



X1000

User's Guide


Installation and Configuration

Copyright © 2001 BinTec Communications AG, all rights reserved.

Version 1.1

Document #71000N

April 2001



Purpose This manual explains the installation and initial configuration of **X1000** with software release 5.3.1. 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 **X1000**, can be found at www.bintec.net.

As an ISDN multiprotocol router, **X1000** sets up ISDN 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.

Other product names and trademarks mentioned are usually 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 **X1000** complies with the following guidelines and standards:

- Low voltage directive 73/23/EEC according to EN60950, complies with German equipment safety regulations
- Interference immunity according to EN50082 1/8.97

- Class B interference emissions according to EN55022 /8.94 + A1/1995 + A2/1997, electromagnetic compatibility according to EU directive 89/336/EEC

- CE directives

Registration:

- CE registration
- German TÜV inspection/GS safety regulations
- BAKOM registration (Switzerland)

In addition to the CE directives, **X1000** also meets the ISDN requirements in France and can be connected to Euro-Numeris.

How to reach

BinTec Communications AG
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 911 96 73 0

Fax: +49 911 688 07 25

Internet: www.bintec.net

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



Table of Contents	5
1 Welcome!	11
1.1 What Do You Need X1000 For?	13
1.2 Scope of Supply	17
1.3 BinTec ISDN Companion CD	18
1.4 BinTec Documentation	20
1.5 System Requirements	21
1.6 Guarantee Terms	22
1.7 About this Manual	24
1.7.1 Contents	24
1.7.2 Meaning	26
2 General Safety Precautions	29
3 Getting Started	31
3.1 Setting Up and Connecting	33
3.2 In Advance of Configuration	36
3.2.1 Gathering Information	36
3.2.2 What to Do in Your Windows Network	40
3.3 Installing BRICKware Under Windows	43
3.4 Solution Scenarios	45
3.4.1 Configuring Internet Access	45
3.4.2 Using Communications Applications	46
3.4.3 Connecting a Branch Office to Head Office	47
3.4.4 Providing Access to Head Office for Field Service Staff without Router Access (Dial-In)	48
3.5 Configuring X1000 Under Windows	50

3.5.1	Configuring the Basic Router Configuration	53
3.5.2	Internet Access with X1000	57
3.5.3	Connecting X1000 to a Corporate Network	59
3.5.4	Completing the Configuration	61
3.6	Remote CAPI Interface on the PC	64
3.6.1	Installing the Remote CAPI Client on all Other PCs	64
3.6.2	Configuring Remote CAPI	64
3.7	Configuring a PC	66
3.7.1	Telling the PC the IP Address, Gateway and DNS	66
3.7.2	Finding PCs on your Partner's Network	68
3.8	Configuring Fax and Answering Machine with RVS-COM Lite	71
3.8.1	Installing RVS-COM Lite	71
3.8.2	Configuring RVS-COM Lite	74
3.9	Testing your Configuration	78
3.9.1	Testing your Internet Access	78
3.9.2	Sending and Receiving E-Mails	78
3.9.3	Sending a Fax	78
3.9.4	Receiving a Fax	80
4	Overview	83
4.1	The Basics of ISDN	84
4.2	Speeding Things up Even More...	87
4.3	Services and Users	88
4.4	X1000 as DHCP Server	92
4.5	How Does Name Resolution Work?	95
4.6	What Are Routes and Default Routes?	98
4.7	Filters and NetBIOS	101
4.8	MIB and SNMP	103

5	Connecting X1000	105
5.1	Connection Methods	106
5.1.1	Connecting Over the Serial Interface	107
5.1.2	Connecting Over a LAN	109
5.1.3	Connection Over ISDN	110
5.2	Logging In	111
5.3	Configuration options	113
5.3.1	Methods of Configuration	113
5.3.2	Operation and Menu Architecture of the Setup Tool	114
6	Basic Configuration with the Setup Tool	127
6.1	Basic Router Settings	129
6.1.1	Entering Licenses	130
6.1.2	Entering System Data	132
6.1.3	Configuring the LAN Interface	135
6.1.4	Configuring the WAN Interface	138
6.1.5	Configuring X1000 as DHCP Server	149
6.1.6	Setting Filters	151
6.2	X1000 and the WAN	156
6.2.1	Configuring WAN Partners	158
6.2.2	Internet Access with X1000	184
6.2.3	Dialing into Corporate Network	190
6.3	Saving the Configuration File	199
7	Advanced Configuration	201
7.1	General WAN Settings	202
7.1.1	Dynamic IP Address Server	202
7.1.2	CAPI User Concept	204
7.1.3	General PPP Settings	208
7.1.4	X.31 TEI	210

7.2	Settings Specific to WAN Partners	211
7.2.1	Delay after Connection Failure	211
7.2.2	Channel Bundling - Basic Configuration for Dialup Connections	212
7.2.3	Channel Bundling - Bandwidth on Demand (BOD) - Advanced Configuration for PPP Connections	214
7.2.4	Always On/Dynamic ISDN (AO/DI)	220
7.2.5	Layer 1 Protocol (ISDN B-Channel)	233
7.2.6	IP Transit Network	235
7.2.7	Transfer of DNS and WINS IP Addresses to WAN Partner	238
7.2.8	Routing Information Protocol (RIP)	242
7.2.9	Compression	245
7.2.10	Proxy ARP (Address Resolution Protocol)	247
7.2.11	Keepalive Monitoring	249
7.3	Basic IP settings	255
7.3.1	System Time	255
7.3.2	Name Resolution in X1000 with DNS Proxy	259
7.3.3	Port Numbers	277
7.3.4	BOOTP Relay Agent	278
7.4	IPX Settings	281
7.4.1	General Settings	281
7.4.2	Configuring the LAN Interface	283
7.4.3	Configuring WAN Partners	284
7.5	Extra License Functions	288
7.5.1	Virtual Private Network (VPN) and Encryption	288
7.5.2	IPSec (Internet Protocol Security)	288
7.5.3	Leased Lines	288
8	Security Mechanisms	289
8.1	Activity Monitoring	290
8.1.1	Syslog Messages	290
8.1.2	Monitoring Functions in the Setup Tool	295

8.1.3	Credits Based Accounting System	299
8.1.4	HTTP Status Page	302
8.1.5	Activity Monitor	305
8.2	Access Security	308
8.2.1	Logging In	308
8.2.2	Checking the Calling Party Number	309
8.2.3	Authentication of PPP Connections with PAP, CHAP or MS-CHAP	310
8.2.4	Callback	310
8.2.5	Closed User Group	312
8.2.6	Access to Remote CAPI	312
8.2.7	NAT (Network Address Translation)	313
8.2.8	Filters (Access Lists)	317
8.2.9	Local Filters	330
8.2.10	Back Route Verification	334
8.2.11	TAF Client	335
8.2.12	Extended IP Routing (XIPR)	335
8.3	Line Tapping Security	336
8.3.1	Encryption	336
8.3.2	VPN (with extra license)	339
8.3.3	IPSec (with extra license)	339
8.4	Special Features	340
8.4.1	Startup Procedure	340
8.4.2	Auto Logout	340
8.4.3	Prevention of Denial-of-Service Attacks	340
8.5	Checklist	342
9	Configuration Management	345
9.1	Administration of Configuration Files	346
9.2	Resetting X1000 to the Ex Works State	353
9.3	Updating Software	355

10	Troubleshooting	359
	10.1 Aids to Troubleshooting	360
	10.1.1 Local SNMP Shell Commands	360
	10.1.2 External Aids	361
	10.2 Typical Errors	362
	10.2.1 System Errors	362
	10.2.2 ISDN Connections	363
	10.2.3 IPX Routing	366
11	Technical Data	369
	11.1 General Product Features	370
	11.2 Front Panel LEDs	373
	11.3 Rear Panel Connections	376
	11.4 Pin Assignment	377
	11.5 BOOT Sequence	380
12	Important Commands	383
	12.1 SNMP Shell Commands	384
	12.2 BRICKtools for Unix Commands	391
13	General Safety Precautions in 15 Different Languages	393
	Glossary	431
	Index	449

1 Welcome!

Congratulations on wisely choosing to buy a personal Internet access router from BinTec Communications AG. Your BinTec Communications AG data router is a new-generation router from our personal access product group. This high-performance multiprotocol router allows you affordable networking of small networks. In future, your **X1000** will make it possible for you to connect your individual workstation or small company to the Internet and other partner networks (e.g. to a corporate network). Moreover, **X1000** will provide all the computers on the network with up-to-the-minute means of office communication (communications applications, such as fax and file transfer).



Where do we go from here?

What your **X1000** gives you...

You will find out what **X1000** means for you and exactly what **X1000** can do on the following pages.

Getting **X1000** up and running...

...is described in [chapter 3, page 31](#). There we show you how to start up **X1000** within a few minutes from a Windows PC with the help of a configuration assistant and how to install other useful online assistants. At the end of the chapter, you will be in a position to surf the Internet, send or receive e-mails or faxes and set up a connection to a partner network, for example, to access data at your corporate headquarters.

And on top of all that...

you will find extensive explanations in [chapter 6, page 127](#), which show all the possible configurations in detail. Even if you do not have a Windows PC, you will find fast ways to configure your **X1000**.

If you have already configured BinTec routers...

...or you are familiar with configuration and you want to get started right away, all you really need to know is the preset user name and password.

User name	Password
admin	bintec



Remember, however, to change the password immediately when you log in to your **X1000** for the first time. All BinTec routers are supplied with the same password, which means they are not protected against unauthorized access until you change the password. How to change the passwords is described in "[Changing the password](#)", page 120.

Otherwise... ... BinTec Communications AG wishes you lots of fun with your new product.

Pick-up Service However, should you have any problems with your **X1000** hardware at any time, BinTec Communications AG offers you free replacement of your defective equipment for a period of one year. Further information on this can be found in [chapter 1.6, page 22](#).

1.1 What Do You Need X1000 For?

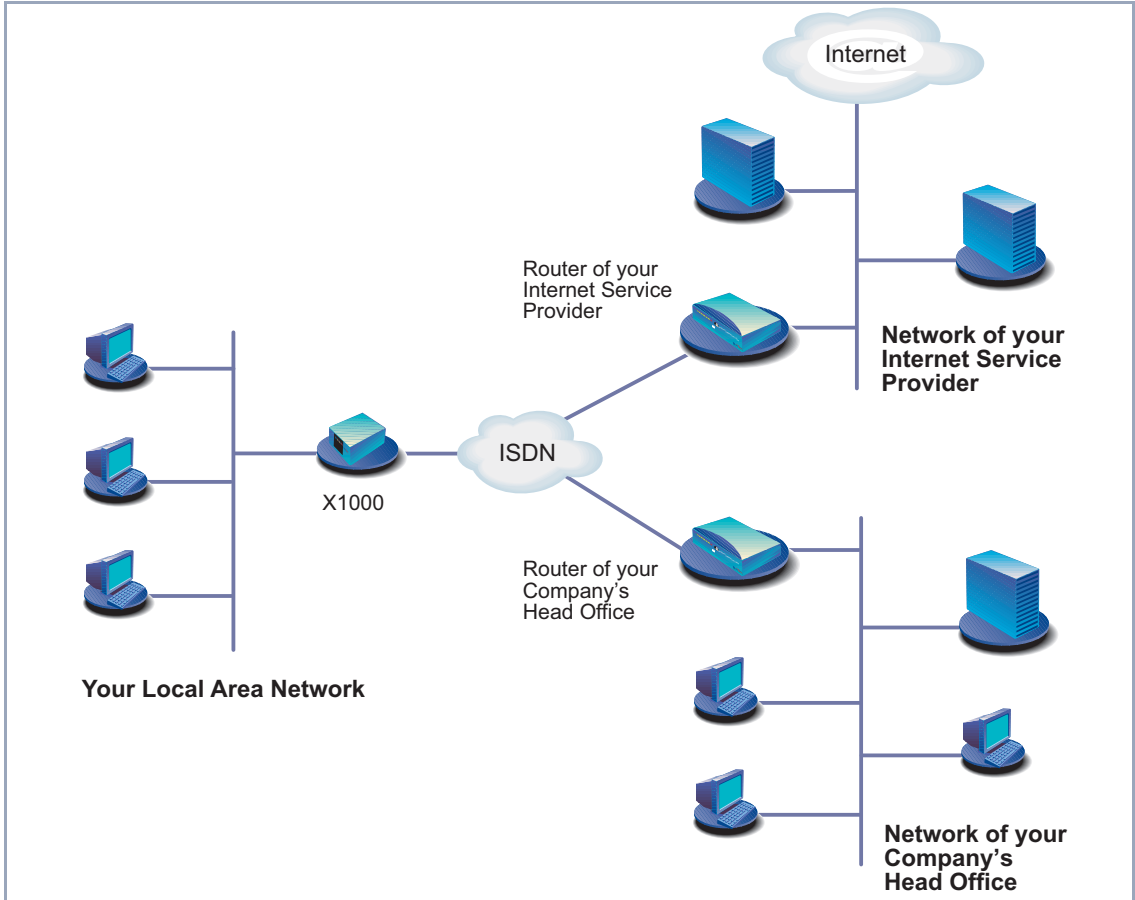


Figure 1-1: Basic scenario

Why a router such as X1000?

Routers are used to interconnect networks and to exchange information between the networks. For example, you can connect to the network of your Internet Service Provider via your router as shown above and use the usual Internet services, such as the World Wide Web (WWW) or e-mail. By connecting to another partner network, e.g. your company's head office, from your home or branch office, you can conveniently access any information you may need from

the headquarters, even if this is hundreds of kilometers away. The connection of these local networks takes place over the ISDN. The size of your own local network – whether it consists of several computers or just one workstation – is irrelevant.

As shown in the previous illustration, your **X1000** is the essential component for connecting the networks: it is your link to the outside world. All the routers in the illustration are linked by ISDN lines to the ISDN and thus serve as links between the individual local networks. Within each LAN, the router is connected to the network like a normal computer. Its task is to transmit information as necessary from its own network to an external network (e.g. to the network of your Internet Service Provider or your head office) and to find the most suitable routes for transmission. Conversely, it receives information and routes it to its own network.

What can **X1000** do that ISDN cards can't? Your **X1000** can do considerably more:

One router for everyone

If you have a local network with several computers, you only need one single router to allow all computers in the network access to the Internet or the head office. The lower expenditure on equipment and administration for several computers in the network means substantial savings. When using ISDN cards, every workplace would have to be equipped separately.

Communication applications

For communications applications on your PC, such as answering machine, fax, file transfer and Eurofile transfer, the same principle applies as for access to the Internet. All LAN users can use these services via BinTec's own Remote CAPI interface while accessing a single ISDN connection over **X1000**. The only requirement is that all users have suitable application software installed to support the CAPI interface. This standard interface is, however, used by most communications applications. **X1000** is supplied as standard with suitable software (RVS-COM Lite). This software covers the spectrum of common communications applications.

Automatic dialing and disconnection

A significant advantage of your **X1000** is also its means of obtaining access to networks. Once configured, your router decides independently if and how it is to set up a connection to the Internet Service Provider. If you enter an external WWW address in your browser, for example, your **X1000** determines that the requested address lies outside your own LAN and establishes a connection to

your Internet Service Provider and the Internet automatically. To save costs, **X1000** disconnects the connection after a predefined time (short hold) if no more information is exchanged.

The same principle is applied for conveniently accessing data at another location, e.g. your company headquarters. While running Windows, for example, you can even connect a network drive to a computer at your head office. You then simply click the icon for this link in Windows Explorer and can surf in the directories and data of the remote computer just as if you were using your own hard disk. **X1000** takes care of setting up and clearing the connection.

Security **X1000** also has a lot to offer with regard to security. Your router offers you integrated firewall mechanisms and provides extensive, low-cost features to meet all the requirements for access security. It protects your network against unauthorized external access. This is made possible by **X1000**'s SAFERNET functions such as NAT, encryption, filters and monitoring.

Configuration and administration A number of options are available for configuring **X1000**. Most of the configuration methods are independent of your computer's operating system.

The simplest method using Windows is the **Configuration Wizard**. This configuration assistant guides you through the configuration step by step and helps you to make the most important settings on your router. **X1000** is ready for operation in only a few minutes.

X1000 can also be configured and administrated remotely. As soon as your router is connected to the ISDN – even in its ex works state, configuration settings can be carried out from a distant location (e.g. by the administrator at your head office). This means you can leave the configuration of the system to be carried out by someone at HQ.

