** of the partner or partner network. You must obviously have this information available.
- You use an additional ISDN IP address each for **X8500** and the WAN partner. This sets up a virtual IP network – called a transit network – during the connection. You do not normally need this setting, but it is necessary for some special configurations.
- You assign the WAN partner a dynamic IP address from a specified IP address pool for the duration of the connection.
- Get the WAN partner to assign you a dynamic IP address for the duration of the connection.

Diagram with example figures:

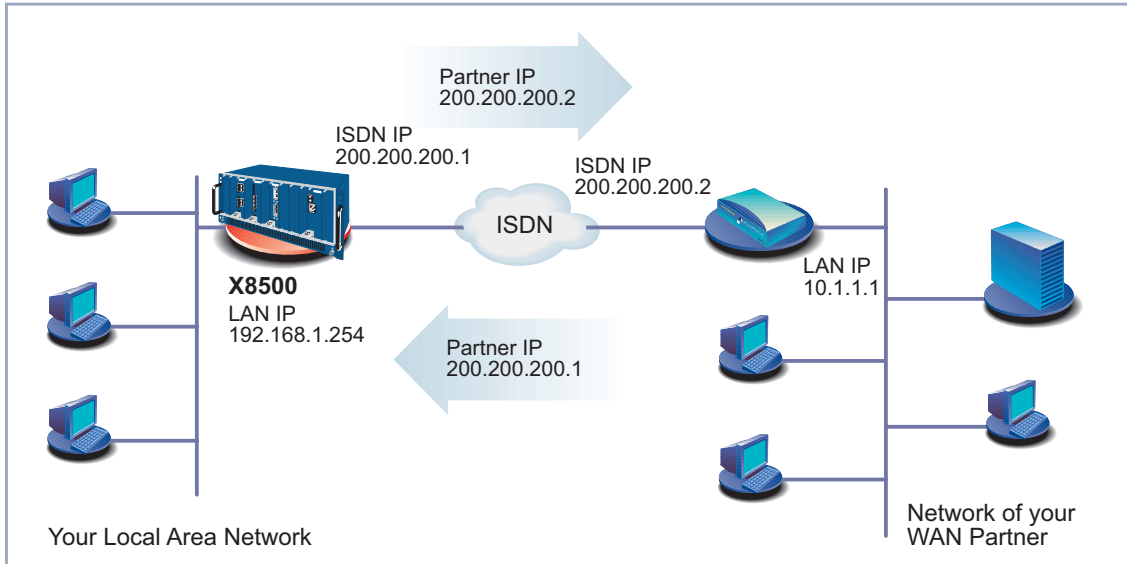


Figure 5-1: LAN-LAN link with transit network

The configuration is made in **WAN PARTNER** ► **EDIT** ► **IP**:

Field	Meaning
IP Transit Network	Defines whether X8500 sets up a transit network to the WAN partner. Possible values: see table 5-23, page 176 .
local IP Address	LAN IP address of X8500 . Appears only for the following value of IP Transit Network : <i>no</i> . You normally do not need to make any entry here. Exception: You set up several WAN partners, use a transit network for one or more WAN partners and no transit network for the other WAN partners. Then enter the Local IP Address (LAN IP address) for all WAN partners without a transit network.

Field	Meaning
local WAN IP Address	Only for the value <i>yes</i> for IP Transit Network . ISDN IP address of X8500 in the transit network.
Partner's WAN IP Address	Only for the value <i>yes</i> for IP Transit Network . WAN partner's ISDN IP address in the transit network.
Partner's LAN IP Address	Only for the value <i>yes</i> or <i>no</i> for IP Transit Network . IP address of LAN of WAN partner or LAN IP address (host).
Partner's LAN Netmask	Only for the value <i>yes</i> or <i>no</i> for IP Transit Network . WAN partner's LAN netmask. If you make no entry, X8500 enters a default netmask for the net class used under Partner's LAN IP Address .
Default Route	Only for the value <i>dynamic client</i> for IP Transit Network . Possible values: <ul style="list-style-type: none"> ■ <i>yes</i>: Route to this WAN partner is defined as default route. ■ <i>no</i>: Route to this WAN partner is not defined as default route.

Field	Meaning
Enable NAT	<p>Only for the value <i>dynamic client</i> for IP Transit Network.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>yes</i>: NAT is activated for this WAN partner. ■ <i>no</i>: NAT is deactivated for this WAN partner. <p>This setting is equivalent to activating NAT in the menu IP ► NETWORK ADDRESS TRANSLATION ► EDIT.</p>

Table 5-22: **WAN PARTNER ► EDIT ► IP**

IP Transit Network contains the following selection options:

Possible values	Meaning
<i>yes</i>	A transit network is used.
<i>dynamic client</i>	X8500 receives its IP address from the WAN partner for the duration of the connection.
<i>dynamic server</i>	X8500 assigns the ►► Remote WAN partner an IP address for the duration of the connection. In this case, X8500 must be configured as a dynamic IP address server, i.e. it has an IP address pool available (see chapter 5.1.1, page 136).
<i>no</i>	No transit network. This setting is adequate for most WAN partners.

Table 5-23: **IP Transit Network**

To do Proceed as follows:

- Go to **WAN PARTNER ► EDIT ► IP**.
- Select the desired value for **IP Transit Network**.

- If you chose *dynamic client* for **IP Transit Network**, select the desired value for **Default Route**.
- If you chose *dynamic client* for **IP Transit Network**, select the desired value for **Enable NAT**.
- Enter **Local IP Address**, if applicable.
- Enter **Local WAN IP Address**, if applicable.
- Enter **Partner's WAN IP Address**, if applicable.
- Enter **Partner's LAN IP Address**, if applicable.
- Enter **Partner's LAN Netmask**, if applicable.
- Confirm with **SAVE**.

The IP addresses for the IP transit network are configured.

5.2.8 Name Server

Name resolution A Domain Name Server (➤➤ **DNS**) or Windows Internet Name Server (WINS) is used for converting host names and ➤➤ **NetBIOS** names into IP addresses (name resolution). Domain Name Servers form a hierarchical tree structure. As soon as a request is sent to a Domain Name Server, it tries to resolve the host name using its internal tables. If it cannot find the host name, the request is forwarded to a higher-level DNS.



If you use the DNS Proxy function, **X8500** can save previously resolved names and IP addresses in a cache and on receipt of a request first checks if the desired address can be answered from the cache. This keeps the costs of setting up WAN connections to name servers outside the LAN at a low level and optimizes performance in the LAN, as requests to frequently used addresses or addresses already resolved are answered by **X8500** itself. How to configure the DNS Proxy function is described in [chapter 5.3.2, page 197](#).

When you enter a WAN partner in **X8500**, you can define whether **X8500** sends or answers requests for WINS or DNS IP addresses.

Configuration is made in:

■ **IP ➤ STATIC SETTINGS**

■ **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**

Relevant fields of the menu **IP** ► **STATIC SETTINGS**:

Field	Meaning
Primary Domain Name Server	IP address of X8500 's first global Domain Name Server (DNS).
Secondary Domain Name Server	IP address of another global Domain Name Server.
Primary WINS	IP address of X8500 's first global WINS (Windows Internet Name Server) or NBNS (Net-BIOS Name Server).
Secondary WINS	IP address of another global WINS or NBNS.

Table 5-24: **IP** ► **STATIC SETTINGS**

Relevant field of the menu **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**:

Field	Meaning
Dynamic Name Server Negotiation	In the event of dynamic name server negotiation, defines whether X8500 receives IP addresses for Primary Domain Name Server , Secondary Domain Name Server , Primary WINS and Secondary WINS from the WAN partner or sends them to the WAN partner.

Table 5-25: **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**

The **Dynamic Name Server Negotiation** field contains the following selection options:

Possible values	Meaning
<i>off</i>	X8500 does not send or answer requests for WINS or DNS IP addresses.

Possible values	Meaning
<i>yes</i>	<p>The response is linked to the mode for issuing/receiving an IP address (setting in WAN PARTNER ► EDIT ► IP under IP Transit Network):</p> <ul style="list-style-type: none"> ■ X8500 sends requests for name server addresses to the WAN partner if <i>dynamic client</i> is selected. ■ X8500 answers requests for name server addresses from the WAN partner if <i>dynamic server</i> is selected. ■ X8500 answers but does not send requests for name server addresses if <i>yes</i> or <i>no</i> is selected.
<i>client (receive)</i>	X8500 sends requests for name server addresses to the WAN partner.
<i>server (send)</i>	X8500 answers requests from the WAN partner for name server addresses.

Table 5-26: Dynamic Name Server Negotiation

WINS, DNS in the LAN If you have configured a Domain Name Server or Windows Internet Name Server in your LAN, enter its IP address.

To do Proceed as follows if you have not made this entry already (see [chapter 5.3.2, page 197](#)):

- Go to **IP** ► **STATIC SETTINGS**.
- Enter **Primary** or **Secondary Domain Name Server**, if applicable.
- Enter **Primary** or **Secondary WINS**, if applicable.
- Confirm with **SAVE**.

Proceed as follows if you want **X8500** to report the name server addresses entered to the WAN partner (Server Mode) or if other name server addresses oth-

er than those in the LAN are to be used for connections to the WAN partner (Client Mode, e.g. for dialing in to an Internet Service Provider):

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**.
- Select the desired function for **Dynamic Name Server Negotiation**.
- Confirm with **OK**.
- Confirm with **SAVE**.



If you do not have a Secondary DNS or WINS server, you can enter the IP address of the Primary DNS or WINS server in the **Secondary Domain Name Server** or **Secondary WINS** field again.

This may be necessary for connection to some data communications clients.



If you do not have a Domain Name Server in your LAN (smaller networks often have no DNS of their own), the name resolution can be carried out, for example, via your Internet Service Provider (Client Mode). However, this requires ISDN connections, which involve charges.



If you work with Windows, you can also obtain name resolution without asking for a DNS. To do this, you must adapt the LMHOSTS file on all PCs in the LAN.

5.2.9 Routing Information Protocol (RIP)

Routing Routing can be described as follows: The ➤➤ **router** receives ➤➤ **data packets**, each of which contains data about the destination host. On the basis of the entries in the so-called Routing Table (see "[Creating a Routing Entry](#)", page 115), the router decides which route to use to forward the data packet to ensure that it arrives at its destination as quickly and cheaply as possible (with the fewest possible intermediate stations). The entries in the routing table can be defined statically or the routing table can be updated constantly by a dynamic exchange of routing information between several routers. This exchange is controlled by a so-called Routing Protocol, e.g. RIP (Routing Information Protocol).

RIP Routers use the **➤➤ RIP** to exchange the information stored in their routing tables by communicating with each other at regular intervals to mutually supplement and renew their routing entries. **X8500** supports both version 1 and version 2 of RIP, either exclusively or parallel.

RIP is configured separately for LAN and WAN.

Active and passive Routers can be defined as active or passive routers: Active routers offer their routing entries to other routers via **➤➤ broadcasts**. Passive routers accept the information from the active routers and store it, but do not pass on their own routing entries. **X8500** can do both.

WAN partner If you negotiate to receive and/or send RIP packets from/to your WAN partner, **X8500** can exchange routing information dynamically with the routers in the LAN of the WAN partner.



Receiving routing tables via the RIP is a possible security loophole, as external computers or routers can change **X8500**'s routing functionality.

RIP packets do not set up or hold ISDN connections.

Configuration is made in:

■ **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**

■ **ETH[x]** ➤ **ADVANCED SETTINGS**

Relevant fields of the menu **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS** resp. **ETH[x]** ➤ **ADVANCED SETTINGS**:

Field	Meaning
RIP Send	Enables RIP packets to be sent via the interface to the WAN partner and LAN interface.
RIP Receive	Enables RIP packets to be received via the interface to the WAN partner and LAN interface.

Table 5-27: **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS** or **ETH[x]** ➤ **ADVANCED SETTINGS**

RIP Send and **RIP Receive** contain the following selection options:

Possible values	Meaning
<i>none</i>	Not activated.
<i>RIP V1</i>	Enables sending and receiving of RIP packets in version 1.
<i>RIP V2</i>	Enables sending and receiving of RIP packets in version 2.
<i>RIP V1 + V2</i>	Enables sending and receiving of RIP packets in both version 1 and version 2.

Table 5-28: **RIP Send** and **RIP Receive**

To do Proceed as follows:

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**.
- Select **RIP Send**.
- Select **RIP Receive**.
- Confirm with **OK**.
- Confirm with **SAVE**.
- Confirm with **SAVE** until you return to the main menu.
- Go to **ETH[x]** ➤ **ADVANCED SETTINGS**.
- Select **RIP Send**.
- Select **RIP Receive**.
- Confirm with **SAVE**.

5.2.10 Compression

Data compression You can increase the data throughput and so reduce the connection costs by using **data compression**. **X8500** supports several options, depending on the **encapsulation** selected, e.g. PPP (see [chapter 4.3, page 94](#)):

■ **STAC:**

The industry standard STAC data compression (Check Mode 3 in RFC 1974) implemented in **X8500** can increase the data throughput on the PPP ISDN connections.

■ **MS-STAC:**

STAC data compression for Windows **clients** (Check Mode 4 in RFC 1974). Select this if you dial into a Windows Remote Access Server.

■ **Van Jacobson Header Compression (VJHC):**

Reduces the size of **TCP/IP** packets. Van Jacobson Header Compression can be used in addition to the above-mentioned compression algorithms.



If the far station does not support data compression or its data compression is not activated, **X8500** detects this during the **PPP** negotiation phase and deactivates data compression for this connection.

Configuration is made in:

■ **WAN PARTNER** ► **EDIT**

■ **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**

Relevant field of the menu **WAN PARTNER** ► **EDIT**:

Field	Meaning
Compression	Defines the type of compression for connections to the WAN partner.

Table 5-29: **WAN PARTNER** ► **EDIT**

The **Compression** field contains the following selection options:

Possible values	Meaning
<i>none</i>	No compression.
<i>STAC</i>	Enables STAC data compression (if Encapsulation = PPP).
<i>MS-STAC</i>	Enables STAC data compression for dialing into a Windows Remote Access Server (if Encapsulation = PPP).

Table 5-30: **Compression**

Relevant field of the menu **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**:

Field	Meaning
Van Jacobson Header Compression	Enables VJHC.

Table 5-31: **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**

STAC, MS-STAC Proceed as follows to set STAC or MS-STAC:

- Go to **WAN PARTNER** ► **EDIT**.
- Select the desired **Compression**.
- Confirm with **SAVE**.

VJHC Proceed as follows to set VJHC:

- Go to **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**.
- Activate **Van Jacobson Header Compression: on**.
- Confirm with **OK**.
- Confirm with **SAVE**.
- Confirm with **SAVE**.

- Leave the **WAN** menu with **EXIT**.

You have returned to the main menu. The settings are temporarily saved and activated.

5.2.11 Proxy ARP (Address Resolution Protocol)

ARP requests The ➤➤ **Proxy ARP** function enables **X8500** to answer ➤➤ **ARP** requests from the LAN and from the LAN of defined WAN partners. If a host in the LAN wants to set up a connection to another host in the LAN or to a WAN partner but does not know its hardware address, it sends a so-called ARP request into the network as a ➤➤ **broadcast**. If Proxy ARP is activated in **X8500** and the desired host can be reached over a WAN connection defined as a host route, **X8500** answers the ARP request with its own hardware address. This is sufficient for establishing the connection: The ➤➤ **data packets** are sent to **X8500**, which then forwards them to the desired host.

Diagram of Proxy ARP:

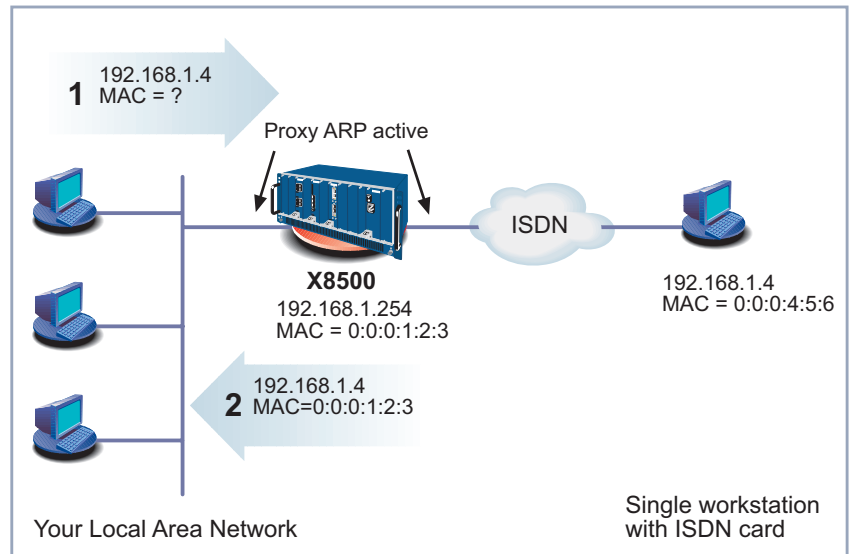


Figure 5-2: Proxy ARP

Configuration is made in:

■ **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**

■ **ETH[x]** ➤ **ADVANCED SETTINGS**

Relevant field in the menu **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS** or **ETH[x]** ➤ **ADVANCED SETTINGS**:

Field	Meaning
Proxy Arp	Enables X8500 to answer ARP requests from its own LAN and from hosts of defined WAN partners.

Table 5-32: **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS** and **ETH[x]** ➤ **ADVANCED SETTINGS**

Proxy Arp in **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS** contains the following selection options:

Possible values	Meaning
<i>off</i>	Disables Proxy ARP for this WAN partner.
<i>on (up or dormant)</i>	X8500 answers an ARP request only if the status of the connection to the WAN partner is <i>up</i> (active) or <i>dormant</i> (idle). In the case of <i>dormant</i> , X8500 only answers the ARP request; the connection is not set up until someone actually wants to use the route.
<i>on (up only)</i>	X8500 answers an ARP request only if the status of the connection to the WAN partner is <i>up</i> (active), i.e. a connection already exists to the WAN partner.

Table 5-33: **Proxy Arp** in **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS** and **ETH[x]** ➤ **ADVANCED SETTINGS**

Proxy Arp in *ETH[x]* ► *ADVANCED SETTINGS* contains the following selection options:

Possible values	Meaning
<i>off</i>	Disables Proxy ARP via the LAN interface.
<i>on</i>	Enables Proxy ARP via the LAN interface.

Table 5-34: **Proxy Arp** in *ETH[x]* ► *ADVANCED SETTINGS*

To do Proceed as follows:

- Go to **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**.
- Select the desired function for **Proxy Arp**.
- Confirm with **OK**.
- Confirm with **SAVE**.
- Confirm with **SAVE**.
- Leave the menu **WAN** with **EXIT**.
- Go to *ETH[x]* ► *ADVANCED SETTINGS*.
- Select the desired function for **Proxy Arp**.
- Confirm with **SAVE**.
- Confirm with **SAVE**.

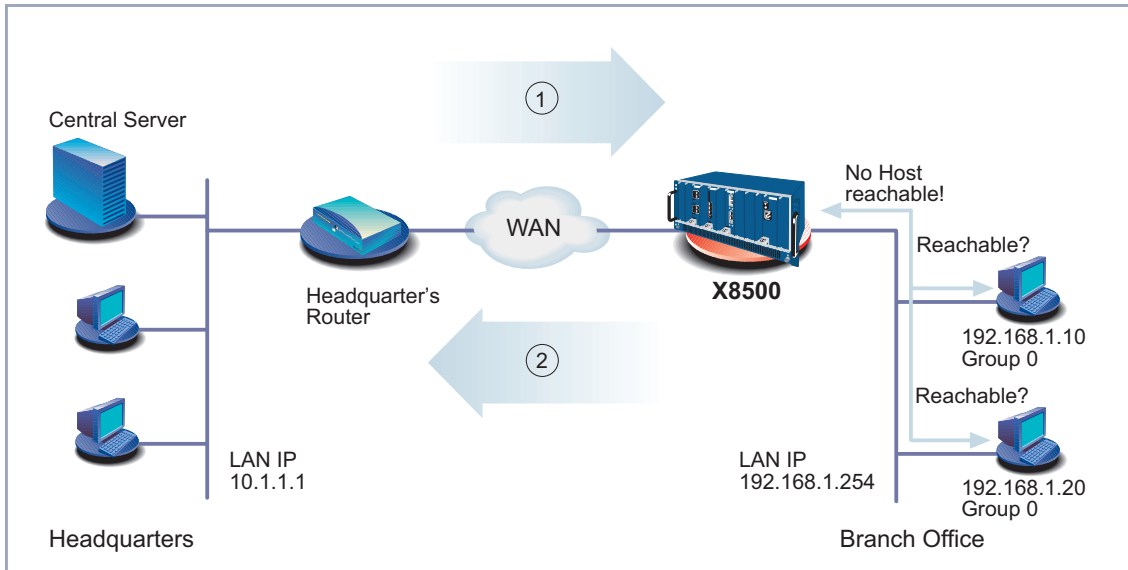
You have returned to the main menu. The settings are temporarily saved and activated.

5.2.12 Keepalive Monitoring

LAN-LAN connection If you have connected two (or more) LANs over a dialup connection, e.g. between the LAN of headquarters and the LAN of a branch office as in [figure 5-3, page 188](#), a central server is frequently located in the LAN at headquarters. If this central server is configured such that it regularly sets up WAN connections to **X8500** in the LAN of the branch office, e.g. for updating data, these connections are superfluous (but unfortunately not free) if none of the hosts in the branch office can be reached, e.g. because all PCs are switched off. As it is not

possible to determine whether the hosts can be reached until the connection is set up, costs are incurred by the calling party, i.e. headquarters.

Diagram of Keepalive Monitoring:



1	Connection setup attempt	2	X8500 is "busy", no connection is possible
---	--------------------------	---	---

Figure 5-3: Keepalive Monitoring

Cutting costs The Keepalive Monitoring function enables to configure **X8500** in the branch office (see [figure 5-3, page 188](#)) to avoid unnecessary WAN connections from headquarters to the branch office. **X8500** checks at regular, adjustable intervals to see whether the hosts to be monitored in the LAN at the branch office can be reached. If none of the hosts to be checked answers a corresponding request after three consecutive attempts, the call from the central server is not accepted by **X8500** in that **X8500** deactivates the interface to headquarters WAN partner. This means that no costs are incurred for a connection, which would have been useless anyway.



In some countries (e.g. Switzerland), costs may still occur for these useless dial-in attempts in spite of using Keepalive Monitoring.

If all PCs in the LAN at the branch office were inactive, a connection to headquarters is not set up automatically as soon as one of the PCs to be monitored is switched on. The interface to headquarters WAN partner is not activated, i.e. a connection cannot be set up to headquarters, until **X8500** has registered that a PC can be reached. The amount of time that expires before **X8500** indicates that a PC can be reached again depends on the monitoring interval set (**Interval**).



The corresponding WAN partner, i.e. the head office (Headquarters, [figure 5-3, page 188](#)), should be identifiable in **X8500** via CLID (Calling Line Identification). If this is not the case, the described benefit of "Keepalive Monitoring" is not available.



Keepalive Monitoring cannot be configured in **X8500** for WAN partners that are authenticated via a RADIUS server!

Configuration is made in **SYSTEM ► KEEPALIVE MONITORING ► ADD**:

Field	Meaning
Group	<p>Defines a group of hosts. X8500 monitors if these hosts are reachable.</p> <p>Each host to be monitored is assigned to a group. A total of ten groups can be configured with up to ten hosts each.</p> <p>Possible values: 0 ... 9</p>
IPAddress	<p>Defines a host that is to be monitored by X8500.</p>

Field	Meaning
Interval	<p>Defines the time interval in seconds to be used for checking if the hosts are reachable (default value: 300 s).</p> <p>The smallest Interval is used within a group.</p>
DownAction	<p>Defines how the status of the X8500 interfaces selected in FirstIndex and Range is set if all hosts in a group are not reachable. Possible values:</p> <ul style="list-style-type: none"> ■ <i>down</i> (default value): Interfaces are deactivated. ■ <i>up</i>: Interfaces are activated. <p>The status of the interfaces is set to the original value again when at least one host in a group can be reached again.</p>
FirstIndex	<p>Defines the first interface of an interface range in X8500, for which the action defined under DownAction is to be executed.</p> <p>Possible values: 10001 ... 15000 (default value: 10001).</p> <p>Interfaces with indices from 10001 to 15000 are provided for dialup connections to WAN partners. The default value 10001 designates the interface to the first WAN partner configured in X8500 (dialup connection). The indices of other interfaces are given in the Software Reference.</p>

Field	Meaning
Range	<p>Defines the range of interfaces in X8500, for which the action defined under DownAction is to be executed.</p> <p>If you set FirstIfIndex = 10001 and Range = 0, only the interface with the index 10001 is affected.</p> <p>If you set FirstIfIndex = 10001 and Range = 4999 (default value), the interfaces with indices 10001 to 15000 are affected.</p>

Table 5-35: **SYSTEM ► KEEPALIVE MONITORING ► ADD**

SYSTEM ► KEEPALIVE MONITORING lists all the hosts that are monitored by Keepalive Monitoring. The reachability of the hosts is listed under **State**: *alive*, if the host was reachable on the last check, *down*, if the host was not reachable.

To do Proceed as follows to configure the example shown in [figure 5-3, page 188](#):

- Go to **SYSTEM ► KEEPALIVE MONITORING**.
- Confirm with **ADD** to add the first host that is to be monitored by **X8500** with Keepalive Monitoring.
- Enter **Group**: 0.
- Enter **IPAddress**: 192.168.1.10.
- Enter **Interval**, e.g. 300.
- Select **DownAction**: *down*.
- Enter **FirstIfIndex**: 10001.
- Type in **Range**: 4999.
- Confirm with **SAVE**.
- Add the second host with **ADD**.
- Enter **Group**: 0.
- Enter **IP Address**: 192.168.1.20.
- Enter **Interval**, e.g. 300.

- Select **DownAction**: *down*.
- Enter **FirstIfIndex**: *10001*.
- Type in **Range**: *4999*.
- Confirm with **SAVE**.
- Leave the menu **SYSTEM** ▶ **KEEPLIVE MONITORING** with **EXIT**.

The settings are temporarily saved and activated.

These settings ensure that **X8500** checks the accessibility of hosts 192.168.1.10 and 192.168.1.20 at intervals of 300 seconds. If neither of the two hosts is reachable after three consecutive attempts, all **X8500** interfaces for dialup connections to WAN partners are deactivated. **X8500** continues to check the hosts at the time interval of 300 seconds and **X8500** activates the interfaces again as soon as at least one host is reachable again.

5.3 Basic IP Settings

Here you will find a number of basic settings you can define in **X8500**:

- Deriving System Time ([chapter 5.3.1, page 193](#))
- Name Resolution (▶▶ **DNS**) in **X8500** ([chapter 5.3.2, page 197](#))
- ▶▶ **Port Numbers** ([chapter 5.3.3, page 214](#))
- ▶▶ **BOOTP** Relay Agent ([chapter 5.3.4, page 215](#))

The necessary configuration steps are explained below.

5.3.1 System Time

System time You need the system time to obtain correct timestamps for recording connection data (for accounting).

You can derive the system time:

- Automatically, e.g. via ISDN or a time server (see "[Deriving the System Time Automatically](#)", page 194).
- By setting it manually in **X8500** (see "[Setting the System Time Manually](#)", page 196).

Deriving the System Time Automatically

Configuration is made in **IP** ► **STATIC SETTINGS**:

Field	Meaning
Time Protocol	<p>Protocol used to derive the current time. Possible values:</p> <ul style="list-style-type: none"> ■ <i>TIME/UDP</i> ■ <i>TIME/TCP</i> ■ <i>SNTP</i> ■ <i>ISDN</i> ■ <i>none</i>
Time Offset (sec)	<p>Number of seconds added to or subtracted from the derived time. If you enter values between -24 and +24, X8500 interprets the input as the number of hours and converts it to the corresponding number of seconds automatically after you confirm with SAVE. Note: If you select <i>ISDN</i> as Time Protocol, you must set the Time Offset to 0.</p> <p>If you change Time Offset (sec) (turn back the time), there should be no data flow.</p>
Time Update Interval (sec)	<p>Time interval in seconds, after which the system time is checked and updated if necessary. If you enter values between 1 and 24, X8500 interprets the input as the number of hours and converts it to the corresponding number of seconds automatically after you confirm with SAVE.</p> <p>For Time Protocol = <i>TIME/UDP</i>, <i>TIME/TCP</i> or <i>SNTP</i>: Current time is checked after every Time Update Interval in seconds.</p> <p>For Time Protocol = <i>ISDN</i>: Current time is checked for each first ISDN connection after expiry of the Time Update Interval.</p>

Field	Meaning
Time Server	IP address of the time server used by X8500 . Time Server is not needed if you set <i>ISDN</i> as Time Protocol .

Table 5-36: **IP** ► **STATIC SETTINGS**

The **Time Protocol** field contains the following selection options:

Possible values	Meaning
<i>TIME/UDP</i>	System time (RFC 868) via ►► UDP .
<i>TIME/TCP</i>	System time (RFC 868) via ►► TCP .
<i>TIME/SNTP</i>	System time as per SNTP (Simple Network Time Protocol, RFC 1769) via UDP.
<i>ISDN</i>	System time from ISDN ►► D-channel (free).
<i>none</i>	System time not derived.

Table 5-37: **Time Protocol**

ISDN Proceed as follows to derive the system time via ISDN:

- Go to **IP** ► **STATIC SETTINGS**.
- Select **Time Protocol**: *ISDN*.
- Enter **Time Offset (sec)**: *0*.
- Enter **Time Update Interval (sec)**, e.g. **86400** (corresponds to 24 hours).
- Confirm with **SAVE**.
X8500 derives the system time over the ISDN when it sets up the first ISDN connection.

Time server Proceed as follows to derive the system time from a time server:

- Go to **IP** ► **STATIC SETTINGS**.
- Select **Time Protocol**, e.g. **TIME/UDP**.

- Enter **Time Offset (sec)**, e.g. **0**.
- Enter **Time Update Interval (sec)**, e.g. **86400** (corresponds to 24 hours).
- Enter, if applicable, IP address or host name for **Time Server**, e.g. **207.46.226.34** (time.windows.de) or **132.187.1.3** (wrzx03.rz.uni-wuerzburg.de).



Bear in mind that a time server that is not in your LAN will cause costs.



The ➤➤ **DIME Tools** contain a time server. If you enter the IP address of your PC for **Time Server**, make sure the time server of **DIME Tools** is active on your PC every time you start **X8500**.



If your computer has no fixed IP address but is assigned its IP address dynamically via ➤➤ **DHCP**, you cannot use your computer as a time server.

- Confirm with **SAVE**.

X8500 now derives the system time via a time server. **X8500** adjusts its system time to the time set on the time server every 24 hours.

Setting the System Time Manually

Configuration is made in **SYSTEM** ➤ **TIME AND DATE**:

Field	Meaning
Time is currently controlled by:	Shows the settings defined under IP ➤ STATIC SETTINGS for deriving the time automatically.
Current Time:	Shows the system time currently set in X8500 (date and time).
New Time:	For entering the new time to be used by X8500 (hours:minutes).

Field	Meaning
New Date:	For entering the new date to be used by X8500 (month/day/year).

Table 5-38: **SYSTEM** ► **TIME AND DATE**

Proceed as follows to enter the system time in **X8500** manually:



If a method for deriving the time automatically is also defined in **X8500**, the values obtained automatically have higher priority. That is, if **X8500** receives a relevant time signal (e.g. from a time server), any system time entered manually is overwritten.

- Go to **SYSTEM** ► **TIME AND DATE**.
- Enter **New Time**.
- Enter **New Date**.
- Confirm the new system time with **SET**.

Current Time: shows the new system time set in **X8500**.

5.3.2 Name Resolution in **X8500** with DNS Proxy

Why Name Resolution?

IP address = ? Name resolution is necessary for converting host names in a LAN or on the Internet into IP addresses. For example, if you would like to reach the host "Goofy" in your LAN (e.g. with `telnet` and `ping`) or enter the ►► **URL** "`http://www.bintec.net`" in your Internet browser, you need the associated IP address before you can set up the required connection. The following options are available:

- **DNS (Domain Name Server):**
A DNS stores the relevant IP addresses for host names in the form of DNS records and resolves the names if a relevant request is received, i.e. the name server sends a DNS record with the IP address associated with the name to the source of the request. Name servers form a hierarchical tree

structure. If a name server cannot resolve a name, it therefore asks a higher-order name server, etc.

■ **HOSTS files:**

HOSTS files are located on the PCs in the LAN. You can use these files to create a table of host names with the associated addresses. This means connections to DNS are no longer needed to resolve these names. As the HOSTS files must be updated on each PC, this method of name resolution is not very practicable.

In practice, the DNS of the Internet Service Provider is often used for name resolution.

Advantages of Name Resolution with X8500

X8500 has the following functions and facilities for name resolution (port 53):

- DNS Proxy, for passing DNS requests to the right DNS
- DNS cache, for saving the results of DNS requests
- Static name entries, for defining assignments of names to IP addresses
- Filter function, to prevent the resolution of certain names
- Monitoring via Setup Tool, to provide an overview of DNS requests in **X8500**

DNS Proxy DNS Proxy makes the tedious updating of HOSTS files on PCs in the LAN unnecessary, as you can enter **X8500** as DNS on the relevant PCs. DNS requests are passed by the PC to **X8500** for processing. The configuration of the PCs in the LAN is then easy and can also be left at provider changes. This also works if the PCs in the LAN do not have any static DNS entries, but are assigned these dynamically by **X8500** as DHCP server.

Forwarding entries enable **X8500** to decide which DNS is to be used for the resolution of certain names. If you have configured two WAN partners in **X8500**, your head office and your Internet Service Provider, it is advisable to have Internet names resolved by the DNS of your ISP, but names from within the corporate network by the DNS of the head office. A DNS request for resolution of an internal company address usually cannot be answered by the DNS of the ISP and is thus superfluous, causes unnecessary costs and resolution takes

longer than necessary. A forwarding entry, which passes DNS requests for names such as "*.intranet.de" to the WAN partner "head office", is therefore advisable.

DNS cache If a DNS request is passed by **X8500** to a DNS and this DNS answers with a DNS record, the resolved name is saved with the associated IP address as a positive dynamic entry in the DNS cache of **X8500**. This means that once a name has been resolved and is required again, **X8500** can answer the request from the cache and a new request to an external name server is not necessary. These requests can therefore be answered more quickly, bandwidth is reduced on the WAN connections and the costs of unnecessary connections are saved.

If a DNS request cannot be answered by any of the DNS asked, this is saved in the cache as a negative dynamic entry. As failed DNS requests (requests that cannot be answered) are not usually saved by applications or IP stacks, these negative dynamic entries in the cache prevent frequent unsuccessful connection setups to external DNS.

The validity of the positive dynamic entries in the cache is given by the TTL (Time To Live), which is contained in the DNS record. Negative entries are assigned the value **Maximum TTL for Neg Cache Entries**. A dynamic entry is deleted from the cache when the TTL expires.

Static name entries You use positive static entries to enter names with the associated IP addresses in **X8500**. If you save frequently needed IP addresses in this way, **X8500** can answer relevant DNS requests itself and the connection to an external name server is not necessary. This speeds up access to these addresses. For a small network, such a name server can be configured in **X8500**. The installation of a separate DNS and the tedious updating of HOSTS files on the PCs in the LAN is not necessary.

With negative static entries, a name is not assigned an IP address, a corresponding DNS request is answered negatively and not passed to any other name server either.



You can change a dynamic entry to a static entry in **IP** ► **DNS** ► **DYNAMIC CACHE** (see [table 5-43, page 208](#)).

Filter function By using negative static entries, you can limit name resolution in **X8500** using a filter function. This makes access to certain domains much more difficult for users in the LAN, as it prevents the corresponding names being resolved. You can use wildcards (*) when entering the name.

When you enter a static entry, you define how long this assignment of name and IP address is valid by setting the TTL. This TTL is entered in each DNS record with which **X8500** answers a relevant DNS request.



Make sure your static entries are always up to date. Names or IP addresses can change at any time!

Monitor function Which IP addresses are requested by hosts in the LAN and how often?

The Setup Tool permits rapid access to this and other statistical information. You can also use the `nslookup` command in the command line (SNMP shell) to check how a name or an IP address is resolved by **X8500** or another name server (see [chapter 10.1, page 386](#)). To obtain help information for the command, enter `nslookup -?`.

Other Options

Global name server In **IP ► STATIC SETTINGS**, you can also enter the IP address of preferred global name servers that are to be asked if **X8500** cannot answer requests itself or with forwarding entries.

For local applications, the IP address of **X8500** or the loopback address (127.0.0.1) can be entered as global name server.

If necessary, **X8500** can send or receive the addresses of name servers to and from WAN partners.

Default interface In **Default Interface**, you can also select a WAN partner to whom a connection is set up as standard for name server negotiation if name resolution was not successful using the methods already stated.

Exchanging DNS Addresses with LAN Partners

DHCP If **X8500** is configured as DHCP server, DHCP clients in the LAN can be sent IP addresses from name servers. In this case, the addresses of the global name servers entered in **X8500** can be sent or the address of **X8500** itself. In the latter case, DNS requests from the DHCP clients are sent to **X8500**, which either answers these itself or passes them on if necessary (proxy function).

Exchanging DNS Addresses with WAN Partners

IP Control Protocol (IPCP) The same applies if the dynamic negotiation of name servers is activated for the IP configuration of a WAN partner and **X8500** is operating in Server Mode (**Dynamic Name Server Negotiation = server (send)**). In this case, the addresses of the global name servers or the address of **X8500** itself can also be sent for name server negotiations via IPCP to the WAN partner, who is the IP address client.

If **X8500** is operating in Client Mode (**Dynamic Name Server Negotiation = client (receive)**), name server addresses can if necessary be negotiated with the WAN partner, who is the IP address server, and sent to **X8500**. These can be entered as global name servers in **X8500** and are thus available for future name resolutions.

Strategy for Name Resolution in X8500

A DNS request is handled by **X8500** as follows:

1. Can the request be answered directly from the static or dynamic cache (IP address or negative answer)?
 - If yes, the information is forwarded.
 - If no, see 2.
2. Is a matching forwarding entry available?

In this case, the relevant DNS are asked. If the connection to the WAN partner is not active, an attempt is made to set it up.

 - If a DNS can resolve the name, the information is forwarded and a dynamic entry created in the cache.
 - If none of the DNS asked can resolve the name or no matching forwarding entry is available, see 3.

3. Are global name servers entered?
In this case, the relevant DNS are asked. If the IP address of **X8500** or the loopback address is entered for local applications, these are ignored here.
 - If a DNS can resolve the name, the information is forwarded and a dynamic entry created in the cache.
 - If none of the DNS asked can resolve the name or no static name servers are entered, see 4.
4. Is a WAN partner selected as default interface?
In this case, the associated DNS are asked. If the connection to the WAN partner is not active, an attempt is made to set it up.
 - If a DNS can resolve the name, the information is forwarded and a dynamic entry created in the cache.
 - If none of the DNS asked can resolve the name or no default interface has been selected, see 5.
5. Is overwriting the global name server addresses admissible (**Overwrite Global Nameserver = yes**)?
In this case, a connection is set up to the first WAN partner, which is configured so that addresses of DNS can be sent – provided this has not previously been attempted. If name server negotiation is successful, these are entered as global name servers and are therefore available for further requests.
6. Request is answered with server error.