In summary **X1000** has the following main advantages:

- A connection to the Internet or another partner network allows everyone in your LAN to use the usual Internet services (e.g. e-mail, WWW, file transfer) and to access data at other locations.
- Use of communications applications in the LAN (e.g. fax, answering machine) via a common ISDN connection.

- Simple configuration for you and remote administration by an administrator at head office.
- Independence from the operating system of your PC.

On top of all that, you need not do without security, convenience and economy.

1.2 Scope of Supply

X1000 is supplied with the following parts:

- Cable sets/mains unit:
 - LAN cable (RJ45, red) for LAN connection to hub
 - Adapter cable (reversed) together with red LAN cable for LAN connection directly to PC
 - ISDN cable (RJ45, black) for ISDN connection
 - Serial cable (gray)
 - Mains unit
- BinTec Companion CD
- Documentation:
 - **User's Guide**
 - **Quick Install Guide**
 - **Release Notes**, if required
- Additional material:
 - License card with license information

1.3 BinTec ISDN Companion CD

You will find all the programs you need for the installation, configuration and administration of **X1000** on your BinTec Companion CD.

- BRICKware**
- The **Configuration Wizard** leads you step by step through the basic configuration of **X1000**.
 - The **Activity Monitor** enables you to monitor the utilization of **X1000** at a glance.
 - You gain access to **X1000** via the serial interface using the terminal program device at COM1 or device at COM2.
 - Remote CAPI Client
The Remote CAPI Client allows you to use communications applications based on the standard CAPI interface (e.g. RVS-COM Lite).
 - Token Authentication Firewall (TAF) program
This software package is required if you are using the Security Dynamics security system.
 - 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 all SNMP tables and variables.
 - **DIME Tools** are for monitoring and administration of your **X1000**.

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

- RVS-COM Lite** In addition to **BRICKware**, your BinTec Companion CD contains the RVS-COM Lite communications program that allows you to use all the usual communications applications on your PC, e.g. answering machine, fax or file transfer. How to do this is explained in [chapter 3.8, page 71](#).



Please note: The license for RVS-COM Lite is a single user license. You can purchase additional licenses from your dealer.

What else? The Companion CD also contains a range of other useful directories in which you can find the following, for example:

- The documentation in electronic form (see [chapter 1.4, page 20](#))
- A copy of the router software (in its unconfigured ex works state), if applicable
- UNIX Tools (administration)
- Adobe's Acrobat Reader
- MIB tables

1.4 BinTec Documentation

Together with **X1000**, you will have received part of the documentation in printed form and all of it in electronic form (PDF, HTML). The electronic versions of the different documents are included on the BinTec Companion CD. In addition to your Companion CD documentation, you can download all the very latest BinTec documentation from our WWW server at www.bintec.net. The following are available:

- **User's Guide** (printed/PDF file)
This manual.
- Leaflet with a **Quick Install Guide** for initial configuration of **X1000** (PDF and printed).
- Reference manuals (English, PDF/HTML).
 - **Software Reference** (PDF)
Online reference with more detailed information about the functions described here; reference for extra functions only available with a separate license (e.g. VPN); reference for operation of the SNMP shell.
 - **MIB Reference**
HTML document with short descriptions about all SNMP tables and variables for **X1000**.
- **BRICKware for Windows** (English, PDF)
User's guide for Windows utility programs (**BRICKware**)
- **Release Notes** (English, 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 Logic**, you will find instructions to help you upgrade the BOOTmonitor and/or firmware logic.
- UK information (English, PDF)
Instructions for the operation of BinTec routers in Great Britain.

1.5 System Requirements

X1000 can be configured from all conventional platforms. **X1000** is a stand-alone device that is independent of the PC or operating system to which it is connected. The router communicates with the PC over a LAN interface (10/100 Mbps) or a serial connection. Your router can therefore be used in many different operating system environments, such as DOS, Windows, UNIX, AS/400, Macintosh or Novell.

For a Windows PC If you use a Windows PC to configure **X1000**, you need a terminal program for the serial connection, e.g. **HyperTerminal**. Make sure that **HyperTerminal** is also installed on the PC during the Windows installation.



Note that **HyperTerminal** is not included in the standard installation of Windows 98 and Windows ME.

Configuration Wizard If you want to use the **Configuration Wizard**, however, you will require the following:

- PC with serial interface (V.24)
 - Windows 95, Windows 98, Windows NT 4.0 or Windows 2000
 - Installed network card (10 Mbps and/or 100 Mbps Ethernet)
 - Installed Microsoft TCP/IP protocol
- Before we start with the configuration, we will explain how you determine whether the required settings have been made on your PC or, if necessary, how you make these settings yourself.
- High color monitor (more than 256 colors) for correct display of graphics

Remote CAPI CAPI support for communication applications and Unified Messaging is available for the following systems:

- Windows 95, Windows 98, Windows 2000 or Windows NT 4.0
- Novell Netware 3.1x, 4.0x and 5.x

1.6 Guarantee Terms

X1000 is guaranteed for 24 months from the date of purchase.

Extend the guarantee period for your **X1000** to 6 years free of charge!

How?

Simply register as BinTec **X1000** customer online at www.bintec.net within 14 days of the date of purchase.

In recognition of your efforts, we will extend your guarantee from 2 to 6 years and give you a small present.

Guarantee

1. BinTec hereby guarantees this equipment against failure due to faulty material and workmanship for a period of 24 months from the date of initial purchase. Should defects attributable to faulty material or workmanship occur in the equipment during the guarantee period, BinTec will repair the equipment in accordance with the following conditions at no charge for labor or material or (at the discretion of BinTec) replace the equipment itself or its damaged parts. Exchanged equipment or parts shall become the property of BinTec. Exchange equipment or spare parts shall be covered for the remaining part of the original guarantee period, subject to a minimum guarantee period of 6 (six) months from the date of repair or exchange.
2. Work shall only be carried out under guarantee if the original bill or sales check (showing date of purchase, product type and name of dealer) and a description of the fault are submitted together with the defective equipment.
3. Before making a claim under guarantee, make sure you save a backup copy of your configuration. BinTec is not liable in the event of loss of these data.
Before you return the equipment for repair via your dealer, please remove all parts, functions, equipment, changes and additional equipment not covered by the guarantee. BinTec is not liable in the event of damage or loss of these parts or devices. BinTec is not liable for changes, deletions or other modifications to the configuration of the equipment. The equipment will be returned to you with a current software version in an unconfigured state.
4. The following items are excluded from this guarantee:
 - (1) Regular maintenance and repair or replacement of parts due to normal

wear and tear.

(2) Expendable items supplied with this equipment.

(3) Removal of signs of use.

(4) Damage or loss of configuration data.

(5) Damage caused by (a) force majeure or reasons beyond the control of BinTec; (b) incorrect use, especially use of the equipment for purposes other than the intended purpose or use not complying with the BinTec operating and maintenance manual; (c) incorrect use or maintenance of the equipment; (d) connection of the equipment to unsuitable power sources; (e) physical damage to housing; (f) repair attempts by third parties not authorized by BinTec; (g) use of equipment with accessories, equipment or additional equipment from manufacturers not authorized by BinTec.

5. If BinTec can prove that no case exists for a claim under the guarantee, the costs of troubleshooting and other related services shall be charged to the customer.
6. This guarantee becomes invalid if the type or serial number of the equipment has been changed, deleted, removed or made unreadable.

Pick-up Service Apart from the guarantee provided, BinTec Communications AG offers you a Pick-up Service for your **X1000**: If problems occur in the equipment hardware within a period of one year, you can replace your **X1000** free of charge. Your defective equipment is usually collected from you on the next working day and a replacement delivered at the same time.

To make it easier for you to use our Pick-up Service, you will find a form for this service enclosed with your equipment and at our World Wide Web site at www.bintec.net.

1.7 About this Manual

1.7.1 Contents

This manual is structured as follows:

Chapter	Contents
1: "Welcome!"	General introduction, scope of supply, guarantee terms, information about this manual.
2: "General Safety Precautions"	General safety precautions.
3: "Getting Started"	Instructions on taking X1000 into operation in a few minutes using the Configuration Wizard and how to install and configure other useful software.
4: "Overview"	Basic information about routers and networks.
5: "Connecting X1000"	A basis for working with the Setup Tool.
6: "Basic Configuration with the Setup Tool"	How to get X1000 working with the Setup Tool (alternative to Configuration Wizard).
7: "Advanced Configuration"	How to carry out more advanced settings with the Setup Tool.
8: "Security Mechanisms"	How to configure security mechanisms using SAFERNET, e.g. ►► NAT or ►► CLID .
9: "Configuration Management"	How to administrate configuration files and how to perform software updates.
10: "Troubleshooting"	Important tips on fault clearance.
11: "Technical Data"	X1000 technical data.
12: "Important Commands"	A brief overview of the most important commands of the SNMP shell and BRICKtools for Unix.

Chapter	Contents
13: "General Safety Precautions in 15 Different Languages"	General safety precautions in various national languages.

Table 1-1: List of chapters

1.7.2 Meaning

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




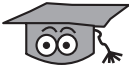

Symbol	Meaning
	Points out useful and relevant tips and tricks.
	Predicts potential pitfalls and explains how to avoid them.
	Brings to your attention general and important points.
	Explains additional background information.
	Brings your attention to important safety precautions. Levels of danger are in accordance with ANSI: <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

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	Indicates menus and submenus in the Setup Tool.
Non-proportional (Courier), e.g. ping 192.168.1.254	■ Indicates commands (e.g. in the SNMP shell) that you must enter as shown. ■ Display in 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 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 **X1000** 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 **X1000**. Place the equipment on a firm flat base.
 - 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.
 - Make sure the nominal voltage on the label of the mains unit is the same as the local power source. **X1000** may only be operated with the original BinTec Communications mains unit (5 V DC). BinTec Communications AG accepts no liability for damage caused by the use of other mains units.
 - Make sure you follow the correct cabling sequence, as described in the manual. Firstly, connect the LAN, ISDN and serial cables, then connect to the mains, and finally, turn on your **X1000**.
 - Make doubly sure the cabling is correct – especially the ISDN and LAN cables – before you turn on **X1000**. **X1000**'s ISDN connection must not be connected to the Ethernet connection of your PC or hub, and **X1000**'s LAN connection should not be connected to the ISDN connection.
 - Use only the cables supplied. If you use other cables, BinTec Communications AG cannot accept liability for any damage occurring or for any adverse effects on operation.
 - Arrange the cables so that they are not in the way and cannot be tripped over or damaged.

Operation according to the regulations

- Do not connect, disconnect or touch the data lines during lightning storms.
- **X1000** is intended for use in offices. As an ISDN multiprotocol router, **X1000** establishes WAN connections depending on the system configuration. To avoid extra charges, you should carefully monitor the product.
- **X1000** meets the relevant safety standards for information technology equipment for use in offices.
- Operation of the system according to IEC 950/EN 60950 is only guaranteed when the top of the housing is fitted (cooling, fire protection, RFI suppression).
- Ambient temperature should not exceed 50 °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

- The equipment should only be opened by trained personnel. Only service centers authorized by BinTec should carry out any repairs to the equipment. Your dealer will tell you where the service centers are situated. Unauthorized opening and improper repairs can result in serious danger for the user (e.g. electric shock). Unauthorized opening of the equipment invalidates the terms of the guarantee and exempts BinTec Communications AG from any liability.
- 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 will help you to configure the most important and common applications for your local network or your single-user system as quickly as possible. A configuration assistant, the **Configuration Wizard**, helps to make the configuration as easy as possible. With its help, you can configure **X1000** in a matter of minutes.



At the end of this chapter you will be able to:

- Reach **X1000** in the LAN
- Surf the Internet
- Sending and receiving faxes
- If necessary, establish a connection to a remote network (LAN-LAN connection, e.g. to your head office) to access corporate data from the comfort of your home office.

In order to set up these applications, you must first carry out the following:

- **X1000** set-up and connections ([chapter 3.1, page 33](#))
- Make a number of preparations ([chapter 3.2, page 36](#))
- Install Windows software:
 - Install **BRICKware** for Windows ([chapter 3.3, page 43](#))
 - Configure **X1000** with the Configuration Wizard ([chapter 3.5, page 50](#))
 - Configure the Remote CAPI interface ([chapter 3.6, page 64](#))
- Make possible additional settings on your PC ([chapter 3.7, page 66](#))
- Install and configure RVS-COM Lite ([chapter 3.8, page 71](#))

We will explain how to test the configuration at the end of this chapter.



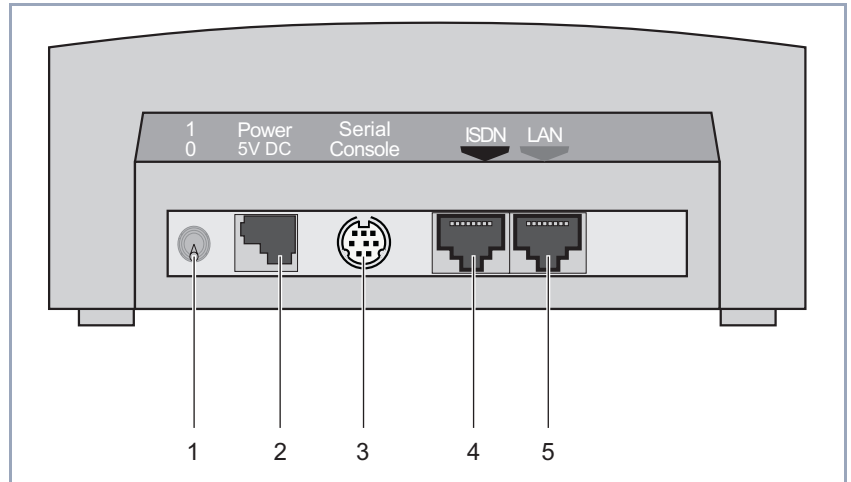
After finishing the basic configuration, you can optimize your configuration as described in [chapter 7, page 201](#).

If you would like to know how to carry out the basic configuration without the Configuration Wizard (e.g. if you are not using a Windows operating system), read [chapter 6, page 127](#).



This chapter is designed to facilitate quick and easy initial configuration with a minimum of technical details. If, however, you want a little more background information, then read [chapter 4, page 83](#).

3.1 Setting Up and Connecting



1	On/off switch	4	ISDN S ₀ port
2	Power supply connection	5	LAN interface (10/100 Base-T Ethernet), marked red on the equipment
3	Serial interface		

Figure 3-1: **X1000** rear view



Alternatively, you can connect **X1000** to the network card of your PC or, if you belong to a small network, to a hub. You only need to make sure you use the right cables.



Connect **X1000** to the ISDN over the ISDN connection (4). It makes no difference to **X1000** whether you use an ISDN socket, an **NTBA** adaptor or a PABX. If, however, you want to use functions specific to a PABX, connect **X1000** to the PABX. This enables you to disable extensions, for example, so that these never reach **X1000** at all. Or you can check the charges for the extensions you assign to **X1000**.



Caution!

The use of the wrong mains adaptor may damage your router!

- Use only the mains unit supplied (5 V DC).
- Make sure the rated voltage marked on the mains unit conforms with the local voltage supply.



Caution!

Incorrect cabling of ISDN or LAN interfaces can cause your router to malfunction!

- Only connect the LAN interface of **X1000** to the LAN interface of your PC/hub and the ISDN interface of **X1000** to the ISDN connection.

Make the connections in the following order:

- Place **X1000** on a firm level surface.
- Connect the serial port of your PC (COM1 or COM2) to the serial interface of your router (3, cf. [figure 3-1, page 33](#)). Use only the serial cable (gray) supplied with the equipment.

You can connect **X1000** to your hub (LAN) or to the network card of your PC (single-user system).

To connect **X1000** to your LAN, you need the red LAN cable supplied with the equipment.

- Connect the LAN interface (marked red) of **X1000** (5) to your LAN. The speed of your LAN (10 Mbps or 100 Mbps) is detected automatically (auto sensing).

If you do not want to connect **X1000** to a LAN, but directly to the network card of your PC (single-user system), you need the adaptor cable as well as the red LAN cable.

- Connect **X1000**'s LAN interface to your PC. This is done by connecting the red LAN cable to the LAN interface of **X1000**, which is marked red (5). Plug the adaptor cable into the red cable. Connect the adaptor cable to the network card of your PC.
- Connect the ISDN interface of the router (4) to your ISDN connection using the black ISDN cable (RJ45) supplied.



If you receive a special cable from Deutsche Telekom AG or another provider for connecting the modem, please use only this cable. If you need to extend this cable, use a standard Ethernet cable.

- Connect **X1000**'s mains connection to the power supply with the mains adaptor supplied.
- Switch the router on with the on/off switch (1).
X1000 performs a selftest. If all cables are correctly connected, the red LED ERR goes out at the end of the selftest and the green LED PWR (operating display) lights up.

3.2 In Advance of Configuration

3.2.1 Gathering Information

Before you start your configuration, you should have information available for the following purposes, according to what you want to do with **X1000**:

- Basic router configuration with licensing (obligatory)
- Internet access (optional)
- Connecting to a corporate network (optional)

In the following table, we have included examples of possible values for the necessary access data. You should supplement the table with your personal data under the heading "Your value". Then you can refer to the values later when needed.

Basic router configuration

For the basic configuration of your **X1000**, you need information about your ISDN connection and network environment:

Access data	Example	Your value
ISDN extensions You received the ISDN extensions with your ISDN connection.	967310 967311 967312	
X1000 IP address	192.168.1.254	
X1000 Netmask	255.255.255.0	



For a point-to-multipoint connection, it is sufficient to enter the final digits of the ISDN extensions that differ for each number. If you have the following extensions (➤➤ **MSNs**), for example: **967310**, **967311** and **967312**, you only need to consider **10**, **11** and **12**.



A description of the settings required for connecting **X1000** to an NTBA adaptor is given below. If you are connecting to a PABX, note the special characteristics of your connection and refer to your PABX documentation if necessary.



If you are not in a network or do not know how to assign IP addresses and net-masks in a new network, then simply use our example values. Otherwise, ask your system administrator.

License card

All you now need for the basic configuration is your license card, which you received together with your **X1000**. On the card you will find a serial number, mask and key, which you will need to activate the features of your **X1000**. You will also find the license number for the communications program RVS-COM Lite.

Internet access

If you want to access the Internet, you will need an Internet Service Provider (ISP), which you have probably already thought of. If not, you should sort this out in the next few days or use an "Internet by call" connection (see next paragraph). If you have an ISP, you will also have received your personal access data. The terms of the required access data may vary slightly from provider to provider. Basically, however, the kind of information required to dial in and establish your personal Internet access remains the same. The following table lists the access data that your **X1000** also needs for a connection to the Internet:

Access data	Example	Your value
Provider name	<i>GoInternet</i>	
Dial-in number The ISDN extension you use to dial in to your Internet Service Provider.	<i>1234567</i>	
User account Your user name	<i>MyName</i>	
Password	<i>TopSecret</i>	



When **X1000** 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.

Some providers such as T-Online require additional information:

Access data	Example	Your value
T-Online number	<i>081512345678</i>	
Joint user account (other user code)	<i>0001</i>	



Some ISPs also offer the option of accessing the Internet without logging in first ("Internet by call"). This means you can check immediately whether your Internet access works with **X1000**, even if you want to apply to another ISP for your personal access data later on.

Corporate network connection

To connect to a WAN partner (e.g. head office), you will need some information about the remote terminal that is to take your call. Likewise, the remote terminal must have information about you. These data must be agreed between both ends of the connection.

X1000 and the router at your HQ check the incoming data before every connection to see if they should take the call from the partner. To protect the network against unauthorized access, the call is accepted only after correct authentication. This authentication is based on a common password and two codes that you and your partner use for the connection.

Access data	Example	Your value
Partner's name Code of head office	BigBoss	
Dial-in number Extension of head office's router	0911987654321	
Local name Your own code. Your partner (at head office) must enter this name as a partner name on his router.	LittleIndian	
Password Common password for this connection	Secret	
Network address(es) of your head office	10.1.1.0	
Netmask(s) of your head office	255.255.255.0	

Table 3-1: Access data



How to use other security mechanisms, e.g. authentication by means of the calling number (CLID) or concealing your own network to the outside (NAT), is explained in [chapter 8, page 289](#).



When **X1000** 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.



You only need the network address and netmask of the WAN partner (head office) if you configure Internet access in addition to a LAN-LAN connection. If you are not configuring Internet access, **X1000** will be configured so that all data not destined for your own local network will be forwarded automatically to the WAN partner (default route).

3.2.2 What to Do in Your Windows Network

You have now gathered all the information **X1000** needs to know.

To make sure everything works correctly, you also need to check whether your PC is suitably configured in the network. If not, you will need to make some settings.

In order that the PCs in your network can communicate with each other, it is necessary that they all speak the same "language". The TCP/IP protocol is just such a language in which PCs exchange information in a LAN or on the Internet. You should therefore ensure that this protocol is installed on your PC before beginning configuration.

Checking the TCP/IP Protocol

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

- 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.

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.
 - Repeat the installation for all the PCs in your network.
- 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.

- Finally** ➤ Repeat the installation for all PCs on the network where you want to use the LAN-LAN connection, Internet access or communications programs over **X1000**.

3.3 Installing BRICKware Under Windows

- 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**.

After 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 software again.

New installation

Proceed as follows to install **BRICKware**:

- Click **Next**.
- Enter the directory in which **BRICKware** is to be installed or accept the default directory.
- Click **Next**.
- Select your router type, i.e. the group *X1000*, *X1200* or *X4000*.
- Click **Next**.

- Select the software components you wish to install. You can accept the default selection or make another selection. Be careful not to cancel the marking of the **Configuration Wizard** if you want to use the **Configuration Wizard** for basic configuration of **X1000**.
- 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.
- If you want to configure **X1000** again, leave the default setting *Continue device configuration* and click **Finish**.
The **Configuration Wizard** starts.

Update After **BRICKware** version 5.2.1, you do not need to deinstall if you have an older version of the software on your PC, but 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.

3.4 Solution Scenarios

This section contains some configuration examples to explain some of the most frequently asked questions about configuration.



You only need to run through the **Configuration Wizard** once, even if you want to combine several suggested configurations.

3.4.1 Configuring Internet Access

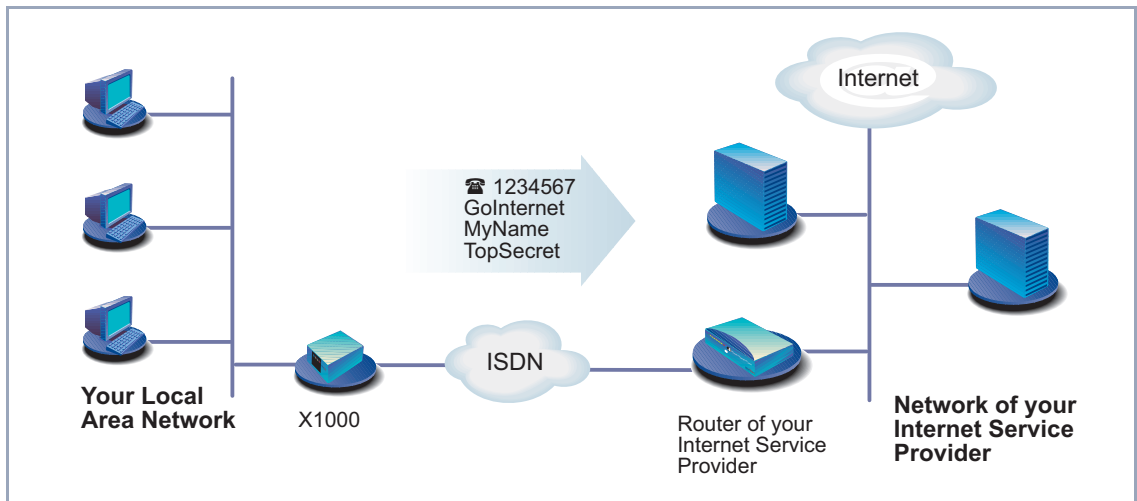


Figure 3-2: **X1000** and your Internet Service Provider

You can quickly and easily configure Internet access for **X1000** under Windows using the .

Proceed as described in [chapter 3, page 31](#). Follow the instructions on the screen, and note the following:

- Select the configuration items (see [chapter 3.5, page 50](#)):

- **Basic Router Configuration**, for making the basic router settings ([chapter 3.5.1, page 53](#)).
 - **Internet Connection**, for configuring your Internet access ([chapter 3.5.2, page 57](#)).
- Complete the configuration as described in [chapter 3.5.4, page 61](#).
 - If you want to access the Internet from several PCs, proceed as described in [chapter 3.7, page 66](#).
 - Finally test your configuration (see [chapter 3.9, page 78](#)).

3.4.2 Using Communications Applications

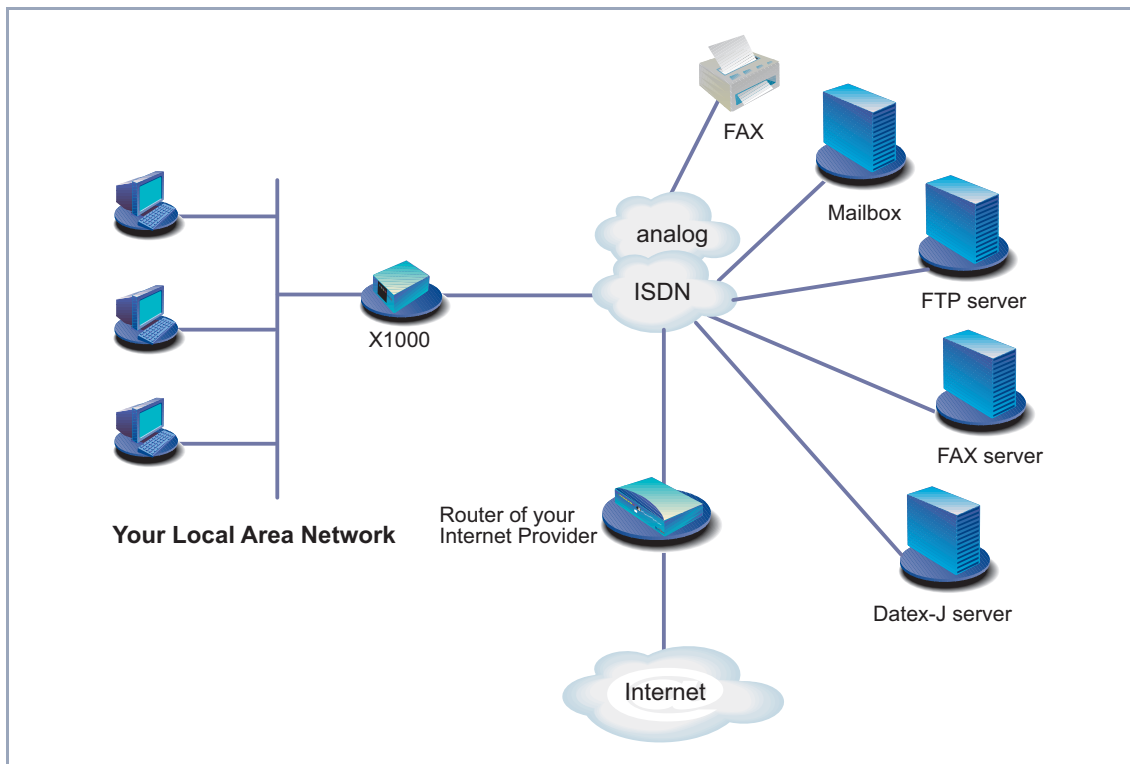


Figure 3-3: **X1000** with communications applications

Use the **Configuration Wizard** under Windows to use communications applications (e.g. fax and answering machine) from several PCs.

Proceed as described in [chapter 3.2, page 36](#) onwards. Follow the instructions on the screen. and note the following:

- Select the configuration items (see [chapter 3.5, page 50](#)):
 - **Basic Router Configuration**, for making the basic router settings ([chapter 3.5.1, page 53](#)).
- Complete the configuration as described in [chapter 3.5.4, page 61](#).
- Configure the Remote CAPI interface (see [chapter 3.6, page 64](#)).
- Configure FAX and answering machine, if required ([chapter 3.8, page 71](#)).

3.4.3 Connecting a Branch Office to Head Office

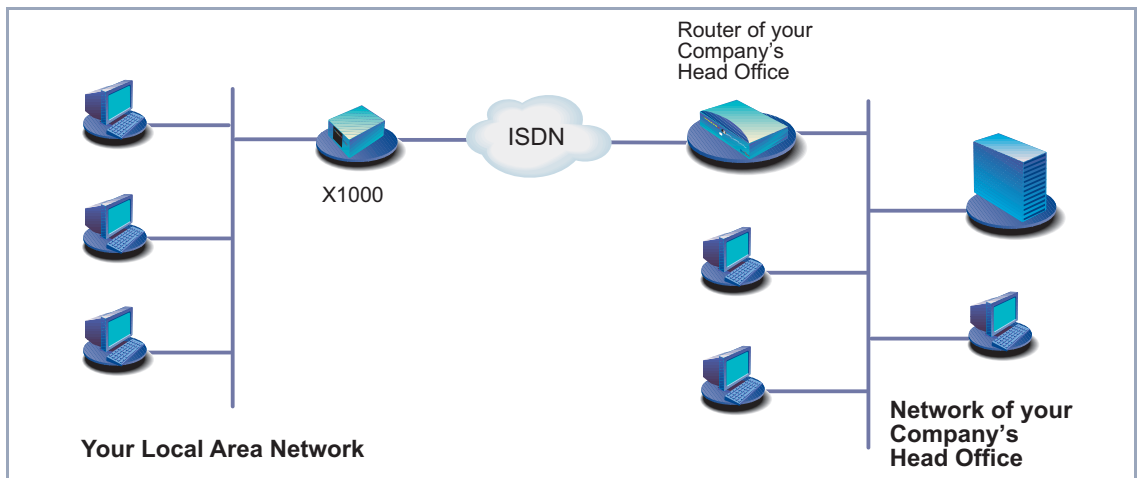


Figure 3-4: **X1000** in your branch office

You can quickly and easily connect branch offices or home offices to the head office using the **Configuration Wizard** under Windows. The employees in the branch office or home office can then access data at the head office as if they were in the head office.

Proceed as described in [chapter 3, page 31](#). Follow the instructions on the screen, and note the following:

- Select the configuration items (see [chapter 3.5, page 50](#)):
 - **Basic Router Configuration**, for making the basic router settings ([chapter 3.5.1, page 53](#)).
 - **Connection to a Corporate Network**, e.g. for connecting to a head office ([chapter 3.5.3, page 59](#)).
- Complete the configuration as described in [chapter 3.5.4, page 61](#).
- Make additional settings on your PCs ([chapter 3.7, page 66](#)).

3.4.4 Providing Access to Head Office for Field Service Staff without Router Access (Dial-In)

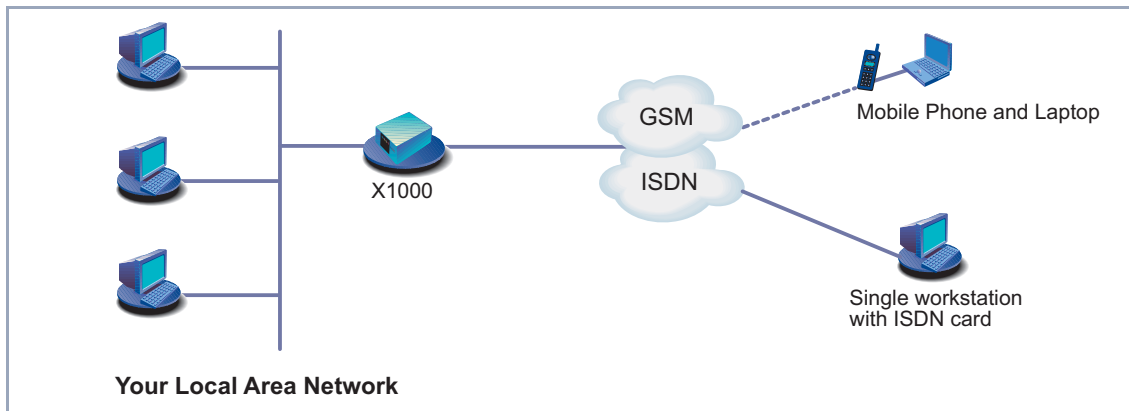


Figure 3-5: **X1000** in head office

To provide field service or home office staff with access to data at their head office (dial-in), you need the Setup Tool for configuring your **X1000**.

A PC in a home office can access the corporate network via an ISDN connection using **dial-up** networking.