If one of the DNS answers with "non-existent domain", this answer is forwarded to the source of the request immediately and included in the cache as negative entry.

Overview of Configuration with the Setup Tool

The configuration and monitoring of name resolution in **X8500** is set in the menus:

- **IP** ▶ **STATIC SETTINGS**
- **IP** ▶ **DNS**
- **IP** ▶ **DNS** ▶ **STATIC HOSTS**

- **IP** ► **DNS** ► **FORWARDED DOMAINS**
- **IP** ► **DNS** ► **DYNAMIC CACHE**
- **IP** ► **DNS** ► **ADVANCED SETTINGS...**
- **IP** ► **DNS** ► **GLOBAL STATISTICS...**
- **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**

The relevant fields of the menu **IP** ► **STATIC SETTINGS**:

Field	Meaning
Domain Name	Defines X8500 's Domain Name.
Primary Domain Name Server	IP address of X8500 's first global Domain Name Server (DNS).
Secondary Domain Name Server	IP address of another global Domain Name Server.
Primary WINS	IP address of X8500 's first global WINS (Windows Internet Name Server) or NBNS (Net-BIOS Name Server).
Secondary WINS	IP address of another global WINS or NBNS.

Table 5-39: **IP** ► **STATIC SETTINGS**

IP ► **DNS** contains the following fields:

Field	Meaning
Positive Cache	<p>Enables positive dynamic entries in the cache. Possible values:</p> <ul style="list-style-type: none"> ■ <i>enabled</i> (default value): Successfully resolved names and IP addresses are saved in the cache. ■ <i>flush</i>: All positive dynamic entries in the cache are deleted.

Field	Meaning
Continuation of Positive Cache	<ul style="list-style-type: none"> ■ <i>disabled</i>: Successfully resolved names and IP addresses are not saved in the cache and existing dynamic positive entries are deleted (static entries are not deleted).
Negative Cache	<p>Enables negative dynamic entries in the cache. Possible values:</p> <ul style="list-style-type: none"> ■ <i>enabled</i> (default value): Names that could not be resolved are saved in the cache as negative entries. ■ <i>flush</i>: All negative dynamic entries in the cache are deleted. ■ <i>disabled</i>: Names that could not be resolved are not saved in the cache and existing dynamic negative entries are deleted (static entries are not deleted).
Overwrite Global Nameservers	<p>Defines whether the addresses of global name servers in X8500 (in IP ► STATIC SETTINGS) may be overwritten with name server addresses sent by WAN partners. Possible values:</p> <ul style="list-style-type: none"> ■ <i>yes</i> (default value) ■ <i>no</i>
Default Interface	<p>Defines the WAN partner to which a connection is set up for name server negotiation if other name resolution attempts were not successful.</p>
DHCP Assignment	<p>Defines which name server addresses are sent to the DHCP client if X8500 is configured as DHCP server. Possible values:</p> <ul style="list-style-type: none"> ■ <i>none</i>: No name server address is sent.

Field	Meaning
Continuation of DHCP Assignment	<ul style="list-style-type: none"> ■ <i>self</i> (default value): The address of X8500 is sent as name server address. ■ <i>global</i>: The addresses of the global name servers entered in X8500 are sent.
IPCP Assignment	<p>Defines which name server addresses are sent by X8500 to a WAN partner for dynamic name server negotiation. Possible values:</p> <ul style="list-style-type: none"> ■ <i>none</i>: No name server address is sent. ■ <i>self</i>: The address of X8500 is sent as name server address. ■ <i>global</i> (default value): The addresses of the global name servers entered in X8500 are sent.
Static Hosts	The number of static entries is displayed in brackets.
Forwarded Domains	The number of forwarding entries is displayed in brackets.
Dynamic Cache	The number of positive and negative dynamic entries in the DNS cache is displayed in brackets.

Table 5-40: **IP** ➤ **DNS**

IP ➤ **DNS** ➤ **STATIC HOSTS** ➤ **ADD** contains the following fields:

Field	Meaning
Default Domain:	The Domain Name of X8500 entered in IP ➤ STATIC SETTINGS is displayed.

Field	Meaning
Name	<p>Host name, which is assigned the Address with this static entry. May also contain wild-cards (*) (only at the start of Name, e.g. *.bin-tec.de).</p> <p>If an incomplete name is entered without a dot, this is completed with ".Default Domain" after confirming with SAVE.</p>
Response	<p>Defines the type of static entry. Possible values:</p> <ul style="list-style-type: none"> ■ <i>positive</i> (default value): A DNS request for Name is answered with a DNS record, which contains the associated Address. ■ <i>ignore</i>: A DNS request is ignored; no answer is given (not even a negative answer). ■ <i>negative</i>: A DNS request for Name is answered with a negative answer.
Address	<p>(Only for Response = <i>positive</i>)</p> <p>IP address, which is assigned to Name.</p>
TTL	<p>Period of validity in seconds for the assignment of Name to Address (only relevant for Response = <i>positive</i>). This value is displayed in the TTL field (Time To Live) if X8500 sends a corresponding DNS record.</p> <p>Default value: <i>86400</i> (= 24 h)</p>

Table 5-41: **IP** ➤ **DNS** ➤ **STATIC HOSTS** ➤ **ADD**

IP ➤ **DNS** ➤ **FORWARDED DOMAINS** ➤ **ADD** contains the following fields:

Field	Meaning
Global Nameservers:	The global name servers entered in IP ➤ STATIC SETTINGS are displayed.

Field	Meaning
Default Interface:	The interface of X8500 entered in the menu IP ► DNS . Only displayed if you did not enter a name server in the menu IP ► STATIC SETTINGS .
Default Domain:	The Domain Name of X8500 entered in IP ► STATIC SETTINGS is displayed.
Name	Host name that is to be resolved with this forwarding entry. May also contain wildcards (only at the start of Name , e.g. *.bintec.de). If an incomplete name is entered without a dot, this is completed with " Default Domain " after confirming with SAVE .
Interface	Defines the WAN partner to which a connection is set up for the resolution of Name .
TTL	Period of validity in seconds for the assignment of Name to Address . Default value: 86400 (= 24 h) If the request of X8500 for Name is answered with a DNS record, this contains a TTL field (= Time To Live in seconds), whose value is not normally changed by X8500 on forwarding the DNS record. If the TTL field received has the value 0 or exceeds Maximum TTL for Pos Cache Entries , then TTL is also sent with the DNS record forwarded.

Table 5-42: **IP ► DNS ► FORWARDED DOMAINS ► ADD**

IP ► DNS ► DYNAMIC CACHE contains the following fields:

Field	Meaning
Name	Host name, which is assigned the Address with this dynamic entry in the cache.

Field	Meaning
Address	IP address, which is assigned to Name .
Resp	<p>Defines the type of dynamic entry. Possible values:</p> <ul style="list-style-type: none"> ■ <i>positive</i>: A DNS request for Name is answered with the associated IP address from the cache. ■ <i>negative</i>: A DNS request for Name is answered with a negative answer from the cache.
TTL	<p>Indicates how many seconds the dynamic entry remains in the cache. The entry is deleted on expiry of TTL.</p> <p>When a positive dynamic entry is saved in the cache, the value of the TTL field (= Time To Live in s) contained in the DNS record is used. If the TTL field in the DNS record is set to 0 or exceeds Maximum TTL for Pos Cache Entries, the value Maximum TTL for Pos Cache Entries is used when saving the entry.</p> <p>When a negative dynamic entry is saved in the cache, Maximum TTL for Neg Cache Entries is always assigned as this value.</p>
Ref	Indicates how often the entry has been referenced, i.e. how often a DNS request has been answered with the entry from the cache.
STATIC	<p>A dynamic entry can be converted to a static entry by tagging the entry with the Space bar and confirming with STATIC. The relevant entry then disappears from IP ► DNS ► DYNAMIC CACHE and is listed in IP ► DNS ► STATIC HOSTS. TTL is transferred in this operation.</p>

Table 5-43: **IP ► DNS ► DYNAMIC CACHE**

IP ► **DNS** ► **ADVANCED SETTINGS...** contains the following fields:

Field	Meaning
Maximum Number of DNS Records	<p>Defines the maximum number of static and dynamic entries.</p> <p>Once this value is reached, an older dynamic entry is deleted from the cache when a new entry is added. The entry deleted is always the dynamic entry that has not been requested for the longest period of time.</p> <p>If Maximum Number of DNS Records is reduced by the user, dynamic entries are also deleted, if necessary.</p> <p>Static entries are not deleted; Maximum Number of DNS Records cannot be set lower than the current number of existing static entries. If Maximum Number of DNS Records corresponds to the number of static entries, no further dynamic entries are possible!</p>
Maximum TTL for Pos Cache Entries	<p>Is assigned to a positive dynamic entry in the cache as TTL if the field of the DNS record has the value 0 or exceeds Maximum TTL for Pos Cache Entries.</p>
Maximum TTL for Neg Cache Entries	<p>Is assigned as TTL to a negative dynamic entry in the cache.</p>

Table 5-44: **IP** ► **DNS** ► **ADVANCED SETTINGS...**

IP ► **DNS** ► **GLOBAL STATISTICS...** contains the following fields (the menu is updated every second):

Field	Meaning
Received DNS Packets	<p>Displays the number of received DNS packets, including the answer packets for forwarded requests.</p>

Field	Meaning
Invalid DNS Packets	Displays the number of invalid DNS packets received.
DNS Requests	Displays the number of correct DNS requests received.
Cache Hits	Displays the number of requests that could be answered with static or dynamic entries from the cache.
Forwarded Requests	Displays the number of requests forwarded to other name servers.
Cache Hitrate (%)	Displays the number of Cache Hits per DNS Request in %.
Successfully Answered Queries	Displays the number of successful requests (positive and negative) answered.
Server Failures	Displays the number of requests that could not be answered by any name server (either positively or negatively).

Table 5-45: *IP ► DNS ► GLOBAL STATISTICS...*

The following part of *WAN PARTNER ► EDIT ► IP ► ADVANCED SETTINGS* is of interest for this configuration step:

Field	Meaning
Dynamic Name Server Negotiation	In the event of dynamic name server negotiation, defines whether X8500 receives IP addresses for Primary Domain Name Server , Secondary Domain Name Server , Primary WINS and Secondary WINS from the WAN partner or sends them to the WAN partner.

Table 5-46: *WAN PARTNER ► EDIT ► IP ► ADVANCED SETTINGS*

The **Dynamic Name Server Negotiation** field contains the following selection options:

Possible values	Meaning
<i>off</i>	X8500 does not send or answer requests for name server addresses.
<i>yes</i>	<p>The response is linked to the mode for issuing/receiving an IP address (setting in WAN PARTNER ► EDIT ► IP under IP Transit Network):</p> <ul style="list-style-type: none"> ■ X8500 sends requests for name server addresses to the WAN partner if <i>dynamic client</i> is selected. ■ X8500 answers requests for name server addresses from the WAN partner if <i>dynamic server</i> is selected. ■ X8500 answers but does not send requests for name server addresses if <i>yes</i> or <i>no</i> is selected.
<i>client (receive)</i>	X8500 sends requests for name server addresses to the WAN partner.
<i>server (send)</i>	X8500 answers requests from the WAN partner for name server addresses.

Table 5-47: Dynamic Name Server Negotiation

Procedure for Configuration with the Setup Tool

Name resolution in X8500 How to configure name resolution with DNS Proxy in **X8500** is described below.

To do If applicable, first enter the global name servers in **X8500**:

- Go to **IP** ► **STATIC SETTINGS**.
- Enter **Domain Name**, e.g. *mycompany.com*.

- Enter **Primary** or **Secondary Domain Name Server**, if applicable.
- Enter **Primary** or **Secondary WINS**, if applicable.



If you do not have a Secondary DNS or Secondary WINS, you can enter the IP address of the Primary DNS or WINS in the **Secondary Domain Name Server** or **Secondary WINS** a second time.

This may be necessary for connection to some data communications clients.

- Confirm with **SAVE**.

Activate or deactivate the cache function and define general settings for DNS Proxy:

- Go to **IP** ➤ **DNS**.
- Select **Positive Cache** and **Negative Cache**, e.g. **enabled**.
- Select **Overwrite Global Nameservers**, e.g. **yes**, if you do not wish to enter any static global name servers under **IP** ➤ **STATIC SETTINGS**.
- Select **DHCP Assignment**, e.g. **self**.
- Select **IPCP Assignment**, e.g. **global**.

Define the values for the static and dynamic entries:

- Go to **IP** ➤ **DNS** ➤ **ADVANCED SETTINGS...**
- Enter **Maximum Number of DNS Records**.
- Enter **Maximum TTL for Pos Cache Entries**.
- Enter **Maximum TTL for Neg Cache Entries**.
- Confirm with **SAVE**.

How to create static entries:

- Go to **IP** ➤ **DNS** ➤ **STATIC HOSTS**.
All the existing static entries are listed here.
- You can create a new entry with **ADD**.
- Enter **Name**.
- Select **Response**.
- Enter **Address**, if applicable.

- Enter **TTL**.
- Confirm with **SAVE**.
- Leave the menu **IP** ➤ **DNS** ➤ **STATIC HOSTS** ➤ **ADD** with **EXIT**.

How to create forwarding entries:

- Go to **IP** ➤ **DNS** ➤ **FORWARDED DOMAINS**.
All the existing forwarding entries are listed here.
- You can create a new entry with **ADD**.
- Enter **Name**.
- Select **Interface**.
- Enter **TTL**.
- Confirm with **SAVE**.
- Leave the menu **IP** ➤ **DNS** ➤ **FORWARDED DOMAINS** ➤ **ADD** with **EXIT**.
- Confirm with **SAVE**.
- Leave the menu **IP** with **EXIT**.
You have returned to the main menu. The settings are temporarily saved and activated.

Activate DNS negotiation

Proceed as follows if you would like to configure a WAN partner so that the address of a name server is sent from **X8500** to the WAN partner or from the WAN partner to **X8500** as applicable:

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**.
- Select the desired function for **Dynamic Name Server Negotiation**.
- Confirm with **OK**.
- Confirm with **SAVE**.
You have returned to the menu **WAN PARTNER** ➤ **EDIT**.
- Confirm with **SAVE**.
- Leave the menu **WAN** with **EXIT**.

You have returned to the main menu. The settings are temporarily saved and activated.

Monitoring and statistics

How to obtain a list of dynamic entries in the cache:

- Go to **IP** ➤ **DNS** ➤ **DYNAMIC CACHE**.

This menu contains a list of all the dynamic entries in the cache.

- To convert a dynamic entry into a static entry, tag the entry with the **Space** bar and confirm with **STATIC**.

The entry disappears from the list of dynamic entries and is listed as a static entry under **IP** ➤ **DNS** ➤ **STATIC HOSTS**.

How to obtain a list of static parameters:

- Go to **IP** ➤ **DNS** ➤ **GLOBAL STATISTICS...**

Here you will find some statistics for DNS Proxy.

5.3.3 Port Numbers

What is a ➤➤ port?

X8500 has a number of services or applications, e.g. HTTP, ➤➤ **telnet**. To be able to reach several services on the same host and as it were to enter an exact destination for the IP packet within the host, a port is also entered in addition to the IP address for a connection to **X8500**. This addresses the relevant service. Ports are only used in the TCP and UDP protocols.

X8500 forwards incoming ➤➤ **data packets** to the port with the number associated with the desired application. This addresses the relevant **X8500** application and the incoming data can be processed.



As the default settings are usually applicable, you should only make changes here if necessary.

You can define important port numbers in **IP** ➤ **STATIC SETTINGS**:

Field	Meaning
Remote CAPI Server TCP Port	Port number for ➤➤ Remote CAPI connections: 2662 (defined by IANA, www.iana.com).

Field	Meaning
Remote TRACE Server TCP Port	Port number for TRACE Requests. Default value: 7000.
RIP UDP Port	Port number for ▶▶ RIP (Routing Information Protocol). Default value: 520. The RIP can be disabled with RIP UDP Port = 0 .

Table 5-48: **IP ▶ STATIC SETTINGS**

To do Proceed as follows to change one of the port numbers:

- ▶ Go to **IP ▶ STATIC SETTINGS**.
- ▶ Enter **Remote CAPI Server TCP port**, **Remote TRACE Server TCP port**, **RIP UDP port** and/or **HTTP TCP port**.
- ▶ Confirm with **SAVE**.
The port numbers are changed.

5.3.4 BOOTP Relay Agent

Bootstrap protocol The Bootstrap Protocol (**▶▶ BOOTP**) defines how a host (**BOOTP ▶▶ client**) in a TCP/IP network receives his IP address and other configuration information on booting. The BOOTP client sends a BOOTP Request, a BOOTP server answers the request with a BOOTP Response and supplies the client with the necessary information. As the server only hears requests from the LAN in which it is located, it is sometimes advisable to set up a BOOTP Relay Agent. The agent forwards all requests and responses between the client and server via a WAN connection to this server.

Following a diagram:

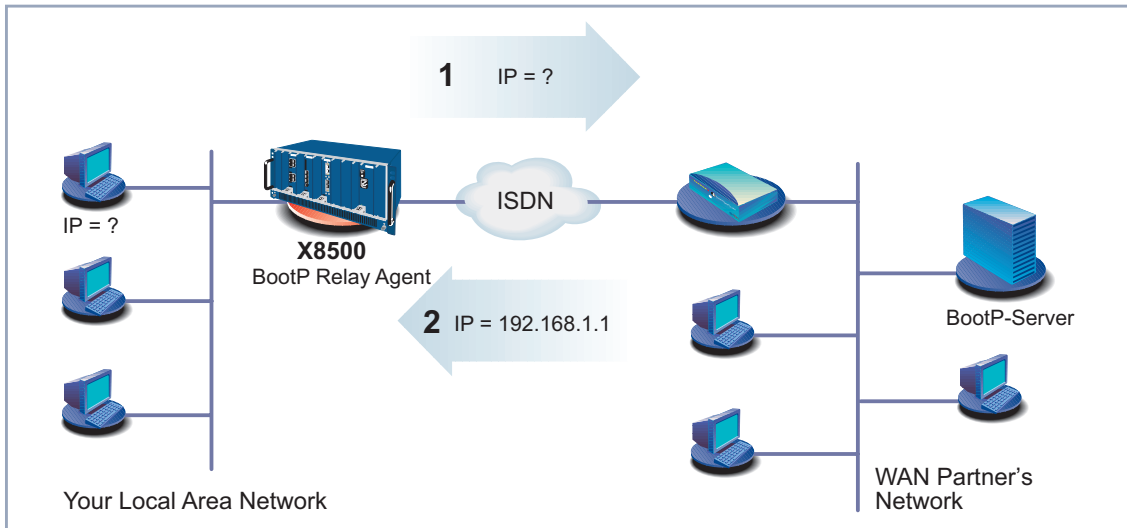


Figure 5-4: **X8500** as BOOTP Relay Agent

Configuration is made in **IP** ➤ **STATIC SETTINGS**:

Field	Meaning
BOOTP Relay Server	IP address of the BOOTP server.

Table 5-49: **IP** ➤ **STATIC SETTINGS**

To do Proceed as follows:



If a WAN connection is needed for the connection between the BOOTP server and BOOTP client, you must configure an appropriate WAN partner ([chapter 4.3, page 94](#)).

- Go to **IP** ➤ **STATIC SETTINGS**.
- Enter the IP address of **BOOTP Relay Server**.
- Confirm with **SAVE**.

- ▶ Leave the menu *IP* with **EXIT**.
X8500 is configured as BOOTP Relay Agent. You have returned to the main menu. The settings are temporarily saved and activated.

5.4 Quality of Service

What is QoS? The increased load on the Internet and Intranet and the tendency towards converging voice data networks makes intelligent bandwidth management essential. Quality of Service enables existing bandwidths to be intelligently and effectively controlled, reserved as necessary and assigned to the various services. It involves the following:

- Avoiding congestion in network segments and WAN paths
- Minimizing the losses of IP packets
- Optimizing the delay (latency) for certain services



You should always use a three-stage process to implement IP QoS: First identify and quantify the traffic flows in your network segments so that you can then assign bandwidths according to the requirements of certain applications and assign priorities to users.

QoS at BinTec **X8500** offers QoS support for the IP protocol family with the Quality of Service feature. The QoS is processed in line with the "Differentiated Services Model", i.e. based on an IP packet classification (service code). The classification – using a set of rules (see also [chapter 7.2.8, page 315](#)) – specifies the IP packets of certain services via IP filters and divides them into packet classes. The classification is interface-specific and can be carried out on both LAN and WAN interfaces. The classified IP packets are assigned a priority. The priority assignment, which is based on configurable strategies (policies), is currently restricted to WAN interfaces and is also carried out for each interface.

A router can use signaling at packet level to inform the adjacent devices that certain data is to be given special handling. This signaling involves tagging previously defined IP packets in the TOS field in the IP header. QoS signaling is useful for coordinating the data traffic determined by QoS functions. The successful end-to-end configuration of network-wide QoS depends mainly on the signaling.

Advantages Quality of Service offers the following advantages:

- Time-critical data (e.g. VoIP) over WAN interfaces can be handled with priority (high-priority class). A special algorithm reduces the latency of such

packets on comparatively slow PPP connections (MLPPP Interleave, see ["Multilink PPP \(MLPPP\)", page 230](#)).

- Traffic flows can be divided into as many as 255 subclasses of the normal priority class and handled differentially.
- It is possible to reserve bandwidth for certain IP packets (services) (this is called traffic shaping).
- Congestion management: Congestion is detected and cleared by various queuing algorithms (PQ, WRR, WFQ, see ["Algorithms", page 228](#)).
- Congestion avoidance: Congestion (TCP flows only) can be avoided by "Random Early Detection". This reduces packet losses especially in cases of exceeding the permissible bandwidth for a short time (see ["Congestion avoidance", page 229](#)).

Configuration Overview

The configuration is set in the **QoS** menu:

```

X8500 Setup Tool                               BinTec Communications AG
[QoS]: QoS Configuration                        MyX8500

                                         IP Filter
                                         IP Classification and Signaling

                                         Interfaces and Policies

                                         Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter

```



You should always use a three-stage process to implement IP QoS: First identify and quantify the traffic flows in your network segments so that you can then assign priorities according to the requirements of certain applications or users.

The IP filters are defined in the submenu **QoS** ➔ **IP FILTER** to enable certain IP packets or services to be specified. The procedure for this corresponds to the procedure for the access lists described in [chapter 7.2.8, page 315](#).

Use the submenu **QoS** ➤ **IP CLASSIFICATION AND SIGNALING** to create the rule chains for classifying the IP packets using the previously defined IP filters. In this way, several IP filters can be interlinked and the traffic flow divided into various packet classes. Totally different types of IP packets can also be combined in a packet class and then handled with the same priority. The signaling in the TOS field for other network components (e.g. switches) is also defined by these rule chains.

Define the interface and rule chain that are to be classified in the submenu **QoS** ➤ **INTERFACES AND POLICIES**. For example, all incoming packets could be checked and classified on the Ethernet (en1) and all outgoing packets on a WAN connection.

You can also make the following settings for one or more WAN interfaces:

- Queuing strategy (PQ, WRR, WFQ, etc.) in the menu **QoS** ➤ **INTERFACES AND POLICIES** ➤ **EDIT** ➤ **QoS SCHEDULING AND SHAPING**
- Bandwidth limitations and reservations in the menu **QoS** ➤ **INTERFACES AND POLICIES** ➤ **EDIT** ➤ **CLASS-BASED QoS POLICIES** ➤ **ADD**
- Congestion avoidance strategies like RED in the menu **QoS** ➤ **INTERFACES AND POLICIES** ➤ **EDIT** ➤ **CLASS-BASED QoS POLICIES** ➤ **ADD**
- Currently only possible on single-link connections (not with channel bundling): MLPPP interleave processes for reducing the latency of high-priority packets on slow WAN connections in the menu **QoS** ➤ **INTERFACES AND POLICIES** ➤ **EDIT**

5.4.1 Defining IP Filters

Proceed as follows to define IP filters:



You will find a detailed description for defining filters in [chapter 7.2.8, page 315](#).

➤ Go to **QoS** ➤ **IP FILTER** ➤ **ADD**.

- Define filters as described in [chapter 7.2.8, page 315](#) and [chapter 7.2.9, page 328](#).
- Continue with [chapter 5.4.2, page 221](#).

5.4.2 Classification and (TOS) Signaling

In the classification process, the IP packets previously specified by filters are assigned either a "high-priority" or "normal" class. The latter can be further subdivided into as many as 255 subclasses using a "class ID". It is then possible for each of these subclasses (interface-specific) to define exactly how the packets are to be handled in case of congestion (policy).

A maximum packet rate can be defined for TOS signaling. Packets that would cause this rate to be exceeded are not manipulated, but preferably discarded in the event of congestion, provided they do not belong to the high-priority packet class.

The classification and (TOS) signaling are defined in the menu **QoS ➤ IP CLASSIFICATION AND SIGNALING ➤ ADD** or **QoS ➤ IP CLASSIFICATION AND SIGNALING ➤ EDIT**:

X8500 Setup Tool		BinTec Communications AG	
[QOS][CLASS][ADD]:Configure IP QoS Classification and Signaling		MyX8500	
Index	1		
Filter	test		
Direction	incoming		
Action	classify M		
Classification> Signaling (TOS)>			
Insert behind Rule	NONE		
	SAVE		CANCEL
Use <Space> to select			

Fields of menu **QoS** ► **IP CLASSIFICATION AND SIGNALING** ► **ADD**:

Field	Meaning
Index	Cannot be changed. X8500 automatically issues a number to new rules defined here or displays the Index of existing rules.
Insert behind Rule	Appears only if a new rule is defined. Defines the rule behind which the new rule is inserted. You start a new independent chain with <i>none</i> .
Filter	IP filter used.
Direction	Direction of data packets checked against the filter conditions to apply the rule accordingly. Possible values: <ul style="list-style-type: none"> ■ <i>incoming</i>: incoming data packets ■ <i>outgoing</i>: outgoing data packets ■ <i>both</i>: incoming and outgoing data packets
Action	Defines the action to be taken for a filtered data packet (see table 5-51, page 223).
Classification	This submenu is used to assign classifications to the IP packets that match the filter conditions (see table 5-52, page 223).
Signaling (TOS)	This submenu is for defining a new value, if applicable, for the TOS field that defines the IP packets that match the filter conditions. This signals in the network that these IP packets must be given special handling (see table 5-53, page 224).
Next Rule	Appears only if an existing rule is edited. Defines the next rule to be used.

Table 5-50: **QoS** ► **IP CLASSIFICATION AND SIGNALING** ► **ADD**

The **Action** field contains the following selection options:

Possible Values	Meaning
<i>disable</i>	Rule is deactivated. Continue with next rule, if available.
<i>classify M</i>	Classify IP packet if it matches the filter.
<i>classify !M</i>	Classify IP packet if it does not match the filter.

Table 5-51: **Action**

The submenu **QoS ► IP CLASSIFICATION AND SIGNALING ► EDIT/ADD ► CLASSIFICATION** contains the following selection options:

Field	Meaning
Class Type	Defines Class Type for the IP packets that match the filter conditions. The QoS policies refer to Class Type . Possible values: <ul style="list-style-type: none"> ■ <i>normal</i> ■ <i>high priority</i>
Class ID	Can only be set if <i>normal</i> has been selected as Class Type . Possible values: <i>1 to 255</i> .

Table 5-52: **CLASSIFICATION**

The submenu **QoS ► IP CLASSIFICATION AND SIGNALING ► EDIT/ADD ► SIGNALING (TOS)** contains the following selection options:

Field	Meaning
Set Type of Service (TOS) Field	Defines a new value for the TOS field in the IP header for the IP packets that match the filter conditions. Possible values: <i>0 to 255</i>

Field	Meaning
Specify TOS Set Rate Limitation	(optional) Activates or deactivates Maximum Rate (Packets per Second) and Maximum Burst Size (Number of Packets) . Possible values: <input type="checkbox"/> <i>no</i> <input type="checkbox"/> <i>yes</i>
Maximum Rate (Packets per Second)	Number of packets to be manipulated per second. Can only be set if Specify TOS Set Rate Limitation is set to <i>yes</i> . Possible values: 0 to 65535.
Maximum Burst Size (Number of Packets)	Defines the maximum number of packets whose TOS field can still be set when the previously defined maximum packet rate has been reached. Can only be set if Specify TOS Set Rate Limitation is set to <i>yes</i> . Possible values: 0 to 65535.

Table 5-53: **SIGNALING (TOS)****Defining classification rules**

Proceed as follows to define classification rules for the QoS filters:

- Go to **QoS** ➤ **IP CLASSIFICATION AND SIGNALING**.
- Add a new entry with **ADD** or select an existing entry and confirm with **Return** to change it.
- Select the desired value for **Direction**.
- Select the desired value for **Action**.
- Select the desired **Filter**.

Classification

- Go only to **QoS** ➤ **IP CLASSIFICATION AND SIGNALING** ➤ **EDIT/ADD** ➤ **CLASSIFICATION**.
- Select the desired value for **Class Type**.
- If applicable, enter a **Class ID** (only for **Class Type normal**).

Activating TOS signaling

- Confirm with **OK**.
- Go to **QoS ➤ IP CLASSIFICATION AND SIGNALING ➤ EDIT/ADD ➤ SIGNALING (TOS)** if TOS signaling is to be configured.
- Enter the desired value for **Set Type of Service (TOS) Field**.
- Select the desired value for **Specify TOS Set Rate Limitation**.
- If applicable, enter the desired value for **Maximum Rate (Packets per Second)**.
- If applicable, enter the desired value for **Maximum Burst Size (Number of Packets)**.
- Confirm with **OK**.
You have returned to the menu **QoS ➤ IP CLASSIFICATION AND SIGNALING ➤ ADD** or **QoS ➤ IP CLASSIFICATION AND SIGNALING ➤ EDIT**.
- Select **Insert behind Rule** if you create a new rule that is to be attached to an existing rule.
- If applicable, select **Next Rule**.
- Press **SAVE**.
You have returned to the menu **QoS ➤ IP CLASSIFICATION AND SIGNALING**.
- Repeat these steps until you have defined all the desired rules.
- Continue with [chapter 5.4.3, page 226](#).

5.4.3 Activating the Classification

Define the interface on which the previously defined classification is to be performed in the menu **QoS ► INTERFACES AND POLICIES**.

```

X8500 Setup Tool                               BinTec Communications AG
[QoS][INTERFACES]: Enable IP QoS Classification and Policies  MyX8500

Interface   First Rule   First Filter   Scheduler   TxRate   Limit
call-by-call   no IP QoS classification
dialup1      no IP QoS classification
en0-1        no IP QoS classification
en0-1-snap   no IP QoS classification
en0-2        no IP QoS classification
en0-2-snap   no IP QoS classification
en6-0        no IP QoS classification
en6-0-snap   no IP QoS classification

EXIT

Use <Space> to select

```



Only one rule chain per interface can be created at any one time. If several IP filters are to be used on an interface, these must be interlinked via a rule chain. You must be especially careful if overlapping occurs between several filters (cut sets or subsets). Note that processing a rule chain for each IP packet stops as soon as one of the filter conditions is fulfilled.

► Select the desired interface, e.g. **en0-1**, and confirm with **Return**.

The following menu opens for Ethernet interfaces:

```

X8500 Setup Tool                               BinTec Communications AG
[QoS][INTERFACES][EDIT]: Configure QoS Policies                MyX8500

Interface                                     en1
IP QoS Classification via                     RI 1 FI 1 (test1)

SAVE                                           CANCEL

Use <Space> to select

```

Field of menu **QoS** ► **INTERFACES AND POLICIES** ► **EDIT** for Ethernet interfaces:

Field	Meaning
IP QoS Classification via	Defines the interface-specific "entry" to a rule chain. The packets to be classified are then checked starting with this first rule and the associated IP filter.

Table 5-54: **QoS** ► **INTERFACES AND POLICIES** ► **EDIT**

Activating IP packet classification

Proceed as follows to activate classification for the desired interface:

- Go to **QoS** ► **INTERFACES AND POLICIES**.
- Select the desired interface and confirm with **Return**.



Only one rule chain per interface can be created at any one time. If several IP filters are to be used on an interface, these must be interlinked via a rule chain. You must be especially careful if overlapping occurs between several filters (cut sets or subsets). Note that processing a rule chain for each IP packet stops as soon as one of the filter conditions is fulfilled.

- Select the first rule to be applied in **IP QoS Classification via**.
- Press **SAVE** and **EXIT**.
You have returned to the **QoS** menu. The entries are temporarily saved and activated.
- If applicable, continue for WAN interfaces with [chapter 5.4.4, page 227](#).

5.4.4 Defining QoS Bandwidth Management Policies

QoS on WAN interface

If QoS is activated on a WAN interface, you must make additional settings in the submenu **QoS** ► **INTERFACES AND POLICIES**. These settings concern the handling "policy" for the previously classified IP packets, e.g. the queuing and discard strategies for these packet classes.

At least three queues are used on the send side: one queue for the high-priority data, 1 to 255 queues for the data with *normal* priority and a (default) queue for

all data not classified. The number of queues of normal priority (class-based type) corresponds to the number of policy entries for this class (menu **QoS** ► **INTERFACES AND POLICIES** ► **EDIT** ► **CLASS-BASED QoS POLICIES** ► **ADD**), so that a separate queue (with relevant policy) can be configured for up to 255 classes of packets (see [chapter 5.4.2, page 221](#)). All packets that are either not classified or not assigned to a class and do not have a defined policy are processed via a default queue. A separate policy can also be defined for the default queue, which means it can be incorporated in the queuing and scheduling process. Only a bandwidth limitation can be meaningfully defined for the high-priority queue.

Algorithms Three scheduling algorithms are currently implemented (only relevant for processing the normal and default queues):

- Priority Queuing (PQ): The priority of a queue defines the order of processing. A queue is not processed until all other queues of higher priority are empty.
- Weighted Round-Robin Scheduling (WRR): The frequency of processing the queues is defined in relation to each other by the weighting to be defined.
- Weighted Fair Queuing (WFQ): Here the different traffic flows are processed as fairly as possible, so that one connection cannot occupy a disproportionately large bandwidth at the expense of the others (within a queue or class).

Only freely available bandwidth is distributed by these algorithms. Queues whose reserved bandwidth has not yet been fully utilized are processed with priority. The high-priority queue is always processed with priority, irrespective of the queuing and scheduling process selected.

Traffic shaping Traffic shaping defines a maximum bit transmission rate for an interface. This limitation includes all data for transmission (both *high-priority* and *normal* and also system messages such as "Keepalive", "RIP", etc.). Traffic shaping is essential for bandwidth limitation of virtual (WAN) interfaces or connections that are set up via an interface with a higher bandwidth, e.g. PPP over PPTP or also PPPoE, i.e. WAN connections implemented over Ethernet.

Policy A policy can be defined for each class, so that the queue in which a packet for transmission is processed as part of the configured scheduling process can be defined. The type of queue or the type of possible configuration is determined by the packet class to which the policy is to apply. You must decide – as previously for classification – between the high-priority class and the up to 255 normal classes, for which relevant queues and policies can be defined. There is also a default queue/class for all packets not previously classified. A policy can also be defined for this class.

It is possible to assign or guarantee each queue and thus each packet class a certain part of the total bandwidth of the interface.



Packets of the high-priority type always take priority over the other data. This ensures that bandwidth reserved for the normal queues may also be used for the benefit of high-priority data in case of inconsistent configuration (total of the individual parts of reserved bandwidth exceeds the total bandwidth available).

Congestion avoidance

TCP connections usually respond to packet losses with a (temporary) reduction of their transmission rate. If packets for transmission are discarded with a probability proportional to the mean level of the queue, this ensures that the queue can be kept smaller on average and the maximum queue size at which packets are discarded is reached less often. This also achieves a smaller mean transit delay and significantly smaller loss rates if bursts should cause the size of the queue to increase again to such a size that the dropping algorithms act. RED (Random Early Detection) – if configured – is active for queue sizes between the "Lower Queue Threshold" and "Upper Queue Threshold".



This algorithm acts only if mainly data on a TCP basis (e.g. by FTP) are transmitted and the respective TCP implementations operate as standard, i.e. compatible with this specific type of signaling. Other traffic flows, e.g. on a UDP basis (such as RTP), are not affected by this.

Thresholds The meaning of the "Lower Queue Threshold" and "Upper Queue Threshold" for the individual queues can be most easily described with the following diagram:

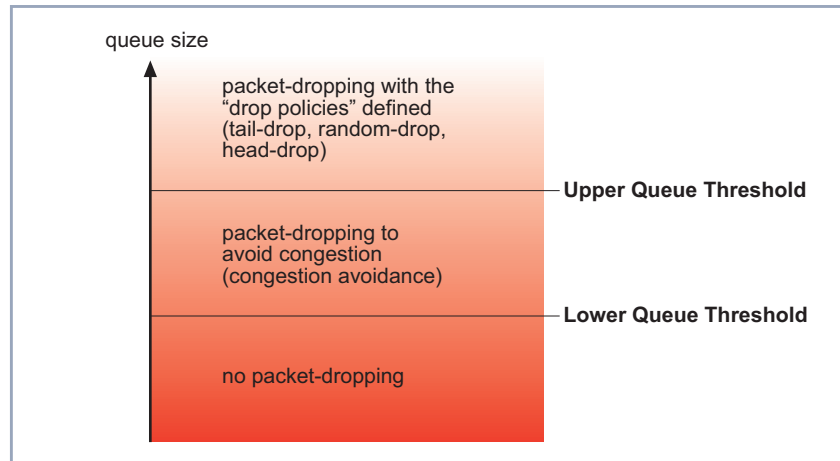


Figure 5-5: Influence of thresholds on packet-dropping

With a large queue size below the Lower Queue Threshold, neither dropping nor congestion avoidance algorithms are used.

With a queue size whose maximum assumes the Upper Queue Threshold, attempts are made to stop the queue growing any more, depending on the dropping algorithm defined.

If the queue exceeds the Upper Queue Threshold, packets are discarded according to the drop policy defined.

Multilink PPP (MLPPP) This is a special PPP mode for comparatively narrowband WAN connections such as ISDN, X.21 (64 kbps). This mode permits the transmission of data classified as high priority with minimum transit delay compared with a normal PPP connection. This is achieved by fragmenting the packets classified as normal and above a certain size (to be configured), so that a high-priority non-fragmented packet can be inserted between these fragments immediately if required.