Field service staff can dial in to the head office via laptop and mobile phone over the GSM.

First you must carry out the basic configuration of the router. You can use the **Configuration Wizard** (cf. [chapter 3.5.1, page 53](#)) or the Setup Tool (see [chapter 6, page 127](#)) for this purpose.

Next you must configure the person who wants to access data at head office as a WAN partner. The exact configuration is explained using an example in [chapter 6.2.3, page 190](#).

3.5 Configuring X1000 Under Windows

You started the **Configuration Wizard** in [chapter 3.3, page 43](#), which you can now use to configure **X1000**. **X1000** must first be ready for operation.

The following configuration options are available:

- Basic router configuration
- Internet access
- Corporate network connection



An extensive online Help Assistant is available if you have any questions during configuration. To activate our context-sensitive online Help Assistant:

- ▶ Press **F1** or click **Help**.



If you have already used the **Configuration Wizard** to create an existing configuration, the Wizard can adopt the preset values. At the end of the configuration, the Wizard transfers the new configuration file to the router and also saves it to your PC.

You can also save the original configuration file of **X1000** at the end of the configuration on the router (under `old_cfg`), as long as you have not forgotten the password.



If you are operating **X1000** on a point-to-point connection, an entry must be made in Setup Tool in addition to the settings under Wizard. In **CM-1BRI, ISDN SO ▶ INCOMING CALL ANSWERING**, set the mode for the comparison of numbers to *left to right (DDI)*. The Wizard does not make these settings automatically as this is not the default setting. See also [chapter 6.1.4, page 138](#).

Starting the Configuration Wizard



If the **Configuration Wizard** has not yet been started, proceed as follows:

- Select the Windows Start menu and click **Program** ➤ **BRICKware** ➤ **Configuration Wizard**.

The start window of the **Configuration Wizard** opens:



Figure 3-6: **Configuration Wizard** start window

- Click **Next**.

Setting the configuration mode

In the following window, choose between Quick and Expert Mode.

- If you are not very familiar with networking technologies, choose **Quick**. The following is an explanation of how to configure using the Quick Mode.
- If you are already familiar with networking technologies and the configuration of routers, you could choose **Expert**.

In this mode, you could:

- configure your router as a DHCP server.
- configure different users for communications applications
- assign different ISDN extensions to different services (e.g. fax)
- define different filters



Configuration with the Quick Mode is sufficient in many cases. You can use Expert Mode to optimize an **X1000** configuration you have created in Quick Mode.

However, if you first use Expert Mode and then Quick Mode, the complete configuration will be overwritten and the previous configuration in Expert Mode will be lost.

- Click **Next**.

A message appears saying the router must be restarted for a serial connection.

Making a serial connection

- Click **Next**.

The **Configuration Wizard** establishes a connection to **X1000**. After that the router is restarted and the type of router identified: in your case, **X1000**.



If the **Configuration Wizard** cannot establish a connection or an error message appears:

- Make sure **X1000** is correctly connected.
- Check to see if a terminal program (e.g. **HyperTerminal**) or another program is running and occupying the serial interface. If yes, close the program.
- Check if **X1000**'s baud rate has changed. The ex works setting is 9600 bps. If you have changed the baud rate, set it to 9600 bps again or use the **Configuration Wizard** in Expert Mode.
- If the **Configuration Wizard** could not boot **X1000**, switch **X1000** off and then on again. Wait until the LEDs stop blinking.
- Click **Next**.

- Click **OK** and then **Next**.

Selecting configuration options

- Select one or more of the following options:
 - **Basic Router Configuration**, for making the basic router settings ([chapter 3.5.1, page 53](#)).
 - **Internet Connection**, for configuring your Internet access ([chapter 3.5.2, page 57](#)).

- **Connection to a Corporate Network**, e.g. for connecting to a head of-
fice ([chapter 3.5.3, page 59](#)).

The basic router settings will have to be made in every case.

- Click **Next**.
A list of the selected configuration options is displayed.
- Click **Next**.

3.5.1 Configuring the Basic Router Configuration

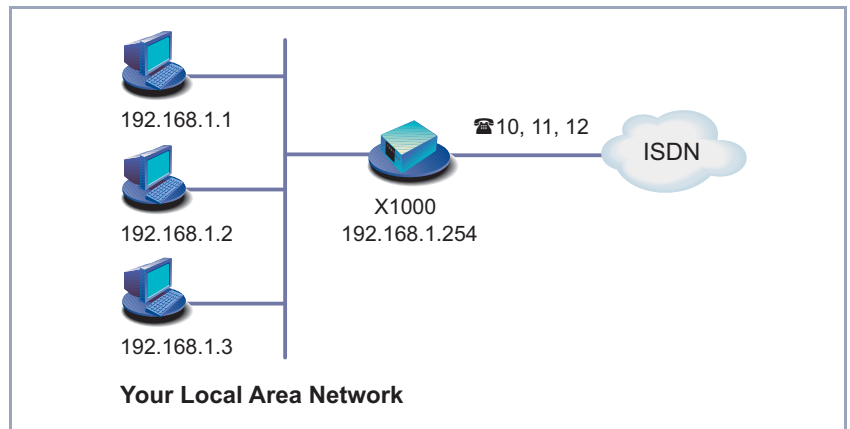


Figure 3-7: **X1000** basic configuration



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 "[Changing the password](#)", page 120.

- You must therefore change your system password when requested to do so.

- First enter your license data, which can be found on your license card. Click **Next**.

The **Configuration Wizard** checks the settings of the PC on which it started and derives suggested values for the configuration.



The **Configuration Wizard** provides different configuration options, according to how your PC is configured.

Unconfigured network

- If your PC is still unconfigured, does not have an IP address and is configured as a DHCP client, the Wizard will ask you if **X1000** should be configured as a DHCP server and if you wish to retain the suggested settings.

- Click **Next**.

Your **X1000** receives the IP address **192.168.1.254** and automatically assigns all PCs in the network an IP address beginning with **192.168.1.1**.



If you are familiar with networking technologies and do not want to configure a DHCP server or you want to configure the settings for a DHCP server and IP addresses yourself, proceed as follows:

- Deactivate the field **Use this Configuration**.
- Now enter **X1000**'s IP address and the corresponding netmask, e.g. **192.168.1.254** and **255.255.255.0**. Click **Next**.
- State whether you want to configure **X1000** as a DHCP server. If you do, enter the IP address range for your PCs and define the number of IP addresses to be assigned by **X1000**.

After configuration, remember to assign your PCs fixed IP addresses if no DHCP server is configured (cf. [chapter 3.7.1, page 66](#)).

An already configured network

- If your PC has a fixed IP address, the Wizard asks you in the **Router IP Address** window for **X1000**'s IP address in the LAN and the corresponding netmask. Enter the values, e.g. **192.168.1.254** and **255.255.255.0**.

- Click **Next**.

- Enter a new password for your access authorization.

- Click **Next**.

All system passwords are provided with this new password.

- Enter the extensions of your ISDN port that you want to use with **X1000**: Enter an extension in the **Extensions** field and click **Add**. Repeat the entry for all other extensions (cf. [figure 3-8, page 55](#)).

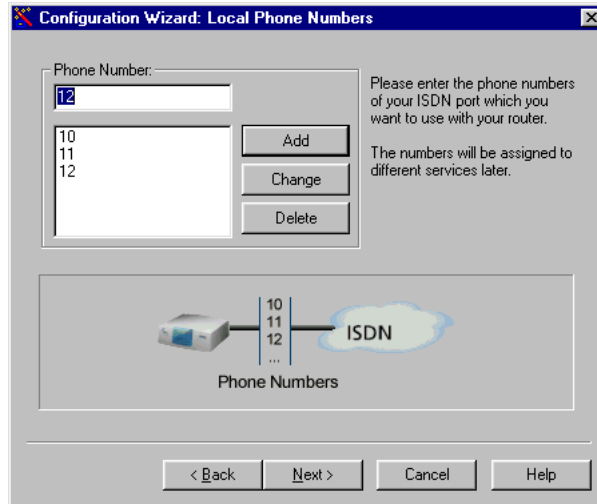


Figure 3-8: Entering extensions in the **Configuration Wizard**

- Click **Next**.
The Wizard automatically assigns the extensions to certain services (more on services and users in [chapter 4.3, page 88](#)). This allocation can only be changed in Expert Mode (cf. [figure 3-9, page 56](#)).

The following window opens:

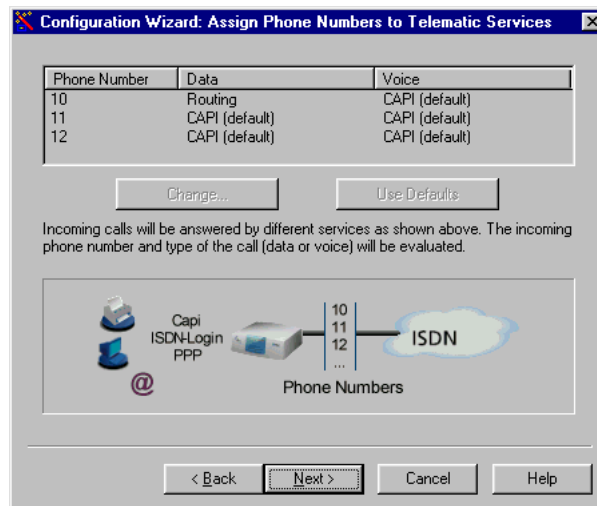


Figure 3-9: Allocation of extensions in the **Configuration Wizard**

➤ Click **Next**.

The basic configuration is now complete. A summary of the configuration data appears.

Configuration in Expert Mode

You can also do the following in Expert Mode:

- Define the software version for which you want to create the configuration.
- Change the system data, e.g. contact, name and location of **X1000**.
- Specify the IP address of a DNS.
- Configure your router as a DHCP server.
- Receive the system time from a source other than ISDN.
- Enable ISDN login.
- Define different system passwords.
- Assign communications applications to different users and extensions.
- Set different filters (NetBIOS, CAPI and TAPI clients).
- Monitor activities (**Activity Monitor**).

- Log system messages.
- Monitor the utilization of **X1000**.
- State the time when charging information is to be obtained from ISDN.
- Configure user accounts for telecommunications applications (CAPI and/or TAPI).

3.5.2 Internet Access with X1000

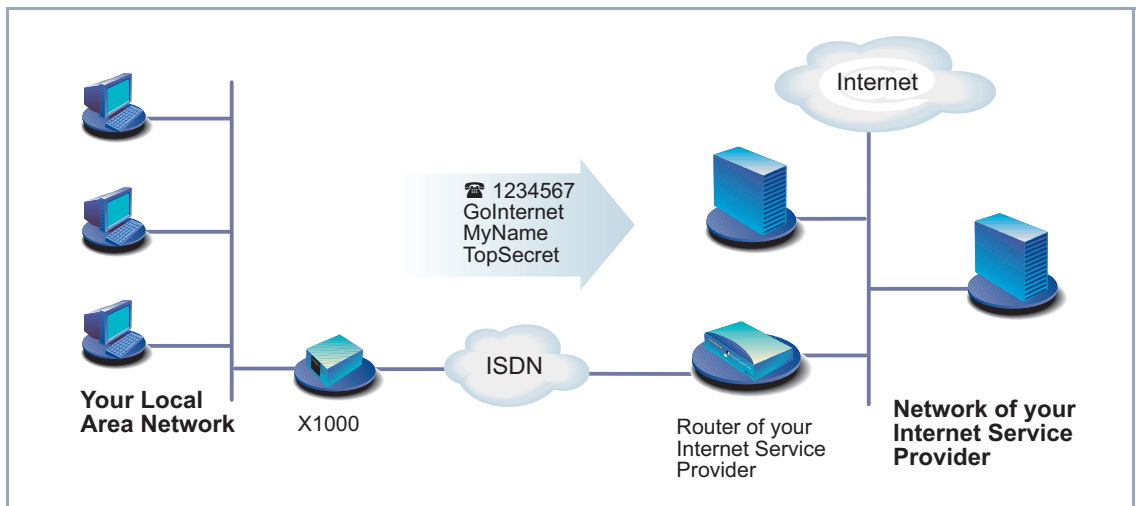


Figure 3-10: **X1000** and your Internet Service Provider

- Click **Next**.
A message window appears.
- Click **Next** after reading the information in the window.

- First define your Internet Service Provider. If you cannot find your Internet Service Provider in the list, select *Other Internet Service Provider*.

**Internet test access
(Internet by call)**

If you would like to test your Internet access with **X1000** immediately, you do not need personal access data from an Internet Service Provider, but can configure a so-called "Internet-by-call" access.

- Select a provider that offers access without first logging in. The text on the right of the selected provider gives you information about this.
- Click **Next**.
- Enter the access number of the Internet Service Provider, e.g. **1234567** or use the preset number.
- Click **Next**.
- Enter your user name and the associated password, e.g. **MyName** and **TopSecret**.
- Click **Next**.

The configuration of your Internet connection is complete.

**Conventional Internet
access**

To configure a conventional Internet access, proceed exactly as for an Internet test access. In this case, you can set up a connection to any Internet Service Provider from which you have previously received access data.

**Configuration in Expert
Mode**

A summary of the configuration data appears at the end of each configuration. You can also do the following in Expert Mode:

- Keep a record of IP connection data.
- Enable data compression.
- More accurately define connection clearance (dynamic and static short hold).
- Activate channel bundling. (this option cannot be selected for all Internet Service Providers).

3.5.3 Connecting X1000 to a Corporate Network

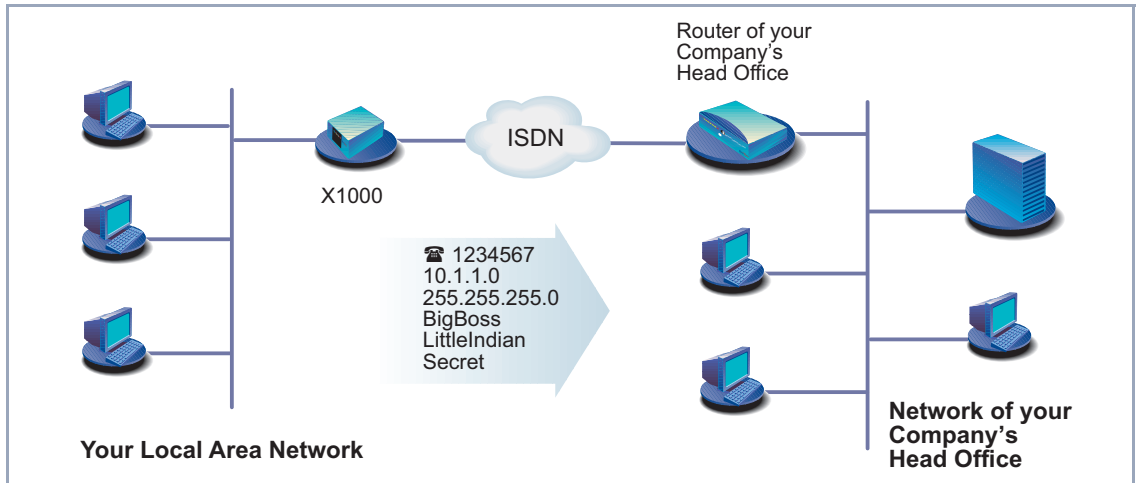


Figure 3-11: X1000 and your head office

- Click **Next**.
A message window appears.
- Click **Next** after reading the information in the window.
Another message window may appear.
- Click **Next** after reading the information in the window.
- First enter the name of your WAN partner (e.g. your head office) and the corresponding access number e.g. **BigBoss** and **0911987654321**.
The name of your WAN partner must be the same name as your partner uses as a local name. Your partner must accept calls to the given access number with the routing service.
- Click **Next**.
- Enter your local name and the common password, e.g. **LittleIndian** and **Secret**.
Your local name must be the same name as your partner uses for you as a WAN partner.
- Click **Next**.

- Add a route to your head office:
If you have not configured Internet access, choose **Use Default Route**.
If you have configured Internet access, then enter the route yourself: Click **Add**. Enter the IP address or network address and the netmask, e.g. **10.1.1.0** and **255.255.255.0**. By setting the route, you define the path connecting you to your WAN partner (e.g. head office) (cf. [figure 3-12](#), page 60).

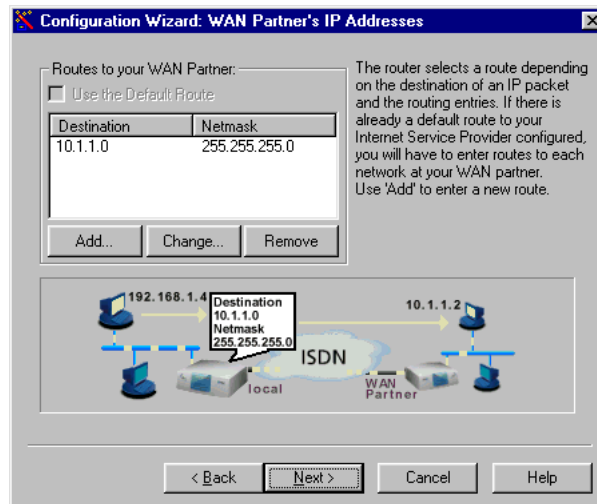


Figure 3-12: Defining the route to the WAN partner in the **Configuration Wizard**



Each route determines the path to a network or subnet of your WAN partner. A route is clearly defined by IP address/network address and netmask.

Instead of the network address, you can choose and enter any IP address from your partner's network. The **Configuration Wizard** determines the network address automatically using the corresponding netmask.

- Click **OK**.
- If the network of your head office comprises several single networks (subnets) and you want access to each of these subnets, you must enter a route for each one of them (cf. [figure 4-3](#), page 99).
- Click **Next**.

The configuration of your WAN partner is complete. A summary of the configuration data appears.

Configuration in Expert Mode

You can also do the following in Expert Mode:

- Configure an automatic callback function, so that only one of the two partners takes the telephone charges.
- Check the number of the caller: Calling Line Identification (CLID).
- Keep a record of IP connection data.
- Activate Back Route Verify to prevent the import of manipulated data packets.
- Define data compression, encryption and channel bundling.
- More accurately define connection clearance (dynamic and static short hold).

3.5.4 Completing the Configuration

- Click **Next**.
- Select **Save the former configuration on the router** to save an existing configuration of **X1000** before overwriting.
- Click **Finish** to complete configuration.

The Wizard logs in to **X1000**. An existing configuration is saved on the router as `old_cfg`. The new configuration is transferred to **X1000** and also saved on your PC under the name `brick.cfg` in the `BRICK` directory. A message appears after a while saying that the configuration is completed.



If an error message appears saying that the **Configuration Wizard** could not log in to the router because the password has been changed, proceed as follows:

- If you know the password of the existing configuration, enter the password and click **OK**.

The Wizard tries to log in to **X1000**.

- If you do not know the password, click **Unknown** and then **OK**.

X1000 is reset to the ex works state and all the previous configurations are lost.



The **Configuration Wizard** always saves your newly created configuration on the PC, even if errors occur during transmission to the router.

Further settings can be made to the configuration file saved on your PC using the Wizard.

- Click **OK**.

If you have configured **X1000** as a DHCP server and your PCs as DHCP clients (the usual case), **X1000** will now assign the PCs their IP addresses. This happens automatically under Windows NT or Windows 2000 (program IPCONFIG), but you must confirm the assignment under Windows 95 (program WINIPCFG).

- Click **Yes** to start WINIPCFG. Click **Renew** and then **OK**.

A message window opens asking if you want to configure the CAPI client.

- Click **Yes**.

The Remote Clients Configuration window opens:

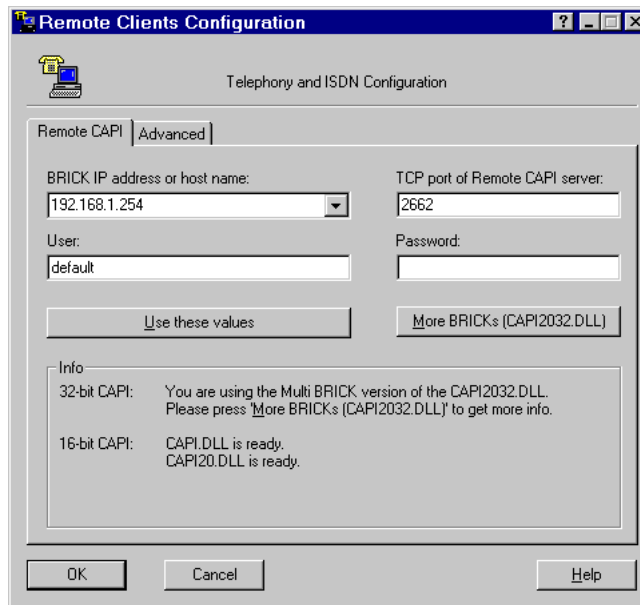


Figure 3-13: Remote CAPI configuration

3.6 Remote CAPI Interface on the PC

Enter **X1000** as CAPI server in the ➤➤ **Remote CAPI** configuration program.

The CAPI server of **X1000** permits the following:

- Operation of communications applications on every PC in the network (e.g. fax services with RVS-COM Lite)
- Simultaneous ISDN access via communications applications from several PCs

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

You have already installed **BRICKware** on the first PC and have opened the configuration window for Remote CAPI configuration (cf. [figure 3-13, page 63](#)). You can shortly proceed with [chapter 3.6.2, page 64](#). You must first install the CAPI configuration program and configure the Remote CAPI interface for all other PCs in the network, as described in [chapter 3.6.1, page 64](#) and [chapter 3.6.2, page 64](#).

3.6.1 Installing the Remote CAPI Client on all Other PCs

- If not yet done, install **BRICKware** as described in [chapter 3.3, page 43](#). If no administration tasks are to be executed from a PC, switch off the **Administration Tools**.
- Follow the instructions on the screen.
- Click **OK**.
The Remote CAPI configuration window appears (cf. [figure 3-13, page 63](#)).

3.6.2 Configuring Remote CAPI

Proceed as follows (see [figure 3-13, page 63](#)):

- Enter **X1000**'s IP address, e.g. **192.168.1.254** in the **Remote CAPI** tab.

- If you have used Quick Mode in the **Configuration Wizard**, retain the entry **default** in the **User** field.
- If you have configured several users in the Expert Mode of the **Configuration Wizard**, enter your user name and password. The rights you have set for these users during configuration are therefore valid on the current PC.
- Click **Use these values**.
The "Remote CAPI is ready" message appears after a short time.
- If no error message appears, click **OK**.



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

- **X1000**'s IP address is correct.
 - You have entered the license data correctly.
 - You have entered a valid user name and the correct password.
 - The right port number 2662 has been entered.
 - Your PC has been configured as a DHCP client and has been assigned an IP address (see [chapter 4.4, page 92](#)).
- Repeat the Remote CAPI installation on all PCs in the network on which you want to enable communications applications (e.g. fax).



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 BinTec routers in the network as CAPI servers.

3.7 Configuring a PC

To ensure that your network and its connection to the outside works properly, you may have to change some additional settings on your PCs:

- If you have not configured **X1000** as a DHCP server with the Wizard and the PCs have not yet been given any IP addresses, you will have to do the following (as per [chapter 3.7.1, page 66](#)):

- define the IP addresses now
- show the PCs "the way out" (gateway, DNS)

If you have used the **Configuration Wizard**'s default settings and have configured your PCs as DHCP clients, you can disregard [chapter 3.7.1, page 66](#). In this case, **X1000** automatically supplies the necessary information.

- 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 [chapter 3.7.2, page 68](#).

3.7.1 Telling the PC the IP Address, Gateway and DNS

If you have not configured **X1000** 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. Proceed as follows:

- Windows 95/98**
- Click the Windows Start button and then **Settings** ➤ **Control Panel**.
 - Double click **Network**.
 - 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 **X1000**'s IP address, e.g. **192.168.1.254**, in the **Gateway** tab. Click **Add**.

- If you do not have your own DNS, enter **X1000**'s IP address in the **DNS Configuration** tab under **DNS Server Search Order**, e.g. **192.168.1.254**.
- Windows NT**
- Click the Windows Start button and then **Settings** ➤ **Control Panel**.
 - Double click **Network**.
 - 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 **X1000** as default gateway.
 - Click **Add** in the **DNS** tab under **DNS Server Search Order** and enter **X1000**'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 **X1000** as default gateway.
 - If you do not have your own DNS, enter the IP address of **X1000** 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**.
- And finally,**
- Confirm all entries and restart your PC.
 - Repeat the installation for all the PCs in your network.

3.7.2 Finding PCs on your Partner's Network

You have now set everything on your **X1000** 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**). Computer names are used especially in Windows networks. PCs, however, only understand IP addresses and not names. Thus, it is necessary for the names to be translated (resolved) into their corresponding IP addresses (cf. [chapter 4.5, page 95](#)). Typical examples of such name resolution are DNS or WINS servers. As you normally do not want to set up your own server in a small network, there is an alternative way of resolving the name **BossPC** into an IP address: the LMHOSTS file.

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. Alternatively, you can use DNS Proxy (see [chapter 7.3.2, page 259](#)).



Caution!

The following configuration can lead to increased connections and thus higher telephone bills. The conditions that lead to connections being set up are largely dependent on the respective network configuration. If you connect a network drive, for example, you must expect regular requests to increase the number of connections made.

- To avoid unintentional charges, it is essential that you monitor your **X1000**. Use the Credits Based Accounting System for this purpose (see [chapter 8.1.3, page 299](#)).



You can only use the following process if you have not configured extensive NetBIOS filtering with the **Configuration Wizard**. 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. If in doubt, ask your system administrator.



You can also register completely with the Windows NT domain of a partner network. To test such a configuration, BinTec provides a test access for your use. How to configure this access is described at www.bintec.net.

You can tell your PC the IP address of the **BossPC** by editing the LMHOSTS text file: Although this method is possible, it is time-consuming and laborious, as you must make the necessary entries for every PC in your LAN. We recommend using DNS Proxy instead (see [chapter 7.3.2, page 259](#)).

To edit 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.

Creating a shortcut on the desktop

➤ To avoid having to look for the **BossPC** every time you restart your PC, right-click the PC icon 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.

Connecting a network drive

Another possible method of setting up a network drive connection is as follows:

➤ 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**.

3.8 Configuring Fax and Answering Machine with RVS-COM Lite

Let's fax something. But how?

After you have successfully configured your PC and **X1000**, install RVS-COM Lite. RVS-COM Lite offers you facilities for the following:

- Sending and receiving faxes
- Configuring an answering machine
- Configuring file transfer and Eurofile transfer services

In the following sections, we describe how to teach your PC and **X1000** how to fax with RVS-COM Lite (version 1.63) and how to set up an answering machine facility.



You have received just one single-user license for RVS-COM Lite with **X1000**. If you want to install RVS-COM Lite on several PCs, please contact RVS Datentechnik GmbH. You can obtain the address from RVS-COM Lite's online help.

3.8.1 Installing RVS-COM Lite

- 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**.
- Click **RVS-COM Lite** in the start window.
The setup program starts.
- Enter your RVS-COM license number, which can be found on your license card.
- Click **Install**.
The start window opens.

- Confirm the following two windows and enter the directory in which RVS-COM Lite should be installed. Click **Next**.

The files are copied. After a moment a window appears saying the setup program is finished.

- Click **Finish**.

The start window of the configuration assistant appears:

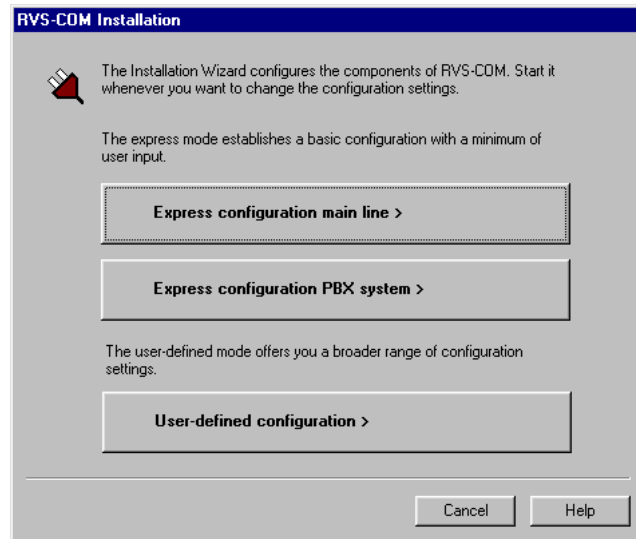


Figure 3-14: Start window of the RVS-COM Lite configuration assistant



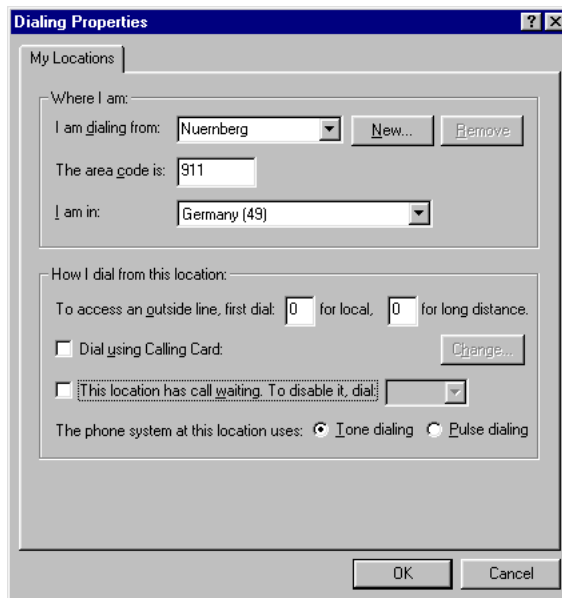
Should an error message appear saying no CAPI interface has been installed:

- Make sure **X1000** is connected to your ISDN connection.
- Make sure your Remote CAPI configuration is configured as described in [chapter 3.6.2, page 64](#).



To manage faxes with a Windows e-mail system instead of with the RVS inbox or to install RVS ISDN modems (also for ➤➤ **dial-up** network), select the configuration mode **User-Defined Configuration**.

- If **X1000** is connected to a main line (e.g. NTBA adaptor), click **Express configuration main line**.
- If **X1000** is connected to a PABX, click **Express configuration PBX system**.
- Click **Next**.
A message appears saying you have configured RVS-COM for operation with an ISDN adaptor with a CAPI interface.
- Click **Next**.
- If a message appears saying you should change the dialing properties (e.g. area code, exchange number), confirm the message to set your dialing properties correctly. Adjust the settings (cf. [figure 3-15, page 73](#)).



The screenshot shows the 'Dialing Properties' dialog box with the following settings:

- Where I am:**
 - I am dialing from: Nuernberg
 - The area code is: 911
 - I am in: Germany (49)
- How I dial from this location:**
 - To access an outside line, first dial: 0 for local, 0 for long distance.
 - Dial using Calling Card
 - This location has call waiting. To disable it, dial: []
 - The phone system at this location uses: Tone dialing, Pulse dialing

Figure 3-15: Dialing properties



The area code must be entered without the "0" prefix.

You only need the exchange number if you are operating **X1000** with a PABX. Normally, the exchange numbers for local and long-distance calls are the same (see [figure 3-15, page 73](#)).

- When you have adjusted the settings, click **Apply** and then **OK**.
- If you selected **Express configuration main line**, enter the extension of your ISDN connection in the next window. Select one of the extensions you have already entered with the **Configuration Wizard** and assigned to the CAPI service. You can only enter one extension with the configuration assistant, but you can add more later.
- If you selected **Express configuration PBX**, enter in the next two windows the extension and ISDN phone numbers (point-to-multipoint) and extension number and prefix of the extension (point-to-point).



If you are operating **X1000** on a point-to-point connection, an entry must be made in Setup Tool in addition to the settings under Wizard. In **CM-1BRI, ISDN SO ▶ INCOMING CALL ANSWERING**, set the mode for the comparison of numbers to *left to right (DDI)*. The Wizard does not make these settings automatically as this is not the default setting. See also [chapter 6.1.4, page 138](#).

- Click **Next**.
- Click **Next** in the following windows and finally **Finish**.
The configuration with the configuration assistant is now complete.

3.8.2 Configuring RVS-COM Lite

In the following section, the numbers you have also set for the CAPI service with the Wizard have to be allocated to different communications applications (fax, answering machine). The following diagram illustrates which number in our configuration example is to be used for a certain facility.