Configuration If you have defined a WAN interface in [chapter 5.4.3, page 226](#) that is to be classified as previously defined, the following menu opens:

X8500 Setup Tool		BinTec Communications AG	
[QoS][INTERFACES][EDIT]: Configure QoS Policies		MyX8500	
Interface	dialup1		
IP QoS Classification via	RI 4 FI 4 (test2)		
QoS Scheduling and Shaping Class-Based QoS Policies			
MLPP Interleave Mode	yes		
MLPPP Fragment Size	250		
	SAVE	CANCEL	
Use <Space> to select			

The submenu **QoS** ► **INTERFACES AND POLICIES** ► **EDIT** ► **QoS SCHEDULING AND SHAPING** has the following selection options:

Field	Meaning
Queuing and Scheduling Algorithm	<p>Activates and deactivates QoS on the WAN interface. The previously classified data are therefore distributed to individual queues, which can then be processed with different algorithms.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>disabled</i> No QoS on this interface, previously classified packets are still sent according to the FIFO process. The entry is not deleted from the configuration and can be activated again if required. ■ <i>delete</i> The entry is deleted. QoS is deactivated on the interface.

Field	Meaning
Continuation of Queuing and Scheduling Algorithm	<ul style="list-style-type: none"> ■ <i>priority queuing (PQ)</i>: Freely available bandwidth is distributed according to (defined) priorities (see Priority, table 5-56, page 235). A queue is not processed until all other queues of higher priority are empty (only relevant for normal and default class). ■ <i>weighted round-robin scheduling (WRR)</i> (only relevant for normal and default queue) Freely available bandwidth is distributed according to (defined) weighting (see Weight, table 5-56, page 235). ■ <i>weighted fair queuing (WFQ)</i> (only relevant for normal and default queue) Freely available bandwidth is distributed as “fairly” as possible among the (automatically detected) traffic flows.
Specify Traffic Shaping	<p>Activates and deactivates bandwidth limitation (shaping in bits per second) on the interface. Can only be set if <i>delete</i> or <i>disabled</i> has not been selected for Queuing and Scheduling Algorithm. This limitation also affects high-priority data. Possible values:</p> <ul style="list-style-type: none"> ■ <i>yes</i> (shaping activated) ■ <i>no</i> (shaping deactivated)
Maximum Transmit Rate (Bits per Second)	<p>Can only be set if Specify Traffic Shaping is set to <i>yes</i>. Indicates the maximum bandwidth of the interface (in transmit direction). Possible values: 0 to 2048000.</p>

Table 5-55: **QoS** ► **INTERFACES AND POLICIES** ► **EDIT** ► **QoS SCHEDULING AND SHAPING**

The submenu **QoS** ► **INTERFACES AND POLICIES** ► **EDIT** ► **CLASS-BASED QoS POLICIES** ► **ADD** offers the following relevant selection options:

Field	Meaning
Class	<p>Defines the packet class to which this policy is to apply. Possible values:</p> <ul style="list-style-type: none"> ■ <i>default</i>: Policy for data not explicitly assigned to a queue (only one entry meaningful). ■ <i>class-based</i>: Policy for normal classes. ■ <i>high priority</i>: Policy for high-priority classes (only one entry meaningful).
Class ID	<p>Can only be set if the value in the Class field is <i>class-based</i>. The Class ID assigns the normal class to the queue or policy. All IDs defined for the classification are possible.</p>
Transmit Rate (Bits per Second)	<p>Defines the bandwidth to be reserved for this class in bits per second. This part of the bandwidth of the interface may only be used for other data if no packets of this class are to be sent. Possible values: 0 to 2048000.</p>
Bound Transmit Rate (Shaping)	<p>Defines whether or not the part of the bandwidth reserved for this class may be exceeded (on average in the long term). Can only be set if the value for Transmit Rate (Bits per Second) is greater than zero. Possible values:</p> <ul style="list-style-type: none"> ■ <i>yes (bounded)</i>: Reserved bandwidth is also the upper limit. ■ <i>no (not bounded)</i>: Bandwidth not needed elsewhere can also be used by this class.

Field	Meaning
Transmit Rate Burst	Defines the maximum number of bytes that may still be transmitted when the throughput determined for this queue equals the reserved value. Can only be set if the value for Transmit Rate (Bits per Second) is greater than zero. Possible values: 0 to 64000.
Weight	Relative weighting of this class. Only relevant if <i>weighted round-robin scheduling (WRR)</i> is set for Queuing and Scheduling Algorithm and <i>default</i> and <i>class-based</i> for Class . Possible values: 1 to 255.
Priority	Relative priority within the normal class/queue. Only relevant if <i>priority queuing (PQ)</i> is set for Queuing and Scheduling Algorithm and <i>default</i> and <i>class-based</i> for Class . Possible values: 0 to 255. The smaller the value, the higher the priority.
Shaping Algorithm	No selection options. Until now only Token Bucket procedure for assignment/limitation of the bandwidth for a queue.
Congestion Avoidance Algorithm	Defines the procedure for handling newly arriving packets for transmission that are received in the queue after the Lower Queue Threshold for this queue is reached; i.e. whether these are unconditionally placed in the queue or possibly discarded. Possible values: ■ <i>none</i> : Packets are always accepted in the queue.

Field	Meaning
Continuation of Congestion Avoidance Algorithm	<ul style="list-style-type: none"> ■ <i>weighted-random (RED)</i>: Packets are discarded with a calculated probability proportional to the long-term mean queue size determined. This procedure ensures a smaller long-term queue size for TCP-based data traffic, so that traffic bursts can also usually be transmitted without large packet losses.
Dropping Algorithm	<p>Specifies the procedure to be used for this class/queue for discarding newly arriving packets for transmission after the Upper Queue Threshold is reached (corresponds to the maximum size of this queue). Possible values:</p> <ul style="list-style-type: none"> ■ <i>tail-drop</i>: The newly arrived packet is discarded. ■ <i>head-drop</i>: The oldest packet in the queue is discarded. ■ <i>random-drop</i>: A randomly selected packet is discarded from the queue.
Lower Queue Threshold	<p>Defines the minimum queue size, below which neither dropping nor congestion avoidance algorithms are used. Possible values: 0 to 256000.</p>
Upper Queue Threshold	<p>Defines the maximum queue size. When this threshold is reached, attempts are made to stop the queue growing, depending on the defined dropping algorithm. Possible values: 0 to 256000.</p>

Table 5-56: **QoS** ► **INTERFACES AND POLICIES** ► **EDIT** ► **CLASS-BASED QoS POLICIES** ► **ADD**

Fields of menu **QoS** ► **INTERFACES AND POLICIES** ► **EDIT** for selecting a WAN interface:

Field	Meaning
MLPPP Interleave Mode	<p>Activates/deactivates the MLPPP Interleave Mode. Possible values:</p> <ul style="list-style-type: none"> ■ <i>yes</i>: Activates the Multilink PPP Interleave Mode for the preferred service of the high-priority packets on slow PPP connections. ■ <i>no</i>: Deactivates the Multilink PPP Interleave Mode.
MLPPP Fragment Size	<p>Defines the maximum size of the fragments into which the normal-priority packets are divided. The smaller the value selected, the lower the latency for a high-priority packet to be transmitted. Can only be set if MLPPP Interleave Mode is set to <i>yes</i>. Possible values: <i>30 to 1500</i>.</p>

Table 5-57: **QoS** ► **INTERFACES AND POLICIES** ► **EDIT**

Defining policies Proceed as follows to configure the relevant QoS bandwidth management on WAN connections:

- Go to **QoS** ► **INTERFACES AND POLICIES**.
- Select the WAN interface on which the QoS bandwidth management is to be activated and press **Return**.
You have returned to the menu **QoS** ► **INTERFACES AND POLICIES** ► **EDIT**.
- If applicable, select the classification **IP QoS Classification via**, as described in [chapter 5.4.3, page 226](#).
- Go to **QoS** ► **INTERFACES AND POLICIES** ► **EDIT** ► **QoS SCHEDULING AND SHAPING**.
- Select the desired **Queuing and Scheduling Algorithm**.

- Traffic shaping**
- Select *yes* for **Specify Traffic Shaping** and enter the desired bandwidth in **Maximum Transmit Rate (Bits per Second)** if you want to define bandwidth limitation (traffic shaping) for the WAN interface.
 - Confirm with **OK**.
You have returned to the menu **QoS** ➤ **INTERFACES AND POLICIES** ➤ **EDIT**.
- Configuring policies for defined classes**
- Go to **QoS** ➤ **INTERFACES AND POLICIES** ➤ **EDIT** ➤ **CLASS-BASED QoS POLICIES**.
 - Create a new policy with **ADD** or select an existing policy.
 - Select the class type to which this policy is to apply in **Class**.
 - If applicable, select a **Class ID**.
You have defined this during the configuration of the IP classification.
 - Enter the desired value for **Transmit Rate (Bits per Second)** if you would like to reserve bandwidth for this class.
 - Use **Bound Transmit Rate (Shaping)** to define whether this bandwidth is limited (*yes*) or not limited (*no*).
 - Enter the desired value for **Transmit Rate Burst** if you have set **Bound Transmit Rate (Shaping)** to *yes*, i.e. the bandwidth is limited.
This defines a permissible burst of **Transmit Rate (Bits per Second)**.
 - Enter the desired relative weighting for **Weight** if you have selected *weighted round-robin scheduling (WRR)* for **Queuing and Scheduling Algorithm**.
 - Enter the desired priority for this class or the assigned queue for **Priority** if you have selected *priority queuing (PQ)* for **Queuing and Scheduling Algorithm**.
 - If applicable, select *weighted-random (RED)* for **Congestion Avoidance Algorithm** if the data for transmission are routed mainly over TCP connections.
 - Select the desired **Dropping Algorithm**.
 - Enter the desired value for **Lower Queue Threshold** (relevant for **Dropping Algorithm** and *weighted-random (RED)*).

- Enter the desired value for **Upper Queue Threshold** (relevant for **Dropping Algorithm** and *weighted-random (RED)*).
 - Confirm with **OK**.
You have returned to the menu **QoS** ➤ **INTERFACES AND POLICIES** ➤ **EDIT** ➤ **CLASS-BASED QoS POLICIES** and can see the list of policies already defined.
 - Repeat the entries until you have configured all the required policies.
 - Leave the menu with **EXIT**.
You have returned to the menu **QoS** ➤ **INTERFACES AND POLICIES** ➤ **EDIT**.
- MLPPP Interleave Mode**
- If applicable, activate **MLPPP Interleave Mode** (*yes*) for comparatively slow WAN connections.
This can decisively reduce the latency for high-priority packets.
 - Enter the desired maximum fragment size for a packet of normal priority for **MLPPP Fragment Size** if you have set **MLPPP Interleave Mode** to *yes*.
This value is determined by the bandwidth of the connection and the desired latency.
 - Press **SAVE**.
- Leaving the menu**
- Leave the menu **QoS** ➤ **INTERFACES AND POLICIES** with **EXIT**.
You have returned to the **QoS** menu.
 - Leave the menu with **EXIT**.
You have returned to the main menu. The entries are temporarily saved and activated.

5.5 Bridging

X8500 supports the bridging function. The description of the configuration of **X8500** as a bridge can be found in the **Software Reference**.

5.6 Extra License Features

This chapter briefly describes the **X8500** features you can activate with extra licenses.

The relevant extra licenses are activated by adding the information received with the license in the Setup Tool menu **LICENSES** (see [chapter 4.1.1, page 56](#)).

Extra licenses are currently obtainable for the following features:

- X.25
- Frame Relay
- VPN (Virtual Private Network)
- TAF (Token Authentication Firewall)
- IPSec (IPSec system software inclusive)

You can find detailed information and configuration instructions (with examples) in the **Software Reference** and for IPSec in your **IPSec Reference Manual**.

6 Configuration of Expansion Cards and Modules

This chapter tells you the configuration steps you can carry out if you have equipped your **X8500** with an expansion card, and possibly communication modules and resource modules. Any expansion card, communication module and resource module equipped are automatically detected by **X8500** on start-up.

To install your expansion card, communication module and resource module, please follow the installation guide supplied with the cards and modules, and the **Hardware Installation Guide**.



The system card X8A-SYS must be installed in the system card slot (fifth slots from the left). Slots 1 to 4 and 5 to 8 are provided for the expansion cards (for numbering of slots, see chapter "**X8500** Basic Unit" in the **X8500 Hardware Installation Guide**).

For optimal performance of **X8500**, slots 5 to 8 should be fully equipped with expansion cards before slots 1 to 4 are used!



Enter any necessary license(s) in the Setup Tool (see [chapter 4.1.1, page 56](#)) before you start the configuration.

This chapter is broken down as follows:

- WAN Interface Expansion Card for ISDN PRI and G.703 ([chapter 6.1, page 243](#))
- Expansion Card X8E-2BC ([chapter 6.2, page 252](#))
- Expansion Card X8E-DSP ([chapter 6.3, page 262](#))
- WAN Interface Expansion Card for X21.V/35 ([chapter 6.4, page 263](#))
- Resource Modules with Digital Modems ([chapter 6.5, page 270](#))
- Resource Modules for Encryption and Compression (XT-VPN) ([chapter 6.6, page 280](#))

- Resource Module for X21./V.35 ([chapter 6.7, page 281](#))

6.1 WAN Interface Expansion Card for ISDN PRI and G.703

The PRI (Primary Rate Interface) or G.703 expansion card is equipped with four ports, each with two sockets (IN and OUT). Depending on the card and the license you purchased, your PRI/G.703 expansion card is equipped with the following:

- two ISDN PRI interfaces (X8E-2PRI)
- two G.703 interfaces (X8E-2G703)
- two ISDN PRI and two G.703 interfaces
- four ISDN PRI interfaces (X8E-4PRI)
- four G.703 interfaces (X8E-4G703)



The number of ISDN PRI or G.703 ports available with the expansion card can vary, depending on how many and which interfaces are activated by licenses (see **Hardware Installation Guide**).

You can obtain licenses from your dealer.

PRI You can connect **X8500**'s ISDN PRI interface to a Primary Rate Interface. This is done by connecting the NT (Network Termination) adapter of your telephone provider to the IN socket of a port activated by license. In Germany, this provides you with 30 B-channels and 1 D-channel, which you can use for both dialup and leased lines over ISDN.

G.703 With an **X8500** G.703 interface, you can install a G.703 leased line to a connection partner. This is also done by connecting the NT (Network Termination) adapter of your telephone provider to the IN socket of a port activated by license. A G.703 leased line is an unstructured high-speed line of up to two Mbps for the transmission of data with HDLC framing.



You can use a PRI interface of a PRI expansion card as both a PRI and G.703 interface.

You can use a G.703 interface only as a G.703 interface.

The PRI or G.703 expansion card can be optionally equipped with up to two resource modules with digital modems (chapter 6.5, page 270).

Configuration with the Setup Tool

The additional interfaces your expansion card offers are shown in the Setup Tool main menu. In the following example, **X8500** is equipped with the expansion card X8E-4PRI in slot 5:

```

X8500 Setup Tool                                     BinTec Communications AG
                                                    MyX8500

Licenses      System
Slot Card (State)  Interfaces/Resource[Unit]
1:
2:
3:
4:
SYS: X8A-SYS (R)   ETH[1]  ETH[2]  BRI[4]
5:  X8E-4PRI (R)   PRI[0]  PRI[1]  PRI[2]  PRI[3]
6:  X8E-2BC (R)   CM-100BT:ETH[0] CM-2BRI:BRI[2]  BRI[3]
7:
8:

WAN Partner
IP      PPP      CREDITS      CAPI      QoS
Configuration Manager
Monitoring and Debugging
Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items.<Return> to enter

```

The ISDN PRI/G.703 interfaces are configured in following menus:

- **PRI[0]** for the first ISDN PRI/G.703 port in slot 5
- **PRI[1]** for the second ISDN PRI/G.703 port in slot 5 etc.

Since these menus are identical, in the following they will be referred to as **PRI[x]**.

In this example, the menu of the first PRI interface in slot 5 (SLOT 5 UNIT 0 ISDN S2M) is shown:

```

X8500 Setup Tool                               BinTec Communications AG
[SLOT 5 UNIT 0 ISDN S2M]: Configure ISDN S2M Interface   MyX8500
-----
Status
  ISDN Switch Type   detected Euro ISDN S2M user profile (TE)
  Layer 1            active
  Layer 2            established
  License usage      1 PRI (not used: PRI: 0, G.703: 0)

Configuration
  ISDN Switch Type   autodetect on bootup
  ISDN Line Framing  standard (CRC4)

  Incoming Call Answering >

                        SAVE                        CANCEL
-----
Use <Space> to select

```

The upper part of this menu shows status information concerning the switch type and layer activity of the PRI port, as well as license usage of the expansion card. The field **License usage** indicates which license is in use for the current configuration as well as how many of the licenses you activated are still available (*not used*) for this expansion card. In our example, all four PRI ports are licensed and configured (*not used: PRI: 0, G.703: 0*). A PRI expansion card with two PRI licenses and only one PRI port already configured would show: *not used: PRI: 1, G.703: 0*. For further detail on status information, see [table 6-1, page 247](#).

The fields under **Status** cannot be modified. They show the current status of this PRI port. The fields have the following meaning:

Field	Meaning
Status: ISDN Switch Type	Shows the currently active protocol on this port and the state of the ISDN autoconfiguration. Possible values: <ul style="list-style-type: none"> ■ <i>autodetection is waiting to run</i>: The router waits until Layer 1 becomes active. Then it starts the ISDN autoconfiguration. ■ <i>autodetection is running</i>: The ISDN autoconfiguration is currently in progress. ■ <i>detected <any switch type name></i>: The specified protocol was detected by ISDN autoconfiguration and is currently working. ■ <i><any switch type name></i>: It shows the currently configured switch type.
Status: Layer 1	Shows the physical state of the PRI port. Possible values: <ul style="list-style-type: none"> ■ <i>active</i>: Layer 1 is OK. ■ <i>no signal</i>: Probably no cable or no license. ■ <i>other messages</i>: Broken cable or wrong value for ISDN Line Framing.
Status: Layer 2	Shows the state of the D-channel Layer 2 protocol LAPD. Possible values: <ul style="list-style-type: none"> ■ <i>connecting</i>: Layer 2 is not connected. ■ <i>established</i>: Layer 2 is connected.

Field	Meaning
Status: License usage	<p>Shows which license is currently assigned to this port. Possible values:</p> <ul style="list-style-type: none"> ■ <i>license missing</i>: The configured switch type needs a license which is not available. All available licenses are currently in use by other ports of this expansion card. ■ <i>not used</i>: No license is needed for current configuration (or available licenses on this expansion card currently not in use). ■ <i>1 PRI</i>: One PRI license is used for this interface. ■ <i>1 G.703</i>: One G.703 license is used for this interface.

Table 6-1: **PRI[x]**: Status information

The menu **PRI[x]** contains the following fields under **Configuration**:

Field	Meaning
ISDN Switch Type	<p>Defines the ISDN >> protocol supplied by your ISDN provider.</p> <p>All switch types may be used with a PRI license. With a G.703 license, only <i>leased line</i>, <i>1 Hyperchannel (G.703 + G.704)</i> and <i>leased line, G.703 (unstructured, no G.704)</i> may be chosen. Possible values:</p> <ul style="list-style-type: none"> ■ <i>autodetect on bootup</i>: automatic D-channel detection (default setting). ■ <i>Euro ISDN S2M user profile (TE)</i> ■ <i>Euro ISDN S2M network profile (NT)</i> ■ <i>1TR6 S2M user profile (TE)</i>

Field	Meaning
Continuation of ISDN Switch Type	<ul style="list-style-type: none"> ■ <i>1TR6 S2M network profile (NT)</i> ■ <i>back to back (dialup)</i> ■ <i>leased line, chan. B1..B31 diff. endpoints: 31 PPP interfaces can be configured. Note: The physical time slot 16 is mapped to channel 0.</i> ■ <i>leased line, chan. B1..B31 bundled: 31 channels bundled to 1 interface with Multi-link PPP.</i> ■ <i>leased line, 1 Hyperchannel (G.703 + G.704): 1984 kbps, structured.</i> ■ <i>leased line, G.703 (unstructured, no G.704): 2048 kbps.</i> ■ <i>not used: If you do not want to use this port and no license should be assigned.</i> <p>Note: Tested only for Euro ISDN.</p>
ISDN Line Framing	<p>(only available, if ISDN Switch Type is not set to <i>leased line, G.703 (unstructured, no G.704)</i> or <i>not used</i>)</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>standard (CRC4):</i> default setting. ■ <i>special (no CRC)</i> <p>The default setting is adequate in most cases for a PRI interface. Occasionally (e.g. in Sweden and France), the setting <i>special (no CRC)</i> is necessary if X8500 is connected to a PABX.</p>

Field	Meaning
Clock Mode	<p>(only available, if ISDN Switch Type is set to <i>back to back (dialup)</i> or <i>leased line, 1 Hyperchannel (G.703 + G.704)</i> or <i>leased line, G.703 (unstructured, no G.704)</i>)</p> <p>Not available for communication module CM-PRI.</p> <p>Defines which connection partner sends the clock signal for synchronization between transmitter and receiver. If the clock signal is not generated by the (PABX) network itself, one of the two connection partners must generate this signal.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>external</i> (default setting): X8500 receives the clock signal ■ <i>internal</i>: X8500 sends the clock signal
Channel Selection	<p>(only available, if ISDN Switch Type is set to <i>Euro ISDN S2M user profile (TE)</i>). Defines how the B-channel for an outgoing call is selected.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>standard (any channel)</i>: (default setting) The (PABX) network chooses the channel to use. ■ <i>no channel identification</i>: No IE (information element) channel identification is sent by X8500. The (PABX) network chooses the channel to use. ■ <i>submit preferred channel</i>: X8500 chooses one channel to use and signals it to the (PABX) network.

Table 6-2: **PRI[x]**: Configuration

Configuration Proceed as follows to configure a PRI interface for dialup connections:

- Go to **PRI[x]** for the ISDN PRI interface you want to configure.
- Select **ISDN Switch Type**: *autodetect on bootup*.
This setting enables **X8500** to use its automatic D-channel detection. As long as the D-channel detection is running, **Status: ISDN Switch Type** shows *autodetection is running*. The setting found is then displayed, e.g. **detected Euro ISDN S2M user profile (TE)**.



If the ISDN protocol is not set correctly, an ISDN connection cannot be established and the provider's exchange (PABX) may disconnect the line if it is not used!

Make sure **X8500** detects the ISDN protocol used correctly and displays it under **Status: ISDN Switch Type** as *detected <any switch type name>*. If not, enter it manually under **ISDN Switch Type**. The automatic D-channel detection is then switched off.

- Select **ISDN Line Framing**, e.g. **standard (CRC4)**, if applicable.
- Select **Clock Mode**, e.g. **external** (only G.703), if applicable.
- Select **Channel Selection**, e.g. **standard (any channel)** (not for G.703).
- Confirm with **SAVE**.

The settings are temporarily saved and activated.

Incoming Call Answering If dialup connections are to be established over the ISDN PRI interface, you should now tell **X8500** your own numbers for this interface:



These settings are not possible for leased lines.

- Go to **PRI[x]** ➤ **INCOMING CALL ANSWERING** for the ISDN PRI interface you want to configure.

This menu lists the previously completed assignment of services to extensions. The menu offers the same options as **BRI[x]** ➤ **INCOMING CALL ANSWERING** for the distribution of incoming calls over the ISDN BRI interface of the system card. For a detailed description, see "[Incoming Call Answering](#)", page 77.

- Use **ADD** to add a new entry or select an existing entry. Confirm with **Return** to change the entry.
- Select the **Item**, e.g. **PPP (routing)**.
- Enter the **Number**, e.g. **30**.
- Select the **Mode**, e.g. **left to right (DDI)**.
- Select the **Bearer**, e.g. **data**.
- Confirm with **SAVE**.

You have returned to menu **PRI[x] ▶ INCOMING CALL ANSWERING**. The entries are saved and displayed in the list.

You have now assigned one of your extensions (**30**) to a possible service (**PPP (routing)**). If a data call is received by called party number 30, it is therefore forwarded to the PPP (routing) service. If the PPP (routing) service initiates an outgoing data call, then 30 is assigned as calling party number.

- Repeat these steps until you have assigned all desired services to one of the available **Numbers**.

You have now configured Incoming Call Answering for this ISDN PRI interface. **X8500** distributes the incoming calls to the internal services and uses the assigned **Number** for outgoing calls.

- Leave **PRI[x] ▶ INCOMING CALL ANSWERING** with **EXIT**.
- Confirm with **SAVE**.
- If applicable, repeat for any ISDN PRI/G.703 interfaces.

WAN partner To enable **X8500** to make connections to networks or hosts outside your LAN, you must configure the partners you want to connect to as WAN partners on your **X8500** in the **WAN PARTNER** menu. This applies to outgoing connections, incoming connections and leased lines. Refer to [chapter 4.3, page 94](#).

6.2 Expansion Card X8E-2BC

The expansion card X8E-2BC can be equipped with up to two of the following communication modules:

- CM-BRI or CM-2BRI ([chapter 6.2.1, page 252](#))
- CM-PRI, from hardware version 2.0 ([chapter 6.2.2, page 255](#))
- CM-100BT ([chapter 6.2.3, page 256](#))
- CM-X21 ([chapter 6.2.4, page 257](#))

6.2.1 Communication Modules for ISDN BRI

By installing a BRI (Basic Rate Interface) communication module (CM-BRI or CM-2BRI) on your X8E-2BC expansion card, you can equip **X8500** with additional ISDN BRI interfaces. You can use these interfaces for both dialup and leased lines over ISDN.

Configuration with the Setup Tool

The additional interfaces are shown in the Setup Tool main menu as in the following example:

```

X8500 Setup Tool                                     BinTec Communications AG
                                                    MyX8500

Licenses      System
Slot Card (State)  Interfaces/Resource[Unit]
1:
2:
3:
4:
SYS: X8A-SYS (R)   ETH[1]  ETH[2]  BRI[4]
5:  X8E-4PRI (R)   PRI[0]  PRI[1]  PRI[2]  PRI[3]
6:  X8E-2BC (R)   CM-100BT:ETH[0]  CM-2BRI:BRI[2]  BRI[3]
7:
8:

WAN Partner
IP      PPP      CREDITS      CAPI      QoS
Configuration Manager
Monitoring and Debugging
Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items.<Return> to enter

```

The interfaces are configured in the following menus:

- **BRI[2]** for the first additional ISDN BRI port of the CM-2BRI module in slot 6
- **BRI[3]** for the second additional ISDN BRI port of the CM-2BRI module in slot 6

Since these menus are identical, in the following they will be referred to as **BRI[x]**.



CM-2BRI in slot/connector 1 of the X8E-2BC expansion card:

- BRI [0] is the upper port
- BRI [1] is the lower port

CM-2BRI in slot/connector 2 of the X8E-2BC expansion card:

- BRI [2] is the upper port
- BRI [3] is the lower port

On the front panel, the ports [2] and [3] are placed above ports [0] and [1].



The number of ISDN BRI ports available depends on the modules you have installed.

To do Proceed as follows to configure the ISDN BRI interface(s) of your communication module (CM-BRI or CM-2BRI) on your X8E-2BC expansion card:

- Go to **BRI[x]** for the interface you want to configure.
This menu offers the same options as **BRI[4]** for the ISDN BRI interface of the system card.
- Configure the interface(s), as described in [chapter 4.2.1, page 73](#).

Incoming Call Answering If dialup connections are to be set up over the ISDN BRI interface, first tell **X8500** how it is to respond to incoming calls over this interface:



These settings are not possible for leased lines.

- Go to **BRI[x]** ➤ **INCOMING CALL ANSWERING**.

This menu lists the services previously assigned to numbers and offers the same options as **BRI[4]** ➤ **INCOMING CALL ANSWERING** for the distribution of incoming calls over the ISDN BRI interface of the system card. For a detailed description, see "[Incoming Call Answering](#)", page 77.

- Use **ADD** to add a new entry or select an existing entry. Confirm with **Return** to change the entry.
- Select the **Item**, e.g. **PPP (routing)**.
- Enter the **Number**, e.g. **12330**.
- Select the **Mode**, e.g. **right to left**.
- Select the **Bearer**, e.g. **data**.
- Confirm with **SAVE**.

You have returned to menu **BRI[x]** ➤ **INCOMING CALL ANSWERING**. The entries are saved and displayed in the list.

You have now assigned a possible service (**PPP (routing)**) to one of your numbers (**123 30**). This means that when a data call is received for the Called Party Number **123 30**, it is put through to the **PPP (routing)** service.

- Repeat these steps until you have assigned to all phone numbers the services to be reached under these numbers.
You have now configured Incoming Call Answering for this ISDN BRI interface and **X8500** distributes the incoming calls to the internal services.
- Leave **BRI[x]** ➤ **INCOMING CALL ANSWERING** with **EXIT**.
- Confirm with **SAVE**.
- If applicable, repeat for any BRI interface.

WAN partner To enable **X8500** to make connections to networks or hosts outside your LAN, you must configure the partners you want to connect to as WAN partners on your **X8500 WAN PARTNER** menu. This applies to outgoing connections, incoming connections and leased lines. Refer to [chapter 4.3, page 94](#).

6.2.2 Communication Module CM-PRI for ISDN PRI

The expansion card X8E-2BC can be equipped up to two communication modules CM-PRI. By installing a Primary Rate Interface communication module (CM-PRI) on a X8E-2BC expansion card, you can equip **X8500** with an additional ISDN PRI interface.



The communication module CM-PRI does not support G.703!

Configuration with the Setup Tool

The additional interfaces are shown in the Setup Tool main menu as in the following example:

```

X8500 Setup Tool                                     BinTec Communications AG
                                                    MyX8500

Licenses      System
Slot Card (State)  Interfaces/Resource[Unit]
1:
2:
3:
4:
SYS: X8A-SYS (R)   ETH[1]  ETH[2]  BRI[4]
5:  X8E-4PRI (R)   PRI[0]  PRI[1]  PRI[2]  PRI[3]
6:  X8E-2BC (R)   CM-100BT:ETH[0]  CM-2BRI:BRI[2]  BRI[3]
7:
8:  X8E-2BC (R)   CM-PRI:PRI[0]   CM-PRI:PRI[2]

WAN Partner
IP      PPP      CREDITS      CAPI      QoS
Configuration Manager
Monitoring and Debugging
Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items.<Return> to enter

```

The interface(s) are configured in the following menus:

- **CM-PRI: PRI[0]** for the first additional ISDN PRI port of the CM-PRI module in slot 8
- **CM-PRI: PRI[2]** for the second additional ISDN PRI port of the CM-PRI module in slot 8

For the configuration of the PRI interface of the CM-PRI communication module, see [chapter 6.1, page 243](#).

6.2.3 Communication Module CM-100BT

The expansion card X8E-2BC can be equipped up to two communication modules CM-100BT. By installing a Ethernet communication module (CM-100BT) on a X8E-2BC expansion card, you can equip **X8500** with an additional Ethernet interface.

The configuration of an Ethernet interface for xDSL is described in [chapter 4.2.2, page 86](#).

Configuration with the Setup Tool

The additional interfaces are shown in the Setup Tool main menu as in the following example:

```

X8500 Setup Tool                                     BinTec Communications AG
                                                    MyX8500

Licenses      System
Slot Card (State)  Interfaces/Resource[Unit]
1:
2:
3:
4:
5:  X8A-SYS  (R)  ETH[1]  ETH[2]  BRI[4]
6:  X8E-4PRI (R)  PRI[0]  PRI[1]  PRI[2]  PRI[3]
7:  X8E-2BC  (R)  CM-100BT:ETH[0]  CM-100BT:ETH[2]
8:  X8E-2BC  (R)  CM-PRI:PRI[0]  CM-PRI:PRI[2]

WAN Partner
IP      PPP      CREDITS      CAPI      QoS
Configuration Manager
Monitoring and Debugging
Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items.<Return> to enter

```

The interfaces are configured in the following menu:

- **CM-100BT: ETH[0]** for the first additional Ethernet port of the first CM-100BT module in slot 6
- **CM-100BT: ETH[2]** for the second additional Ethernet port of the second CM-100BT module in slot 6

Since these menus are identical, in the following they will be referred to as **CM-100BT: ETH[x]**.



Information about bridging can be found in the **Software Reference**.

To do Proceed as follows to configure the LAN interfaces of the communication modules:

- Go to **CM-100BT: ETH[x]** for the interface you want to configure. This menu offers the same options as **ETH[1]** resp. **ETH[2]** for the LAN interfaces of the system card. For a detailed description, see [chapter 4.1.3, page 61](#).
- Enter **Local IP Number**, e.g. **192.168.1.250**.
- Enter **Local Netmask**, e.g. **255.255.255.0**.
- If applicable, enter **Second Local IP Number** and **Second Local Netmask**.
- Select **Encapsulation**, e.g. **Ethernet II**.
- Select **Mode**, e.g. **auto**.
- Press **SAVE**.

You have returned to the main menu and the entries are temporarily saved and activated.

6.2.4 Serial WAN Interfaces Communication Module CM-X21

The **X8500** expansion card X8E-2BC can be equipped with up to two CM-X21 communication modules with the serial WAN interfaces of the type X.21/V.11.

Configuration with the Setup Tool The additional interfaces are shown in the Setup Tool main menu as in the following example:

```

X8500 Setup Tool                                     BinTec Communications AG
                                                    MyX8500

Licenses      System
Slot Card (State)  Interfaces/Resource[Unit]
1:
2:
3:
4:
SYS: X8A-SYS (R)   ETH[1]  ETH[2]  BRI[4]
5:  X8E-4PRI (R)   PRI[0]  PRI[1]  PRI[2]  PRI[3]
6:  X8E-2BC (R)   CM-100BT:ETH[0]  CM-100BT:ETH[2]
7:
8:  X8E-2BC (R)   CM-X21:X21[0]   CM-X21:X21[2]

WAN Partner
IP      PPP      CREDITS      CAPI      QoS
Configuration Manager
Monitoring and Debugging
Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items.<Return> to enter

```

The interfaces are configured in the following menu:

- **CM-X21: X21[0]** for the first X.21/V.11 interface of the first CM-X21 module in slot 8
- **CM-X21: X21[2]** for the second X.21/V.11 interface of the second CM-X21 module in slot 8

Since the menus **CM-X21: X21[0]** and **CM-X21: X21[2]** are identical, in the following they will be referred to as **CM-X21: X21[x]**.

In this example, the menu of the first X.21/V.11 interface in slot 8 (SLOT 8 UNIT 0 X.21) is shown:

X8500 Setup Tool	BinTec Communications AG
[SLOT 8 UNIT 0 X.21]: Configure X21 Interface	MyX8500
Layer 1 Mode	dce
Speed	64000 bit/s
Layer 2 Mode	auto
Interface Leads	disabled
SAVE	CANCEL
Use <Space> to select	

The menu **CM-X21: X21[x]** of the communication module CM-X21 contains the following fields:

Field	Meaning
Layer 1 Mode	<p>The mode X8500 operates in for Layer1. Possible values:</p> <ul style="list-style-type: none"> ■ <i>dce</i> : used if X8500 is operating as the network provider (always required by one side of a private X.25 data network) ■ <i>dte</i> : if X8500 is conneted to a public data network, such as Datex-P in Germany. <p>DCE is clock generator for the X.21 interface; DTE is recipient of signal created by clock generator.</p>
Speed	<p>Transmission rate of connection, if Layer 1 Mode is set to <i>dce</i>; scalable from 2400 bit/s to 2048 kbit/s.</p> <p>The value to be set depends on the quality and length of the cable and on the connection type (balanced/unbalanced).</p> <p>Default value: 64000 bit/s</p>

Field	Meaning
Layer 2 Mode	<p>Defines the value of the HDLC address field in the transmitted command frames (Layer 2). Possible values:</p> <ul style="list-style-type: none"> ■ <i>auto</i> (default value): You can accept this setting, e.g. for access to a public data network such as Datex-P. ■ <i>dte</i>: The address field has the value for DTE. ■ <i>dce</i>: The address field has the value for DCE. <p>For X.21 leased line, one side of the link must be configured as <i>dte</i>, the other as <i>dce</i>.</p>
Interface Leads	<p>Defines whether X8500 checks the status of the interface lines. The same value should be set for both connection partners. Possible values:</p> <ul style="list-style-type: none"> ■ <i>enabled</i>: The status of the signal line (Indicator (I) for X.21) is checked and transferred as L1State. ■ <i>disabled</i> (default value): The status is not checked; the physical line is always up. In this setting, you should monitor the interface line in some other way, e.g. with PPP Keepalive.

Table 6-3: **CM-21: X21[x]** of communication module CM-X21

To do Proceed as follows to configure the serial interfaces (the example values given are necessary if you connect **X8500** to Datex-P):

- Go to **CM-X21: X21[x]**.
- Select **Layer 1 Mode**, e.g. *dte*.
- Select **Layer 2 Mode**: e.g. *auto*.

➤ Select **Interface Leads**: e.g. *disabled*.

➤ Confirm with **SAVE**.

➤ Confirm with **EXIT**.

You have returned to the main menu and the entries are temporarily saved and activated.

Advanced configuration If you use a leased line, you can implement a backup solution using the Bandwidth on Demand feature (see [chapter 5.2.3, page 149](#)). If you use this facility, a dialup connection is set up to the connection partner if the leased line fails.

6.3 Expansion Card X8E-DSP

The expansion card X8E-DSP is designed to be equipped with up to two resource modules. For configuration of the resource modules, see [chapter 6.5, page 270](#) and [chapter 6.6, page 280](#).

6.4 Expansion Card for X.21/V.35

The X.21/V.35 expansion card is equipped with either two or four X.21/V.35 interfaces depending on the card you purchased.

The X.21/V.35 expansion card is designed for a much higher data throughput than the CM-X21 communication module without drawing upon **X8500**'s resources. It also offers feasibility for a number of different serial interface types.

Configuration with the Setup Tool

The additional interfaces your expansion card offers are shown in the Setup Tool main menu. In the following example, **X8500** is equipped with the expansion card X8E-SYNC with four X.21/V.35 interfaces in slot 7:

```

X8500 Setup Tool                                     BinTec Communications AG
                                                    MyX8500
-----
Licenses      System
Slot Card (State)  Interfaces/Resource[Unit]
1:
2:
3:
4:
SYS: X8A-SYS   (R)  ETH[1]  ETH[2]  BRI[4]
5:  X8E-4PRI  (R)  PRI[0]  PRI[1]  PRI[2]  PRI[3]
6:  X8E-2BC   (R)  CM-100BT:ETH[0]  CM-2BRI:BRI[2]  BRI[3]
7:  X8E-SYNC  (R)  X21[0]  X21[1]  X21[2]  X21[3]
8:

WAN Partner
IP      PPP      CREDITS      CAPI      QoS
Configuration Manager
Monitoring and Debugging
Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items.<Return> to
enter

```

The X.21/V.35 interfaces are configured in following menus:

- **X21[0]** for the first X.21/V.35 port in slot 7
- **X21[1]** for the second X.21/V.35 port in slot 7 etc.

Since these menus are identical, in the following they will be referred to as **X21[x]**.