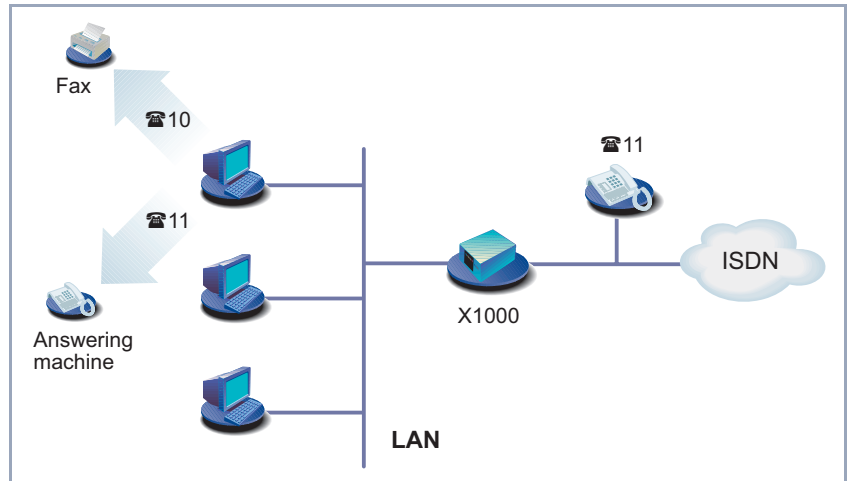


Figure 3-16: Scenario: 1 telephone, 1 PC with fax and answering machine



It is assumed that a telephone responds to one of the numbers you have entered with the Wizard (**11** in example).

- Select the Start button in the Windows menu and click **Program** ➤ **RVS-COM Lite** ➤ **CommCenter**.
- Click **Add** in the **Phone Numbers** tab to enter more phone numbers. Enter the numbers that you have already used for router configuration with the Wizard (cf. [figure 3-17, page 76](#)).

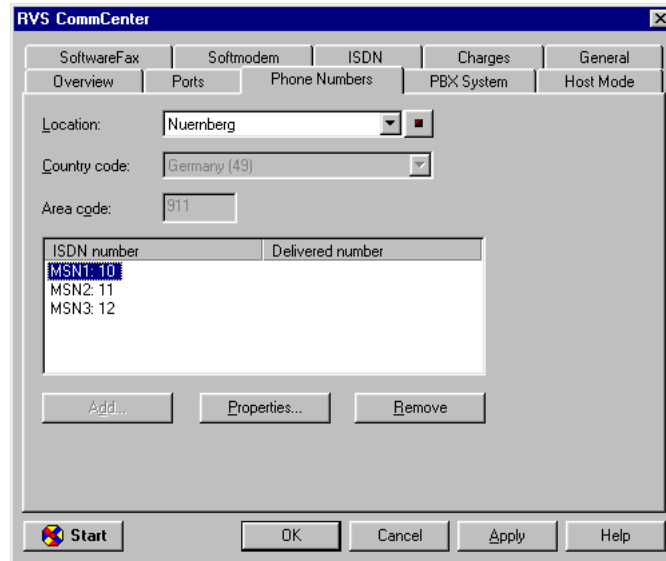


Figure 3-17: Phone number configuration in RVS-COM Lite

- Click **Apply** after you have entered all the numbers. Make sure that the options **Use software fax for sending fax** and **Use software fax for receiving fax** are active in the **Software fax** tab.

- Click **Properties** in the **Ports** tab to allocate the numbers to the various services (cf. figure 3-18, page 77).

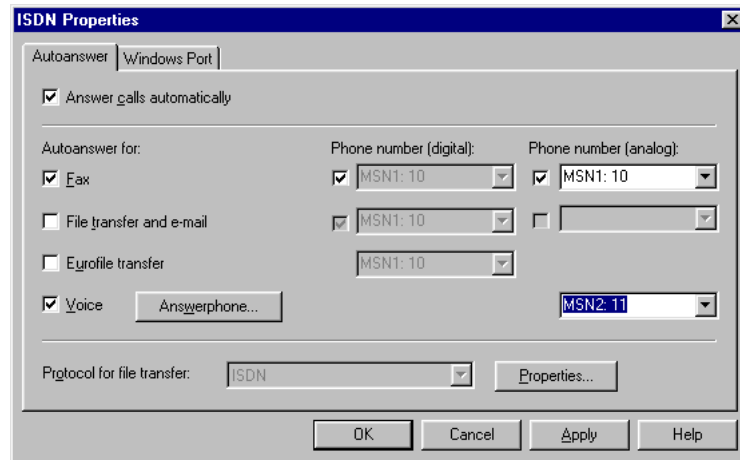


Figure 3-18: Allocation of phone numbers to services in RVS-COM Lite

- Allocate the first phone number to the fax service, the second number to voice (answering machine). Use different phone numbers.
- To adjust the answering service facility, click **Answerphone** and, if necessary, change the recorded message and the number of rings before the call is taken.
- Click **OK**.
- Click **Apply** and finally **OK**.

The following message appears in the list of connections: "ISDN: waiting for call." RVS CommCenter is ready to take calls and faxes.

3.9 Testing your Configuration

Your configuration is now complete, so let's make sure everything works!

3.9.1 Testing your Internet Access

- Configure your browser if you have not done so already. If you have received the IP address of a proxy server from your Internet provider, you can enter this address. Make sure you configure a connection over your local network.
- Try contacting us by typing www.bintec.net in your browser. The home page of BinTec Communications AG appears.

3.9.2 Sending and Receiving E-Mails

- Open an account in the e-mail program if you have not already done so. You should have received the servers for incoming and outgoing mail from your Internet provider. Make sure you configure a connection over your local network.
- Just send an e-mail to a good friend or – if you like – send one to BinTec! Use the following e-mail address for this:
testmail@bintec.de - enter test mail as reference.
You will receive an immediate reply from us to reassure you that the mail arrived successfully.

3.9.3 Sending a Fax

Send a friend a test fax or send it to yourself by using your own new fax number as the recipient's number.

First make sure that several attempts are made to send each fax if it cannot be sent at the first attempt.

- Select the Start button in the Windows menu and click **Program** ➤ **RVS-COM Lite** ➤ **CommCenter**.

- Click **Start** and then **Inbox**.
You receive a list of the faxes received and sent.
- Click **Fax** ➤ **Fax Settings**.
Set the number of attempts you want to make to send a fax and the time interval between each attempt in the **Schedule** tab.
- Enter the number of attempts, e.g. **3**.
- Enter the waiting time between attempts, e.g. **5** minutes.
- Click **OK**.
- Close the **Inbox** and **RVS CommCenter**.

Create the desired fax and then send it.

- Select the Windows Start button and then click **Program** ➤ **RVS-COM Lite** ➤ **Create new fax**.
The window **RVS Fax: Recipients** appears.
- Type in the extension, e.g. **967310**, and the name of the recipient.
- Click **Next**.
- Enter a reference and select the cover sheet **Normal**.
- Click **Next**.
- Type in a short message, e.g. **Test Fax**.
- Click **Next**.
- If you want, you can attach a file for sending with the fax.
- Click **Next** and finally **Send** to send your fax.
The RVS Mail Spooler appears and informs you about the status of the fax being sent.
If you have sent a fax to yourself, you should receive it right away (cf. [chapter 3.9.4, page 80](#)). This is the best way to check your fax application is working properly.



You can send a fax from any program (e.g. Word).

- Write your fax message (e.g. in Word).
- Print the document by using the RVS FAX printer driver from RVS-COM Lite. This is done in the **File** menu by clicking **Print** and setting the printer driver to **RVS Fax**.
- Confirm the print job.

The window **RVS Fax: Recipients** you used a short time ago appears.

3.9.4 Receiving a Fax



As the fax solution with **X1000** and RVS-COM Lite is a softfax solution, the fax software must always be started if you want to receive faxes. RVS-COM Lite is created automatically in the Windows task bar during installation of RVS-COM Lite. The application is always ready to receive as long as you do not terminate RVS-COM Lite.

All incoming and outgoing faxes (including mailing errors) are displayed in the RVS-COM inbox, as are voice messages you receive over your RVS-COM answerphone.

- Select the Windows Start button and then click **Program** ➤ **RVS-COM Lite** ➤ **Inbox**.

All faxes and voice messages received are listed in the inbox.

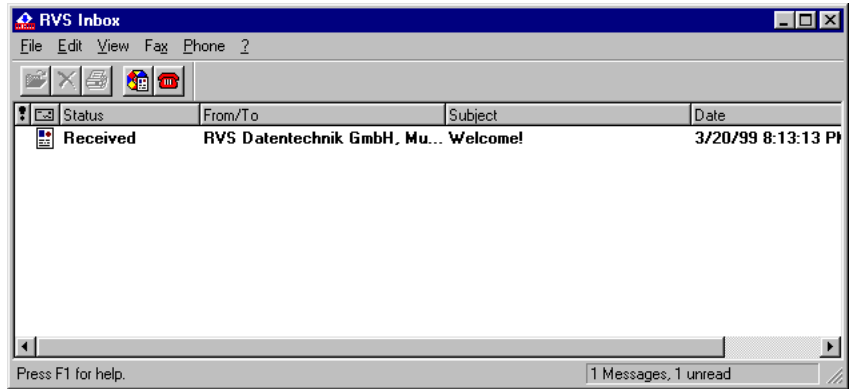


Figure 3-19: RVS inbox

- Double-click the fax entry to open your received fax messages (including the test messages created by RVS-COM). The RVS Fax Viewer opens. If you have sent yourself a fax, you should find it in the inbox.

4 Overview



To help you understand some of **X1000**'s functions and connections, we will now explain some of the basic elements concerning **X1000** and networking technology in general.

If you asked yourself some of the questions listed below in the course of the configuration in [chapter 3, page 31](#), you should read this chapter thoroughly. It will contribute to your understanding of the chapters to come and also help you to understand some of the connections in the last chapter.

- What is ISDN?
- What is compression?
- What are services, what is the user?
- How does routing work? What are routes and default routes?
- What is a DHCP server?
- How does name resolution work?
- How do filters function, what is NetBIOS?
- What are MIB and SNMP?



In case you want even more information than is described here, you should refer to our **Software Reference**. There you will find all the relevant technical connections described in detail.

4.1 The Basics of ISDN

What is ISDN? ISDN means Integrated Services Digital Network and describes a telecommunications service that is supported worldwide.

In contrast to the previous analog transmission of data, ISDN permits – as the name explains – the digital transmission of data. Data is forwarded over the existing lines as before, but digitally and not in the form of continuously varying analog signals. Data that you send digitally from your PC (e.g. e-mail) does not first have to be converted to analog tones as in a modem.

The **PPP** protocol (Point-to-Point Protocol) is used to transmit data over ISDN.

Every ISDN Basic Rate Interface (S₀ connection) consists of three channels:

- 2 B-channels
- 1 D-channel

Channel bundling of B-channels

Data transmission takes place over the B-channels (voice, text, data). Each B-channel has a data transmission rate of 64 kbps. Since you have two B-channels, you can, as you probably know, make telephone calls simultaneously from two different telephones. **X1000** can also use both B-channels simultaneously to exchange data with two different far end terminals. You can even “combine” both B-channels to transmit data over both channels to a single far end terminal. You must naturally pay for the use of both channels, but your data transmission takes only half the time. You can do this with **X1000** by using the channel bundling function. You can configure channel bundling in Expert Mode of the **Configuration Wizard** or with the Setup Tool (cf. [chapter 7.2.2, page 212](#)).

D-channel

The D-channel is used for connection setup and transfers control information at a data transmission rate of 16 kbps. Such control information is used, for example, for identifying the caller (Calling Party Number) and the called party (Called Party Number) from their extensions. You can configure your router, for example, so that it only accepts calls from partners whose extension reported over the D-channel is the same as the extension you have defined for the partner. This security mechanism is known as Calling Line Identification – abbreviated to CLID. Other authentication mechanisms check the user name and password of the far end terminal.

CLID can only be set in Expert Mode of the **Configuration Wizard** or in the Setup Tool.

The advantage of CLID is that authentication takes place early over the D-channel and thus provides increased security.

Charging information and short hold

Many ISDN connections provide charging information. You usually receive this information at the end of a call, although some ISDN connections even offer it during a call (AOCD: advice of charge during the call; you often have to request this function separately). **X1000** can evaluate this information to save your costs.

X1000 is normally configured (in Quick Mode) so that the connection is ended after a certain time (default time 20 seconds) if no more data is exchanged. After this fixed time in which there is no further data transfer, **X1000** cuts the connection – even if a new charging unit has just begun (static short hold).

If you now know for sure that you receive charging pulses during a connection, you can optimize the automatic disconnection of calls by making full use of charging units that have already begun. Provided **X1000** receives regular charging pulses from the ISDN, you can tell your router not to disconnect until shortly before the start of the next charging pulse (dynamic short hold). The time range is not calculated here in seconds, but in the form of a percentage value based on a charging unit (e.g. the connection should be cut after 80% of the charging unit is used up). Dynamic short hold can only be set in Expert Mode of the **Configuration Wizard** or in the Setup Tool (cf. [chapter 6.2.1, page 158](#)).

If you want to use dynamic short hold in addition to static short hold, static short hold should always be set longer than a charging unit, otherwise dynamic short hold has no effect.

Extensions MSN

Normally, you receive three extension numbers with an ISDN Basic Rate Interface (in Germany), the so-called MSNs (Multiple Subscriber Number). The MSN is a complete telephone number without a prefix. If three extensions are not enough, you can usually request more MSNs from your telephone provider.

You have already entered your extensions in Quick Mode of the Wizard. We have already stated that it is sufficient to enter only the digits that differ between the extensions (i.e. usually the last two digits). **X1000** normally begins checking the extensions from the back (right to left mode). As soon as the configured

number matches the incoming number, the call can be clearly assigned to a service. It is therefore not necessary to enter the complete MSNs every time.

Normally, an exchange uses a main number and several extension numbers. In this case, you should obtain information about any special characteristics of your connection. It could be the case that extensions (S₀ bus) are registered differently in different exchanges. Since you must always enter the extensions to which **X1000** (or also RVS-COM Lite) should react, you should know these registered extensions. If you do not know how your exchange forwards the extensions, you can find out using **X1000** (see [chapter 6.1.4, page 138](#)).

4.2 Speeding Things up Even More...

Compression processes help you to achieve a higher throughput rate in the same amount of time. When using compression processes, you must always ensure that the opposite terminal also supports the same processes. Otherwise, no connection can be made. No compression was activated in Quick Mode of the Wizard. To do so, you need to use Expert Mode or the Setup Tool (cf. [chapter 7.2.9, page 245](#)).

X1000 supports:

- Van Jacobson Header Compression (VJHC):
Compression of the head of an IP packet
- STAC Data Compression
Compression of the total IP packet

It is possible that the ADSL connections of other Internet Service Providers may differ from the T-DSL connection of Deutsche Telekom AG. You should obtain information about your connection from your provider.

4.3 Services and Users

Handling a call All routers use an internal algorithm to react to incoming calls from the ISDN. **X1000** can distribute incoming calls to the following services:

- PPP (routing)
- ISDN Login
- CAPI

What do these services do? PPP is **X1000**'s general routing service. This enables incoming data calls from WAN partners via a dialup connection to your LAN. You can therefore allow partners outside your local network to access PCs in your LAN.

The ISDN Login service allows incoming data and voice calls to access **X1000**'s SNMP shell. This is how **X1000** can be remotely configured and administrated, for example.

The CAPI service allows incoming data and voice calls a connection to communications applications on hosts in the LAN that access **X1000**'s Remote CAPI interface. This enables hosts connected to **X1000** to receive faxes, for example.

CAPI and Remote CAPI Most communications programs use the standard CAPI interface. This permits typical services such as answering service, fax (conventional and digital fax), file transfer and Eurofile transfer over ISDN. On its own, the CAPI interface allows only one PC to use the services over the ISDN connection. With the support of BinTec's own Remote CAPI, it is possible for all users in the network to use these services, provided all users have installed the required application software. All users share a single ISDN connection.

What have you configured? In Quick Mode of the Wizard, you have activated the services PPP (Routing) and CAPI. You can only activate ISDN Login in Expert Mode or in the Setup Tool. The Wizard normally allocates numbers to the services as follows (the assignment can only be changed in Expert Mode):

Extension	Data services	Voice services
1 (e.g. 10)	PPP (routing)	CAPI
2 (e.g. 11)	CAPI	CAPI
3 (e.g. 12)	CAPI	CAPI

Table 4-1: Standard allocation of numbers to services

Theoretically, a WAN partner could now call you at the number **10** to access data from your network – as long as you have specified him as a WAN partner.