In this example, the menu of the first X.21/V.35 port in slot 7 (SLOT 7 UNIT 0 SERIAL) is shown:

X8500 Setup Tool		BinTec Communications AG	
[SLOT 7 UNIT 0 SERIAL]: Configure Serial Interface - Unit 0		MyX8500	
Cable Detection	interface & connector type		
Interface Type	V.35 (autodetected)		
Connector	dte (autodetected)		
Layer 2 Mode	auto		
Interface Leads	disabled		
	SAVE	CANCEL	
Use <Space> to select			

The menu contains the following fields:

Field	Meaning
Cable Detection	<p>Defines whether the interface type and connector type you use are autodetected or set manually. Possible values:</p> <ul style="list-style-type: none"> ■ <i>interface & connector type</i>: Interface and connector type are autodetected. ■ <i>interface type</i>: Only the interface type is autodetected. The connector type must be set manually. ■ <i>connector type</i>: Only the connector type is autodetected. The interface type must be set manually. ■ <i>manual</i>: Both the interface type and the connector type must be set manually.

Field	Meaning
Interface Type	<p>Defines the interface type of the port used.</p> <p>If you choose the value <i>interface type</i> or <i>interface & connector type</i> for the field Cable Detection, the interface type is autodetected. The autodetected value is shown, e.g. V.35 (autodetected).</p> <p>If you choose the value <i>connector type</i> or <i>manual</i> for the field Cable Detection, you must set the field Interface Type manually. Possible values are shown in table 6-5, page 267.</p>
Connector	<p>Defines the connector type of the port used.</p> <p>If you choose the value <i>connector type</i> or <i>interface & connector type</i> for the field Cable Detection, the connector type is autodetected. The autodetected value is shown, e.g. dte (autodetected).</p> <p>If you choose the value <i>interface type</i> or <i>manual</i> for the field Cable Detection, you must set the field Connector manually. Possible values are shown in table 6-6, page 268.</p>

Field	Meaning
Speed	<p>The Speed field appears only if the Connector field shows the value <i>dce</i>.</p> <p>Transmission rate of connection. Possible values:</p> <ul style="list-style-type: none"> ■ <i>2400 bit/s, 9600 bit/s, 14400 bit/s, 19200 bit/s, 38400 bit/s, 64000 bit/s</i> ■ <i>128 kbit/s, 256 kbit/s, 512 kbit/s</i> ■ <i>1 Mbit/s, 2 Mbit/s, 4 Mbit/s, 8 Mbit/s</i> ■ <i>custom</i>: The field Speed: Value (bit/s) appears. Scalable from <i>2400 bit/s</i> to <i>8 Mbit/s</i>. <p>The value to be set depends on the quality and length of the cable, on the connection type, and on the min/max acceptable speed on the opposite DTE side. Up to 8 Mbps are possible over a short distance of up to 5 m if shielded and twisted pair cables are used.</p> <p>Default value: <i>64000 bit/s</i></p>
Layer 2 Mode	<p>Defines the value of the HDLC address field in the transmitted command frames (Layer 2). Possible values:</p> <ul style="list-style-type: none"> ■ <i>auto</i> (default value): The selection made for Connector is accepted. You can usually accept this setting, e.g. for access to a public data network such as Datex-P. ■ <i>dte</i>: The address field has the value for DTE. ■ <i>dce</i>: The address field has the value for DCE.

Field	Meaning
Interface Leads	<p>Defines whether X8500 checks the status of the interface lines. The same value should be set for both connection partners. Possible values:</p> <ul style="list-style-type: none"> ■ <i>enabled</i>: The status of the signal line (I for X.21, CTS for V.35) is evaluated as layer-1 signaling of the opposite device. This will influence the variable L1State appropriately. ■ <i>disabled</i> (default value): The layer-1 signaling of the opposite device is not checked; X8500 assumes the physical line is always up. In this setting, you should monitor the interface line in some other way, e.g. with PPP Keepalive.

Table 6-4: **X21[x]**

The field **Interface Type** includes the following selection options:

Possible Values	Meaning
<i>unknown (autodetected)</i>	There is no cable connected to the port or the cable connected does not support autodetection.
<i>none</i>	Port is not used.
<i>X.21 (term)</i>	V.11 on all lines, 120 ohm termination on critical input lines.
<i>V.35</i>	V.35 on critical lines, V.28 on uncritical lines.
<i>V.36</i>	V.11 on critical lines, V.10 on uncritical lines.
<i>X.21bis</i>	V.28 on all lines.
<i>X.21 (not term)</i>	Not terminated V.11 on all lines.
<i>RS-449</i>	V.11 on critical lines; V.10 on uncritical lines.
<i>RS-530</i>	V.11 on critical lines; V.10 on uncritical lines.

Table 6-5: **Interface Type**



If you use a X.21 cable with autodetection the value *X.21 (term)* is selected automatically. Should you wish not to use termination, you must deactivate autodetection in the Setup Tool and set your value manually.



Data and clock lines are usually called critical lines.
Control lines are usually called uncritical lines.

The field **Connector** includes the following selection options:

Possible Values	Meaning
<i>unknown (autodetected)</i>	There is no cable connected to the port or the cable connected does not support autodetection.
<i>dte</i>	The pins are assigned as DTE interface. This setting is necessary, for example, if X8500 is connected to a public data network (e.g. Datex-P in Germany).
<i>dce</i>	The pins are assigned as DCE interface.

Table 6-6: **Connector**

Configuration Proceed as follows to configure a serial WAN interfaces of the X8E-SYNC expansion card:

- Go to **X21[x]**.
- Select **Cable Detection**, e.g. **interface & connector type**.
Interface and connector type are autodetected.
- If you chose the value *connector type* or *interface & connector type* for the field **Cable Detection**, select **Interface Type**, e.g. **X.21 (term)**.
- If you chose the value *interface type* or *interface & connector type* for the field **Cable Detection**, select **Connector**, e.g. **dte**.

- If you chose the value *dce* for the field **Connector**, select **Speed**, e.g. **64000 bit/s**.
- If you chose the value *custom* for the field **Speed**, type in the desired value for **Speed: Value (bit/s)**.
- Select **Layer 2 Mode**, e.g. **auto**.
- Select **Interface Leads**, e.g. **disabled**.
- Confirm with **SAVE**.

You have returned to the main menu. The entries are temporarily saved and activated.

Advanced configuration If you use a leased line, you can implement a backup solution using the Bandwidth on Demand feature (see [chapter 5.2.3, page 149](#)). If you use this facility, a dialup connection is set up to the connection partner if the leased line fails.

6.5 Resource Modules with Digital Modems

ISDN PRI/G.703 and X8E-DSP expansion cards (see [chapter 6.1, page 243](#) and [chapter 6.3, page 262](#)) can be equipped with resource modules with digital modems.

The following resource modules with digital modems are available:

- XT-S: resource modules with 8 digital modems
- XT-M: resource modules with 12 digital modems
- XT-2M: resource modules with 24 digital modems
- XT-L: resource modules with 30 digital modems

If your **X8500** is equipped with resource modules with digital modems for analog data, it can be used as Remote Access Server for ISDN and GSM connections and for analog connections (dial-in and dial-out).

X8500 with Digital Modems as Remote Access Server

X8500 equipped with digital modems can be used for modem connections, e.g. by home office staff with analog modems or by field service staff with laptop, mobile phone and modem.

X8500 uses the digital modems of the resource modules as a modem pool and always dynamically takes the next available modem for an incoming and outgoing connection.



For the use of modem functionality you must have installed a CM-PRI communication module or a PRI ISDN expansion card.

A diagram of a dial-in procedure is shown below:

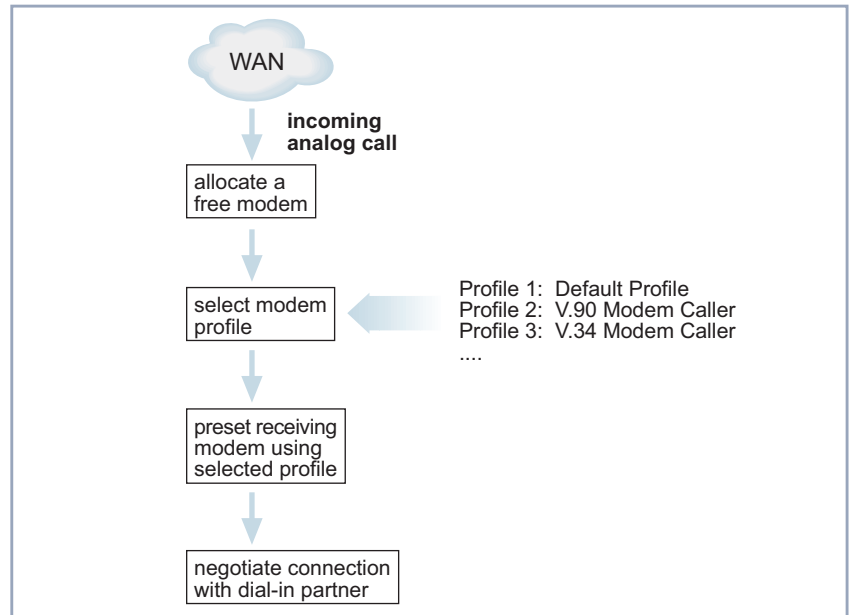


Figure 6-1: Dial-in to **X8500** with digital modems

Modem profiles

The modems (e.g. 30 modems with an XT-L resource module) need not be individually configured, as **X8500** uses a flexible concept of modem profiles. Up to eight modem profiles can be configured for **X8500** in the menu **MODEM ► PROFILE CONFIGURATION**. The modem actually used then dynamically assumes the settings of the appropriate modem profile on connection setup. A modem profile defines the modem settings that are required for a connection to the opposite terminal, e.g. automatic baud rate negotiation, compression and maximum or minimum baud rate. The creation of several modem profiles gives you a tuning option if you do not want to limit your use to the default settings only.

When defining the settings for Incoming Call Answering, e.g. in menu **PRI[x] ► INCOMING CALL ANSWERING** for a ISDN PRI interface (see "[Incoming Call Answering](#)", page 250), you can explicitly define which modem profile is to be used for which of your own extensions. If you do not specifically assign modem profiles to your own extensions, the router modem automatically uses modem **Profile 1**.

Modem **Profile 1** is therefore used as default setting and should allow maximum selection of the settings. As all dial-in users that cannot be authenticated by CLID etc. are assigned modem **Profile 1** for the connection, modem **Profile 1** should be able to operate all modems. You can use the remaining seven modem profiles to define user groups, so that the dial-in connection partners find optimum modem settings in **X8500**.

Example scenario A typical scenario, e.g. for an Internet Service Provider, could look like this:

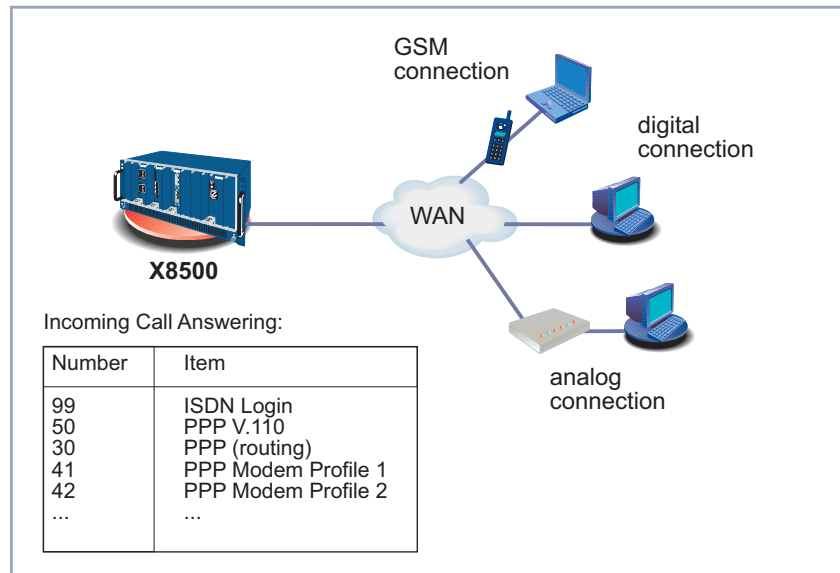


Figure 6-2: Scenario for dial-in

- Incoming calls to the number 99 are connected through to the ISDN Login service.
- Modem connections over 0911 12330 are assigned to modem **Profile 1**.
- Dial-in users who dial in with a mobile phone over a GSM connection use 0911 123 50.
- Dial-in users who use an ISDN connection use 0911 123 30.
- Dial-in users who dial in over an analog connection use the numbers 0911 123 41 to 0911 123 48 for dialing in (according to which analog modem type you use).

Setup Tool with digital modems If **X8500** is equipped with a resource module with digital modems, the menu **MODEM** appears in the Setup Tool main menu:

X8500 Setup Tool		BinTec Communications AG	
		MyX8500	
Licenses	System		
Slot Card (State)	Interfaces/Resource[Unit]		
1:			
2:			
3:			
4:			
SYS: X8A-SYS (R)	ETH[1]	ETH[2]	BRI[4]
5: X8E-4PRI (R)	PRI[0]	PRI[1]	PRI[2] PRI[3] MOD[4] MOD[5]
6: X8E-2BC (R)	CM-100BT:ETH[0]	CM-2BRI:BRI[2]	BRI[3]
7:			
8:			
WAN Partner			
IP	PPP	MODEM	CREDITS CAPI QoS
Configuration Manager			
Monitoring and Debugging			
Exit			
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items.<Return> to enter			

The modem profiles whose settings are used by the digital modems in **X8500** are defined in the menu **MODEM**.

General procedure for the configuration of dial-in connections:

- Define the settings for the default modem profile **Profile 1** in **MODEM** ► **PROFILE CONFIGURATION**.
- If applicable, define other modem profiles **Profile 2 ... 8** in **MODEM** ► **PROFILE CONFIGURATION**.
- Use the settings for Incoming Call Answering to control the use of the modem profiles according to the called party number, e.g. in **BRI[4]** ► **INCOMING CALL ANSWERING**.
- Configure a WAN partner entry for each dial-in user in **WAN PARTNER**.

The menus **MODEM** ► **PROFILE CONFIGURATION** ► **PROFILE 1 ... 8** contain the following fields:

Field	Meaning
Name	Profile 1 ... 8 is displayed.

Field	Meaning
Description	Optional description of the modem profile.
Modulation	<p>Defines the modem standard to be used (V.34 in ex works state). The selected modem standard must be supported by the analog modem of the opposite terminal.</p> <p>V.90 and lower are supported by 56000-modems, V.34 and lower by 33600-modems, V.32bis and lower by 14400-modems.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ V.90 ■ V.21 ■ V.22 ■ V.22bis ■ V.23 ■ V.32 ■ V.32bis ■ V.34 ■ k56flex <p>More modem standards are in preparation. See www.bintec.net for further information.</p>
Error Correction	<p>Defines the error correction to be used.</p> <p>For possible values, see table 6-8, page 276.</p>
Automode	<p>Defines whether dynamic negotiation of modulation is permitted with the dial-in user.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>on</i> (default value): Free negotiation is permitted regardless of the modulation set. ■ <i>off</i>: Only the modulation set is used.

Field	Meaning
Min Bps	<p>Defines the minimum baud rate that can be used with the modem profile. Any speed supported by the modem standard set under Modulation can be set here.</p> <p>The connection is cleared if the only baud rates that can be negotiated with the opposite terminal are smaller than the value set here.</p> <p>Scalable from 75 to 56000, default value: 300.</p>
Max Receive Bps	<p>Defines the maximum baud rate of incoming data ("upstream") that can be used with the modem profile. Any speed supported by the modem standard set under Modulation can be set here.</p> <p>The value set under Max Transmit Bps is used here if this value is less than the value set here.</p> <p>Scalable from 75 to 56000, default value: 33600.</p>
Max Transmit Bps	<p>Is only used if Modulation = V.90.</p> <p>Defines the maximum baud rate of outgoing data ("downstream") that can be used with the modem profile.</p> <p>Scalable from 75 to 56000, default value: 33600.</p>
V.42bis Compression	<p>Defines whether V.42bis compression can be negotiated for a connection.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>auto</i>: Negotiation is allowed. ■ <i>off</i>: V.42bis compression is not used.

Field	Meaning
MNP5 Compression	<p>Defines whether MNP5 compression can be negotiated for a connection.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>auto</i>: Negotiation is allowed. <input type="checkbox"/> <i>off</i>: MNP5 compression is not used.

Table 6-7: Menu **MODEM** ► **PROFILE CONFIGURATION** ► **PROFILE 1 ... 8**

The **Error Correction** field contains the following selection options:

Possible Values	Meaning
<i>none</i>	Error correction is not used.
<i>required</i>	First LAPM and then MNP4 is tried for error correction. If both fail, the modem clears the connection.
<i>auto</i> (default value)	First LAPM and then MNP4 is tried for error correction. If both fail, error correction is not used.
<i>LAPM</i>	LAPM (Link Access Protocol for Modems) is used. If this fails, the modem clears the connection.
<i>MNP</i>	MNP4 (Microcom Networking Protocol) is used. If this fails, the modem clears the connection.

Table 6-8: **Error Correction**

Modem profile 1 configuration



Proceed as follows:

Modem **Profile 1** is used as default setting for modem connections and should allow maximum selection of the settings. As all dial-in users that cannot be authenticated by CLID etc. are assigned modem **Profile 1** for the connection, modem **Profile 1** should be able to operate all modems.

► Go to **MODEM** ► **PROFILE CONFIGURATION**.

- Select **PROFILE 1** and confirm with **Return**.
- Enter **Description**, e.g. **Default Modem Profile**.
- Select **Modulation**, e.g. **V.90**.
- Select **Error Correction**, e.g. **auto**.
- Select **Automode**, e.g. **on**.
- Select **V.42bis Compression**, e.g. **auto**.
- Select **MNP5 Compression**, e.g. **auto**.
- Confirm with **SAVE**.

Modem profile 2 ... 8 configuration

- Configure other modem profiles as necessary, see [table 6-9, page 279](#).

Incoming Call Answering

Proceed as follows to assign the defined modem profiles to your own extensions (the example values are taken from the scenario in [figure 6-2, page 272](#)):

- Go to **PRI[x]** ➤ **INCOMING CALL ANSWERING** if you wish to assign an incoming dial-in connection over the ISDN PRI interface to a modem profile.
- Add a new entry with **ADD**.
- Select **Item**, e.g. **PPP Modem Profile 2**.
- Enter **Number**, e.g. **42**.
- Select **Mode**, e.g. **right to left**.
- Select the **Bearer**, e.g. **voice**.
- Confirm with **SAVE**.
- Add other entries as necessary.

WAN partner entries for modem users

Proceed as follows to create WAN partner entries for the dial-in users:

- Go to **WAN PARTNER**, add a new entry with **ADD**. You will find detailed information about configuring a WAN partner in [chapter 4.3, page 94](#).

The following settings are essential here:

- Enter **Partner Name**, e.g. **homeoffice_2**.
- Select **Encapsulation**, e.g. **PPP**.

- Select authentication information in **WAN PARTNER** ➤ **ADD** ➤ **PPP**.
 - Go to **WAN PARTNER** ➤ **ADD** ➤ **ADVANCED SETTINGS**.
 - Select **Layer 1 Protocol**, e.g. **Modem Profile 2**.
 - Confirm with **OK**.
 - Go to **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** ➤ **ADD**.
 - Enter the number to be used by **X8500** under **Number**, e.g. **09117890**.
 - Select **Direction**, e.g. **both (CLID)**.
 - Confirm with **SAVE**.
 - Leave **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** with **EXIT**.
 - Select the necessary settings in **WAN PARTNER** ➤ **ADD** ➤ **IP** (see "[Carrying out IP Configuration](#)", page 110).
 - Confirm with **SAVE**.
- The WAN partner entry is displayed.
- Configure other WAN partner entries for the modem user, if applicable.

A general example in [table 6-9, page 279](#) shows how you could meaningfully use the modem profiles in **X8500**:

Settings	Profile1	Profile 2	Profile 3	Profile 4	Profile 5	Profile 6	Profile 7
Modulation	<i>(Modulation is freely negotiated)</i>	V.90	V.90	V.90	V.32bis	V.32	V.23
Error Correction	auto	auto	auto	auto	auto	auto	auto
Automode	on	off	off	off	off	off	off
Min Bps	2400	28800	28800	14400	4800	4800	300
Max Receive Bps	33600	31200	31200	31200	14400	9600	1200
Max Transmit Bps	33600	50000	44000	40000	14400	9600	1200
V.42bis	auto	auto	auto	auto	auto	auto	auto

Settings	Profile1	Profile 2	Profile 3	Profile 4	Profile 5	Profile 6	Profile 7
MNP5	<i>auto</i>	<i>auto</i>	<i>auto</i>	<i>auto</i>	<i>auto</i>	<i>auto</i>	<i>auto</i>

Table 6-9: Example of modem profiles

6.6 Resource Module for Encryption and Compression (XT-VPN)

The ISDN PRI/G.703 and the X8E-DSP expansion card can be equipped with up to two resource modules (XT-VPN) that support encryption under IPsec. The XT-VPN resource module provides hardware acceleration of symmetrical as well as asymmetrical encryption using DES or 3DES. Additionally the message hash algorithms MD5 and SHA1 are supported. Both, encryption and hash algorithms, are essential for the processing of IP packets under IPsec. Moreover, IKE (Internet Key Exchange) is accelerated by the XT-VPN module: The Diffie Hellman exchange as well as the algorithms employed for authentication and/or encryption (DSA and RSA) are supported.

Configuration with the Setup Tool IPsec is configured in the menu **IPSEC**. Please, note that you need a valid IP-Sec license to make use of its functions.

6.7 Resource Module for X.21/V.35 (XT-2SYNC)

The X8E-SYNC expansion card with two X.21/V.35 interfaces can be equipped with the resource module XT-2SYNC, adding two X.21/V.35 interfaces.

Configuration with the Setup Tool

In this example, **X8500** is equipped with four X.21/V.35 interfaces in slot 7:

```

X8500 Setup Tool                                     BinTec Communications AG
                                                    MyX8500
-----
Licenses                System
Slot Card (State)      Interfaces/Resource[Unit]
1:
2:
3:
4:
SYS: X8A-SYS   (R)  ETH[1]  ETH[2]  BRI[4]
5:  X8E-4PRI  (R)  PRI[0]  PRI[1]  PRI[2]  PRI[3]  MOD[4]  MOD[5]
6:  X8E-2BC   (R)  CM-100BT:ETH[0]  CM-2BRI:BRI[2]  BRI[3]
7:  X8E-SYNC  (R)  X21[0]  X21[1]  X21[2]  X21[3]
8:

WAN Partner
IP      PPP      MODEM  CREDITS  CAPI  QoS
Configuration Manager
Monitoring and Debugging
Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items.<Return> to enter

```

The X.21/V.35 interfaces of the resource module XT-2SYNC are configured in the same way as X.21/V.35 interfaces of the expansion card: in the menu **X21[x]**, as described in [chapter 6.4, page 263](#).

7 Configuration of Security Functions and Firewall

SAFERNET The **X8500** from BinTec Communications AG gives you a high degree of security for your network and connections. The security functions available (SAFERNET) offer monitoring of activities via the router and effective access and line tapping security. The necessary configuration steps are described in this chapter.

Some of the features can only be configured by making entries directly in the ►► **MIB** tables and not by using the Setup Tool. The relevant tables and variables are given in the respective section.



You can make MIB entries either by commands in the ►► **SNMP shell** or via external SNMP managers, e.g. the **Configuration Manager**. A description of the SNMP commands is given in the **Software Reference**.

This chapter is broken down as follows:

- Activity Monitoring ([chapter 7.1, page 284](#))
- Access Security ([chapter 7.2, page 299](#))
- Line Tapping Security ([chapter 7.3, page 338](#))
- Special Features ([chapter 7.4, page 343](#))
- Checklist ([chapter 7.5, page 345](#))

7.1 Activity Monitoring

A major requirement for a high degree of security is the possibility of accurately monitoring all activities on and over the router. BinTec Communications AG provides a variety of facilities for this purpose:

- Syslog Messages ([chapter 7.1.1, page 284](#))
- Monitoring Functions in the Setup Tool ([chapter 7.1.2, page 289](#))
- Credits Based Accounting System ([chapter 7.1.3, page 293](#))
- **Activity Monitor** ([chapter 7.1.4, page 296](#))

7.1.1 Syslog Messages

All major events on **X8500**'s various subsystems (▶▶ ISDN, ▶▶ PPP, ▶▶ CAPI, etc.) are logged in the form of syslog messages (system logging messages).

The number of details visible depends on the level set (eight steps from *critical* and *info* to *debug*). The logged data are saved by **X8500** in a list of adjustable length. All information can be and should be passed to one or more external computers for saving and further processing, e.g. to the system administrator's computer. The syslog messages are lost when you restart **X8500**.



Avoid forwarding syslog messages to log hosts reached over a dialup connection. This raises your telephone bill unnecessarily.



Make sure you only pass syslog messages to a safe computer. Check the data regularly and ensure that there is always enough spare capacity available on the hard disk of your PC.

Syslog Demon All Unix operating systems support the recording of syslog messages (for setting up a Syslog Demon in Unix, see the **Software Reference**). For Windows PCs, the Syslog Demon included in **DIME Tools** can record the data and dis-

tribute to various files depending on the contents (see **BRICKware for Windows**).

Settings for syslog messages are made in:

- **SYSTEM**
- **SYSTEM** ▶ **EXTERNAL SYSTEM LOGGING**
- **ETH[x]** ▶ **ADVANCED SETTINGS**
- **WAN PARTNER** ▶ **EDIT** ▶ **IP** ▶ **ADVANCED SETTINGS**

Following the relevant fields of the menu **SYSTEM**:

Field	Meaning
Syslog Output on Serial Console	<p>Enables the display of syslog messages on the PC connected to the serial interface of X8500. Use this setting only if you make a fault analysis, as a very large output over the serial console adversely affects the throughput of the other interfaces. Possible values:</p> <ul style="list-style-type: none"> ■ <i>yes</i> ■ <i>no</i>

Field	Meaning
Message Level for Syslog Table	<p>Specifies the priority of the syslog messages to be recorded internally. Possible values:</p> <ul style="list-style-type: none"> ■ <i>emerg</i>: emergency messages (highest priority) ■ <i>alert</i>: alert messages ■ <i>crit</i>: critical messages ■ <i>err</i>: error messages ■ <i>warning</i>: warning messages ■ <i>notice</i>: notice messages ■ <i>info</i>: info messages ■ <i>debug</i>: debug messages (lowest priority) <p>Syslog messages are only recorded internally if they have a higher or identical priority to that indicated.</p>
Maximum Number of Syslog Entries	Maximum number of syslog messages saved internally in X8500 (possible values: 0 ... 1000).

Table 7-1: **SYSTEM**

Following the fields of the menu **SYSTEM** ► **EXTERNAL SYSTEM LOGGING**:

Field	Meaning
Log Host	►► IP address of the host to which syslog messages are passed.
Level	Priority of the syslog messages to be sent to Log Host . Corresponds to Message Level for Syslog Table in SYSTEM .
Facility	Syslog facility at Log Host . Only required if the Log Host is a Unix computer.

Field	Meaning
Type	Message type. Possible values: <ul style="list-style-type: none"> ■ <i>all</i>: all messages. ■ <i>system</i>: syslog messages except >> accounting messages. ■ <i>accounting</i>: accounting messages.
Timestamp	System time of X8500 . Possible values: <ul style="list-style-type: none"> ■ <i>all</i>: system time with date ■ <i>time</i>: system time without date ■ <i>none</i>: no system time indicated

Table 7-2: **SYSTEM** ▶ **EXTERNAL SYSTEM LOGGING**

Following the relevant field of the menu **ETH[x]** ▶ **ADVANCED SETTINGS**:

Field	Meaning
IP Accounting	For saving accounting messages for >> TCP , >> UDP and >> ICMP sessions. Possible values: <i>on</i> , <i>off</i> .

Table 7-3: **ETH[x]** ▶ **ADVANCED SETTINGS**

Following the relevant field of the menu **WAN PARTNER** ▶ **EDIT** ▶ **IP** ▶ **ADVANCED SETTINGS**:

Field	Meaning
IP Accounting	For saving accounting messages for >> TCP , >> UDP and >> ICMP sessions. Possible values: <i>on</i> , <i>off</i> .

Table 7-4: **WAN PARTNER** ▶ **EDIT** ▶ **IP** ▶ **ADVANCED SETTINGS**

To do Make the desired settings for syslog messages as follows:

- Go to **SYSTEM**.
- Select the desired value for **Syslog Output on Serial Console**.
- Select the desired value for **Message Level for Syslog Table**.
- Enter the desired value for **Maximum Number of Syslog Entries**.
- Go to **SYSTEM** ➤ **EXTERNAL SYSTEM LOGGING** to pass syslog messages to external hosts.
- Select an existing entry and confirm it with **Return** or add a new entry with **ADD**.
- Enter **Log Host**.
- Select the desired value for **Level**.
- Select the desired value for **Facility**.
- Select the desired value for **Type**.

IP accounting LAN side Proceed as follows to activate IP accounting for a LAN partner. **X8500** then generates and records accounting messages for the selected LAN partner from TCP, UDP and ICMP sessions:

- Go to **ETH[x]** ➤ **ADVANCED SETTINGS**.
- Activate **IP Accounting** with *on*.

IP accounting WAN side Proceed as follows to activate extended IP accounting. **X8500** then generates and records accounting messages for the selected WAN partner from TCP, UDP and ICMP sessions:

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**.
- Activate **IP Accounting** with *on*.

Displaying syslog messages Proceed as follows to display syslog messages:

- Go to **MONITORING AND DEBUGGING** ➤ **MESSAGES**.

This displays the syslog messages saved internally in **X8500**:

X8500 Setup Tool		BinTec Communications AG
[MONITOR][MESSAGE]: Syslog Messages		MyX8500
Subj	Lev	Message
SNMP	DEB	sent TRAP (linkUp,0) 115 bytes to circindex 1001 Port 36880
SNMP	DEB	sent TRAP (linkUp,0) 115 bytes to 199.1.1.13 Port 162
EXIT		RESET
Press <Ctrl-n>, <Ctrl-p> to scroll		

Deleting syslog messages



➤ Select **RESET** to delete the syslog messages in **X8500**.

For interpretation of syslog messages, see the **Software Reference**.

7.1.2 Monitoring Functions in the Setup Tool

You can also use the Setup Tool to display other data in addition to syslog messages. The current status of certain subsystems is updated periodically and displayed. Display modules are available for the following functional areas:

- ISDN connections
- Credits Based Accounting System
- Interface statistics (comparative display of several interfaces)
- ➤➤ **TCP/IP** statistics
- Syslog messages (see [chapter 7.1.1, page 284](#))

ISDN connections

Proceed as follows to display ISDN connections:

➤ Go to **MONITORING AND DEBUGGING** ➤ **ISDN MONITOR**.

A list of the existing ISDN connections (incoming and outgoing calls) is displayed:

X8500 Setup Tool		BinTec Communications AG			
[MONITOR][ISDN CALLS]: ISDN Monitor - Calls		MyX8500			
Dir	Remote Name/Number	Charge	Duration	Stack	Channel State
in	2		2910	0	B1 active
out	3		106	0	B2 active
EXIT					
(c)alls (h)istory (d)etails (s)tatistics (r)elease					

This menu also offers you other options:

- Select **c** to display the list of existing ISDN connections again.
- Select **h** to display a list of the last 20 ISDN calls (incoming and outgoing) completed since the last system start.
- Place the cursor on an existing or completed ISDN connection and select **d** to display detailed information about this connection.
- Select **s** to display statistics on the activity of the existing ISDN connections.
- Select **r** to release the tagged ISDN connection.

Credits Based Accounting System

Proceed as follows to display the state of the Credits Based Accounting System ([chapter 7.1.3, page 293](#)):

- Go to **MONITORING AND DEBUGGING** ➤ **ISDN CREDITS**.
- Select a subsystem and confirm with **Return**.

The current status of the Credits Based Accounting System for the selected subsystem is displayed:

X8500 Setup Tool		BinTec Communications AG	
[MONITOR][CREDITS][STAT]: Monitor isdnlogin Credits		MyX8500	
Time till end of measure interval(sec)	Total	Maximum	% reached
	7794	86400	91
Number of Incoming Connections	0	2	0
Number of Outgoing Connections	0	20	0
Time of Incoming Connections	4	28800	0
Time of Outgoing Connections	13	28800	0
Charge	0		
Number of Current Incoming Connections	0		
Number of Current Outgoing Connections	0		
Number of Current Connections	0		
EXIT			

Information about configuring the Credits Based Accounting System can be found in [chapter 7.1.3, page 293](#).

Credits Based Accounting System for PPPoE connections

Proceed as follows to display the credits status for PPPoE connections:

- Go to **MONITORING AND DEBUGGING** ➤ **XDSL CREDITS** ➤ **PPPoE CREDITS**.
The current status of the Credits Based Accounting System for PPPoE connections is displayed.

Interface statistics

Proceed as follows to display the current values and activities of **X8500**'s interfaces:

- Go to **MONITORING AND DEBUGGING** ➤ **INTERFACES**.

The values for two interfaces are displayed side by side:

X8500 Setup Tool			BinTec Communications AG	
[MONITOR][INTERFACE]: Interface Monitoring			MyX8500	
Interface Name	en0-1	PROVIDER		
Operational Status	up	dormant		
	total	per second	total	per second
Received Packets	5512	0	0	0
Received Octets	920664	0	0	0
Received Errors	0		0	
Transmit Packets	9	0	0	0
Transmit Octets	1193	0	0	0
Transmit Errors	0		0	
Active Connections	N/A		0	
Duration	N/A		0	
EXIT	EXTENDED		EXTENDED	

Use <Space> to select

- Select the interface to be displayed under **Interface Name**.
- Select **EXTENDED** to display additional information. You can then change the status of the interface under **Operation** and confirm the entry with **START OPERATION**.

TCP/IP statistics Proceed as follows to display the statistics for connections to ➤➤ **protocols** ICMP, ➤➤ **IP**, UDP and TCP:

- Go to **MONITORING AND DEBUGGING** ➤ **TCP/IP**.

The statistics for IP connections are displayed:

X8500 Setup Tool		BinTec Communications AG	
[MONITOR][IP]: IP Statistics		MyX8500	
InReceives	3912	OutNoRoutes	0
InHdrErrors	0	ReasmTimeout	500
InAddrErrors	0	ReasmReqds	0
ForwDatagrams	0	ReasmOKs	0
InUnknownProtos	0	ReasmFails	0
InDiscards	0	FragOKs	0
InDelivers	3321	FragFails	0
OutRequests	9	FragCreates	0
OutDiscards	0	RoutingDiscards	0
EXIT			
I(C)MP	(I)P	(U)DP	(T)CP

You can find the meaning of the MIB variables in the **MIB Reference**.

- Select **C** to display statistical data for ICMP.
- Select **I** to display statistical data for IP.
- Select **U** to display statistical data for UDP.
- Select **T** to display statistical data for TCP.

7.1.3 Credits Based Accounting System

Charges **X8500's** Credits Based Accounting System enables you to control the costs billed for charges for data connections. This means you can keep the effects of possible configuration errors within limits. For example, the system enables you to define the maximum number of connections allowed in a certain period of time. You can make settings for each subsystem (➤➤ **PPP**, ➤➤ **CAPI**, ➤➤ **ISDN Login**) to define the number of connections, the connection time and the charges billed. If the defined limit is exceeded, **X8500** cannot set up any more connections within the defined period of time. This means you can detect configuration errors in good time, before your telephone bill gets too big!

Syslog messages Syslog messages are generated if the number of connections reaches 90 % or 100 % of the limit and if a connection is prevented by the Credits Based Accounting System because the limit is exceeded.

The whole account is available again if you switch **X8500** off and then switch it on again (i.e. reboot).

The configuration is made in **CREDITS** ▶ **ISDN CREDITS** or in **CREDITS** ▶ **XDSL CREDITS** ▶ **PPPoE CREDITS**:



The fields for incoming connections are only available for ISDN.

Field	Meaning
Surveillance	Defines whether the Credits Based Accounting System is to be activated for the respective subsystem. Possible values: <i>off</i> , <i>on</i> . With <i>on</i> , you can define the parameters listed below.
Measure Time (sec)	Time in seconds for which the limit applies.
Maximum Number of Incoming Connections	Number of incoming connections allowed during the Measure Time (sec) ; displayed only for ISDN connections. If you activate this setting with <i>on</i> , you can enter the desired value in the line below.
Maximum Number of Outgoing Connections	Number of outgoing connections allowed during the Measure Time (sec) . If you activate this setting with <i>on</i> , you can enter the desired value in the line below.
Maximum Charge	Maximum charges allowed (amount, units) during the Measure Time (sec) ; displayed only for ISDN connections. If you activate this setting with <i>on</i> , you can enter the desired value in the line below.

Field	Meaning
Maximum Time for Incoming Connections (sec)	Maximum time in seconds allowed for incoming connections during the Measure Time (sec) ; displayed only for ISDN connections. If you activate this setting with <i>on</i> , you can enter the desired value in the line below.
Maximum Time for Outgoing Connections (sec)	Maximum time in seconds allowed for outgoing connections during the Measure Time (sec) . If you activate this setting with <i>on</i> , you can enter the desired value in the line below.
Maximum Number of Current Incoming Connections	Maximum number of incoming connections allowed at any one time; displayed only for ISDN connections. If you activate this setting with <i>on</i> , you can enter the desired value in the line below.
Maximum Number of Current Outgoing Connections	Maximum number of outgoing connections allowed at any one time; displayed only for ISDN connections. If you activate this setting with <i>on</i> , you can enter the desired value in the line below.

Table 7-5: **CREDITS** ▶ **ISDN CREDITS** and **CREDITS** ▶ **xDSL CREDITS** ▶ **PPPoE CREDITS**

To do Proceed as follows:

- ▶ Go to **CREDITS** ▶ **ISDN CREDITS**.
- ▶ Select **Subsystem** and confirm with **Return**.
- ▶ Select **Surveillance**: *on*, if you want to use the Credits Based Accounting System for the selected **Subsystem**.
- ▶ Enter **Measure Time (sec)**, e.g. **86400** (= 24 hours).
- ▶ Activate **Maximum Number of Incoming Connections**, if applicable, and enter the desired value.
- ▶ Activate **Maximum Number of Outgoing Connections**, if applicable, and enter the desired value.

- Activate **Maximum Charge**, if applicable, and enter the desired value.
- Activate **Maximum Time for Incoming Connections (sec)**, if applicable, and enter the desired value.
- Activate **Maximum Time for Outgoing Connections (sec)**, if applicable, and enter the desired value.
- Activate **Maximum Number of Current Incoming Connections**, if applicable, and enter the desired value.
- Activate **Maximum Number of Current Outgoing Connections**, if applicable, and enter the desired value.
- Confirm with **SAVE**.

The Credits Based Accounting System for ISDN connections is configured.

Proceed as follows to configure a Credits Based Accounting System for PPPoE connections:

- Go to **CREDITS** ➤ **XDSL CREDITS** ➤ **PPPoE CREDITS**.
- Select **Surveillance**: *on*, if you want to use the Credits Based Accounting System.
- Enter **Measure Time (sec)**, e.g. **86400** (= 24 hours).
- Activate **Maximum Number of Outgoing Connections**, if applicable, and enter the desired value.
- Activate **Maximum Time for Outgoing Connections (sec)**, if applicable, and enter the desired value.
- Press **SAVE**.

The Credits Based Accounting System for PPPoE connections is configured.

7.1.4 Activity Monitor

What do you need it for? The **Activity Monitor** enables Windows users to monitor the activities of **X8500**. Important information about the status of physical interfaces (e.g. ISDN line) and virtual interfaces (e.g. WAN partner) is easily obtained with ONE tool. A permanent overview of the utilization of **X8500**'s interfaces is possible.

How does it work? A Status Demon collects information on **X8500** and transfers it in the form of UDP packets to the broadcast address of the LAN (default setting) or to an explicitly entered IP address. One packet is sent per **X8500** interface and time interval, which can be adjusted individually to values from 1 - 60 seconds. Physical interfaces and up to 100 virtual interfaces can be monitored, provided the UDP packet size of approx. 4000 bytes is not exceeded. A Windows application on your PC receives the packets and displays the information received in various forms. This application is obtainable with **BRICKware** Release 6.1.1 and higher.



Not all interfaces will be displayed if the maximum UDP packet size is exceeded!

Activate the **Activity Monitor** as follows:

- Appropriately configure the **X8500(s)** to be monitored.
- Start and use the Windows application on your PC (see **BRICKware for Windows**).

The configuration is made in **SYSTEM** ► **EXTERNAL ACTIVITY MONITOR**:

Field	Meaning
Client IP Address	<p>IP address to which X8500 sends the UDP packets.</p> <p>The default value <code>255.255.255.255</code> means that the broadcast address of the first LAN interface is used.</p> <p>Note: If you enter the IP address of a WAN partner that can be reached over an ISDN dialup connection, you will get a large telephone bill due to frequent setting up of ISDN connections (a packet is sent every 5 seconds in the ex works setting).</p>

Field	Meaning
Client UDP Port	Port number for Activity Monitor (default value: <i>2107</i> , registered by IANA - Internet Assigned Numbers Authority).
Type	Type of information sent in the UDP packets to the Windows application. Possible values: <ul style="list-style-type: none"> ■ <i>off</i>: deactivates Activity Monitor (default value) ■ <i>physical</i>: only information about physical interfaces ■ <i>physical_virt</i>: information about physical and virtual interfaces
Update Interval (sec)	Update interval in seconds. Possible values: <i>0</i> to <i>60</i> (default value: <i>5</i>).

Table 7-6: **SYSTEM** ► **EXTERNAL ACTIVITY MONITOR**

The breakdown of **X8500**'s interfaces into physical and virtual interfaces is described in detail in the **Software Reference**.

Note: A leased line always represents a physical interface, but a group of leased lines is displayed as both a physical and virtual interface!

To do Proceed as follows:

- Go to **SYSTEM** ► **EXTERNAL ACTIVITY MONITOR**.
- Enter **Client IP Address**, **Client UDP Port**, **Type** and **Update Interval (sec)**.
- Confirm with **SAVE**.

7.2 Access Security

There are several ways of restricting logging in and access to **X8500** to authorized users only:

- Logging In ([chapter 7.2.1, page 299](#))
- Checking the Calling Party Number (CLID) ([chapter 7.2.2, page 300](#))
- Authentication of PPP Connections ([chapter 7.2.3, page 301](#))
- Callback ([chapter 7.2.4, page 302](#))
- Closed User Group ([chapter 7.2.5, page 304](#))
- Access to Remote CAPI ([chapter 7.2.6, page 304](#))
- Network Address Translation (NAT) ([chapter 7.2.7, page 304](#))
- Filters (Access Lists) ([chapter 7.2.8, page 315](#))
- Local Filters ([chapter 7.2.9, page 328](#))
- Back Route Verification ([chapter 7.2.10, page 331](#))
- TAF ([chapter 7.2.11, page 332](#))
- Extended IP Routing (XIPR) ([chapter 7.2.12, page 332](#))

7.2.1 Logging In

Password Logging in to **X8500** can be done in several ways as described in [chapter 3.2, page 30](#), but is always protected by a password. Every unsuccessful attempt to log in is logged with the source of the attempt by a syslog message and creates a corresponding SNMP trap. Pauses are inserted after several unsuccessful attempts to make it difficult for automatic attempts to find the password.



Caution!

All BinTec routers are shipped with the same user names and passwords. As long as the password remains unchanged, they are not protected against unauthorized use. How to change the passwords is described in [chapter 3.4.5, page 38](#).

- Change the passwords to prevent unauthorized access to **X8500**.
- Also make sure that unauthorized persons do not have access to the **X8500** power supply, serial console and ➤➤ **Ethernet** connection.
- Remember your password!
If you forget your password, you will have to reset **X8500** to the ex works state and your configuration is lost!

The permission rights of the possible user names and passwords can be found in [chapter 3.2, page 30](#).

Until you have changed the default password for the user name `admin`, a warning is always given after logging in.

Auto logout

To make unauthorized access difficult, the connection to **X8500** is disconnected if no keyboard entry is made for a period of 15 minutes. You can change the time with the command `t <time in seconds>` (see [chapter 10.1, page 386](#)).



If you carry out a software update (see [chapter 8.3, page 368](#)), you should deactivate auto logout as follows: Enter `t 0` in the SNMP shell.



You can create additional user accounts with the aid of SNMP commands (see the **Software Reference**). A certain password and a certain action can be assigned to a user.

7.2.2 Checking the Calling Party Number

CLID **X8500** uses Calling Line Identification (➤➤ **CLID**) to check the calling party number of an incoming call.

Screening indicator You can also determine whether calling party numbers have been modified by the calling parties. With some connections, it is possible that another number (e.g. **5678**) is displayed at the called party's terminal, instead of the calling party's own extension number (e.g. **1234**). **X8500** can detect this from the screening indicator in the setup message of the ISDN **▶▶ D-channel**. The screening indicator has four possible values:

- *user*: The calling party number indicated originates from the far end and has not been checked by the network.
- *user_verified*: The calling party number has been checked by the exchange and is correct.
- *user_failed*: The calling party number has been checked by the exchange and is incorrect.
- *network*: The calling party number indicated originates directly from the exchange (normal case).

Change variable Screening in MIB If you want **X8500** to check the screen indicator for incoming calls, you must enter one of the values stated in the following MIB tables or variables (only incoming calls with the corresponding screening indicator are accepted):

- ▶ For incoming PPP connections: **Screening** variable in **biboDialTable**.
- ▶ For incoming ISDN Login connections: **Screening** variable in **isdnloginAllowTable**.

For changing MIB variables, see [chapter 3.3, page 32](#).

7.2.3 Authentication of PPP Connections with PAP, CHAP or MS-CHAP

▶▶ PAP, ▶▶ CHAP and MS-CHAP are the common procedures used for authentication of **▶▶ PPP** connections. These use a standard procedure to exchange a user ID and a password for checking the identity of the far end. You can find further information in [chapter 4.3, page 94](#) and [chapter 5.1.3, page 142](#).

7.2.4 Callback

Callback The callback mechanism can be used for each WAN partner to obtain additional security regarding the connection partner or to clearly allocate the costs of connections. A connection is then not set up until the calling party has been clearly identified by calling back. **X8500** can answer an incoming call with a callback or dial into a WAN partner and then wait for a callback.

Identification can be based on the calling party number or PAP/CHAP/MS-CHAP authentication. Identification is made in the first case without call acceptance, as the calling party number is transferred over the ISDN D-channel, and in the second case with call acceptance.



You can find a detailed description of the callback mechanism in the **Software Reference**.

This is configured in **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**:

Field	Meaning
Callback	Activates the callback function.

Table 7-7: **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**

Callback offers the following selection options:

Possible Values	Meaning
<i>no</i>	X8500 does not call back.
<i>expected (awaiting callback)</i>	X8500 calls the WAN partner to initiate call-back.

Possible Values	Meaning
<i>yes (PPP negotiation)</i>	X8500 calls back with the extension entered for the WAN partner. If no number is entered, the required number can be reported by the caller in a PPP negotiation. This setting should be avoided if possible for security reasons. However, no alternative is currently available for connecting Microsoft >> clients over data transmission networks.
<i>yes (delayed, CLID only)</i>	X8500 calls back after approx. four seconds, if requested to by the WAN partner.
<i>yes (PPP negotiation, callback optional)</i>	Like <i>yes (PPP negotiation)</i> with abort option. The Microsoft client has the option of aborting callback and maintaining the initial connection to X8500 without callback. This is done by pressing CANCEL to close the dialog box that appears. Exception: This abort option cannot be used if the WAN partner dialing in uses Windows NT and his extension number is entered in X8500 .
<i>yes</i>	X8500 calls back immediately, if requested to by the WAN partner.

Table 7-8: **Callback**

If *yes (PPP negotiation)* is used as the setting for **Callback**, a B-channel is always opened, which results in costs.

To do Proceed as follows to activate callback for a WAN partner:

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS**.
- Select the desired value for **Callback**.
- Confirm with **OK**.

7.2.5 Closed User Group

X8500 supports the use of the "Closed User Group" service feature, which you can request for your ISDN line from your telephone company. The external/internal reachability is monitored and controlled by the exchanges if this feature is selected.

To do Proceed as follows to activate a Closed User Group for a WAN partner:

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **WAN NUMBERS** ➤ **EDIT** ➤ **ADVANCED SETTINGS**.
- Select **Closed User Group**: *specify*.
- Enter the CUG index.
You can obtain information about CUGs from your telephone provider.
- Confirm with **OK**.

7.2.6 Access to Remote CAPI

The special features offered by BinTec routers include implementation of the ➤➤ **Remote CAPI** and for PABXs the Remote TAPI programming interfaces. This enables applications on computers in the LAN to use the resources of the router as if these components were installed directly in the computer.

User concept By using BinTec's user concept, you can make sure that only users authenticated by user name and password can access **X8500**'s Remote CAPI interface (see [chapter 5.1.2, page 138](#)).

Filters You can also prevent unauthorized access by defining filters (see [chapter 7.2.8, page 315](#)) and local filters (see [chapter 7.2.9, page 328](#)).

7.2.7 NAT (Network Address Translation)

➤➤ **NAT** is a simple-to-operate procedure that can be used for several purposes in the BinTec implementation:

- Hiding the internal host addresses of a LAN by remapping to one or more external addresses.

- Controlling external to internal access. In the external direction, the router forwards all ►► **data packets** (forward NAT) and connections from external callers are only allowed if explicitly enabled.
- Permanent monitoring of the connections via the router with indication of the source and destination addresses and ►► **ports**. See your syslog messages for this purpose!

Diagram of Forward NAT:

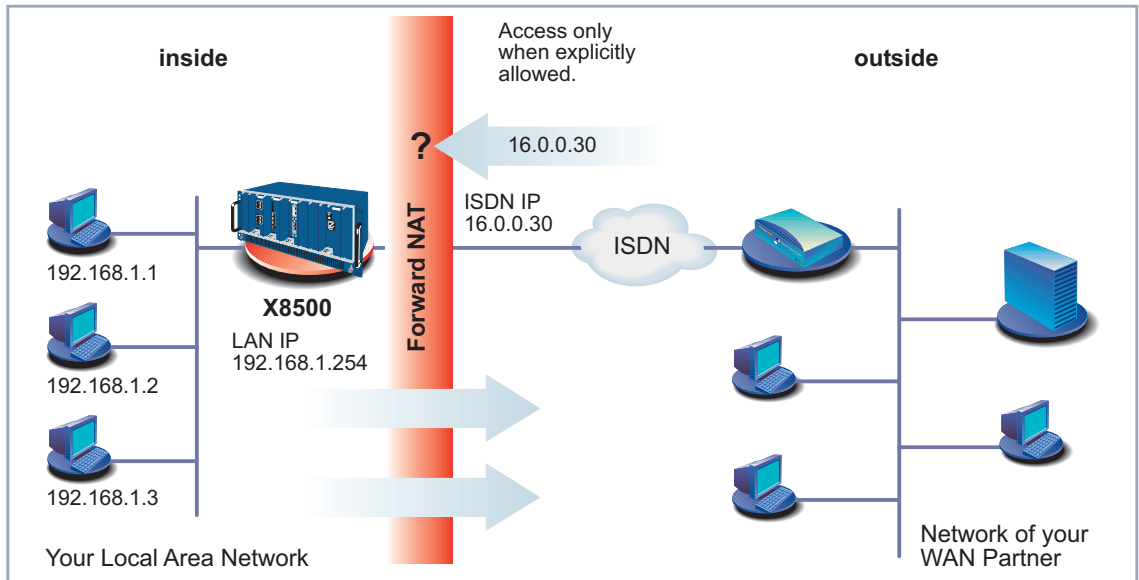


Figure 7-1: Forward NAT

NAT always refers to an interface. You will find more information on NAT in the **Software Reference**.

Configuration Configuration is made in **IP ► NETWORK ADDRESS TRANSLATION**.

X8500 Setup Tool		BinTec Communications AG	
[IP][NAT]: NAT Configuration		MyX8500	
Select IP Interface to be configured for NAT			
Name	Nat	Static mappings from Outside	Static mappings from Inside
en0-1	off	0	0
en0-1-snap	off	0	0
en0-2	off	0	0
en0-2-snap	off	0	0
en6-0	off	0	0
en6-0-snap	off	0	0
EXIT			
Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select			

IP ► NETWORK ADDRESS TRANSLATION lists all **X8500** interfaces with a status display for current NAT settings:

Field	Meaning
Name	Interface name
Nat	Indicates if NAT is activated for the relevant interface. Possible values: <ul style="list-style-type: none"> ■ <i>off</i>: NAT not activated. ■ <i>on</i>: Forward NAT activated. ■ <i>reverse</i>: Reverse NAT activated
Static mappings from Outside	For Nat = on or Nat = reverse . Indicates the number of entries that have been made for this interface for certain allowed IP connections from outside in IP ► NETWORK ADDRESS TRANSLATION ► EDIT ► REQUESTED FROM OUTSIDE ► EDIT/ADD .

Field	Meaning
Static mappings from Inside	<p>For Nat = on or Nat = reverse. Indicates the number of entries that have been made for this interface for certain IP connections from inside in IP ► NETWORK ADDRESS TRANSLATION ► EDIT ► REQUESTED FROM INSIDE ► EDIT/ADD.</p> <p>The IP addresses of these connections are mapped to external IP addresses.</p>

Table 7-9: **IP ► NETWORK ADDRESS TRANSLATION**

Activate NAT for an **X8500** interface in **IP ► NETWORK ADDRESS TRANSLATION ► EDIT**:

X8500 Setup Tool		BinTec Communications AG
[IP][NAT][CONFIG]: NAT Configuration (en0-1)		MyX8500
Network Address Translation	off	
Silent Deny	no	
Enter configuration for sessions:	requested from OUTSIDE	
	requested from INSIDE	
SAVE	CANCEL	

The menu **IP ► NETWORK ADDRESS TRANSLATION ► EDIT** contains the following fields:

Field	Meaning
Network Address Translation	<p>Defines the type of NAT for the selected interface. Possible values:</p> <ul style="list-style-type: none"> ■ <i>off</i>: Do not execute NAT. ■ <i>on</i>: Execute Forward NAT. ■ <i>reverse</i>: Execute Reverse NAT.

Field	Meaning
Silent Deny	<p>Defines whether the sender of a packet is to be informed of its denial. Possible values:</p> <ul style="list-style-type: none"> ■ <i>no</i>: Packet is denied, sender is informed by a corresponding ICMP error message. ■ <i>yes</i>: Packet is denied, sender is not informed.

Table 7-10: **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT**

Reverse NAT is mainly of interest for system administrators, e.g. for performing NAT to a WAN partner who cannot do this himself. In this process, **X8500** does not automatically conceal the local network using the global IP address assigned by the service provider. An increased configuration effort is necessary to ensure the same degree of security.

NAT for sessions from inside and for session from outside

You must explicitly allow IP connections to a certain host (or a group of hosts in a subnet) in the LAN of **X8500** for sessions requested from outside.

Furthermore, you may define additional address mappings to external addresses on the desired interface for IP connections requested from inside.



If you do not make any entries in these menus, and you activate NAT for the chosen interface, sessions requested from outside will not be allowed.

For sessions requested from inside, the IP address of the host in the LAN of **X8500** is mapped to the external IP address configured in the **IP** menu of the respective WAN partner.

For additional configuration, the menu **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT** contains two submenus:

■ **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT** ➤ **REQUESTED FROM OUTSIDE**

■ **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT** ➤ **REQUESTED FROM INSIDE**

➤ Add an entry with **ADD** or select an existing entry and confirm with **Return**.

The following menu opens (here the submenu *REQUESTED FROM INSIDE* **ADD**):

X8500 Setup Tool		BinTec Communications AG
[IP][NAT][CONFIG][INSIDE][ADD]:NAT-sessions from INSIDE (en0-1)MyX8500		
Service	user defined	
Protocol	icmp	
Remote Address		
Remote Mask		
Remote Port	any	
External Address		
External Mask		
External Address	any	
Internal Address		
Internal Mask		
Internal Address	any	
	SAVE	CANCEL
Use <Space> to select		

The submenus **REQUESTED FROM INSIDE** ► **EDIT/ADD** and **REQUESTED FROM OUTSIDE** ► **EDIT/ADD** contain the following fields:

Field	Meaning
Service	<p>Service allowed for connections to the host or host group in the LAN defined in the menu REQUESTED FROM OUTSIDE ► EDIT/ADD.</p> <p>Service for which the address mapping defined in the menu REQUESTED FROM INSIDE ► EDIT/ADD is performed.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>ftp</i> ■ <i>telnet</i> ■ <i>smtp</i> ■ <i>domain/udp</i> ■ <i>domain/tcp</i> ■ <i>http</i> ■ <i>nntp</i> ■ <i>user defined</i> (if you do not use any of the predefined services)

Field	Meaning
Protocol	<p>Only for Service = <i>user defined</i>.</p> <p>Defines the protocol.</p> <p>Possible values:</p> <ul style="list-style-type: none">■ <i>icmp</i>■ <i>tcp</i>■ <i>udp</i>■ <i>gre</i>■ <i>esp</i>■ <i>ah</i>■ <i>l2tp</i>■ <i>any</i>
Remote Address	<p>Optional.</p> <p>IP address of host or host group at the remote site.</p> <p>For incoming connections, only packets of this host/this group are accepted.</p>
Remote Mask	<p>Netmask of Remote Address at the remote site.</p> <p>Entering the netmask ensures that incoming connections from all hosts of the remote network are accepted.</p>

Field	Meaning
Remote Port	<p>Only in the menu REQUESTED FROM INSIDE ➤ EDIT/ADD.</p> <p>Only for Service = <i>user defined</i>.</p> <p>Defines port number of the service on the host or host group at the remote site.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>any</i> ■ <i>specify</i> ■ <i>specify range</i>
Remote Port: Port	<p>Only for the value <i>specify</i> for Remote Port.</p> <p>Port number of service on remote host.</p>
Remote Port: Port to Port	<p>Only in the menu REQUESTED FROM OUTSIDE ➤ EDIT/ADD.</p> <p>Only for the value <i>specify range</i> for Remote Port.</p> <p>Port number range of services on remote host.</p>
External Address	<p>External IP address of X8500 for this interface.</p> <p>For an external IP network address, enter the appropriate network mask, as well.</p>
External Mask	<p>External netmask of External Address.</p> <p>If you use external and internal IP network addresses, ensure that the values for External Mask and Internal Mask are identical.</p>

Field	Meaning
External Port	<p>Only for Service = <i>user defined</i>.</p> <p>Defines port number of the service of X8500 for this interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>any</i> ■ <i>specify</i> ■ <i>specify range</i> (only in the menu REQUESTED FROM OUTSIDE ► EDIT/ADD)
External Port: Port	<p>Only for the value <i>specify</i> for External Port.</p> <p>Port number of the service of X8500 for this interface.</p>
External Port: Port to Port	<p>Only in the menu REQUESTED FROM OUTSIDE ► EDIT/ADD.</p> <p>Only for the value <i>specify range</i> for External Port.</p> <p>Port number range of the services of X8500 for this interface.</p>
Internal Address	<p>IP address of internal host or group of hosts in a subnet.</p> <p>For an internal IP network address, enter the appropriate internal network mask, as well.</p>
Internal Mask	<p>Netmask of Internal Address.</p> <p>If you use external and internal IP network addresses, ensure that the values for External Mask and Internal Mask are identical.</p>
Internal Port	<p>Defines port number of the service on the internal host or group of hosts.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>any</i> ■ <i>specify</i>

Field	Meaning
Internal Port: Port	Only for the value <i>specify</i> for Internal Port . Port number of service on Internal Address .

Table 7-11: **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT** ➤ **REQUESTED FROM OUTSIDE/INSIDE** ➤ **EDIT/ADD**

Activate NAT Proceed as follows to activate NAT:

- Go to **IP** ➤ **NETWORK ADDRESS TRANSLATION**.
- Select the interface for which you want to activate NAT and confirm with **Return**.
You are in the menu **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT**.
- Select **Network Address Translation on**.
This activates NAT for the selected interface.
- Confirm with **SAVE**.



If you enable NAT on **X8500** from a remote host, e.g. with telnet, bear in mind that the entry takes effect immediately after confirming with **SAVE!**

Configure NAT Proceed as follows to configure NAT:

- Go to **IP** ➤ **NETWORK ADDRESS TRANSLATION**.
- Select an existing entry and confirm with **Return**.
You are in the menu **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT**.
- Go to **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT** ➤ **REQUESTED FROM OUTSIDE** to allow IP connections requested from outside.
Go to **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT** ➤ **REQUESTED FROM INSIDE** to define additional address mappings for IP connections requested from inside.
- Add an entry with **ADD** or select an existing entry and confirm with **Return**.
- Select the desired value for **Service**.

- Select the desired value for **Protocol**, if you chose the value *user defined* for **Service**.
- Enter **Remote Address** and **Remote Mask**.
- Enter **Remote Port**, if you chose the value *user defined* for **Service** in the menu **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT** ➤ **REQUESTED FROM INSIDE** ➤ **EDIT/ADD**.
- Enter **External Address**, **External Mask** and **External Port**.
- Enter **Internal Address**, **Internal Mask** and **Internal Port**.
- Confirm with **SAVE**.
The entries are temporarily saved and activated.
- Select further entries and repeat these steps, if applicable.
- Leave the menu **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT** ➤ **REQUESTED FROM OUTSIDE** or **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT** ➤ **REQUESTED FROM INSIDE** with **EXIT**.
You are in the menu **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT**.
- Confirm with **SAVE**.
You are in the menu **IP** ➤ **NETWORK ADDRESS TRANSLATION**.
- Leave the menus with **EXIT**, until you are in the main menu.
All entries are temporarily saved and activated.

7.2.8 Filters (Access Lists)

IP filters (➤➤ **Access Lists**) in **X8500** are based on a concept of ➤➤ **filters**, rules and so-called chains. IP filters react to incoming data packets. You can therefore allow or deny access to **X8500** for certain data.

Filters A filter describes a certain part of the IP data traffic based on the source and/or destination IP address, ➤➤ **netmask**, protocol and source and/or destination port. If you define a filter, you should therefore tell **X8500**: "Watch out for all data packets that match the following: ...".

Rule You use a rule to tell **X8500** what the router is to do with the data packets filtered out, i.e. whether or not it should allow them to pass through. You can also define

several rules, which you arrange in the form of a chain to obtain a certain sequence.

Chain There are various approaches for the definition of rules and rule chains:

- Allow all packets that are not explicitly prohibited, i.e.:
 - Deny all packets that match Filter 1.
 - Deny all packets that match Filter 2.
 - ...
 - ...
 - Allow the rest.
- Allow only what is explicitly permitted, i.e.:
 - Allow all packets that match Filter 1.
 - Allow all packets that match Filter 2.
 - ...
 - ...
 - Deny the rest.
- Combination of the two possibilities described above
Several rule chains can be created, either completely or partly separated from each other. The common use of filters is possible and practicable.

Interface You can also define a rule chain individually for each **X8500** interface:

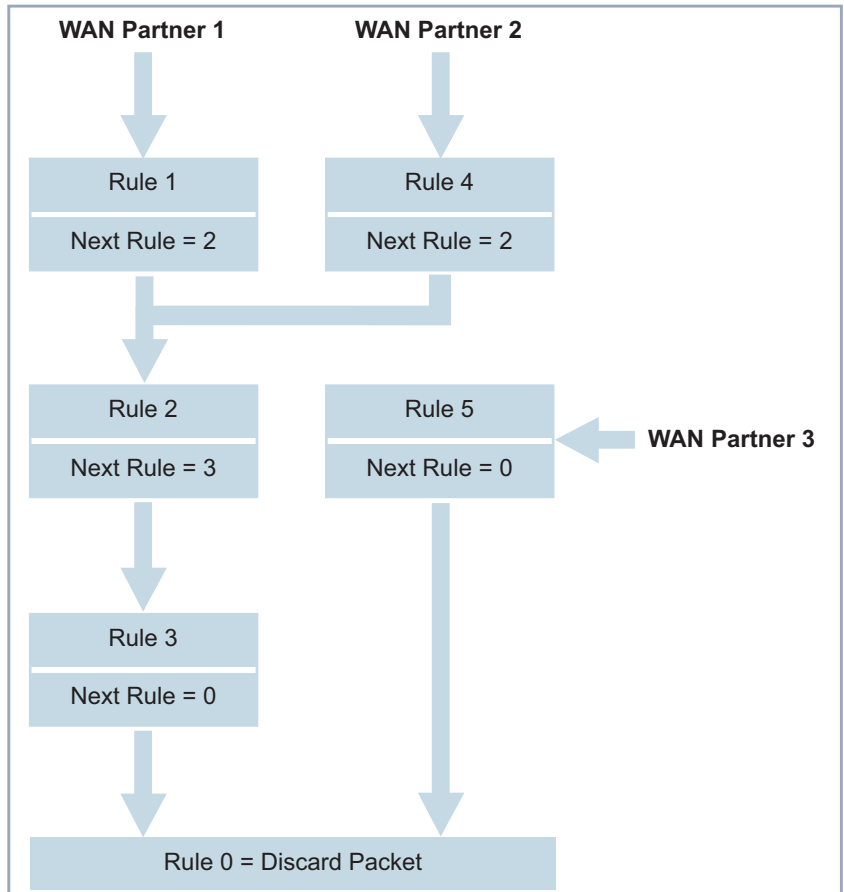


Figure 7-2: Rule chains for various interfaces

Configuration is made in:

- **IP** ► **ACCESS LISTS** ► **FILTER**
- **IP** ► **ACCESS LISTS** ► **RULES**
- **IP** ► **ACCESS LISTS** ► **RULES** ► **REORG**
- **IP** ► **ACCESS LISTS** ► **INTERFACES**

You can define filters in **IP** ► **ACCESS LISTS** ► **FILTER**:

Field	Meaning
Description	Designation of the filter. Note that only the first 10 or 15 characters are visible in other menus.
Index	Cannot be changed here. X8500 automatically issues a number to new filters defined here.
Protocol	Defines a protocol. Possible values: <i>any, icmp, ggp, ip, tcp, egp, igp, pup, chaos, udp, hmp, xns_idp, rdp, rsvp, gre, esp, ah, tlsp, skip, kryptolan, iso-ip, igrp, ospf, ipip, ipx-in-ip, vrrp, l2tp.</i> <i>any</i> matches any protocol, <i>tcp</i> matches only TCP data packets, etc.
Type	Only if Protocol = <i>icmp</i> . Possible values: <i>any, echo reply, destination unreachable, source quench, redirect, echo, time exceeded, param problem, timestamp, timestamp reply, address mask, address mask reply.</i> See RFC 792.
Connection State	If Protocol = <i>tcp</i> , you can define a filter based on the status of the TCP connection. Possible values: <ul style="list-style-type: none"> ■ <i>established</i>: All TCP packets that would not open any new connection on routing over X8500 match the filter. ■ <i>any</i>: All TCP packets match the filter.
Source Address	Source IP address of the data packets that matches the filter.
Source Mask	Source netmask. The combination of Source Address and Source Mask describes a range of IP addresses that match the filter.

Field	Meaning
Source Port	Source port number or range of source port numbers that matches the filter.
Specify Port	If Source Port or Destination Port = <i>specify</i> or <i>specify range</i> : Enter port number or range of port numbers (to Port).
Destination Address	Destination IP address of the data packets that matches the filter.
Destination Mask	Destination netmask. The combination of Destination Address and Destination Mask describes a range of IP addresses that match the filter.
Destination Port	Destination port number or range of destination port numbers that matches the filter.
Type of Service (TOS)	Type of Service.
TOS Mask	Mask for Type of Service.

Table 7-12: IP ► ACCESS LISTS ► FILTER

The **Source Port** and **Destination Port** fields contain the following selection options:

Possible Values	Meaning
<i>any</i>	All ►► port numbers match the filter.
<i>specify</i>	Permits the entry of a port number under Specify Port .
<i>specify range</i>	Permits the entry of a range of port numbers under Specify Port .
<i>priv (0..1023)</i>	Port numbers: 0 ... 1023.
<i>server (5000..32767)</i>	Port numbers: 5000 ... 32767.
<i>clients 1 (1024.0.4999)</i>	Port numbers: 1024 ... 4999.

Possible Values	Meaning
<i>clients 2 (32768..65535)</i>	Port numbers: 32768 ... 65535.
<i>unpriv (1024..65535)</i>	Port numbers: 1024 ... 65535.

Table 7-13: **Source Port** and **Destination Port**

Port numbers The port numbers are distributed as follows:

0 ... 1023	1024 ... 4999	5000 ... 32767	32768 ... 65535
Well-known ports, i.e. permanently assigned.	The ports are created by >>> clients and >>> servers dynamically and have no fixed meaning (except for special agreements): <i>unpriv (1024..65535)</i>		
<i>priv (0..1023)</i>	<i>clients 1 (1024.0.4999)</i>	<i>server (5000..32767)</i>	<i>clients 2 (32768..65535)</i>

Table 7-14: Ranges of port numbers

The following table contains a list of some frequently used port numbers with the services assigned to them:

Service	Protocol	Port number
File Transfer Protocol (>>> FTP) (data)	TCP	20
File Transfer Protocol (FTP) (commands)	TCP	21
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (>>> DNS)	TCP, UDP	53
Trivial File Transfer Protocol (>>> TFTP)	UDP	69
HTTP	TCP	80
POP3 (e-mail inquiry)	TCP	110
Network Time Protocol	TCP, UDP	119

Service	Protocol	Port number
➤➤ NetBIOS Name (NBNAME)	UDP	137
NetBIOS Datagram (NBDATA)	UDP	138
NetBIOS Session (NBSESSION)	TCP	139
Simple Network Management Protocol (SNMP) (Port Lists)	UDP	161
SNMP (Trap Port)	UDP	162
Syslog Service (SYSLOG)	UDP	514
Network File System (NFS)	UDP	2049
Remote CAPI	TCP	2662
Remote TAPI	TCP	2663

Table 7-15: Services and port numbers

Example A simplified FTP connection is used as an example to illustrate how to use source and destination ports: In addition to source and destination IP addresses, the IP protocol also uses source and destination port numbers to uniquely identify data connections. The FTP client creates a number, e.g. **xyz**, which is used as source port. As destination port, the client uses the number under which the FTP server offers the FTP service, e.g. **21**. The FTP server then answers with IP packets that use 21 as source port and xyz as destination port.

This is shown in the diagram below:

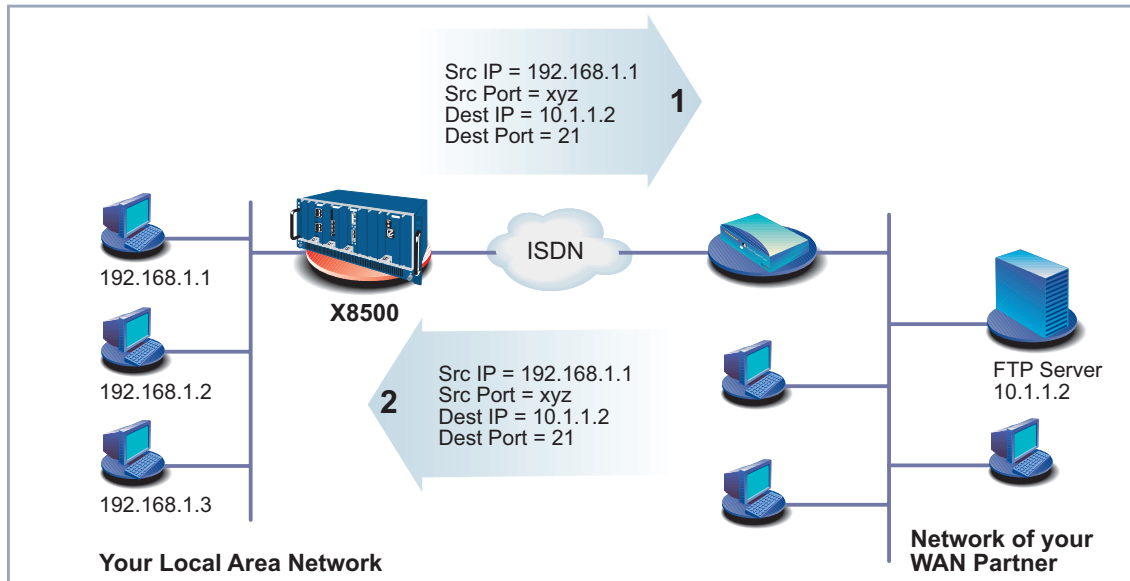


Figure 7-3: Example: FTP connection

You can define rules in **IP** ➤ **ACCESS LISTS** ➤ **RULES**:

Field	Meaning
Index	Cannot be changed. X8500 automatically issues a number to new rules defined here or displays the Index of existing rules.
Insert behind Rule	Appears only if a new rule is defined. Defines the rule behind which the new rule is inserted. You start a new independent chain with <i>none</i> .
Action	Defines the action to be taken for a filtered data packet.
Filters	Filter used.
Next Rule	Appears only if an existing rule is edited. Defines the next rule to be used.

Table 7-16: **IP** ➤ **ACCESS LISTS** ➤ **RULES**

The **Action** field contains the following selection options:

Possible Values	Meaning
<i>allow M</i>	Allow packet if it matches the filter.
<i>allow !M</i>	Allow packet if it does not match the filter.
<i>deny M</i>	Deny packet if it matches the filter.
<i>deny !M</i>	Deny packet if it does not match the filter.
<i>ignore</i>	Use next rule.

Table 7-17: **Action**

You can change the order of rules in a chain in the submenu **IP ► ACCESS LISTS ► RULES ► REORG**:

Field	Meaning
Index of Rule that gets Index 1	Defines the first rule in the chain.

Table 7-18: **IP ► ACCESS LISTS ► RULES ► REORG**

If you reorganize such a chain, **X8500** renumbers the remaining rules according to the selection in **Index of Rule that gets Index 1**:

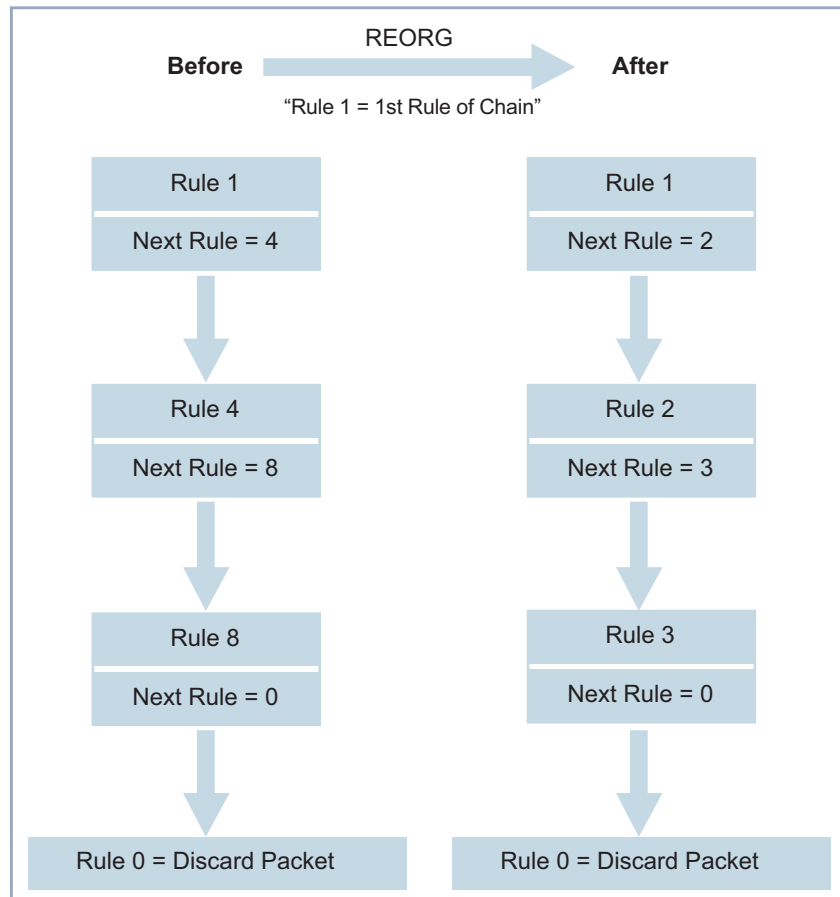


Figure 7-4: Example of chain reorganization



The rule with **Index = 1** is normally always used as the first rule for a newly created interface (e.g. to a WAN partner).

In **IP** ► **ACCESS LISTS** ► **INTERFACES**, you can define which interface starts with which rule and if and how the sender of a packet is to be informed if the packet is denied by **X8500** due to a filter violation:

Field	Meaning
Interface	X8500 interface
First Rule	Defines which rule is used first for data packets that reach X8500 via the interface . If you enter <i>none</i> , you specify that no filters are used for the Interface .
Deny Silent	Defines whether the sender of a packet is to be informed of its denial due to a filter violation. Possible values: <ul style="list-style-type: none"> ■ <i>no</i>: Packet is denied, sender is informed by a corresponding ICMP error message. ■ <i>yes</i>: Packet is denied, sender is not informed.
Reporting Method	Defines whether the denial of a packet due to a filter violation creates a syslog message. Possible values: <ul style="list-style-type: none"> ■ <i>none</i>: No syslog message. ■ <i>info</i>: A syslog message is generated with the protocol number, source IP address and source port number. ■ <i>dump</i>: A syslog message is generated with the contents of the first 64 bytes of the denied packet.

Table 7-19: **IP** ► **ACCESS LISTS** ► **INTERFACES**

To do Proceed as follows to define filters and rules:



Ensure that you don't lock yourself out when configuring the filters. For example, if you link the first filter to a rule that executes **Action = Allow M**, only what you have expressly allowed with the filter actually gets through. It may easily occur that your telnet access to **X8500** is no longer allowed as soon as you enter the rule and confirm with **SAVE**.

- Do not use any filters on the LAN interface (**First Rule = none**) if you access **X8500** from the LAN via telnet.

The serial interface and ISDN Login are independent of the filter settings for LAN interfaces.