Under the numbers **11** and **12**, you can set up data and voice services in RVS-COM Lite.

In our example configuration (cf. [figure 3-16, page 75](#)), we used the number **10** as a fax number and the number **11** for an answering service. As you have certainly noticed, the number **10** has been assigned twice: for PPP and CAPI.

Voice or data? Since on call acceptance, a distinction is made between data and voice calls as well as the extension, **X1000** can handle this double assignment of services without problems. **X1000** realizes that an incoming fax for the number **10** must be voice data (tones) and forwards the information to the CAPI service. On the other hand, if a WAN partner dials into your network, it must be digital information (data) and **X1000** forwards the data to the PPP service.

Data is:

- Digital data exchange (PPP routing)
- G4 fax (digital fax)

Voice is:

- Voice (telephone)
- G3 fax (conventional fax)
- Modem

Who is faster? We also presumed that you can be reached at the number **11** over a telephone connected to the same S_0 bus as **X1000**. All devices connected to the same S_0 bus and reachable under the same extension also respond to calls. This means

if an incoming call is received for the number **11**, your telephone rings, but RVS-COM Lite also thinks it has been called. As you have set RVS-COM Lite for the number of ringing tones before call acceptance, RVS-COM Lite waits for the time being. If you lift the receiver first, you are quicker and get the call. If you do not get to your phone before the number of ringing tones for RVS-COM Lite is reached, RVS-COM Lite is quicker and accepts the call.

Several users We have not yet assigned one extension: **12**. If you have a network with two PCs in the LAN, you could theoretically assign each of these two PCs its own fax number. In RVS CommCenter of PC 1, you would leave the number **11** as extension, in RVS CommCenter of PC 2, you would enter the number **12** as the extension for fax (cf. [figure 4-1, page 90](#)).

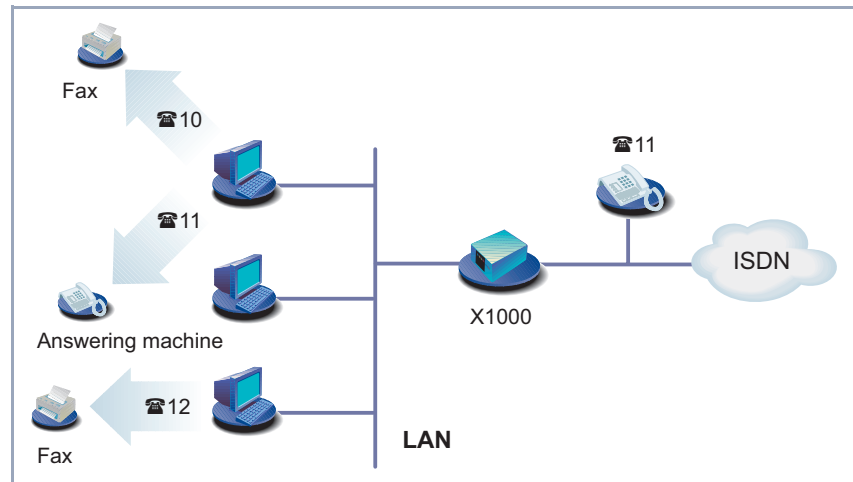


Figure 4-1: Scenario: 2 PCs, 2 fax numbers and 1 telephone

So far, so good. But what if one of the two users of PC 1 or PC 2 changes the extension! Both RVS CommCenters would, for example, react to an incoming call under the number **11**. Whoever is first off the mark gets the fax...

This is a bit of a nuisance, but not necessarily a security problem. Perhaps you have data that nobody else should see?

More security If you want to make sure from the outset that certain data/voice calls do not arrive at one of the two RVS CommCenters of RVS-COM Lite, you can protect ac-

cess by using a user name and password. The CAPI user concept can help you here:

Default user account You have configured the so-called default user account in Quick Mode. This is an easy way to configure. All users in the network can use the communications applications via the Remote CAPI interface. A default user without a password is entered in the CAPI configuration program and on the router. All users in the network have equal rights.

Several user accounts Every user who should be allowed certain communications applications receives his own user name and password. The settings for name and password must be made on the router (e.g. with the Wizard in Expert Mode or the Setup Tool, see [chapter 7.1.2, page 204](#)) and on the respective PC (Remote CAPI configuration). You also allocate a separate extension to each user on the router (e.g. fax number). Only the communications application of the PC on which the corresponding user is also entered in the CAPI configuration reacts to this extension.

4.4 X1000 as DHCP Server

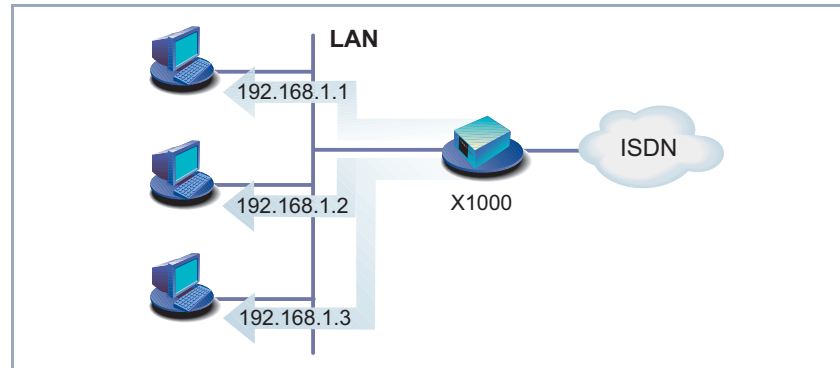


Figure 4-2: **X1000** as DHCP server

What do we need IP addresses for?

Every PC in your LAN requires its own address, just as **X1000** does. Otherwise the devices could not communicate with each other. When you send a letter by "snail mail", you also have to write the receiver's and your own address. If you don't, the letter can neither arrive at its destination nor be returned to sender.

IP addresses are used for such purposes in a TCP/IP network. In other networks, such as IPX or X.25 networks, the principle is the same. You can find out more about IP addresses in our **Software Reference**.

How do I know who I am?

You can permanently configure these IP addresses on your PC. The disadvantage: If you reconfigure or change your network configuration, you must tell each PC its IP address individually. This can mean a lot of work if you have several PCs in your network.

Having a DHCP server (DHCP = Dynamic Host Configuration Protocol) reduces your effort. The DHCP server relieves you of almost all the work. A DHCP server allocates IP addresses to all the PCs on the LAN automatically. The PCs are then DHCP clients. All you have to do is to define a pool of IP addresses that the DHCP server may allocate to computers on the network. In addition, you must tell the PCs that they should request their IP address from the server.



X1000 cannot be configured as a DHCP client. It is possible, however, to assign **X1000** an IP address over a BootP server (cf. [chapter 5.1.2, page 109](#)). Moreover, a network cannot contain several DHCP servers with the same address pools.

X1000 as DHCP server You can use **X1000** as a DHCP server if you do not have another DHCP server (cf. [chapter 6.1.5, page 149](#)). It assigns IP addresses to all PCs in your own network. Perhaps you have already configured **X1000** as a DHCP server in Quick Mode with the Wizard. If you accepted the values suggested, your PCs will receive IP addresses from **192.168.1.1** to **192.168.1.8**.

When are IP addresses allocated? Every new PC that logs in to the network – after booting, for example – sends out an address request and receives its IP address in reply. The PC usually retains this address for a specified period of time (you can set the length of time in the Setup Tool). The address is then reassigned. You can also explicitly tell your PC to request an IP address. The Wizard has done this for you in Quick Mode, if you have configured **X1000** as a DHCP server.

If you are running Windows 95 or Windows 98, call up the program WINIPCFG to check or reassign IP addresses. If you are running Windows NT or Windows 2000, use the program IPCONFIG.

Windows 95/98 **Calling up WINIPCFG**

- 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.
- To reassign an IP address, click **Renew**.

Windows NT **Calling up IPCONFIG**

- 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.
- Type in `ipconfig/renew` to reassign an IP address.
- Type in `ipconfig/release` to release an IP address.

Windows 2000 Calling up IPCONFIG

- Select the Windows Start menu and click **Program** ➤ **Accessories** ➤ **Command Prompt**.
- Type in `ipconfig` or `ipconfig/all` to request the IP address of your PC and other network information.
- Type in `ipconfig/renew` to reassign an IP address.
- Type in `ipconfig/release` to release an IP address.

4.5 How Does Name Resolution Work?

You have now heard quite a bit about why you need an IP address. But what if you want to set up a connection to the **BossPC** or view the Internet pages at **www.bintec.de**? **BossPC** and **www.bintec.de** are clearly not IP addresses, but names. As computers only understand IP addresses and not names, it is necessary for the names to be translated (resolved) into their corresponding IP addresses.

Name resolution The following options are available for name resolution:

- A DNS (in the LAN, at the ISP or in a partner's network)
- **X1000** as a DNS proxy server
 - **X1000**'s IP address is entered as a DNS on the PC.
 - **X1000** is configured as a DHCP server, your PCs are configured as DHCP clients and automatically receive their IP address from **X1000**, which is then used for DNS requests.
- WINS
- HOSTS and LMHOSTS file

DNS (Domain Name Server) The **➤➤ DNS** service translates the host names or computer names into their IP address equivalents. A DNS contains tables with lists of computer/host names and their corresponding IP addresses, which can be made known.

DNS are structured hierarchically in tree form. As soon as the primary DNS receives a request, it tries to resolve the name. If it cannot resolve the name, it refers the request to the next higher DNS.

X1000 as DNS proxy server If you use **X1000** as a DNS proxy (usual case), your router forwards all DNS requests to DNS it knows (usually a DNS at your ISP).

WINS A service called WINS is available in Windows networks. With WINS you can only resolve computer names or NetBIOS names, but not host names. NetBIOS is used as transport protocol analogously to TCP/IP. Computer and host names are mostly identical in Windows networks.

HOSTS and LMHOSTS file You may have already met the LMHOSTS file in the previous chapter. In the LMHOSTS file, you configure a table containing computer names and corre-

sponding IP addresses. The HOSTS file is similarly structured, but instead of computer names, translates host names into IP addresses.

How does name resolution function in practice?

Internet access If you have configured Internet access with the Wizard and you do not have your own DNS, **X1000** normally obtains the IP address of a Domain Name Server automatically from the Internet Service Provider. **X1000** is known as the DNS proxy on the PCs in the LAN. When a request is made for name resolution (e.g. for *www.bintec.de*), the PC asks the router, and the router in turn refers to the ISP's DNS. The address can then be resolved.

So far, so good. But what if you want to configure a corporate network connection as well?

Internet access and corporate network connection If, in addition to an Internet connection, you have configured a corporate network connection, entered **X1000** as a DNS proxy server, and the DNS settings of your **X1000** lead to the Internet provider (default setting), all requests for name resolution would be sent to your provider. If you now want to reach a PC in your partner's network (*BossPC*), **X1000** establishes a connection to the provider and asks for the IP address of *BossPC*. Unlike addresses such as *www.bintec.de*, computer names are not known on the Internet. They are used only within a corporate network (domain, work group). This means the Domain Name Server at the provider's cannot normally resolve the name. This connection would be a waste of time, you still cannot reach *BossPC*.

To prevent such unintentional and useless connections being established, you must prevent requests for computer names in your partner's network. This task is carried out for you by the simple NetBIOS filter (see [chapter 4.7, page 101](#)).

This does not, however, solve your problem. You still want to know the IP address of the name *BossPC*.

One possible solution would be: You configure your own Domain Name Server in which all assignments you want to reach (PCs of partner network and their IP addresses) can be found. As it is not always worth the trouble setting up your own server in a small network if you only have one or two such assignments to make, there is a second alternative:

You save the assignment of IP address to name on your PC. However, this must be done on all PCs that require this information. You can use the LMHOSTS file for such purposes.

How to add an entry to the LMHOSTS file has already been explained in [chapter 3.7.2, page 68](#).

To make sure our solution functions, you must observe a few additional points.

- Domain and work group names must be the same in your network and your partner's network.
- You must be known as a user on the partner network.
- You must not have set any extensive NetBIOS filters with the Wizard (see [chapter 4.7, page 101](#)), otherwise certain Windows functions such as a network drive connection cannot be used.



The subject of "Connection of Windows Networks" is very complex and extensive. A range of factors determine the success of such a project. As a more detailed treatment of this subject would exceed the scope of this manual, we can only refer you at this point to related technical literature: e.g. "Windows NT 4.0 Connectivity Guide" by Richard Grace (ISBN 0-7645.3160-3) or the Microsoft Knowledge Base on the World Wide Web at www.support.microsoft.com/directory.

4.6 What Are Routes and Default Routes?

Routing To be able to send IP packets to a partner network or an Internet provider, **X1000** must know which packets should be forwarded and to where.

This is why we define the routes to these destinations. The routes lead to a certain network with a defined **>>> network address** and **>>> netmask**. You must define the route to every network

you want to access. You could define, for example, the route to your WAN partner (e.g. head office). All packets whose IP addresses match the netmask and network address are then sent to this partner network.

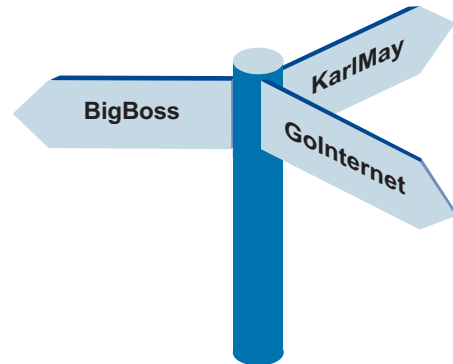
But where do all the other IP packets go?

Default route By means of a so-called default route, you can decide that all packets whose destination is unknown to **X1000** be sent to a certain network. Generally, the route to the Internet provider is used as the default route, because most unknown packets are bound for the Internet anyway (e.g. www.bintec.de). The Wizard automatically enters the route to your provider as the default route, as long as you have configured an Internet access. If you have only configured a partner network and no Internet access, the Wizard simply uses the route to your partner's network as a default route.



If you have not configured Internet access, but your head office has an Internet Service Provider, you can access the Internet via your head office.

Due to the fact that you have configured your default route to your head office, all unknown packets are sent there and your partner's network then routes all unknown IP packets to an Internet provider, you can access the Internet via your partner's network by arrangement with your WAN partner.



Several routes for a WAN partner Your corporate network can consist of several LANs with different network addresses and netmasks (subnets). In this case, you must specify a separate route to each subnet you want to reach at head office (cf. [figure 4-3, page 99](#)).

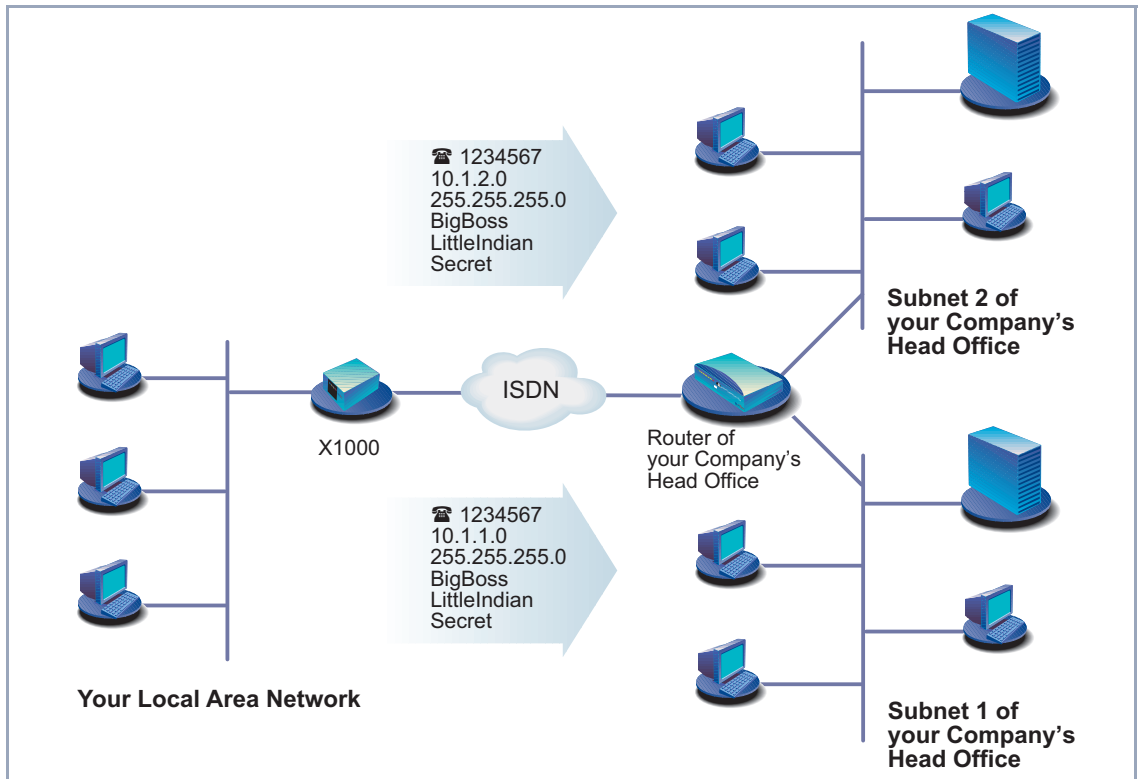


Figure 4-3: Scenario: WAN partner with two subnets

Routes, name resolution and gateway Not only does **X1000** use a default route, your PCs also have one: the gateway. Your PC sends all packets to this gateway whose destination is not within your own network. **X1000** acts as a gateway. As soon as your router receives such a packet, it forwards it in turn over one of its known routes (e.g. to the Internet provider or to another partner's network).