- Filters**
- Go to **IP** ➤ **ACCESS LISTS** ➤ **FILTERS**.
 - Use **ADD** to add a new entry or select an existing entry. Press **Return** to change it.
 - Enter **Description**.
 - Select the desired **Protocol**.
 - Enter **Source Address**, if applicable.
 - Enter **Source Mask**, if applicable.
 - Select the desired value for **Source Port**.
 - Enter the desired value for **Specify Port**, if applicable.
 - Enter **Destination Address**, if applicable.
 - Enter **Destination Mask**, if applicable.
 - Select the desired value for **Destination Port**.
 - Enter the desired value for **Specify Port**, if applicable.
 - Enter the desired value for **Type of Service (TOS)**, if applicable.
 - Enter the desired value for **TOS Mask**, if applicable.
 - Confirm with **SAVE**.
 - Repeat these steps until you have defined all desired filters.



Do not forget to define a filter, if necessary, for enabling the remaining data packets (**Protocol** = *any*, **Source Port** = *any*, **Destination Port** = *any*).

➤ Leave **IP** ➤ **ACCESS LISTS** ➤ **FILTERS** with **EXIT**.

Rules

- Go to **IP** ➤ **ACCESS LISTS** ➤ **RULES** to interconnect the filters to form rule chains.
- Add a new entry with **ADD** or select an existing entry and confirm with **Return** to change it.
- Select **Insert behind Rule** if you create a new rule.
- Select the desired value for **Action**.
- Select the desired value for **Filter**.
- Select **Next Rule** if you change an existing rule.
- Confirm with **SAVE**.
- Repeat these steps until you have defined all desired rules.



Do not forget to define the last rule in the chain, if necessary, as a rule with a suitable filter for enabling all the remaining data packets (**Action** = *allow M*).



You can open a new rule chain with **Insert behind Rule** = *none*.

➤ Leave **IP** ➤ **ACCESS LISTS** ➤ **RULES** with **EXIT**.

Interface

- Go to **IP** ➤ **ACCESS LISTS** ➤ **INTERFACES**.
- Select an interface and confirm with **Return** if you wish to use a rule as the first rule for this interface that is not the rule displayed.
- Select **First Rule**.
- Select the desired value for **Deny Silent**.

- Select the desired value for **Reporting Method**.
- Confirm with **SAVE**.

Reorganizing a chain Proceed as follows to reorganize an existing chain of rules:

- Go to **IP** ➤ **ACCESS LISTS** ➤ **RULES** ➤ **REORG**.
- Select **Index of Rule that gets Index 1**.
- Confirm with **REORG**.



If you work with Windows PCs in your network, it is usually advisable to define a NetBIOS filter. An example of this configuration is explained step by step in [chapter 4.1.5, page 68](#).

7.2.9 Local Filters

Access to the local UDP and TCP services on **X8500** (telnet, ➤➤ **CAPI**, trace, etc.) can be controlled via the separate Setup Tool menu **IP** ➤ **LOCAL SERVICES ACCESS CONTROL**. One or more restrictions can be defined here for each service. If no entry exists for a service, there are no access restrictions for this service, i.e. access is possible to this service over all interfaces and from any source address, provided this is not prohibited by the use of NAT (see [chapter 7.2.7, page 304](#)) or global filters (see [chapter 7.2.8, page 315](#)).

Strategy As soon as at least one entry for local filters exists in **X8500**, incoming requests for the corresponding local services of **X8500** are only allowed if one of the following conditions is fulfilled:

- The source address is 127.0.0.1 (loopback address).
- No entry exists for the corresponding service.
- The incoming call is expressly allowed by at least one entry.

The existing entries are processed in the order in which they are listed in the corresponding table in the SNMP shell (**localTcpAllowTable** or **localUdpAllowTable**). If an entry in this sorted list does not apply, the next entry is checked. This enables requests over several interfaces or from several IP addresses to be admitted individually to a certain service.

If a matching entry for a request has still not been found after checking the last entry in the list, there are two alternatives:

- The request is forwarded to the relevant service if no entry in the list refers to this service.
- The request is rejected if one or more entries for this service exist in the list, but none of these matches the request.

Local filters therefore provide an additional tool that is different to handle than global filters and does not adversely affect performance in normal routing either.

Configuration is made in **IP** ► **LOCAL SERVICES ACCESS CONTROL** ► **ADD**:

Field	Meaning
Service	<p>Defines the local X8500 service to which access is to be controlled with this entry. Possible values:</p> <ul style="list-style-type: none"> ■ <i>snmp(udp)</i> ■ <i>rip(udp)</i> ■ <i>bootps(udp)</i> ■ <i>dns(udp)</i> ■ <i>telnet(tcp)</i> ■ <i>trace(tcp)</i> ■ <i>snmp(tcp)</i> ■ <i>capi(tcp)</i> ■ <i>tapi(tcp)</i> ■ <i>rfc1086(tcp)</i> ■ <i>http(tcp)</i> ■ <i>nbns(udp)</i> ■ <i>statmon(udp)</i>

Field	Meaning
Verify IP Address	<p>Defines if the source IP address is to be checked when an incoming call is received for the service selected under Service. Possible values:</p> <ul style="list-style-type: none"> ■ <i>verify</i> ■ <i>don't verify</i>
IP Address	<p>(Only if Verify IP Address = <i>verify</i>)</p> <p>Defines an IP address or network address (together with Mask) from which incoming requests are allowed for the service selected under Service. If a request has a different source address, the next entry is checked.</p>
Mask	<p>(Only if Verify IP Address = <i>verify</i>)</p> <p>Defines a netmask. A network address is thus defined together with the IP Address from which incoming requests are allowed to the service selected under Service. If a request has a different source address, the next entry is checked.</p> <p>If the value of Mask is <i>0.0.0.0</i> or <i>255.255.255.255</i>, the entry is a host entry, i.e. the IP address must match exactly.</p>
Verify Interface	<p>Defines if a check is to be made to determine which X8500 interface is used for an incoming call received for the service selected under Service. Possible values:</p> <ul style="list-style-type: none"> ■ <i>verify</i> ■ <i>don't verify</i>

Field	Meaning
Interface	(Only if Verify Interface = <i>verify</i>) Defines an interface of X8500 . If X8500 receives an incoming call over this interface for the service selected under Service , the connection is allowed. If the incoming call crosses another interface, the next entry is checked.

Table 7-20: **IP** ► **LOCAL SERVICES ACCESS CONTROL** ► **ADD**

Proceed as follows to restrict access to a local service:

If an entry defines both an address and an interface for checking, both criteria must be fulfilled for an incoming call before **X8500** accepts this call.



- Go to **IP** ► **LOCAL SERVICES ACCESS CONTROL**.
All the entries made until now are listed here.
- Confirm with **ADD** to add a new entry.
- Select the desired value for **Service**.
- Select **Verify IP Address**, e.g. *verify*.
- Enter the desired value for **IP Address**, if applicable.
- Enter the desired value for **Mask**, if applicable.
- Select **Verify Interface**, e.g. *verify*.
- Select the desired value for **Interface**, if applicable.
- Confirm with **SAVE**.
The entry is listed.

7.2.10 Back Route Verification

This term conceals a simple but very effective **X8500** function. If Back Route Verification is activated at a WAN partner, only those data packets are trans-

ported via the interface to the WAN partner that would be routed over the same interface on the back route. You can therefore prevent packets with fake IP addresses being fed to your LAN – even without filters. This means you can easily prevent known and as yet unknown Denial-of-Service and IP spoofing attacks.

To do Proceed as follows to activate Back Route Verification for a WAN partner:

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**.
- Activate **Back Route Verify** with *on*.
- Confirm with **OK**.

Backroute verification is temporarily saved and activated.

7.2.11 TAF Agent

Personalized authentication

The Token Authentication Firewall (TAF) function permits personal authentication of IP connection partners. BinTec's solution integrates the Token Authentication mechanisms from Security Dynamics and does not allow data packets to cross the router until the associated source address has been authenticated successfully.

You can enable this function (with extra license) on **X8500** and configure the router as TAF agent. A detailed description of the operation and the necessary configuration steps is contained in **BRICKware for Windows** and in the **Software Reference**.

7.2.12 Extended IP Routing (XIPR)

In addition to the normal routing table, **X8500** can also make routing decisions based on an additional table called the Extended Routing Table (Extended IP Routing). Apart from the destination address, **X8500** can also include the protocol, source and destination port, type of service (TOS) and the status of the destination interface in the decision. If there are entries in the **Extended Routing Table**, these are treated preferentially compared with entries in the normal routing table.

Example XIPR is useful, for example, if two networks are connected via ISDN with a LAN-LAN connection, but certain services (e.g. telnet) should be routed over an X.25 link and not over an ISDN switched connection. By making entries in the **Extended Routing Table**, you can allow part of the IP traffic to run over the ISDN dialup connection and part of the IP traffic (e.g. for telnet) to run over an X.25 link (see also the **Software Reference**).

Configuration Configuration is made in the Setup Tool menu **IP ► ROUTING ► ADDEXT**:

X8500 Setup Tool		BinTec Communications AG	
[IP][ROUTING][ADD]: IP Routing - Extended Route		MyX8500	
Route Type	Network route		
Network	WAN without transit network		
Destination IP Address			
Netmask			
Partner / Interface	BigBoss	Mode	always
Metric	1		
Source Interface	don't verify		
Source IP Address			
Source Mask			
Type of Service (TOS)	00000000	TOS Mask	00000000
Protocol	tcp		
Source Port	any		
Destination Port	any		
	SAVE	CANCEL	
Use <Space> to select			

The menu contains the following fields:

Field	Meaning
Route Type	Type of route. Possible values: <ul style="list-style-type: none"> ■ <i>Host route</i>: Route to a single host ■ <i>Network route</i>: Route to a network ■ <i>Default route</i>: Is only used if no other suitable route is available.
Network	Defines the type of connection (LAN, WAN), see table 7-22, page 335 .

Field	Meaning
Destination IP Address	Only for the value <i>Network route</i> or <i>Host route</i> for the field Route Type . IP address of the destination host or LAN.
Netmask	Only for the value <i>Network route</i> for the field Route Type . Netmask of Destination IP Address .
Partner / Interface	Only for the value <i>WAN without transit network</i> for the field Network . WAN partner.
Mode	Only for the value <i>WAN without transit network</i> for the field Network . Defines when the interface selected under Partner / Interface is to be used. Possible values, see table 7-23, page 336 .
Gateway IP-Address	Only for the value <i>LAN</i> or <i>WAN with transit network</i> for the field Network . IP address of "next hop" over which Destination IP Address is reached.
Metric	The lower the value, the higher the priority of the route (possible values <i>0...15</i>).
Source Interface	Interface over which the data packets reach X8500 .
Source IP Address	Source IP address of the source host or LAN.
Source Mask	Source netmask.
Type of Service (TOS)	Possible values: <i>0..255</i> as bit string.
TOS Mask	Bitmask for Type of Service .
Protocol	Defines a protocol. Possible values: <i>tcp, egp, pup, udp, hmp, xns, rdp, rsvp, gre, esp, ah, igmp, ospf, l2tp, dont ver, icmp, ggp.</i>

Field	Meaning
Source Port	Only for the value <i>tcp</i> or <i>udp</i> for the field Protocol . Source port number or range of source port numbers (see table 7-24, page 336).
Destination Port	Only for the value <i>tcp</i> or <i>udp</i> for the field Protocol . Destination port number or range of destination port numbers (see table 7-24, page 336).

Table 7-21: IP ► ROUTING ► ADDEXT

The **Network** field contains the following selection options:

Possible Values	Meaning
<i>LAN</i>	Route to a destination host or LAN that can be reached via X8500 's LAN interface.
<i>WAN without transit network</i>	Route to a destination host or LAN that can be reached via a WAN partner without including any transit network available.
<i>WAN with transit network</i>	Route to a destination host or LAN that can be reached via a WAN partner only via a transit network.
<i>Refuse</i>	X8500 discards data packets using this route and sends the sender a message saying the destination of the packet is unreachable.
<i>Ignore</i>	X8500 discards data packets using this route without sending a status message.

Table 7-22: Network

The **Mode** field includes the following selection options:

Possible Values	Meaning
<i>always</i>	Always use the route.
<i>dialup-wait</i>	Use the route if the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up". Otherwise reroute.
<i>dialup-continue</i>	Use the route if the interface is "up". If the interface is "dormant", then dial but reroute until the interface is "up". Otherwise reroute.
<i>up-only</i>	Use the route if the interface is "up". Otherwise reroute.

Table 7-23: **Mode**

The **Source Port** and **Destination Port** fields contain the following selection options:



Possible Values	Meaning
<i>any</i>	All   port numbers match the filter.
<i>specify</i>	Enables the entry of a port number.
<i>specify range</i>	Enables the entry of a range of port numbers.
<i>priv (0..1023)</i>	Port numbers: 0 ... 1023.
<i>server (5000..32767)</i>	Port numbers: 5000 ... 32767.
<i>clients 1 (1024.0.4999)</i>	Port numbers: 1024 ... 4999.
<i>clients 2 (32768..65535)</i>	Port numbers: 32768 ... 65535.
<i>unpriv (1024..65535)</i>	Port numbers: 1024 ... 65535.

Table 7-24: **Source Port** and **Destination Port**

Configuration Proceed as follows to configure extended IP routing:

 Go to **IP**  **ROUTING**  **ADDEXT**.

- Select a **Route Type**.
- Select the desired **Network**.
- Enter the desired **Destination IP Address**.
- Enter the desired **Netmask**.
- Select the desired **Partner / Interface**.
- Select the desired **Mode**.
- Enter the desired **Metric**.
- Select the desired **Source Interface**.
- Enter the desired **Source IP Address**.
- Enter the desired **Source Mask**.
- Select **Type of Service**.
- Enter the **TOS Mask**.
- Select the desired **Protocol**.
- Select the desired **Source Port**.
- Select the desired **Destination Port**.
- Define the **Source Port**, if applicable.
- Define the **Destination Port**, if applicable.
- Press **SAVE**.

Extended IP routing is configured for the interfaces entered.

You will find a detailed description (including configuration using the MIB variables) in the **Software Reference**.

7.3 Line Tapping Security

You can use an encryption mechanism to obtain data security for critical PPP connections over connections with critical security, provided both connection partners support this mechanism. The following functions are possible:

- Encryption ([chapter 7.3.1, page 338](#))
- VPN (with extra license) ([chapter 7.3.2, page 341](#))
- IPSec (with extra license) ([chapter 7.3.3, page 341](#))

7.3.1 Encryption

X8500 supports encryption of PPP connections to WAN partners.

The **MPPE** (Microsoft Point to Point **Encryption**) version 1 and 2, DES and Blowfish methods are used. DES and Blowfish are implemented as BinTec proprietary solutions.

MPPE V2 The MPPE Version 2 encryption protocol, the successor to MPPE, has been developed by Microsoft and also uses a 40-bit, 56-bit or 128-bit key. These are generated on authentication.

If one connection partner is set to MPPE V1 as encryption protocol, MPPE V2 is also accepted on connection setup if the set key length is the same.

DES and Blowfish If these proprietary encryption algorithms are used, either **X8500** can generate a key automatically or you can define an individual key statically in consultation with the connection partner.



The DES and Blowfish encryption algorithms are only supported if a license for VPN is entered in **X8500**.

Configuration is made in:

- **WAN PARTNER** ➤ **EDIT**

■ **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS (OPTIONAL)**

The following field in **WAN PARTNER** ► **EDIT** is relevant for this configuration step:

Field	Meaning
Encryption	<p>Defines the type of encryption that should be used for data traffic to the WAN partner. Can only be used if STAC compression is not activated for the connection. Possible values:</p> <ul style="list-style-type: none"> ■ <i>MPPE 40</i>: MPPE version 1 with 40-bit key ■ <i>MPPE V2 40</i>: MPPE version 2 with 40-bit key ■ <i>MPPE 56</i>: MPPE version 1 with 56-bit key ■ <i>MPPE V2 56</i>: MPPE version 2 with 56-bit key ■ <i>DES 56</i>: DES with 56-bit key (only available if VPN license is activated) ■ <i>Blowfish 56</i>: Blowfish with 56-bit key (only available if VPN license is activated) ■ <i>MPPE 128</i>: MPPE version 1 with 128-bit-key ■ <i>MPPE V2 128</i>: MPPE version 2 with 128-bit-key ■ <i>DES3 168</i>: Triple DES with 168-bit key (only available if VPN license is activated) ■ <i>Blowfish 168</i>: Blowfish with 168-bit key (only available if VPN license is activated) ■ <i>none</i>: No encryption <p>These values are only available if <i>PPP</i>, <i>Async PPP over X.75</i>, <i>Async PPP over X.75/T.70/BTX</i> or <i>X.25_PPP</i> has been selected under Encapsulation.</p>

Table 7-25: **WAN PARTNER** ► **EDIT**

If DES or Blowfish are used, the key can be generated automatically with authentication or defined statically. The following fields in the **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS (OPTIONAL)** menu are relevant for this purpose:

Field	Meaning
Encryption Key Negotiation	<p>Defines whether a key for the connection to the WAN partner is generated automatically or defined statically.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>authentication</i> (default value): Key is generated automatically by X8500. ■ <i>static</i>: The key is defined statically and must be entered under Encryption Key (TX) and Encryption Key (RX).
Encryption Key (TX)	<p>(Only for Encryption Key Negotiation = static)</p> <p>Key (in hexadecimal format) for encryption of outgoing data (must be the same as the entry under Encryption Key (RX) at the connection partner's).</p>
Encryption Key (RX)	<p>(Only for Encryption Key Negotiation = static)</p> <p>Key (in hexadecimal format) for encryption of incoming data (must be the same as the entry under Encryption Key (TX) at the connection partner's).</p>

Table 7-26: **WAN PARTNER** ► **ADD** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS (OPTIONAL)**

To do Proceed as follows to exchange data in encrypted form with a WAN partner:

- Go to **WAN PARTNER**.
- Select a WAN partner and confirm with **Return** to encrypt the PPP connections to this partner.
- Select **Encryption**, e.g. **DES 56**.

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS** ➤ **EXTENDED INTERFACE SETTINGS (OPTIONAL)**.
- Select **Encryption Key Negotiation**, e.g. **static** (if you wish to define the key yourself).
- Enter **Encryption Key (TX)**, if applicable, e.g. **1A:35:EF:C1:7B:56:D9** (RX for correspondent).
- Enter **Encryption Key (RX)**, if applicable, e.g. **89:A1:28:8C:D1:31:F7** (TX for correspondent).
- Confirm with **SAVE**.
- Confirm with **OK**.
- Confirm with **SAVE**.

The PPP connection with the selected VPN partner will be encrypted.

7.3.2 VPN (with extra license)

X8500 can set up a VPN (Virtual Private Network) using the PPTP (Point-to-Point Tunneling Protocol). This provides secure transmission of data over WAN connections, e.g. over the Internet. It can be used, for example, by field service staff to obtain low-cost access to data in the company network via Internet and laptop (dial-in via a local Internet Service Provider).



You can find detailed information and configuration instructions (with examples) in the **Software Reference**.

7.3.3 IPSec (with extra license)

The IPSec security standard (Internet Protocol Security) enables you to exchange IP-based data securely over public networks (e.g. the Internet).

More and more companies are handling more and more data communication over the Internet. To make sure their data remain confidential and cannot be seen by third parties or misused, these companies increasingly use encryption

technologies. A whole series of partly standard methods have been developed, which provide the technical basis for various VPN solutions. The PPTP (Point-to-Point Tunneling Protocol) and IPSec (IP Security) methods have become established as promising solutions in recent years. **X8500** supports both processes.

Whereas PPTP transmits the data in a tunnel at layer 2 (OSI model), IPSec operates at layer 3. The data are encrypted with a key length of up to 168 bits. IPSec also offers methods for authentication and administration of keys. As IPSec operates at layer 3, it is fully transparent for the user. This means that the data for transmission is always heavily encrypted without any action by the user. The encryption and negotiation of the different keys is carried out either by the router or for single users by an IPSec client that has been installed on the workstation. BinTec offers such a client in conjunction with the BinTec IPSec solution.

If you want to implement an IPSec solution with the **X8500**, you need an IPSec extra license. You can obtain this from your dealer.

Detailed information and configuration instructions can be found in the **IPSec Reference Manual**, which you receive together with your IPSec license.

7.4 Special Features

The following special features support your network security:

- Start-up Procedure ([chapter 7.4.1, page 343](#))
- Auto logout ([chapter 7.4.2, page 343](#))
- Prevention of Denial-of-Service Attacks ([chapter 7.4.3, page 343](#))

7.4.1 Start-up Procedure

X8500 does not start its routing activities until the complete configuration is loaded, especially the defined filters. This means it is not possible to provoke a system start to make use of an intermediate system state in which perhaps routing takes place before the filters are active.

7.4.2 Auto Logout

Connections to **X8500** via telnet, **isdnlogin** or serial interface are disconnected automatically if no entry is made on the keyboard for a period of 15 minutes. This makes it difficult to read out or change the system configuration on "forgotten" connections. You can change the time with the command `t <time in seconds>` (see [chapter 10.1, page 386](#)).

7.4.3 Prevention of Denial-of-Service Attacks

A Denial-of-Service (DoS) attack is an attempt to flood a system or force a restart by sending certain packets. This means the system or a certain service can no longer be used.

Some Denial-of-Service attacks on the router itself are already prevented by the internal coding.

For example, all **X8500** interfaces for which you activate Network Address Translation (NAT) protect the connected PCs against some DoS attacks with

fragmented packets. The packet fragments are assembled again on passing through NAT, before the packet can pass the router.

You can prevent some DoS attacks that operate with fake source IP addresses by using the Back Route Verification function (see [chapter 7.2.10, page 331](#)).

You can counter DoS attacks that speculate on destroying the system by causing the log files to overflow (syslog messages) by suitably positioning and limiting the size of these files.

7.5 Checklist

The following list indicates the most important critical security points that you should observe when configuring **X8500**:

- Have you changed all three passwords for system access (`admin`, `read`, `write`)? See [chapter 3.2, page 30](#).
- Are the activities of your **X8500** sufficiently accurately logged on at least one external computer and do you check the syslog messages regularly? See [chapter 7.1.1, page 284](#).
- Have you restricted access to the local services and resources to known computers or networks? In particular, you should only allow access via CA-PI, SNMP, trace and telnet to known computers.
- Are configuration files saved by TFTP kept in a safe place?
- Have you protected all PPP accesses with a password?
- If applicable, have you activated Network Address Translation (NAT) for the connection to the Internet Service Provider (ISP)? See [chapter 7.2.7, page 304](#).
- Have you limited the IP data traffic at critical interfaces, if necessary with the aid of filters, and prevented IP address spoofing? You should pay special attention to the interfaces you have not protected with NAT! See [chapter 7.2.8, page 315](#).
- Have you restricted remote maintenance access via ISDN Login? Have you made an entry under **BRI[x] ▶ INCOMING CALL ANSWERING** and/or **PRI[x] ▶ INCOMING CALL ANSWERING**? See "[Incoming Call Answering](#)", [page 77](#).

You should also observe the following additional points:

- Do you use the Microsoft callback procedure for PPP connections? Please refer to the information in [chapter 7.2.4, page 302](#).
- Do you use an encryption protocol for line tapping security on connections with critical security? See [chapter 7.3.1, page 338](#).

- Do you use personal authentication on connections with critical security?
- Do you allow the influence of routing protocols (e.g. RIP) only on trustworthy networks? See [chapter 5.2.9, page 180](#).
- Do you check what computers have access to the Remote CAPI interface, what applications are used on them and whether the connections used with these applications are desired? Do you use BinTec's user concept ([chapter 5.1.2, page 138](#))?
- Are any additional user accounts created trouble-free?
- Have you prevented the interception of connections on the Ethernet by a suitable LAN infrastructure?

8 Configuration Management and Flash Card

In this chapter, you will find instructions on the administration of your configuration files, handling the Smart Media Flash Card (SMFC) and on updating the **X8500** software. The following areas are covered:

- Administration of configuration files ([chapter 8.1, page 348](#))
 - Where are the configuration files?
 - What is flash and memory?
 - How do I handle configuration files?
- Working with the SMFC ([chapter 8.2, page 356](#))
- Updating software ([chapter 8.3, page 368](#))
 - How do I keep in touch with the latest developments?
 - How do I update the BOOTmonitor?
 - How do I load a new system software (software image/boot image)?
 - How do I update the module logic of the expansion cards?

8.1 Administration of Configuration Files

Internal flash EEPROM **X8500** reads its configuration information from configuration files. These configuration files are usually in the internal flash EEPROM (electronically erasable programmable read-only memory) of **X8500**. Several different configuration files can be stored in the internal flash EEPROM. The data also remains stored in the internal flash EEPROM when **X8500** is switched off.

Smart Media Flash Card (SMFC) The system card of **X8500** is equipped with one internal and one external slot for Smart Media Flash Cards (for installation, see **Hardware Installation Guide** and **Installation Guide Expansion Cards and Modules**). Smart Media Flash Cards (such as obtainable from photo shops) can be used for saving configurations and different versions of **X8500**'s system software. Cards with 16 MB and 32 MB of memory (all 3.3 V only) are supported. You will find a description of handling the SMFC in [chapter 8.2, page 356](#).

X8500 can also access system software or a configuration stored on the internal SMFC when it restarts.

Memory The current configuration and all changes you set during the operation of **X8500** are stored in the memory (RAM). The contents of the RAM are lost when **X8500** is switched off. So if you modify your configuration and want to keep these changes for the next time you start **X8500**, you have to save the modified configuration to the internal flash EEPROM before switching off: **Exit** ► **Save as boot configuration and exit** (see [chapter 4.4, page 126](#)). This file is then saved in the internal flash EEPROM as a boot configuration file under the name "boot". When **X8500** is started, it is usually this configuration file (see [chapter 8.3, page 368](#)) with the name "boot" that is loaded into the memory and takes effect.

Operations Imagine the internal flash EEPROM as a directory of configuration files. The files in this directory can be copied, moved, erased and newly created. It is also possible to transfer configuration files between **X8500** and a remote host by TFTP.

Windows In Windows, you can use the TFTP server of **DIME Tools** (see **BRICKware for Windows**). You can then, for example, save a configuration file from **X8500** on your local PC.



The names of the files to be transferred with the TFTP server of DIME Tools must be named according to the DOS name convention in "8.3" format and upper and lower case are ignore, e.g. ***b6101_b1.x8a***.

Unix A TFTP server is part of the system under Unix. Please read the instructions included in the **Software Reference**.

You can perform the various operations with the help of the Setup Tool:



You will find a detailed description of using the SMFC in [chapter 8.2, page 356](#).

➤ Go to the **CONFIGURATION MANAGEMENT** menu.

The following menu opens:

X8500 Setup Tool		BinTec Communications AG
[CONFIG]: Configuration Management		MyX8500
Operation	get (TFTP --> FLASH)	
TFTP Server IP Address	192.168.1.1	
TFTP File Name	x8500.cf	
Flash Type	removable Flash Card (internal)	
Name in Flash	boot	
Type of last operation	get (TFTP --> FLASH)	
State of last operation	done	
START OPERATION	EXIT	
Use <Space> to select		

The menu contains the following fields:

Field	Meaning
Operation	Operation you want to perform.

Field	Meaning
TFTP Server IP Address	<p>Only for the value <i>put</i>, <i>get</i> or <i>state</i> for the field Operation.</p> <p>The IP address or host name (if the host name can be resolved) of the TFTP server which you want to transfer a configuration file from or to.</p>
TFTP File Name	<p>Only for the value <i>put</i>, <i>get</i> or <i>state</i> for the field Operation.</p> <p>Name of the configuration file on the TFTP server (without path data).</p> <p>In exceptional cases, it may be necessary for certain Unix TFTP servers to enter the file name here with path data.</p>
Flash Type	<p>Here you enter the type of flash (internal flash EEPROM of X8500 or SMFC).</p> <p>Possible values:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>internal Flash Memory</i> (default value) <input type="checkbox"/> <i>removable Flash Card (internal)</i> <input type="checkbox"/> <i>removable Flash Card (external)</i> <p>This field appears only for the operations <i>save</i>, <i>load</i>, <i>put</i> and <i>get</i> to enable the relevant flash to be selected if using SMFCs.</p>
Name in Flash	Name of the configuration file in the flash.
New Name in Flash	<p>Only for the value <i>move</i> or <i>copy</i> for the field Operation.</p> <p>Name of the configuration file to be newly created in the internal flash EEPROM.</p>
Type of last operation	Type of previous operation (since the last X8500 start).
State of last operation	State of the last operation executed.

Table 8-1: **CONFIGURATION MANAGEMENT**

The **Operation** field contains the following selection options:

Possible Values	Meaning
<i>save</i> (MEMORY --> FLASH)	Save all current settings from memory to flash (internal flash EEPROM or SMFC) as configuration file Name in Flash . Name in Flash is overwritten or recreated.
<i>load</i> (FLASH --> MEMORY)	Loading the configuration file Name in Flash from flash to memory. The settings in Name in Flash take immediate effect.
<i>move</i> (FLASH --> FLASH)	Rename configuration file from Name in Flash to New Name in Flash in the internal flash EEPROM.
<i>copy</i> (FLASH --> FLASH)	Copy configuration file Name in Flash as New Name in Flash in the internal flash EEPROM.
<i>delete</i> (FLASH)	Delete configuration file Name in Flash in the internal flash EEPROM.
<i>put</i> (FLASH --> TFTP)	Transfer configuration file Name in Flash from flash (internal flash EEPROM or SMFC) to TFTP host with the IP address TFTP Server IP Address . TFTP File Name is then overwritten or recreated on the TFTP host with the contents of Name in Flash . TFTP File Name is saved in ASCII format and can be edited.
<i>get</i> (TFTP --> FLASH)	Transfer configuration file TFTP File Name from TFTP host with the IP address TFTP Server IP Address to flash (internal flash EEPROM or SMFC). Name in Flash is then overwritten or recreated with the contents of TFTP File Name . As the configuration file is transferred to flash (internal flash EEPROM or SMFC) and not to memory, the file must then be loaded (<i>load FLASH --> MEMORY</i>), so that the settings can take effect on X8500 .

Possible Values	Meaning
<i>state</i> (MEMORY --> TFTP)	Save all current settings in the memory as TFTP File Name on the TFTP host with the IP address TFTP Server IP Address . TFTP File Name is then overwritten or recreated.
<i>reboot</i>	Restart X8500 . Settings in the memory are replaced with the settings in the "boot" configuration file from the internal flash EEPROM or SMFC.

Table 8-2: Operation

The **State of last operation** field can display the following:

Possible Values	Meaning
<i>todo</i>	The operation has not yet been started.
<i>running</i>	The operation is being executed.
<i>done</i>	The operation has been executed successfully.
<i>error</i>	The operation could not be fully executed (see syslog message).

Table 8-3: State of last operation



If an error should occur while running *get (TFTP --> FLASH)* and the operation is aborted, the file to be overwritten in the flash (internal flash EEPROM or SMFC) is deleted. So if you transfer a "boot" file, **X8500**'s boot file will be deleted and **X8500** cannot load a configuration on restarting. If necessary, rename the file to be transferred!



To run *put (Flash --> TFTP)*, *get (TFTP --> Flash)* and *state (MEMORY --> TFTP)*, you need a TFTP server on the host to or from which you can transfer a configuration file.

If the TFTP host is a Windows PC, click **Program** ► **BRICKware** ► **DIME Tools** in the Windows Start menu to open **DIME Tools** and activate the TFTP server with **File** ► **TFTP Server** before you run the operation in question.



If you want to use your Windows PC as a TFTP host but are not sure what the IP address of the PC is, proceed as follows:

For Windows 95 and 98:

- Click **Run** in the Windows Start menu.
- Type in `winipcfg`.

A window opens where you can see the IP address of your PC and other network information.

For Windows NT and 2000:

- Click **Program** ➤ **Command Prompt** in the Windows Start menu.
- Enter `ipconfig` or `ipconfig/all` to request the IP address of your PC and other network information.

Running an operation To run an operation, proceed as follows:

- Select **Operation**.
- Activate a TFTP server if you have selected *put*, *get* or *state* as the **Operation**.
- Select or type in the necessary settings in **CONFIGURATION MANAGEMENT**.
- Select **START OPERATION** and press **Return**.

As long as the operation is being carried out, *OPERATING* appears in the help line of the Setup Tool; **State of last operation** displays *running*.

When the operation has been executed successfully, the operation is displayed under **Type of last operation**, **State of last operation** assumes the value *done*.



If *error* is displayed under **State of last operation**, check your settings:

- Have you entered the right IP address under **TFTP Server IP Address**?
- If using older versions of **BRICKware for Windows**: Does the name of the configuration file consist of a maximum of eight characters and the extension of a maximum of three characters (when using **DIME Tools**)?
- Does the host support TFTP (did you start the TFTP server of **DIME Tools** before starting the operation)?
- Is the source file in the configured directory of the TFTP path of **DIME Tools** (when **Operation** = *get*)? To change the TFTP path, refer to **BRICKware for Windows**.

If no errors are found in the above points, proceed as follows to find the cause of the problem:

- Leave the Setup Tool.
- Type in the following in the SNMP shell: `debug config &`.
- Reopen the Setup Tool with `setup`.
- Carry out the desired operation in **CONFIGURATION MANAGEMENT**.

If an error occurs, an error message is displayed in the help line of the Setup Tool to indicate the cause.

- Leave **CONFIGURATION MANAGEMENT** with **EXIT**.

Example You have created the configuration file X8500.cf. You have not transferred the file to **X8500** over the serial interface; X8500.cf can be found for example in the directory C:\PROGRAM FILES\BINTEC on your PC. Your PC has the IP address **192.168.1.1**. If you want to transfer X8500.cf from your PC to **X8500**, proceed as follows:

- For a Windows PC: Click the Windows Start button then **Program** ➤ **BRICKware** ➤ **DIME Tools** to start **DIME Tools**. The TFTP server must be located in the same directory as the configuration file and be activated.
- Activate a TFTP server under Unix: see the **Software Reference**.
- Go to **CONFIGURATION MANAGEMENT**.

TFTP host --> flash ➤ Select **Operation**: *get* (*TFTP --> FLASH*).

- Type in **TFTP Server IP Address**, e.g. **192.168.1.1**.
- Type in **TFTP File Name**: *X8500.cf*.
- Leave *internal Flash Memory* as **Type of Flash**.
- Type in **Name in Flash**, e.g. **boot**.
- Select **START OPERATION** and press **Return**.

As long as the operation is being carried out, *OPERATING* appears in the help line of the Setup Tool; **State of last operation** displays *running*.

When the operation has been successfully executed, *get (TFTP --> FLASH)* is displayed under **Type of last operation**; **State of last operation** assumes the value *done*.

The configuration file *X8500.cf* is saved, for example, in **X8500**'s flash under the name *boot*.

To make the settings of *X8500.cf* take immediate effect in **X8500**, proceed as follows:

Flash --> memory

- Reselect **Operation**: *load (FLASH --> MEMORY)*.
- Leave *internal Flash Memory* as **Type of Flash**.
- Select **Name in Flash**, e.g. **boot**.
- Select **START OPERATION** and press **Return**.

As long as the operation is being carried out, *OPERATING* appears in the help line of the Setup Tool; **State of last operation** displays *running*.

When the operation has been successfully executed, *load (FLASH --> MEMORY)* is displayed under **Type of last operation**; **State of last operation** assumes the value *done*.

The configuration file **boot** has been loaded to **X8500**'s memory and the settings have been activated.

- Leave **CONFIGURATION MANAGEMENT** with **EXIT**.

You have returned to the main menu.



There is another way to transfer configuration files using the XMODEM protocol over the serial interface. The procedure for this is explained in the **Software Reference**.

8.2 Smart Media Flash Card

Smart Media Flash Cards (such as obtainable from photo shops) can be used for saving configurations and different versions of **X8500**'s system software. Cards with 16 MB and 32 MB of memory (all 3.3 V only) are supported. The slots for the SMFCs on the system card of **X8500** are described in **Hardware Installation Guide** and **Installation Guide Expansion Cards and Modules**.

Configurations and versions of the system software are stored on the SMFCs in files, which are administrated using a DOS file system. The file names to be administrated must have the "8.3" format. Upper and lower case are ignored.

Configuration files are loaded and saved via the Setup Tool. Other functions for administrating the files on the SMFC are executed via the command line application "fssh" in the SNMP shell.

8.2.1 Formatting the Flash Card

Before being used for the first time, the SMFC must be formatted with the command `fssh format` in the SNMP shell. Refer to the description of the commands in [chapter 8.2.5, page 363](#).

The file system described below and the default directories are created on the SMFC with the command `format`.

8.2.2 File System and Directory Structures on the Flash Card

The SFMC contains an FAT-12 file system. All files must be named according to the DOS name convention in "8.3" format and upper and lower case are ignored.

The main directory of the internal SMFC is called `/card0/`, that of the external SMFC `/card1/`. The working directory is `/card0/x8500/autoexec/` for the internal SMFC and `/card1/x8500/autoexec/` for the external SMFC. All system software files or configuration files are saved automatically in this sub-directory using the command `fssh` (see [chapter 8.2.5, page 363](#)) or the Con-

figuration Management via the Setup Tool (see [chapter 8.2.4, page 359](#)). If directories other than the working directory are to be administrated with the command `fssh` or the Configuration Management commands, the full path name must always be given (also in the Setup Tool). The file name is sufficient for files in the working directory.

This is what to enter to copy a configuration file from the internal SMFC to the external SMFC:

```
fssh> copy /card0/x8500/autoexec/X8500.cf /card1/x8500/autoexec/X8500.cf
```

Table 8-4: Example entry to copy a configuration file from the internal SMFC to the external SMFC

This is what to enter to copy a configuration file from the external SMFC to the internal SMFC:

```
fssh> copy /card1/x8500/autoexec/X8500.cf /card0/x8500/autoexec/X8500.cf
```

Table 8-5: Example entry to copy a configuration file from the external SMFC to the internal SMFC

8.2.3 Behavior of X8500 with Flash Card in Boot Operation and Saving the Configuration

System software If at the time of restarting **X8500** the working directory of the internal SMFC contains a system software file with the attribute `boot` (see "[chattr](#)", [page 365](#)), **X8500** uses this system software for the restart.

A system message shows which system software **X8500** used for booting.

Booting the system software from the SMFC:

```
Searching image on Flash Card
Booting image from Flash Card .....OK (1114112 bytes)
Checking image ... OK
```

Table 8-6: Example of a system message for booting the system software from the internal SMFC

Loading and saving the system configuration

If at the time of restarting **X8500** the working directory of the internal SMFC contains a configuration file with the name "boot", this configuration is loaded during the restart and the configuration in the internal flash EEPROM is ignored. If this file is not present on the internal SMFC, **X8500** uses the configuration from the internal flash EEPROM as usual.

Syslog messages give you information about the configuration used for the restart. You can view syslog messages in **X8500**'s Setup Tool in the **MONITORING AND DEBUGGING** ► **MESSAGES** menu.

The following syslog message is created on loading the system configuration from the internal SMFC:

```
INFO/CONFIG: Flash Card configuration loaded
```

Table 8-7: Example of a system message for loading from the SMFC

If a SMFC is inserted in **X8500** at the time of saving the configuration with the Setup Tool (**EXIT** ► **SAVE AS BOOT CONFIGURATION AND EXIT**) and this card contains a configuration file with the name "boot", the configuration is written to this "boot" file when the configuration is saved on the SMFC. The existing content of the configuration file with the name "boot" on the SMFC is lost.

If no SMFC is inserted that contains a configuration file with the name "boot", the configuration is saved to the internal flash EEPROM under the name "boot" using **EXIT** ► **SAVE AS BOOT CONFIGURATION AND EXIT**.

8.2.4 Configuration Management for the Flash Card

Configuration Management with the Setup Tool (in the **CONFIGURATION MANAGEMENT** menu) has been extended for the SMFC:

X8500 Setup Tool		BinTec Communications AG
[CONFIG]: Configuration Management		MyX8500
Operation	get (TFTP --> FLASH)	
TFTP Server IP Address	192.168.1.1	
TFTP File Name	x8500.cf	
Flash Type	removable Flash Card (internal)	
Name in Flash	boot	
Type of last operation	get (TFTP --> FLASH)	
State of last operation	done	
START OPERATION		EXIT
Use <Space> to select		

For the meaning of the individual fields of the Setup Tool, see [table 8-1, page 350](#), [table 8-2, page 352](#) and [table 8-3, page 352](#).



To copy a configuration file from the internal flash EEPROM to the SMFC or vice versa, the desired configuration file must first be loaded into the RAM (**MEMORY**) of **X8500** using *load*. The configuration must then be saved again to the SMFC or internal flash EEPROM using *save*.



If an error should occur while running *get (TFTP --> FLASH)* and the operation is aborted, the file to be overwritten in the flash (internal flash EEPROM or SMFC) is deleted. So if you transfer a "boot" file to the internal flash EEPROM of **X8500**, **X8500**'s boot file will be deleted. **X8500** can no longer load a configuration on booting. If necessary, rename the file to be transferred!



To run *put (Flash --> TFTP)*, *get (TFTP --> Flash)* and *state (MEMORY --> TFTP)*, you need a TFTP server on the host which you want to transfer a configuration file to or from.

If the TFTP host is a Windows PC, click **Program** ► **BRICKware** ► **DIME Tools** in the Windows Start menu to open **DIME Tools** and activate the TFTP server with **File** ► **TFTP Server** before you run the operation in question.



If you want to use your Windows PC as a TFTP host but are not sure what the IP address of the PC is, proceed as follows:

For Windows 95 and 98:

- Click **Run** in the Windows Start menu.
- Type in `winipcfg`.
A window opens where you can see the IP address of your PC and other network information.

For Windows NT and 2000:

- Click **Program** ➤ **Command Prompt** in the Windows Start menu.

Type in `ipconfig` or `ipconfig/all` to request the IP address of your PC and other network information.

Running an operation

Proceed as follows to run an operation in the **CONFIGURATION MANAGEMENT** menu:

- Select **Operation**.
- Activate a TFTP server if you have selected *put*, *get* or *state* as the **Operation**.
- Select or type in the necessary settings in the **CONFIGURATION MANAGEMENT** menu.
- Select **START OPERATION** and press **Return**.

As long as the operation is being carried out, *OPERATING* appears in the help line of the Setup Tool and **State of last operation** displays *running*.

When the operation has been successfully executed, it is shown under **Type of last operation**. **State of last operation** shows the value *done*.



If *error* is displayed under **State of last operation**, check your settings:

- Have you entered the right IP address under **TFTP Server IP Address**?
- If using older versions of **BRICKware for Windows**: Does the name of the configuration file consist of maximum eight characters and the extension of maximum three characters (when using **DIME Tools**)?
- Does the host support TFTP (did you start the TFTP server of **DIME Tools** before starting the operation)?
- Is the source file in the configured directory of the TFTP path of **DIME Tools** (when **Operation = get**)? To change the TFTP path, refer to **BRICKware for Windows**.

If no errors are found in the above points, proceed as follows to find the cause of the problem:

- Leave the Setup Tool.
- Type in the following in the SNMP shell: `debug config &`.
- Reopen the Setup Tool with `setup`.
- Carry out the desired operation in **CONFIGURATION MANAGEMENT**.
If an error occurs, an error message is displayed in the help line of the Setup Tool to indicate the cause.

- Leave **CONFIGURATION MANAGEMENT** with **EXIT**.

Example Your SMFC contains the file "X8500.cf". You want to copy the file with the name "boot" from the SMFC to the internal flash EEPROM of **X8500**. The file is then available as a new configuration file when **X8500** restarts. Copying a configuration file from the SMFC into the internal flash EEPROM is only possible by loading it into the RAM (memory) of **X8500**.



Note that the operation described here will overwrite any existing file with the name "boot" that is present in the internal flash EEPROM of **X8500**. We recommend that you rename it first or make a backup copy of the old "boot" file.

The SMFC must be inserted in **X8500**.

- Go to **CONFIGURATION MANAGEMENT**.

Loading from the Flash Card into X8500's RAM

- Select **Operation**: *load (FLASH --> MEMORY)*.
- Select **Flash Type**: *removable Flash Card (internal)*.
- Select **START OPERATION** and press **Return**.

OPERATING appears in the help line of the Setup Tools as long as the operation is running. **State of last operation** shows *running*.

When the operation has been successfully executed, *load (FLASH --> MEMORY)* is shown under **Type of last operation**. **State of last operation** shows the value *done*.

The configuration file "X8500.cf" has been loaded to X8500's memory and the settings are active immediately.

Finally, proceed as follows to save the now active configuration file to the internal flash EEPROM of X8500:

Saving a Configuration File from the RAM to the Internal Flash EEPROM of X8500

- Select **Operation**: *save (MEMORY --> FLASH)*.
- Select **Flash Type**: *internal Flash Memory*.
- Enter **Name in Flash**: *boot*.
- Select **START OPERATION** and press **Return**.

OPERATING appears in the help line of the Setup Tools as long as the operation is running. **State of last operation** shows *running*.

When the operation has been successfully executed, *save (MEMORY --> FLASH)* is shown under **Type of last operation**. **State of last operation** shows the value *done*.

The configuration file "boot" has been saved to the internal flash EEPROM of X8500. Your settings remain active and will also be loaded again on a restart even if the SMFC is not inserted.

- Leave **CONFIGURATION MANAGEMENT** with **EXIT**.

How to use the commands `cmd=load`, `cmd=save`, `cmd=put` and `cmd=get` in the SNMP shell is described in BinTec's **Software Reference**. You can use these commands to access the SMFC by inserting the file name `"/card0/"` for



the internal SMFC and `/card1/` for the external SMFC before the parameter path. See [chapter 8.2.2, page 356](#).

8.2.5 Command `fssh` in the SNMP Shell of X8500

The command `fssh` is available in the SNMP shell for operations with the SMFC. With the command `fssh -n0`, you select the working directory of the internal SMFC; with the command `fssh -n1` you select the working directory of the external SMFC. `fssh` can be started in command line mode (`fssh <command> <parameter>`) or in interactive mode (`fssh -i`).



Please note:

Parameters shown in the command lines inside square brackets [] represent optional values. Terms inside angle brackets < > can have different values. Do not enter any brackets!



If you enter the command `fssh` without the parameters `-n0` or `-n1`, you select the working directory of the internal SMFC.

Command Line Mode

```
fssh -n0 <command> <parameter> (for the internal SMFC)
```

```
fssh -n1 <command> <parameter> (for the external SMFC)
```

In this mode, you must always enter the command `fssh` first and then the relevant command for executing an operation.

Interactive Mode

```
fssh -i -n0 (for the internal SMFC)
```

```
fssh -i -n1 (for the external SMFC)
```

`fssh -i` starts the interactive mode for SMFC operations. If you are in interactive mode, `fssh >` appears as input prompt. You can now enter all com-

mands directly – without "fssh". To leave the interactive mode enter the command `quit`.

The following commands are available for operations on the SMFC:

format

```
format
```



The command `format` deletes all data on the SMFC!

The command `format` is used to format a SMFC. The SMFC must be formatted before being used for the first time in order to create the file system and directory structure described in [chapter 8.2.2, page 356](#).

dir

```
dir [<directory name>]
```

Shows the content of the SMFC (file names and attributes set) in the working directory without parameters. Entering a directory shows the content of this directory.

del

```
del <file name>
```

Deletes the file `<file name>` from the SMFC.

- `file name`: File name of the file to be deleted.

copy

```
copy <file name> <new file name>
```

Creates a copy of the file `<file name>` under the new name `<new file name>`.

- `file name`: File name of the original file.
- `new file name`: File name of the copy of the file.

move

```
move <file name> <new file name>
```

Renames the file <file name> to the file <new file name>.

- file name: File name of the file.
- new file name: New file name of the file.

update

```
update <host> <remote file> [<local file>]
```

Loads the system software file <remote file> from the PC <host> via TFTP with the file name <local file> into the working directory (see [chapter 8.2.2, page 356](#)) on the SMFC. The attribute `boot` is set for the system software file. This makes the file bootable. See also "[chattr](#)", [page 365](#).

- host: The IP address of the PC (TFTP server) on which the file is located.
- remote file: File name of the system software file.
- local file: File name of the system software file on the SMFC.

If the parameter `local file` is not used, the system software file is automatically given the file name "X8nnn.X8A" on writing to the SMFC, where "nnn" stands for the version number of the system software file. If the parameter `local file` is used, the system software file on the SMFC is given this name. The file name is not assigned automatically as described above.



Information about patch or beta versions of system software is lost if the command `update` is used without the parameter `local file`.

Example: The system software file for version 6.1.1 is overwritten by the system software file version 6.1.1 Patch 4, because both files are given the same file name on writing to the SMFC.

Use the parameter `local file` for such cases.

chattr

```
chattr <file name> <+boot | -boot>
```

Changes the `boot` attribute of a file. Only one system software file can be bootable on the SMFC at any one time. If the `boot` attribute is set for a second file, this automatically resets the `boot` attribute of the first file.

- `file name`: File name of the file for which the `boot` attribute is to be set or removed.
- `+boot`: Sets the `boot` attribute of a file.
- `-boot`: Removes the `boot` attribute of a file.

For checking the attributes, see "[dir](#)", [page 364](#).

tftpget



The commands `tftpget` and `tftpput` are only to be used for transferring system software files. For the management of configuration files, the commands described in [chapter 8.2.4, page 359](#) must be used.

A configuration file that is saved to the SMFC by a TFTP server using the command `tftpget` cannot be read by the system software of **X8500!**

```
tftpget <host> <remote file> <file name>
```

Loads the file `<remote file>` from the PC (TFTP server) `<host>` and saves it under the indicated name `<file name>` on the SMFC.

- `host`: The IP address of the PC (TFTP server) on which the file is located.
- `remote file`: File name of the file on the TFTP server.
- `file name`: File name of the file on the SMFC.

tftpput



The commands `tftpget` and `tftpput` are only to be used for transferring system software files. For the management of configuration files, the commands described in [chapter 8.2.4, page 359](#) must be used.

A configuration file that is saved to the SMFC by a TFTP server using the command `tftpget` cannot be read by the system software of **X8500!**

```
tftpput <host> <remote file> <file name>
```

Saves the file `<file name>` under the name `<remote file>` via TFTP on the PC (TFTP server) `<host>`.

- `host`: The IP address of the PC (TFTP server) on which the file is to be saved.
- `remote file`: File name of the file on the TFTP server.
- `file name`: File name of the file on the SMFC.

fsck

`fsck`

Checks the file system of the SMFC, but makes no corrections.

8.3 Updating Software

As BinTec Communications AG is constantly improving the software for all its products and you certainly want to use the latest features of **X8500**, this chapter tells you how to update your software.

www.bintec.net If you want to update your software, load the new system software in **X8500** (software image/boot image). Every system software includes new features, better performance and any necessary bugfixes from the previous version. You can find the most up-to-date system software available from BinTec Communications AG on the World Wide Web at www.bintec.net. Here you can also find current product-specific documentation (**Release Notes**, **User's Guides**) and general product information (**Software Reference**, **BRICKware for Windows**).



If you want to update your software, make sure you read the corresponding release notes. The **Release Notes** describe the changes provided by the new system software (software image/boot image).

update There are various ways to update software. This chapter will show you how to update with the help of the update command in the SNMP shell, which is described step for step. The alternatives to this method can be found in the **Software Reference**.



Caution!

An update of the module logic, BOOTmonitor and/or firmware logic is also recommended in isolated cases. If this should be the case with a new release, this is clearly noted in the corresponding **Release Notes** at www.bintec.net. The result of incorrect updating operations (e.g. power cut during the update) could be that **X8500** no longer boots!

► Update the module logic, BOOTmonitor or firmware logic only if BinTec Communications AG explicitly recommends such action!

8.3.1 BOOT Sequence

X8500 passes through various functional states on starting:

- Start Mode
- BOOTmonitor Mode
- Normal Operation Mode

After several selftests have been performed successfully in Start Mode, **X8500** changes to the BOOTmonitor Mode. The BOOTmonitor prompt is displayed if you are connected to **X8500** via a terminal program.

BOOTmonitor Press **Space** within four seconds of the display of the BOOTmonitor prompt if you want to use the BOOTmonitor functions. If you do not make an entry within four seconds, **X8500** changes back to Normal Mode.

Functions The BOOTmonitor provides the following functions, which you select by entering the relevant digit (for more detailed information, refer to **Software Reference**):

- (1) Boot system:
X8500 loads the compressed boot file from the flash memory to the RAM memory. This happens automatically when started.
- (2) Software update via TFTP:
X8500 performs a software update via a TFTP server.
- (3) Software update via XMODEM:
X8500 performs a software update over a serial interface with XMODEM.
- (4) Delete configuration:
X8500 is reset to the unconfigured ex works state. All configuration files are deleted and the BOOTmonitor settings are set to the default values.
- (5) Default BOOTmonitor parameters:
You can change the default settings of **X8500**'s BOOTmonitor, e.g. the baud rate for serial connections.



If you change the baud rate (the preset value is 9600 bauds), make sure the terminal program used also uses this baud rate. If this is not the case, you will not be able to establish a serial connection to **X8500**!

- (6) Show system information
Shows system information of **X8500**, such as serial number, MAC address and software version.

8.3.2 Updating BOOTmonitor

Proceed as follows to update the BOOTmonitor:

- Log in to **X8500** from a computer serially connected to **X8500**.
- Activate a TFTP server on your PC.
For a Windows PC: Click the Windows Start menu and then **Program** ➤ **BRICKware** ➤ **DIME Tools** to start **DIME Tools** (for installation of **DIME Tools**, see [chapter 3.5.3, page 49](#)). Activate the TFTP server.
For a Unix computer: Follow the instructions in the **Software Reference**.
- Restart **X8500**, e.g. `cmd=reboot`.
- Press **Space** to enter the BOOTmonitor menu, as described in "[BOOT Sequence](#)", [page 369](#).
- Carry out the software update via TFTP (option 2) in the BOOTmonitor. You must enter the IP address of **X8500**, the IP address of the TFTP server and the file name of the file for the BOOTmonitor.

```
Your choice<2
Enter local IP address [192.168.1.254]:
Enter IP address of TFTP server [192.168.1.1]:
Enter file name of image [b6101.x8a]: bm6101.x8a

Are your entries correct (y or n) ?
```

- Re-examine your settings. If your settings are correct, confirm with `y` and the **RETURN** key.

```
Are your entries correct (y or n) ? y

Starting file transfer .....OK (131124 bytes received)
Checking new image ... OK

Loaded new bootmonitor has release 6.1.1.

*** Don't power-off your router while the update takes place ***
```

- If no errors have occurred, confirm with `y` to update the BOOTmonitor.

```
Do you want to update your bootmonitor (y or n) ? y
Bootmonitor update complete
```

- After the message saying the update is finished appears, restart **X8500**.



Caution!

At this point, it is extremely important that **X8500** is switched on and off, so that there is an interruption to the power supply.

- After a message appears saying the update was successful, switch **X8500** off and on again.

8.3.3 Update System Software

To do Proceed as follows to update the system software:

- Make sure a formatted SMFC is inserted in the internal SMFC slot.



Do not turn **X8500** off during the update!

Before starting the update, deactivate auto logout by entering `t 0` in the SNMP shell.

- Type in the URL `www.bintec.net` in your browser (e.g. Internet Explorer or Netscape Navigator).

The BinTec home page opens.

- Click **Downloads** and choose the ftp or http link.
Here you will find the latest software and documentation for BinTec products.
- Click **X8500**.
Here you will find the latest software and documentation for **X8500**.
- Click (right-click for ftp) the current system software (software image/boot image), e.g. **Software Image Rel. 6.1 Rev.1**.
- In the context menu, type in the directory and name under which the new system software (software image/boot image) should be saved on your PC. Use a clearly recognizable name, e.g. **b6101.x8a**.
- Confirm with **SAVE**.
The system software is saved on your PC.
- Activate a TFTP server on your PC.
For a Windows PC: Click the Windows Start menu and then **Program** ➤ **BRICKware** ➤ **DIME Tools** to start **DIME Tools** (for installation of **DIME Tools**, see [chapter 3.5.3, page 49](#)). Activate the TFTP server. The TFTP server must be located in the same directory as the system software.
For a Unix computer: Follow the instructions in the **Software Reference**.
- Log in to **X8500** as "admin", if you have not already done so.
- Deactivate auto logout with `t 0`.
- In the SNMP shell, type in `fssh update <IP address> <file name>`.
The `<IP address>` is the IP address of the TFTP server, e.g. the IP address of your Windows PC on which the TFTP server of **DIME Tools** is running and on which you have saved the new system software (e.g. **192.168.1.1**).



In exceptional cases, it may be necessary for certain Unix TFTP servers to enter the file name here with path data.

<file name> is the name of the system software you have saved on your PC (e.g. **b6101.x8a**).

The file <file name> is first transferred to the memory of **X8500**. The new system software is loaded in the internal SMFC.

- Enter `cmd=reboot` and confirm with **Return**.
X8500 starts with the new system software. The existing configuration is transferred.

8.3.4 Updating Module Logic

This chapter describes how you update the module logic of the expansion cards.

Proceed as follows to update the module logic:

- Save the new module logic on your PC.
- Log in to **X8500** as "admin", if you have not already done so.
- In the SNMP shell, type in `update <IP address> <file name>`.
The <IP address> is the IP address of the TFTP server, e.g. the IP address of your Windows PC on which the TFTP server of **DIME Tools** is running and on which you have saved the new system software (e.g. **192.168.1.1**).
<file name> is the name of the module logic you have saved on your PC (e.g. **x8e-2bc.x8a**, the module logic for the expansion card X8E-2BC).
The following appears: Perform Flash-ROM update (y or n)?
- Enter `y` and confirm with **Return**.
The software update is executed and the new module logic is loaded in the internal flash memory.
- Reboot **X8500**, e.g. with `cmd=reboot`, to activate the new module logic, and confirm with **Return**.
X8500 starts with the new module logic. The existing configuration is transferred.

9 Troubleshooting

Tips If you are having problems with **X8500**, the following tips should help you to overcome some of the more usual stumbling blocks:

- Log in to **X8500** and enter in the SNMP shell:
`debug all`
This makes available all the debugging information in the SNMP shell.
- Check the syslog messages created by **X8500** (see [chapter 7.1.1, page 284](#)). It is wise to forward syslog messages to an external host and save them to be able to evaluate the outputs for a longer period of time.

To interpret debugging information and syslog messages, see the **Software Reference**.

This chapter shows you what the causes of particular problems can be and how to determine these causes. It is structured as follows:

- Aids to Troubleshooting ([chapter 9.1, page 376](#))
- Typical Errors ([chapter 9.2, page 379](#))

9.1 Aids to Troubleshooting

Here you can find aids to help narrow down the possible causes of your problem:

- Local SNMP Shell Commands
- External Aids

9.1.1 Local SNMP Shell Commands

These commands are entered directly in **X8500**'s SNMP shell:

debug

You can use the `debug` command for troubleshooting in one or more sub-systems of **X8500**. A detailed explanation of the syntax and options can be found in [chapter 10.1, page 386](#).

Examples:

- Enter `debug all` to display debugging information for all subsystems.



If you add `&` to an SNMP shell command, the program runs in the background. You cancel the command with **Ctrl-C**.

isdnlogin

You can use the `isdnlogin` command to verify that an ISDN connection can be made. This is explained in [chapter 10.1, page 386](#).

Example:

- Enter `isdnlogin 1234 telephony` to establish a connection to the telephone in your local office with the number 1234.
If a connection is made, the telephone will ring.

trace



Caution!

If you use the trace command with remote sessions be careful not to trace your own session.

- Do not trace your own session!

The `trace` command can be used to display and interpret data packets sent or received over ISDN (D and B-channels) and over the LAN. An explanation of the syntax can be found in [chapter 10.1, page 386](#).

Examples:

- Enter `trace -ip` next to display data packets that are to run over the next B-channel to be opened.
- Enter `trace -h2i -s me -d 0:a0:f9:d:5:a 0 0 1` to output data packets sent from **X8500**'s MAC address over the LAN to the host with the MAC address 0:a0:f9:d:5:a.



You cancel the command with **Ctrl-C**.

9.1.2 External Aids

You can analyze connections to **X8500** using the following utility programs on a Windows PC or Unix workstation.

DIME Tracer (Windows)

The DIME Tracer enables you to trace **X8500**'s ISDN and CAPI data traffic from a Windows PC. DIME Tracer is a part of DIME Tools. A detailed explanation can be found in **BRICKware for Windows**.

bricktrace (Unix)

The bricktrace program enables data sent over **X8500**'s ISDN channels to be inspected at a Unix workstation. "bricktrace" is part of BRICKtools for UNIX on your BinTec Companion CD. A detailed explanation can be found in [chapter 10.2, page 393](#).

9.2 Typical Errors and Procedure

A compilation of typical error situations with instructions for error detection and clearance is given below. Try to narrow down the causes of the problem. This chapter is divided into two categories:

- System errors ([chapter 9.2.1, page 379](#))
- ISDN connections ([chapter 9.2.2, page 380](#))

9.2.1 System Errors

I have forgotten my password.

You must reset **X8500** to the unconfigured initial state (ex works state):

- Connect your PC over the serial interface to **X8500** as explained in the **Hardware Installation Guide** you received with X8A-BOSS.
- Switch **X8500** off and then switch it on again.
You see various selftests and then "Press <sp> for BOOTmonitor or any other key to boot system".
- Now press the **Space** bar.
A BOOTmonitor menu is displayed.
- Select "(4) Delete Configuration" and press **Return**. Note and confirm the following safety prompts.
The password as well as the complete configuration of **X8500** are deleted.
- Select "(1) Boot System".
X8500 is restarted.
- Reconfigure **X8500**.

I can't reach **X8500** in the LAN.

Try to set up a serial connection:

- Connect your PC to **X8500** over the serial interface.
- Log in as the user `admin` with the corresponding password.

- Start the Setup Tool with `setup`.
- Check if a configuration error is the cause: Have you entered a filter under **IP** ➤ **ACCESS LISTS** that is locking you out? If so, make the required corrections.
- Check NAT on LAN interface ([chapter 7.2.7, page 304](#)): Have you activated NAT for this interface?
- Check IP address and netmask for this interface: Are they valid?
- Try to connect to the router with the IP address instead of the symbolic name.

If a serial connection does not work either:

- Check the settings of the terminal program (see [chapter 3.1.1, page 25](#)). If you have changed the default settings in BOOTmonitor, adjust your terminal settings accordingly.
- If this doesn't succeed, proceed as described under "[I have forgotten my password.](#)", [page 379](#).

9.2.2 ISDN Connections

Here you will find possible causes of errors in ISDN connections.

Your telephone bill is unusually high.



Use the Credits Based Accounting System (see [chapter 7.1.3, page 293](#)). This enables you to set a limit for connections to **X8500** to prevent unnecessary charges accumulating as a result of mistakes made during configuration.

X8500 possibly has ISDN connections that remain connected or unwanted ISDN connections are set up, which cause additional costs.

- Use `debug all` or `trace` to check if a PC in the LAN is using a different netmask from the one entered on **X8500**.
- Use `debug all` or `trace` to check if a PC in the LAN is configured for Remote CAPI with an incorrect IP address (destination port 2662).

- Use **SYSTEM ▶ EXTERNAL SYSTEM LOGGING** to check if **X8500** is configured so that syslog messages are sent to a host outside the LAN (destination port 514).
- Use **IP ▶ STATIC SETTINGS** to check if an IP address located outside the LAN has been entered for **X8500** under **Time Server**.
- Use **SYSTEM ▶ EXTERNAL ACTIVITY MONITOR** to check if **X8500** is configured so that **Activity Monitor** data packets are sent to a host outside the LAN (destination port 2107).
- Check the MIB table **biboAdmTrapHostTable** to determine if **X8500** is configured so that SNMP traps are sent to a host outside the LAN (destination ports 161, 162).
- Check if the second B-channel is frequently set up and cleared for connections with dynamic channel bundling due to fluctuating traffic.
- Use `debug all` or `trace` to check if a PC in the LAN is configured for the WINS server with an incorrect IP address (destination ports 137-139). If necessary, configure the PC properly or set the corresponding filters.
- Use `debug all` or `trace` to check if a PC in the LAN is configured for the resolution of NetBIOS names with the help of DNS (it is accessed from a client port to destination port 53). Do not try to resolve NetBIOS names with DNS!
- Use `debug all` or `trace` to check if an application on a PC in the LAN is trying to resolve names that the name server at the Internet provider does not know (it is accessed from a client port to destination port 53). Install a local HOSTS file in the Windows directory that can carry out name resolution.
- Use `debug all` or `trace` to check if "NetBIOS over IP" is configured on a PC in the LAN (it is accessed from source port 137 to destination port 53). An attempt is thus made to resolve NetBIOS names over DNS. Disable "NetBIOS over IP" or insert filters. Configuration of the corresponding filters can be found in [chapter 7.2.8, page 315](#)).
- Check if you have configured Callback (see [chapter 7.2.4, page 302](#)) and in doing so entered an incorrect number (**Number** under **WAN PARTNER ▶ EDIT ▶ WAN NUMBERS ▶ EDIT**).

- Check if you left a trace program running over an ISDN-PPP connection. This would cause packets to be sent constantly over ISDN and the connection would remain permanently open.

Outgoing calls cannot be made.

- Use `isdnlogin` to check if outgoing calls are possible.
- Check **MONITORING AND DEBUGGING** ➤ **ISDN MONITOR** to see if any outgoing calls have been recorded at all, if the number dialed is correct and if the call was connected.
- Check if ISDN syslog messages with "disconnect cause" have been recorded.
- Check if **Encapsulation** in **WAN PARTNER** ➤ **EDIT** is the same for both connection partners.
- Check if **Authentication** in **WAN PARTNER** ➤ **EDIT** ➤ **PPP** is the same for both connection partners.
- Use `trace` to check what is being sent over the ISDN channels.
- Check in the MIB table **isdnStkTable** if the MIB variable **Status** has the value *loaded*.
- Make sure your own number is correctly entered in **PRI[x]** ➤ **INCOMING CALL ANSWERING** ➤ **ADD** resp. **BRI[x]** ➤ **INCOMING CALL ANSWERING** ➤ **ADD**. This also applies to outgoing calls.
- Check the settings of your PABX.
- Make sure your provider's settings are correct (if in doubt, ask your provider).

Incoming calls cannot be made.

- Check **MONITORING AND DEBUGGING** ➤ **ISDN MONITOR** to see if an incoming call has been recorded.
- Check **WAN PARTNER** ➤ **EDIT** ➤ **WAN NUMBERS** to see if a suitable number for incoming calls has been entered.

- Check the MIB variables **DSS1Cause** and **LocalCause** in the MIB table **isdnCallHistoryTable**. To interpret the entries, see the **Software Reference**.
- Check **PRI[x] ➤ INCOMING CALL ANSWERING** resp. **BRI[x] ➤ INCOMING CALL ANSWERING** to determine if you have made the necessary entries for incoming calls.
- Check if **Encapsulation** in **WAN PARTNER ➤ EDIT** is the same for both connection partners.
- Check if **Authentication** in **WAN PARTNER ➤ EDIT ➤ PPP** is the same for both connection partners.
- Check the settings of your PABX.
- Make sure your provider's settings are correct (if in doubt, ask your provider).

10 Important Commands

This chapter describes the following commands:

- SNMP shell commands:
 - telnet
 - ping
 - traceroute
 - trace
 - isdnlogin
 - debug
 - ifconfig
 - ifstat
 - netstat
 - date
 - t
 - nslookup
- BRICKtools for Unix commands:
 - bricktrace
 - capitrace

10.1 SNMP Shell Commands

X8500 contains several pre-installed programs that can be started directly from the SNMP shell. A short description of the most commonly used programs and the associated command lines for starting the respective programs in the SNMP shell are given below.



Entering `?` displays a list of the most important commands available on **X8500**.



Please note:

Parameters shown in the command lines inside square brackets [] represent optional values. Terms inside angle brackets < > can have several values. Do not enter any brackets!

telnet

```
telnet [-f] <host> [<port>]
```

Is used to communicate with another host.

- `-f`: specifies that the telnet session should be transparent. This option is especially useful for establishing connections to non-telnet ports (e.g. uucp or smtp).
- `host`: IP address or name of host.
- `port`: port number.

ping

```
ping [-i] [-f <precount>] [-d <msec>] [-c <count>] <target> [<size>]
```

Is used to test communication to another host.

- `-i`: sends each packet one byte larger.
- `-f <precount>`: `<precount>` packets are sent first. The next packet is sent as soon as a packet has been received.

Output: a dot appears on the screen for each packet sent and a dot is

deleted for each packet received.

- f 1 without the additional parameter -d <msec> causes approx. half the equipment's bandwidth to be loaded by sending and receiving packets.
- -d <msec>: waits <msec> until the next packet is sent, default: 1000 milliseconds.
- -c <count>: limits the number of packets sent, <count> sets the number of packets.
- target: IP address or name of host to which icmp_echo packets are sent.
- size: sets the length of the packets to be sent.



If you do not specify -c <count>, packets will be sent to the host until you stop the operation, e.g. by pressing **Ctrl-C**.

traceroute

```
traceroute [-n] [-w <waittime>] [-m <maxhops>] [-p <port>]
[-q <nqueries>] <addr> [<packetsize>]
```

Is used to print the route packets take to network host.

- -n: do not resolve received host ip.
- -w <waittime>: set response timeout in seconds.
- -m <maxhops>: maximum number of hops.
- -p <port>: UDP port to use.
- -q <nqueries>: queries to send
- <addr>: host name or ip address.
- <packetsize>: packet size.

trace

For WAN interfaces:

```
trace [-h23aFADtpixX] [-T <tei>] [-c <cref>]
[<channel> <unit> <slot> | next | <ifcname>]
```

For LAN interfaces:

```
trace [-h23ixX] [-d <destination MAC filter>] [-o]
[-s <source MAC filter>]0 <unit> <slot>
```

Is used to display and interpret data packets sent and received.

- -h: hexadecimal output.
- -2: layer 2 output.
- -3: layer 3 output.
- -a: asynchronous HDLC (B-channel only).
- -F: fax (B-channel only).
- -A: fax and AT commands (B-channel only).
- -D: additional time parameter (delta).
- -t: output in ASCII text (B-channel only).
- -p: PPP (B-channel only).
- -i: IP output (B-channel only).
- -x: raw dump mode.
- -X: asynchronous PPP over X.75 (B-channel only).
- -T <tei>: set TEI filter (D-channel only).
- -c <cref>: set callref filter (D-channel only).
- channel: 0 = D-channel or X.21 interface, 1 ... 31 = Bx-channel.
- unit: 0 ... 3. selects the physical interface.
- slot: 0 ... 8. indicates the slot in which the interface is installed.
- next: only display information for the next B-channel opened.
- <ifcname>: name or index of the interface (see "[ifstat](#)", page 390).
- -d <destination MAC filter>: set destination MAC address filter (LAN only).
- -s <source MAC filter>: set source MAC address filter (LAN only).
- -o: combine two or more -d filters or -s filters with a logical OR operation.
- specific <MAC filter>: me = **X8500**'s MAC address, bc = broadcast packets.



You can combine a `-d` MAC filter and an `-s` MAC filter with a logical AND operation by simply specifying them both.

To combine two or more `-d` and `-s` MAC filters with a logical OR operation, specify the filters and separate them with `-o`.

isdnlogin

```
isdnlogin [-c <stknumber>] [-C] [<service>] [<addinfo>]
[-b <bits>] isdn-number [isdn-service|layer1-protocol]
```

Is used to open a remote login shell on **X8500** over ISDN.

- `-c <stknumber>`: defines the ISDN stack (if several ISDN interfaces are available).
- `-C`: tries to use compression (V.42bis).
- `-b <bits>`: use only `<bits>` bits for transmission (e.g. enter `-b 7` for 7-bit ASCII transmission).
- `isdn-number`: isdn number of the ISDN partner you want to log in to.
- `isdn-service`: the ISDN service you want to use (data, telephony, fax g3, fax g4, btx).
- `layer1-protocol`: Possible values: v110_1200, v110_2400, v110_4800, v110_9600, v110_19200, v110_38400, modem, dovb56k, telephony.

debug

```
debug [show] [[-q] all|acct|system|<subs> [<subs> ...]]
```

Is used to selectively display debugging information originating from one of **X8500**'s subsystems.

- `show`: displays all possible subsystems that can be debugged.
- `-q`: no timestamp attached before each debugging message.
- `all`: displays debugging information for all subsystems.
- `acct`: displays debugging information for the accounting subsystem.
- `system`: displays debugging information for all subsystems except the accounting subsystem.
- `subs`: subsystem for which debugging information is to be displayed. Several entries are possible (separated by a space).

ifconfig

```
ifconfig <interface> [destination <destaddr>] [<address>]
[netmask <mask>] [up | down | dialup] [-] [metric <n>]
```

Assigns the IP address and the associated netmask to the interface <interface> and configures the associated parameters. The routing table is changed accordingly.

If you only enter `ifconfig <interface>`, the current interface parameters are displayed.

- `interface`: name of the interface (**ifDescr** or **ifIndex**).
- `destination <destaddr>`: destination IP address of a host. This adds a host route for this host in the routing table (**ipRouteDest**).
- `address`: **X8500**'s IP address for the interface (**ipRouteNextHop**).
- `netmask <mask>`: netmask of the interface (**ipRouteMask**).
- `up`: sets the interface to the up status or dormant status for dialup interface.
- `down`: sets the interface to the down status.
- `dialup`: sets the interface to the dialup status.
- `-`: does not define its own IP address (**ipRouteNextHop** = *0.0.0.0*).
- `metric <n>`: sets route metric to *n* (**ipRouteMetric1**).

ifstat

```
ifstat [-lur] [<ifcname>]
```

Is used to display status information for the system's interfaces, based on the contents of the MIB table **ifTable**.

- `-l`: displays the full length of the interface information (normally the information is only displayed up to the twelfth character).
- `-u`: only displays information on interfaces that are in the up status.
- `-r`: displays the filters defined for the interface.
- `ifcname`: only displays information on interfaces whose names start with the characters entered (e.g. `ifstat en0-1` will display information on the interfaces `en0-1`, `en0-1-llc` and `en0-1-snap`). Alternatively, you can use interface numbers (**Index**).

netstat

```
netstat [[-i | -r | -p [<interface>]] | -d <dest. IP addr.>]
```

Is used to display a short list of system information.

- `-i`: displays a list of the interfaces.
- `-r`: displays a list of routing table entries.
- `-p`: displays a list of WAN partners.
- `interface`: limits the information displayed to the selected interface.
- `-d <dest. IP addr.>`: displays routes to the IP address entered.

date

```
date [YYMMDDHHMMSS]
```

X8500 has a clock. Entering `date` displays the time set.

Entering `date YYMMDDHHMMSS` sets the clock to the corresponding value (year, month, day, hour, minute, second).

t

```
t [<seconds>]
```

Is used to define the auto logout time for the current login session (a connection to **X8500** over telnet, isdnlogin or serial interface is normally disconnected automatically if no entry is made on the keyboard for 15 minutes).

- `seconds`: auto logout is activated after `seconds`. Entering `t 0` deactivates auto logout.

nslookup

```
nslookup [-an] [-t <type>] [-w <sec>] [-r <ret>] ipaddr |  
name [<server>]
```

Is used to check how a name or an IP address is resolved by **X8500** or another name server.

- `-a`: displays all the data received.

- `-n`: prevents the resolution of the indicated name server address (without this option, an attempt is made to resolve the address of the name server).
- `-t <type>`: executes `<type>` requests. Possible values for type: 0, A, NS, MD, MF, CNAME, SOA, MB, MG, MR, NULL, WKS, PTR, HINFO, MINFO, MX, TXT, ANY or any decimal number.
- `-w <sec>`: wait `<sec>` before sending a new request (default value: 3).
- `-r <ret>`: send a request maximum `<ret>` times (default value: 5).
- `ipaddr`: IP address to be resolved.
- `name`: name to be resolved.
- `<server>`: IP address of the name server that is to be asked for (default value: 127.0.0.1). An attempt is made to have this name server address resolved by the local DNS proxy.



Entering a command with `-?` usually provides a help text.

The `update` command can be found in [chapter 8.2.5, page 363](#) and [chapter 8.3, page 368](#).

Further SNMP commands can be found in the **Software Reference**.

10.2 BRICKtools for Unix Commands

The bricktrace and capitrace programs are included in BRICKtools for UNIX on the BinTec Companion CD. They are started on a Unix workstation by entering the following commands.

bricktrace

```
bricktrace [-h23aeFpitxs] [-T <tei>] [-c <cref>]
[-r <cnt>] [-H <host>] [-P <port>] <channel> <unit> <slot>
```

Is used to trace and evaluate ISDN messages (D- and B-channels).

- -h: hexadecimal output.
- -2: layer 2 output.
- -3: layer 3 output.
- -a: asynchronous HDLC (B-channel only).
- -e: ETS300075 (Euro File Transfer) output.
- -F: fax (B-channel only).
- -p: PPP (B-channel only).
- -i: IP output (B-channel only).
- -t: output in ASCII text (B-channel only).
- -x: raw dump mode.
- -s: Check **X8500** for available trace channels.
- -T <tei>: set TEI filter (D-channel only).
- -c <cref>: set callref filter (D-channel only).
- -r <cnt>: only receive cnt bytes.
- -H <host>: IP address or name of IP host.
- -p <port>: specify trace TCP port (default: 7000).
- channel: 0 = D-channel or X.21 interface, 1 ... 31 Bx-channel.
- unit: 0 ... 3. selects the physical interface.
- slot: 0 ... 8. indicates the slot in which the interface is installed.

capitrace

```
capitrace [-h] [-s] [-l]
```

Is used to trace and evaluate CAPI messages. All CAPI messages sent or received by **X8500** are displayed. The IP address of **X8500** must be entered as the environment variable `CAPI_HOST`.

- `-h`: hexadecimal output.
- `-s`: short output. Only the application ID, a connection identifier and the name of the CAPI message are displayed at the end of the information line.
- `-l`: long output (default). A detailed interpretation is given for each parameter in the CAPI message.