Assuming **X1000**'s default route leads to an Internet provider, your PCs are DHCP clients and are assigned their IP addresses by **X1000**. In such a case, the PCs also get their IP addresses from **X1000** acting as a DNS proxy server and gateway. (The example also applies if your PCs are not DHCP clients, but

are configured in such a way that **X1000**'s IP address is entered as the DNS and gateway.)

As soon as you enter ***www.bintec.de***, for example, in the browser, the PC sends a DNS request to **X1000**, as **X1000** is known as a DNS proxy server. **X1000** itself as DNS proxy server sends the packet with the DNS request to the Internet provider, where the name ***www.bintec.de*** can be resolved; the DNS request is successful and the PC receives the IP address for the name ***www.bintec.de*** as answer. The packet can now be sent on its actual journey to ***www.bintec.de***. As **X1000** is entered as a gateway and the packet has an IP address outside its own network, the packet is sent out via the **X1000** gateway. As no separate route is entered for the IP address to ***www.bintec.de***, **X1000** uses the default route.

4.7 Filters and NetBIOS

You have just learned a lot about name resolution and routes. This is all very practical, but...

Why filters? Every Windows network uses computer names. If, for example, your PC is called Winnetou and another PC in the network OldShatterhand, these computer names are not known on the Internet, as they are only used within a corporate network (which differs from addresses such as www.bintec.de). These computer names are resolved in all Windows networks via the NetBIOS service. NetBIOS in turn tries to have these computer names resolved by your Internet provider. As the provider cannot resolve the WINS names, **X1000** would constantly establish an unnecessary connection to your provider (the requests are approximately every 12 to 15 minutes and thus quite frequent!). After all, the names are only known in your network (work group, domain).

This is where filters come in.

Simple NetBIOS filter If you have activated the simple NetBIOS filter with the Wizard, all IP packets that are sent to **X1000** to have their names resolved are discarded. The **Configuration Wizard** always configures a simple filter in Quick Mode for a LAN-LAN connection.

Extensive NetBIOS filters The **Configuration Wizard** performs extensive filtering in Quick Mode automatically if Internet access is configured but no corporate network connection. In Expert Mode or with the Setup Tool, you can select between no filtering, simple filtering or extensive filtering. With extensive filters, all NetBIOS data traffic (NetBIOS broadcasts) is filtered – that means not just requests for name resolution. Effects: All NetBIOS services such as shared use of drives and printers cannot be used.

CAPI filter You can also configure a CAPI filter in Expert Mode with the Wizard. Let's assume that instead of **X1000**'s IP address, you have unintentionally entered an incorrect IP address in the CAPI configuration. Your PC would always send CAPI requests to the wrong address. As the wrong IP address could lie outside your network, **X1000** would try to forward the packet in question to your Internet provider. Yet another unnecessary connection. The CAPI filter causes CAPI requests to be discarded if they do not remain within the LAN of origin.



Filter mechanisms not only enable you to avoid unwanted connections. The primary function of filters is to protect your own network against external accesses (cf. [chapter 8.2.8, page 317](#)).

4.8 MIB and SNMP

What is SNMP? SNMP (Simple Network Management Protocol) is a protocol that belongs to the TCP/IP protocol suite. SNMP is used to transport management information of network components (e.g. routers, printers, PCs) in a network. It is used to monitor and administrate the components in a network. Monitoring takes place from a central location via an SNMP Manager. This SNMP Manager is a program that can request data from the network components over SNMP. An administrator who operates this SNMP Manager can monitor all devices in his network from one central location. As a protocol, SNMP defines the rules with which the management program communicates with the clients (e.g. **X1000**). There is one such SNMP manager on your BinTec Companion CD, the **Configuration Manager** (for Windows operating systems). Instead of the **Configuration Manager**, you can also use any SNMP Manager to manage your network, e.g. HP OpenView. Instead of a graphically oriented program, you can even work directly on the level of command lines (SNMP shell).

What is MIB? We have just explained that management information is exchanged in a network over SNMP. But what exactly is this management information? The name MIB is an acronym for Management Information Base and is thus directly related to this management information.

Objects (Information Base) that can be requested, changed or created over SNMP (Management) are stored in an MIB. The objects themselves are information containers in which information about the states and values of the object is stored. An object you have changed while configuring the router with the Wizard could be, for example, an object containing your access authorization to **X1000**. Originally, the value *bintec* was defined as password, now your own entry is stored there as password.

Each of these objects is unique and has a name, in the example of access authorization: **bintecsec**. An object is also referred to as a table. Each table has, in turn, a number of variables which define certain properties, e.g. the variable **biboAdmAdminCommunity** in which the value of your password is now stored.

5 Connecting X1000

This chapter includes explanations about the different access and configuration methods.

You will learn the following:

- How to access **X1000**
- How to log in
- What methods of configuration are available
- How the **▶▶ Setup Tool** is constructed

5.1 Connection Methods

Before you can configure your >>> **router**, you must connect it. There are three ways to do this:

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

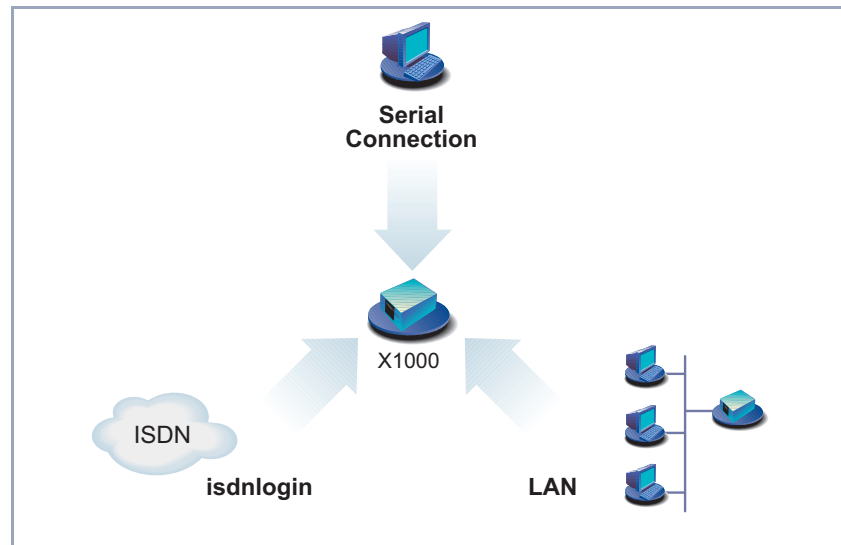


Figure 5-1: Possible connections to **X1000**

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

If you use the >>> **Configuration Manager (BRICKware for Windows)** under Windows, you connect to **X1000** over the LAN. If you use the **Configuration Wizard**, you connect to **X1000** over the serial interface.

5.1.1 Connecting Over the Serial Interface

Initial configuration A serial interface connection is the most appropriate method if you are configuring your **X1000** for the first time. To connect **X1000** to your PC over the serial port, proceed as explained in [chapter 3.1, page 33](#).

Windows If you use a Windows PC, you need a terminal program for the serial connection, e.g. **HyperTerminal**.



Make sure that **HyperTerminal** is also installed on the PC during the Windows installation.

Note that **HyperTerminal** is not included in the standard installation of Windows 98 and Windows ME.

If you use **HyperTerminal** under Windows 2000 or Windows ME, it is possible that the cursor keys for navigation in the Setup Tool do not work. In this case, use the tabulator key or **Ctrl+P** for moving forwards and **Ctrl+N** for navigation backwards.

- To do**
- 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 **X1000**.
 - Continue with [chapter 5.2, page 111](#).



If the login prompt does not appear after pressing **Return** several times, the connection to **X1000** has not been set up successfully. Check the settings of COM1 or COM2:

- 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 **X1000** and then make 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 cannot use **HyperTerminal**. You will require 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.

5.1.2 Connecting Over a LAN



You can reach **X1000** from the LAN over the **telnet** service. Telnet is normally available on every PC. To be able to reach your router over the LAN, it should already have an **IP address** and **netmask**. If this is not the case and **X1000** has therefore not yet been configured, you have two options:

- If you are working with Windows, you can assign **X1000** an IP address before you start telnet. To do this, you will need the assistant, **DIME Tools**. If you have not yet installed **DIME Tools** with **BRICKware for Windows**, proceed as explained in [chapter 3.3, page 43](#).
- If you are not working with Windows, use an alternative connection method for initial configuration (over the serial interface or ISDN).

To do ➤ Connect **X1000** to your LAN as explained in [chapter 3.1, page 33](#).

Assigning IP addresses To assign your **X1000** an IP address (if necessary) with the **DIME Tools** program, 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. A **BootP** server window will appear after a short time if **X1000** is still unconfigured.
- Enter the name and IP address of your **X1000** in the window under **BRICK Parameter** (if you are unsure, refer to [chapter 3.2, page 36](#)).
- Click **OK**.
- Close **DIME Tools**.

Running telnet Now establish a connection to **X1000** with telnet:

- Windows**
- Click the Windows Start button and then **Run...**
 - Type `telnet <IP address of X1000>`.
 - Click **OK**.

A window with the login prompt appears. You are now in the SNMP shell of **X1000**. Continue with [chapter 5.2, page 111](#).

Unix ➤ Type `telnet <IP address of X1000>` into a terminal.
A window with the login prompt appears. You are now in the SNMP shell of **X1000**. Continue with [chapter 5.2, page 111](#).

Configuration Manager The ➤➤ **Configuration Manager** also connects to **X1000** over the LAN. Communication between the PC and **X1000** uses the SNMP protocol.

5.1.3 Connection Over ISDN

Remote configuration Access over ➤➤ **ISDN** with ➤➤ **ISDN Login** is particularly useful if **X1000** is situated at a different location and you want to configure or administrate it from a distance. This is also possible even if **X1000** has not been initially configured, i.e. is still in the ex works state. For this purpose, you must have another already configured BinTec router at your disposal (in LAN 1) and you must know the extension of your (new) router (in LAN 2). This makes it possible, for example, for the administrator at a head office to configure the router of an employee in a home office which is hundreds of kilometers away. The **X1000** in the home office merely has to be connected to the ISDN outlet and turned on.



Access over ISDN costs money. If **X1000**, router and PC are in the same LAN, it is cheaper to access **X1000** over the LAN or the serial interface.

➤ Connect **X1000** to the ISDN as explained in [chapter 3.1, page 33](#).

To reach **X1000** over ISDN login, proceed as follows:

➤ Log in on your BinTec router (in LAN 1) in the usual way.

➤ Enter `isdnlogin <extension of your X1000>` in the SNMP shell.

The login prompt will appear in the window. You are now in the SNMP shell of **X1000**. Continue with [chapter 5.2, page 111](#).

5.2 Logging In

Regardless of how you access **X1000**, the **SNMP shell** of **X1000** with the login prompt always appears first. (Exceptions to this rule are the **Configuration Wizard** and **Configuration Manager** under Windows.)

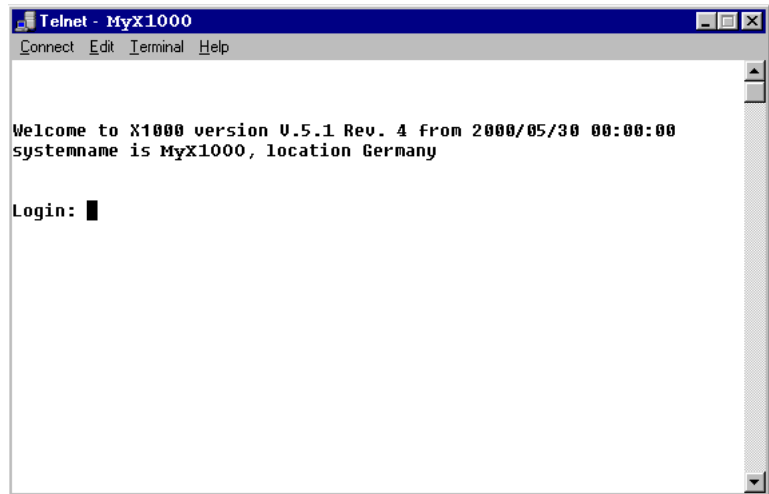


Figure 5-2: Login prompt

In order to log in, you need to know the user name and password. In its ex works state, **X1000** 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	Read system variables (changes are lost when X1000 is turned off).
read	public	Read system variables.
http	bintec	Call up HTTP status page of X1000 , read system variables, no login.

Table 5-1: 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 also only be changed if you log in with the user name `admin`. For security reasons, passwords are not normally shown on the Setup Tool screen in plain language, but only as asterisks. The user names appear in plain language. The security concept of **X1000** enables you to read all the other 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.

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. `X1000: >`. The login was successful.



Caution!

To prevent unauthorized access to **X1000**, you should change the passwords right away, in case you did not do this during the basic configuration with the **Configuration Wizard**.

- Change the passwords as described in [chapter 6.1.2, page 132](#).

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

5.3 Configuration options

Before you set to work with the configuration, you must select a method. For this reason, we would first like to give you an overview of the different configuration methods and an introduction to using the Setup Tool. This manual explains how to configure **X1000** by means of the Setup Tool.

5.3.1 Methods of Configuration

Methods of configuring **X1000**:

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

Configuration Wizard You have already learnt about configuration with the **Configuration Wizard** in [chapter 3.5, page 50](#). It is useful for quick, initial configuration of **X1000** and can be used if you have a Windows PC. This usually covers most standard configurations. If, however, you require further settings, you can use the other aforementioned options. You could first configure **X1000** with the **Configuration Wizard** and subsequently extend or change this initial configuration with one of the other tools. In many cases, the **Configuration Wizard** alone will be sufficient!

Setup Tool The Setup Tool is a menu-driven tool for the configuration and administration of **X1000**. Configuration with the Setup Tool is much easier and clearer than configuration with SNMP commands, although not all settings can be made with the Setup Tool. Besides the assistance of the **Configuration Wizard**, this manual only explains how to configure with the Setup Tool. The Setup Tool is independent of the operating system on your PC. If a configuration step is only possible in isolated cases with the help of an SNMP command, the procedure for this is also 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 provided by BinTec Communications AG as an SNMP manager for Windows PCs. You can use the **Configuration Manager** with its interface based on Microsoft Explorer to access all MIB tables and variables of **X1000** (see [chapter 4.8, page 103](#)). You can also use other SNMP managers, such as SNM, HP Open View or Transview, to access and modify the MIB tables and variables. As more detailed knowledge of the structure and interrelations of **X1000** 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**.

5.3.2 Operation and Menu Architecture of the Setup Tool

You can call up the Setup Tool once you have logged in to **X1000**:

➤ Type `setup` after the input prompt and press **Return**.

The main menu of the Setup Tool appears.

Main menu

X1000 Setup Tool		BinTec Communications AG MyX1000	
Licenses		System	
LAN:	CM-100BT, Fast Ethernet		
WAN:	CM-1BRI, ISDN S0		
WAN Partner			
IP	IPX	PPP	ISDN CAPI
Configuration Management			
Monitoring and Debugging			
Exit			
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter			



The appearance of the main menu of the Setup Tool differs according to whether or not the license data have already been entered. The illustration shows the main menu with the data already entered for a standard license.



To use the Setup Tool, you must log in with the user name `admin`! If you don't know the corresponding password, you cannot open the Setup