Each CAPI message is preceded by a line containing the following information:

- Timestamp ("seconds.milliseconds" local time).
- Sent/received flag (X = sent, R = received).
- Name of the CAPI message (ASCII string).
- Command of the CAPI message (0xABXY, AB = <subcommand> XY = <command>).
- Number of the tracer message (#<decimal>).
- Length of the CAPI message ([<decimal>]).
- Application ID (ID = <decimal>).
- Number of the CAPI message (no. (<decimal>)).
- Short output only: connection identifier (ident = 0x<hexadecimal>).

11 General Safety Precautions in German

Allgemeine Sicherheitshinweise in deutsch

In den nachfolgenden Abschnitten finden Sie Sicherheitshinweise, die Sie beim Umgang mit Ihrem Gerät unbedingt beachten müssen.

- Transport und Lagerung**
- Transportieren und lagern Sie **X8500** nur in der Originalverpackung oder in einer anderen geeigneten Verpackung, die Schutz gegen Stoß und Schlag gewährt.
- Aufstellen und in Betrieb nehmen**
- Beachten Sie vor dem Aufstellen und Betrieb von **X8500** die Hinweise für die Umgebungsbedingungen (vgl. Technische Daten).
 - Beachten Sie bei der Installation externer ISDN-Basisanschlüsse die jeweils gültigen Rahmenbedingungen Ihres Landes. Gegebenenfalls ist ein Techniker erforderlich, der über die entsprechende Zulassung verfügt. Informieren Sie sich über die Besonderheiten nationaler Verordnungen und beachten Sie deren rechtliche Grundlagen bei der Installation.
 - Elektrostatische Aufladungen können zu Geräteschäden führen. Tragen Sie daher eine geerdete Manschette um das Handgelenk oder berühren Sie eine geerdete Fläche, bevor Sie Buchsen oder Erweiterungskarten von **X8500** berühren. Berühren Sie die Erweiterungskarten grundsätzlich nur an den Rändern und fassen Sie nicht auf Bauteile oder Leiterbahnen.
 - Halten Sie nicht benutzte Erweiterungssteckplätze mit der Blindabdeckung verschlossen, um elektromagnetische Störung zu vermeiden.
 - Wenn das Gerät aus kalter Umgebung in den Betriebsraum gebracht wird, kann Betauung sowohl am Geräteäußeren als auch im Geräteinneren auftreten. Warten Sie, bis Ihr Gerät temperaturangeglichen und absolut trocken ist, bevor Sie es in Betrieb nehmen. Beachten Sie die Umweltbedingungen in den Technischen Daten.
 - Öffnen Sie nicht das Netzteil, da sonst Lebensgefahr durch einen Stromschlag besteht. Bei Öffnen des Netzteils erlöschen außerdem die Gerätegarantie und die Produkthaftung.

- Achten Sie darauf, daß die für das Netzteil angegebenen Anschlußwerte eingehalten werden.
- **X8500** darf nur eingeschaltet werden, wenn das Netzteil vollständig eingesteckt und komplett verschraubt wurde. Hierdurch wird die zuverlässige Schutzerdung des Gehäuses sichergestellt.
- Das Netzkabel darf nur an ein vollständig eingestecktes und verschraubtes Netzteil angeschlossen werden.
- Prüfen Sie, ob die örtliche Netzspannung mit den Nennspannungen des Netzteils übereinstimmt. Das **X8500**-Netzteil X8A-PS darf nur unter folgenden Bedingungen betrieben werden:
 - 100 - 240 VAC
 - 50/60 Hz
 - max. 3 A
- Schließen Sie das Gerät nur an eine vorschriftsmäßig geerdete Schutzkontakt-Steckdose an (das Gerät ist mit einer sicherheitsgeprüften Netzleitung ausgerüstet).
- Stellen Sie sicher, daß die Schutzkontakt-Steckdose der Installation frei zugänglich ist.
- Beachten Sie beim Verkabeln die Reihenfolge, wie im Handbuch beschrieben. Verwenden Sie nur Kabel, die den Spezifikationen in diesem Handbuch genügen oder original mitgeliefert wurden. Falls Sie andere Kabel verwenden, übernimmt BinTec Communications AG für auftretende Schäden oder Beeinträchtigung der Funktionalität keine Haftung. Die Gerätegarantie erlischt in diesen Fällen.
- Beachten Sie beim Anschluß des Geräts die Hinweise im Handbuch.
- Verlegen Sie Leitungen so, daß sie keine Gefahrenquelle (Stolpergefahr) bilden und nicht beschädigt werden.
- Schließen Sie Datenübertragungsleitungen während eines Gewitters weder an noch ziehen Sie sie ab oder berühren Sie diese.
- Schließen Sie an **X8500** nur Endgeräte an, die den allgemeinen Sicherheitsanforderungen für Kommunikationsgeräte entsprechen. Endgeräte mit einer Zulassung durch das CETECON (ehemals BZT) entsprechen diesen

Anforderungen. ISDN-Endgeräte, die an **X8500** angeschlossen werden, müssen für das Euro-ISDN (DSS1) zugelassen sein.

**Bestimmungsgemäße
Verwendung, Betrieb**

- **X8500** baut in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen.
- Die Umgebungstemperatur sollte 40°C nicht übersteigen. Vermeiden Sie direkte Sonneneinstrahlung.
- Achten Sie darauf, daß keine Gegenstände (z. B. Büroklammern) oder Flüssigkeiten ins Innere des Geräts gelangen (elektrischer Schlag, Kurzschluß). Achten Sie auf ausreichende Kühlung.
- Unterbrechen Sie in Notfällen (z. B. beschädigtes Gehäuse oder Bedienelement, Eindringen von Flüssigkeit oder Fremdkörpern) sofort die Stromversorgung und verständigen Sie den Service.

**Reinigung und
Reparatur**

- Das Gerät darf auf keinen Fall naß gereinigt werden. Durch eindringendes Wasser können erhebliche Gefahren für den Benutzer (z. B. Stromschlag) und erhebliche Schäden am Gerät entstehen.
- Niemals Scheuermittel, alkalische Reinigungsmittel, scharfe oder scheuernde Hilfsmittel benutzen.

- 10Base-T** Twisted pair connection. Network connection for 10-Mbps networks with **▶▶ RJ45** connector.
- 100Base-T** Twisted pair connection, Fast Ethernet. Network connection for 100-Mbps networks.
- 1TR6** D-channel protocol used in the German ISDN. Today the more common protocol is the **▶▶ DSS1**.
- Access list** A rule that defines a set of packets that should or should not be transmitted by the router.
- Accounting** Recording of connection data, e.g. date, time, connection duration, charging information and number of data packets transferred.
- ADSL** Asymmetric **▶▶ Digital Subscriber Line**
The data rate is up to 640 kbps **▶▶ upstream** and 1.5 - 9 Mbps **▶▶ downstream** over ranges of up to 5.5 km.
The main ADSL applications are: Internet access, video-on-demand (digital and compressed) and high-speed data communication over **▶▶ POTS**.
- ARP** Address Resolution Protocol
ARP belongs to the **▶▶ TCP/IP protocol family**. ARP resolves IP addresses into their corresponding **▶▶ MAC addresses**.
- Asynchronous transmission** A method of data transmission in which the time intervals between transmitted characters can vary in length. This allows computers and peripheral devices to intercommunicate without being synchronized by clock signals. The beginning and end of the transmitted characters must be marked by start and stop bits – in contrast to **▶▶ synchronous transmission**.
- B-channel** Control and signaling channel of the **▶▶ ISDN Basic Rate Interface** or the **▶▶ Primary Rate Interface** for transmission of traffic (voice, data). An ISDN Basic Rate Interface consists of two B-channels and one **▶▶ D-channel**. A B-channel has a data transmission rate of 64 kbps.
The data transmission rate of an ISDN Basic Rate Interface with **X8500** can be increased to up to 128 kbps using **▶▶ channel bundling**.
- BOD** Bandwidth on Demand

Bandwidth on Demand is an extended method of **▶▶ channel bundling**, in which it is also possible to connect **▶▶ dialup connections** to **▶▶ leased lines** or to configure dialup connections as a backup facility for leased lines.

BootP Bootstrap protocol

Based on the **▶▶ UDP** or **▶▶ IP protocol**. Automatically assigns an **▶▶ IP address**. **DIME Tools** contain a BootP server that you can start on your PC to assign the as yet unconfigured router an IP address.

Bridge Network components for connecting homogeneous networks. As opposed to a **▶▶ router**, bridges operate at layer 2 (data link layer) of the **▶▶ OSI model**, are independent of higher-level protocols and transmit data packets using **▶▶ MAC addresses**. Data transmission is transparent, which means the information contained in the data packages is not interpreted.

Bridges are used to physically decouple networks and to reduce network data traffic. This is done by using filter functions that allow data packets to pass to certain network segments only.

Some BinTec routers can be operated in Bridging Mode.

Broadcast Broadcasts (data packages) are sent to all stations in a network in order to exchange information. Generally, there is a certain address (broadcast address) in the network that allows all stations to interpret a message as a broadcast.

Bus A data transmission medium for use by all the devices connected to a network. Data is forwarded over the entire bus and received by all devices on the bus.

Called Party Number Number of the terminal called.

Calling Party Number Number of the calling terminal.

CAPI Common ISDN Application Programming Interface

A software interface standardized in 1989 that allows application programs to access ISDN hardware from the PC. Most ISDN-specific software solutions work with the CAPI interface. Such communications applications enable you, for example, to send and receive faxes or transfer data over the ISDN from your PC. See also **▶▶ Remote CAPI**.

CCITT Consultative Committee for International Telegraphy and Telephony

A predecessor organization of the >>> **ITU** that passed recommendations for the development of communications standards for public telephony and data networks and data transmission interfaces.

Channel bundling Channel bundling

One of **X8500**'s features. Channel bundling is a method of increasing the data throughput. The data throughput is doubled by switching in a second >>> **B-channel** for data transmission. Channel bundling can be either dynamic (= on demand) or static (= always).

CHAP Challenge Handshake Authentication Protocol

A security mechanism during the establishment of a connection with a >>> **WAN partner** using >>> **PPP**. This protocol is used for checking the WAN partner name and the password defined for the WAN partner. If the partner name and password at both ends are not the same, a connection is not set up. The user name and password are encoded in CHAP before they are sent to the partner – as opposed to >>> **PAP**.

CLID Calling Line Identification

A security mechanism during the establishment of a connection with a >>> **WAN partner**. A caller is identified by means of his ISDN extension number before the connection is established. If the extension number is not the same as the extension number you have defined for a WAN partner, a connection is not established.

Client A client uses the services provided by a >>> **server**. Clients are usually workstations.

Data compression A process for reducing the amount of data transmitted. This enables higher throughput to be achieved in the same transmission time. Examples of this technique include >>> **STAC**, >>> **VJHC** and >>> **MPPC**.

Datagram A self-contained >>> **data packet** that is forwarded in the network with minimum protocol overhead and without an acknowledgment mechanism.

Data packet A data packet is used for information transfer. Each data packet contains a prescribed number of characters (information and control characters).

DCE Data Circuit-Terminating Equipment

Data Circuit-Terminating Equipment (see >>> [V.24](#))

D-channel Control and signalling channel of the >>> [ISDN Basic Rate Interface](#) or the >>> [Primary Rate Interface](#). The D-channel has a data transmission rate of 16 kbps. In addition to the D-channel, each ISDN BRI has two >>> [B-channels](#).

DCN Data communications network

DHCP Dynamic Host Configuration Protocol

A Microsoft protocol that provides a mechanism for dynamic assignment of >>> [IP addresses](#). A DHCP server allocates each >>> [client](#) in a network an IP address from a defined address pool compiled by the system administrator. Prerequisite: >>> [TCP/IP](#) must be configured at the clients so that they can request their IP address from the server. [X8500](#) can be used as a DHCP server.

Dialup connection A connection is set up when required by dialing an extension number, in contrast to a >>> [leased line](#).

DIME Desktop Internetworking Management Environment

DIME Tools is a collection of tools for the configuration and monitoring of routers over Windows applications. They are included with all BinTec routers free of charge.

Direct dialing range See >>> [extension numbers range](#)

DNS Domain Name System

Each device in a >>> [TCP/IP network](#) is usually located by its >>> [IP address](#). Because >>> [host names](#) are often used in networks to reach different devices, it is necessary for the associated IP address to be known. This task can be performed by a Domain Name Server (DNS), which resolves the host names into IP addresses. Alternatively, name resolution can also take place over the HOSTS file, which is available on all PCs.

Domain A domain refers to a group of devices in a network, whose host names share a common suffix, the domain name. Thus, in the >>> [Internet](#), a part of a naming hierarchy (e.g. bintec.de).

Downstream Data transmission rate from the >>> [Internet Service Provider](#) to the client.

- DSL/xDSL** Digital Subscriber Line
- Data transmission technique that enables high transmission rates to be achieved on normal telephone lines.
- The data rate is dependent on the distance to be covered and the quality of the line and therefore varies.
- xDSL is used as a bookmark for the different DSL variants, such as [▶▶ ADSL](#), [▶▶ RADSL](#), [▶▶ VDSL](#), [▶▶ HDSL](#), [▶▶ SDSL](#), [▶▶ U-ADSL](#), etc., which are part of the family of DSL techniques.
- DSS1** Digital Subscriber Signalling System.
- A common D-channel protocol used in the Euro ISDN.
- DTE** Data Terminal Equipment
- Data Terminal Equipment (see [▶▶ V.24](#))
- DTMF** Dual Tone Multi Frequency (tone dialing system)
- Dialing method for telephony systems. In this method, pressing a key on the telephone keypad generates two simultaneous tones, which are correspondingly evaluated by the PABX or exchange.
- E1/T1** E1: European variant of the 2.048 Mbps [▶▶ ISDN](#) [▶▶ Primary Rate Interface](#), which is also called the E1 system.
- T1: American variant of the ISDN Primary Rate Interface with 23 basic channels and one D-channel (1.544 Mbps).
- EAZ** Terminal Selection Digit
- Is only used in the [▶▶ 1TR6](#) system and designates the last digit of an extension number. It is used for dialing various terminals connected to the ISDN Basic Rate Interface (e.g. fax). This occurs by attaching one digit between 0 and 9 to the actual ISDN telephone number. In Euro ISDN (DSS1), the complete extension number, [▶▶ MSN](#), is transferred instead of the EAZ.
- Encapsulation** Encapsulation of [▶▶ data packets](#) in a certain protocol for transmitting the packets over a network that the original protocol does not directly support (e.g. NetBIOS over TCP/IP).
- Encryption** Refers to the encoding of data, e.g. [▶▶ MPPE](#).

- Ethernet** A local network that connects all devices in the network (PC, printers, etc.) via a twisted pair or coaxial cable.
- Extension** An extension is an internal number for a terminal or subsystem. In **point-to-point ISDN accesses**, the extension is usually a number from the **extension numbers range** assigned by the telephone provider. In point-to-multipoint connections, it can be the MSN or a part of the MSN.
- Extension numbers range** (direct dialing range)
A **point-to-point ISDN access** includes a **PABX number** and an extension numbers range. The PABX number is used to reach the PABX. The extension numbers range is a group of numbers used for selecting terminals within the **PABX**.
- Filters** A rule that defines a set of packets that should or should not be transmitted by the router.
- Firewall** Designates the whole range of mechanisms to protect the local network against external access. **X8500** provides protection mechanisms such as **NAT**, **CLID**, **PAP/CHAP**, access lists, etc.
- FTP** File Transfer Protocol
A TCP/IP protocol used to transfer files between different hosts.
- Gateway** Entrance and exit, transition point
Component in the local network that offers access to other networks, also offers transitions between different networks, e.g. **LAN** and **WAN**.
- HDSL** High Data Rate **DSL**
The **upstream** and **downstream** data rates are: **T1** 1.554 Mbps and **E1** 2.048 Mbps over ranges up to 4 km.
The main HDSL applications are: High-speed data communication over leased lines.
- HDSL2** High Data Rate **DSL**, version 2
The **upstream** and **downstream** data rate is 1.554 Mbps over ranges up to 4 km.

The main HDSL applications are: High-speed data communication over leased lines.

Host name A name used in [▶▶ IP networks](#) as a replacement for the corresponding [▶▶ IP address](#). A host name consists of an ASCII string that uniquely identifies the host computer.

Hub Network component used to connect several network components together to form a local network (star-shaped).

ICMP Internet Control Message Protocol

An extension to the Internet Protocol ([▶▶ IP](#)) that allows for IP-related error messages, test packets, and informational messages. It is defined in STD 5, RFC 792.

Internet The Internet consists of a range of regional, local and university networks. The [▶▶ IP protocol](#) is used for data transmission in the Internet.

IP Internet Protocol

One of the [▶▶ TCP/IP](#) suite of protocols used for the connection of Wide Area Networks ([▶▶ WANs](#)).

IP address The first part of the address by which a device is identified in an IP network, e.g. 192.168.1.254. See also [▶▶ netmask](#).

IPX/SPX Internet Packet Exchange/Sequenced Packet Exchange

Protocol suite from Novell for the transmission of data in a network. The two parts of this protocol suite are IPX (layer 3 of the OSI model) and SPX (layer 4 of the OSI model).

ISDN Integrated Services Digital Network

The ISDN is a digital network for the transmission of voice and data. There are two possible subscriber connections for ISDN, the [▶▶ ISDN Basic Rate Interface](#) and the [▶▶ Primary Rate Interface](#). ISDN is an international standard. For ISDN protocols, however, there is a range of variations.

ISDN Basic Rate Interface An ISDN subscriber interface. The Basic Rate Interface consists of two [▶▶ B-channels](#) and a [▶▶ D-channel](#). Compare [▶▶ Primary Rate Interface](#).

The interface to the subscriber is provided by an [▶▶ S₀ bus](#).

- ISDN BRI** ISDN Basic Rate Interface
 >> **ISDN Basic Rate Interface**, also >> **S₀ interface**.
- ISDN Login** One of **X8500**'s features. **X8500** can be configured and administrated remotely using ISDN Login. ISDN Login operates on routers in the ex works state as soon they are connected to an ISDN connection and therefore reachable via an extension number.
- ISDN PRI** ISDN Primary Rate Interface
 ISDN >> **Primary Rate Interface**, also >> **S_{2M} interface**.
- ISO** International Standardization Organization
 An international organization for the development of world-wide standards, e.g.
 >> **OSI model**.
- ISP** Internet Service Provider
 Allows companies or private individuals access to the Internet.
- ITU** International Telecommunication Union
 International organization that co-ordinates the construction and operation of telecommunications networks and services.
- LAN** Local Area Network
 A network covering a small geographic area and controlled by its owner. Usually within the confines of a building or corporate center.
- Leased line** Leased line
 Fixed connection to a subscriber. In contrast to a >> **dialup connection**, neither an extension number nor connection setup or clearing is necessary.
- MAC address** Every device in the network is defined by a fixed hardware address (MAC address). The network card of a device defines this internationally unique address.
- Main number** A >> **point-to-point ISDN access** includes a main number and an >> **extension numbers range**. The main number is used to reach the PABX. A certain terminal of the PABX is then dialed via one of the extension numbers of the extension numbers range.
- MIB** Management Information Base

The MIB is a database that describes all the manageable devices and functions connected to a network. All MIBs (including the BinTec MIB) contain objects specific to the manufacturer. >> **SNMP** is based on MIB.

MMI Man-Machine Interface

Is a convenient user guide with LC display and input keys for the user to navigate the basic functions of **X8500**.

Modem Modulator/Demodulator

An electronic device used to convert digital signals to analog tone signals and vice versa, so that data can be transmitted in an analog medium.

MPPC Microsoft Point-to-Point Compression

>> **data compression** procedure for

MPPE Microsoft Point-to-Point Encryption

Data encryption process.

MSN Multiple Subscriber Number

Multiple number for an ISDN BRI in Euro ISDN. The MSN is the extension number that permits a terminal to be addressed specifically on the >> **S₀ bus** in Euro ISDN. An MSN has up to eight digits, e.g. 49 911 7654321, where 7654321 corresponds to the MSN.

Usually three such MSNs are assigned to each ISDN BRI (point-to-multipoint connection) in Germany.

Multiprotocol router A >> **router** that can route several protocols, e.g. >> **IP**, >> **IPX**, etc.

NAT Network Address Translation

Used as a security mechanism in **X8500**. Using NAT conceals your complete network to the outside world. The IP addresses of all devices in your own network remain confidential, only one IP address is made known for connections to the outside.

NetBIOS Network Basic Input Output System

A programming interface that activates network operations on a PC. It is a set of commands for transmitting and receiving data to and from other Windows PCs on the network.

Netmask The second part of an address in an IP network, used for identification of a device, e.g. 255.255.255.0. See also [▶▶ IP address](#).

Network address A network address designates the address of a complete local network.

NT Network Termination

An NT adapter is the network termination unit of an [▶▶ ISDN](#) connection. In Germany, this is obtained from Deutsche Telekom AG. It is used to connect a private network ([▶▶ S₀ bus](#)) to the public ISDN network. It is equivalent to the terminal socket used for connecting an analog telephone.

NTBA Network Termination for Basic Access.

An NTBA adapter is the network termination unit of an [▶▶ ISDN](#) Basic Rate Interface. In Germany, this is obtained from Deutsche Telekom AG. It is used to connect a private network ([▶▶ S₀ bus](#)) to the public ISDN network. It is equivalent to the terminal socket used for connecting an analog telephone.

OSI model OSI = Open Systems Interconnection

[▶▶ ISO](#) reference model for networks. Defines interface standards between computer manufacturers for software and hardware requirements.

OSPF Open Shortest Path First

Routing protocol used in networks to exchange information (routing tables) between [▶▶ routers](#).

PABX Private Automatic Branch Exchange

An ISDN [▶▶ PABX](#) is a telephone exchange with [▶▶ S₀ interface](#) and [▶▶ 1TR6](#) or other manufacturer-specific [▶▶ D-channel protocols](#) on the subscriber side.

An ISDN PABX is used to set up an internal telephone infrastructure allowing internal connections between the PABX extensions without the need to connect to the telephone service provider. Not all BinTec routers include an exchange.

- PABX number** A point-to-point ISDN access includes a PABX number and an **extension numbers range**. The PABX number is used to reach the PABX. A certain terminal of the **PABX** is then dialed via one of the numbers of the extension numbers range.
- PAP** Password Authentication Protocol
- Authentication process for connecting over **PPP**. Functions like **CHAP**, except that the user name and password are not encoded before being transmitted to the partner.
- Ping** Packet Internet Groper
- Command that can be used to determine the range to remote network components. Ping is also used for test purposes to determine if the remote device can actually be reached at all.
- Point-to-multipoint** Feature of a connection that is permanently connected between three or more data stations or set up via switching systems.
- Point-to-multipoint connection** **Point-to-multipoint)**
- Several different terminals can be connected to a point-to-multipoint connection. The individual terminals are addressed via certain extension numbers (**MSNs**).
- Point-to-point** Feature of a connection between two data stations only. The connection can be permanently switched or set up via switching systems.
- Point-to-point ISDN access** A point-to-point ISDN access is used for the connection of a **PABX**. The PABX can forward calls to a number of terminals. A point-to-point access includes a **PABX number**, via which the PABX is reached from outside and a group of numbers (**extension numbers range**), with which the terminals connected to the PABX can be dialed.
- Port** Input/output
- The port number is used to decide to which service (telnet, WWW) an incoming data packet should be sent.
- POTS** Plain Old Telephone System
- The traditional analog telephone network.

PPP Point-to-Point Protocol

A protocol suite for authentication of the connection parameters of a **point-to-point connection**. PPP is used to connect local networks over the **WAN**. Multiprotocol packets are encapsulated (**encapsulation**) in a standard format before transmission. Establishing a connection involves a number of other components and subprotocols, such as the authentication mechanisms **PAP/CHAP**.

PPP authentication Security mechanism. A method of authentication using passwords in **PPP**.

PPPoE Point to Point Protocol over Ethernet

The PPP-over-Ethernet (PPPoE) protocol permits Internet access over Ethernet via an **xDSL** modem or xDSL router.

Primary Rate Interface (PRI) An ISDN subscriber interface. The PRI consists of a D-channel and 30 B-channels (in Europe). (In America: 23 B-channels and a D-channel.) Compare **ISDN Basic Rate Interface**.

Protocol Protocols are used to define the manner and means of information exchange between two systems. Protocols control and rule the course of data communication at various levels (decoding, addressing, network routing, control procedures, etc.).

Proxy ARP ARP = Address Resolution Protocol

Process used to determine the associated **MAC address** for a host whose **IP address** is known.

RADSL Rate-Adaptive **Digital Subscriber Line**

The data rate is up to 640 kbps **upstream** and 1.5 - 9 Mbps **downstream** over ranges of up to 18.5 km.

The main RADSL applications are: Internet access, video-on-demand (digital and compressed) and high-speed data communication over **POTS**.

Real Time Clock (RTC) Hardware clock with buffer battery

Remote Remote, as opposed to local.

If a far station is not located in your own local network (LAN), but in another LAN, this is referred to as remote.

This LAN must be connected to the local LAN over a WAN connection (over **X8500**).

Remote access Opposite to local access, see **➤➤ Remote**.

Remote CAPI BinTec's own interface for **➤➤ CAPI**.

The Remote CAPI interface enables all subscribers of a network to use CAPI services, but over **X8500** to a single ISDN connection. All subscribers must have the corresponding application software installed to support the CAPI interface. This standard interface is, however, used by most communications applications.

X8500 is supplied as standard with suitable software.

BinTec's CAPI interface is implemented as a dual-mode CAPI. CAPI 1.1 and 2.0 applications can access ISDN resources parallel to one another. This means new CAPI 2.0 applications can be used on the network or on the same PC parallel to old applications based on CAPI 1.1.

RIP Routing Information Protocol

Routing protocol used in networks to exchange information (routing tables) between **➤➤ routers**.

RJ45 Plug or socket for maximum eight wires. Connection for digital terminals.

Router A device that connects different networks at layer 3 of the **➤➤ OSI model** and routes information from one network to the other.

Routers are able to recognize blocks of information and evaluate addresses (as opposed to a **➤➤ bridge**, which operates with a transparent protocol). The best paths (routes) from one point to another are chosen by using routing tables. In order to keep the routing tables up to date, routers exchange information between themselves via routing protocols (e.g. **➤➤ OSPF**, **➤➤ RIP**).

Modern routers such as **X8500** are **➤➤ multiprotocol routers** and thus capable of routing several protocols (e.g. IP and IPX).

- S₀ bus** All ISDN sockets and the **NTBA** of an ISDN point-to-multipoint connection. All S₀ buses consist of a four-wire cable. The lines transmit digital ISDN signals. The S₀ bus is terminated with a terminating resistor after the last ISDN socket. The S₀ bus starts at the NTBA and can be up to 150 m long. Any ISDN devices can be operated on this bus. However, only two devices can use the S₀ bus at any one time, as only two **B-channels** are available.
- S₀ interface** See **ISDN Basic Rate Interface**
- S_{2M} interface** See **ISDN Primary Rate Interface**
- SDSL** Single line **Digital Subscriber Line**
- The **upstream** and **downstream** data rate is up to 768 kbps over ranges up to 3.5 km.
- The main SDSL applications are: **E1/T1** and **POTS**.
- Server** A server offers services used by **clients**. Often refers to a certain computer in the LAN, e.g. DHCP server.
- In client-server architecture, a server is the software part that executes functions for its clients, e.g. **TFTP server**. In such a case, the server is not necessarily a computer server.
- Setup Tool** Menu-driven tool for the configuration of **X8500**. The Setup Tool can be used as soon as the router has been accessed (serial, **ISDN Login**, **LAN**).
- Short hold** Is the defined amount of time, after which a connection is cleared if no more data is transmitted. Short hold can be set to static (fixed amount of time) or dynamic (according to charging unit).
- SNMP** Simple Network Management Protocol
- A protocol in the **TCP/IP protocol suite** that is used to transport management information about network components. Every SNMP management system contains an **MIB**. SNMP can be used to configure, control and administrate various network components from one system. Such an SNMP tool is included in your router: the **Configuration Manager**. As SNMP is a standard protocol, you can use any other SNMP managers, e.g. HP OpenView.
- SNMP shell** Input level for SNMP commands.

- SOHO** Small Offices and Home Offices
Small offices and home offices.
- Spoofing** Technique for reducing data traffic (and thus saving costs), especially in WANs.
The router answers as proxy for remote PCs to cyclically transmitted data packets with a monitoring function (e.g. sign of life messages).
- STAC** Data compression procedure.
- Subnet** A network scheme that divides individual logical networks into smaller physical units to simplify routing.
- Switch** LAN switches are network components with a similar function to **bridges** or even **routers**. They switch data packets between the input and output port. In contrast to bridges, switches have several input and output ports. This increases the bandwidth in the network. Switches can also be used for conversion between networks with different speeds (e.g. 100-Mbps and 10-Mbps networks).
- Synchronous** Transmission process in which the transmitter and receiver operate with exactly the same clock signals – in contrast to **asynchronous**. Spaces are bridged by a stop code.
- TCP** Transmission Control Protocol
One of the **TCP/IP** suite of protocols used for the connection of Wide Area Networks (**WANs**).
- TCP/IP** Transmission Control Protocol/Internet Protocol.
A protocol suite for the connection of Wide Area Networks (**WANs**). The two parts of this protocol suite are **IP** (layer 3 of the OSI model) and **TCP** (layer 4 of the OSI model).
- T-DSL** Name of **DSL** services of Deutsche Telekom AG.
- TE** Terminal Equipment
Terminal equipment for subscriber access, e.g. telephone, fax or PC.
- TEI** Terminal Endpoint Identifier

The TEI in >>> **ISDN** is an address field in layer 2 that is used for identifying a certain terminal.

Telematics Telematics is a combination of telecommunication and computer technology and describes data communication between systems and devices.

Telnet Protocol from the >>> **TCP/IP protocol suite**. Telnet enables communication with a remote device in the network.

TFTP Trivial File Transfer Protocol

Protocol for data transmission.

TFTP server software is a part of >>> **DIME Tools**. It is used for the transfer of configuration files and software to and from the router.

U-ADSL Universal >>> **Asymmetric Digital Subscriber Line**

The data rate is 128 kbps >>> **upstream** and 1 Mbps >>> **downstream** over ranges of up to 5.5 km.

The main U-ADSL applications are: >>> **POTS** Internet access.

UDP User Datagram Protocol

A transport protocol similar to >>> **TCP**. UDP offers no control or acknowledgment mechanisms, but is faster than TCP. UDP is connectionless in contrast to TCP.

Upstream Data transmission rate from the client to the >>> **Internet Service Provider**.

URL Universal/Uniform Resource Locator

Address of a file on the Internet

V.11 ITU-T recommendation for balanced dual-current interface lines (up to 10 Mbps).

V.24 CCITT and ITU-T recommendation that defines the interface between a PC or terminal as Data Terminal Equipment (>>> **DTE**) and a modem as Data Circuit-terminating Equipment (>>> **DCE**).

V.28 TU-T recommendation for unbalanced dual-current interface lines

V.35 ITU-T recommendation for data transmission at 48 kbps in the range from 60-108 kHz.

- V.36** Modem for >> **V.35**.
- V.90** ITU standard for 56 kbps analog modems. In contrast to older V.34 modems, data is sent in digital form to the client when the V.90 standard is used and does not need to be first converted from digital to analog on one side of the modem (provider), as was the case with V.34 and earlier modems. This makes higher transmission rates possible. A maximum speed of 56 kbps can be achieved only under optimum conditions.
- VDSL** Very high bit rate >> **Digital Subscriber Line** (also called VADSL or BDSL).
The data rate is 1.5 to 2.3 Mbps >> **upstream** and 13 to 52 Mbps >> **downstream** over ranges of 300 m to 14 km.
The main VDSL applications are: as for >> **ADSL**, but at higher transmission rates and with synchronization over short ranges.
- VJHC** Van Jacobson Header Compression
>> **data compression** procedure for IP header compression.
- VPN** Virtual Private Network
The use of existing structures such as the >> **Internet** structure for connecting private networks (e.g. SOHO exchange). The data can be encrypted between the two endpoints of the VPN to meet increased security requirements.
- WAN** Wide Area Network
Wide Area Network connections, e.g. over ISDN, X.25.
- WAN interface** WAN interface
WAN interfaces connect the local network to the (>> **WAN**). This is usually done by means of analog or digital telephone lines (>> **switched** or >> **leased lines**).
- WAN partner** Remote station that is reached over a >> **WAN**, e.g. ISDN.
- X.21** The X.21 recommendation defines the physical interface between two network components in packet-switched data networks (e.g. Datex-P).
- X.21bis** The X.21bis recommendation defines the >> **DTE**/>> **DCE** interface to V-series synchronous modems.

- X.25** An internationally agreed standard protocol that defines the interface between network components and a packet-switched data network.
- X.31** For integration of X.25-compatible DTEs in ISDN.

A	About this manual	16
	contents	16
	meaning of symbols	17
	typographical elements	18
	Access lists	68, 315
	Access security	299
	Activity monitor	296
	Activity monitoring	284
	Additional license	240
	Advanced configuration with Setup Tool	135
	ARP	185
	Authentication	301
	CHAP	301
	MS-CHAP	301
	PAP	301
	TAF	332
	Auto logout	343
B	Back route verification	331
	Bandwidth on Demand	149
	Basic configuration with Setup Tool	53
	Basic IP settings	193
	Basic router settings	55
	BinTec's X8500 CD	13
	BOOT sequence	369
	BOOTmonitor update	370
	BOOTP relay agent	215
	BRI interface	73, 252
	BRICKware	13, 130
	Bridging	239
	Broadband	86
C	Callback	302

CAPI	77
configuring Remote CAPI	130
installing Remote CAPI	130
Channel bundling	147
CHAP	142, 301
Chapter description	16
Checking the calling party number	300
Checklist for security functions	345
CLID	300
Closed User Group	304
CM-100BT configuration	252, 256
CM-2BRI configuration	252
CM-BRI configuration	252
CM-PRI configuration	252, 255
CM-X21 configuration	252, 257
Commands	385
BRICKtools for Unix	393
SNMP shell	386
Communication modules	
CM-100BT	252, 256
CM-2BRI	252
CM-BRI	252
CM-PRI	252, 255
CM-X21	252, 257
configuration	252
Compression	183
MS-STAC	183
STAC	183
Van Jacobson Header Compression	183
CompuServe	122
Computers in the partner network	131

Configuration	
advanced configuration with Setup Tool	135
basic configuration with Setup Tool	53
basic router settings	55
configuration management	347
distribution of incoming calls	77
expansion cards and modules	241
instructions for initial configuration	45
preparation	45
saving	126
security functions	283
testing	134
Configuration file administration	348
Configuration management	347
Configuration options	32
Configuring PCs	127
Connection methods	24
Credits	293
Credits Based Accounting System	293
configuration	293
display	290
D Default route	115
Delay after connection failure	146
Denial-of-Service attacks	343
DHCP server	65
Digital modems	270
Distribution of incoming calls	77
DNS	
DNS Proxy	197
DNS server	127
name resolution	177
Documentation from BinTec	14
Domain Name	197
Dynamic IP address server	136
E Encryption	280, 338

Errors, typical	379
Expansion card	
communication modules	252
configuration	241
PRI/G.703 expansion card	241, 243
resource modules	241
X8E-2BC	241, 252
X8E-DSP	241, 262
Extended IP routing	332
Extensions	
CAPI	77
ISDN Login	77
routing	77
F Features X8500	11
Filters	68, 315, 328
Firewall	283
Flash Card	347
Flash memory	348
FRAME RELAY	57, 240
G G.703	243
General PPP settings	142
General WAN settings	136
I Incoming calls	
CAPI	77
ISDN Login	77
routing	77
Installing BRICKware	49
Installing the TCP/IP protocol	47
Instructions for initial configuration	45
Internet access	
Compuserve	122
Telekom Austria	91
T-Online	122

IP		
basic settings		193
name resolution		197
Transit Network		173
IP address		
DHCP server		65
entering with the Setup Tool		61
IP address pools		136
IP address server		136
PCs in the LAN		127
Pool		136
IPSEC	57, 240, 280, 338, 341	
ISDN B-channel		171
ISDN Login		28, 77
L		
LAN interface		
configuring		61
xDSL access		86
Layer 1 Protocol		171
Leased line		
BRI interface		73, 84
configuring		84
G.703		243
License		
entering		56
features		240
Line tapping security		338
Local filters		328
Logging in		30, 299
M		
Memory		348
Monitoring functions in the Setup Tool		289
MPPE		338
MS-STAC		183
N		
Name resolution		177
NAT		121, 304

NetBIOS	177
NetBIOS filters	68
Netmask entering with the Setup Tool	61
Network Address Translation	121, 304
P	
PAP	142, 301
Passwords	30, 58
PCs in the LAN	127
Port numbers	214, 315
PPP authentication	301
PPP over PPTP	91
PPP settings	142
PPPoE	86, 142
PPTP	86, 91, 341
PRI	
configuration	243
expansion card	243
WAN partner	94, 251
Proxy ARP	185
Q	
Quality of Service	218
activating classification	226
classification and signaling	221
defining IP filters	220
defining policies	227
R	
RAM	348
Remote CAPI	77, 304
configuring	130
installation	130
Resetting to ex works state	379

Resource modules	
compression	280
configuration	270, 280
encryption	280
XT-2M	270
XT-L	270
XT-M	270
XT-S	270
XT-VPN	280
RIP	180
Routing entry	115
Routing Information Protocol	180
Rule	315
S SAFERNET	283
Saving the configuration	126
Security functions	283
access security	299
activity monitoring	284
checklist	345
configuration	283
line tapping security	338
special features	343
Service	214, 315
Setup Tool	33
advanced configuration	135
basic configuration	53
menu architecture	33
monitoring functions	289
using it	33
Short hold	106
Smart Media Flash Card	347, 348, 356

SMFC	347, 348, 356
boot operation	357
command fssh	356, 363
external	348
internal	348
saving configuration	357
SNMP shell	30
Software update	368
STAC	183
Start-up procedure	343
Syslog messages	284
System data, entering	58
System time	193
T	
TAF	57, 240, 332
T-DSL	86
Telekom Austria	91
Telnet	27
Time server	193
Token Authentication Firewall	332
T-Online	122
Transit Network	173
Troubleshooting	375
aids	376
ISDN connections	380
system errors	379
TUNNELING	57, 240, 341
Typographical elements	18
U	
Update	368
User concept	77, 138
V	
V.35	263, 281
Van Jacobson Header Compression	183
Virtual Private Network	57, 338, 341
VPN	57, 338, 341

W	WAN partner	
	advanced functions	146
	Compuserve	122
	computers in the partner network	131
	configuration	94
	DNS	177
	examples	122
	Internet access	122
	T-Online	122
	WINS	177
	WINS	177, 197
X	X.21	263, 281
	X25	57, 240
	X8E-2BC	252
	X8E-2G703	243
	X8E-2PRI	243
	X8E-4G703	243
	X8E-4PRI	243
	X8E-DSP	262
	X8E-SYNC	263
	xDSL	86
	XIPR	332
	XT-2M	270
	XT-2SYNC	281
	XT-L	270
	XT-M	270
	XT-S	270
	XT-VPN	280

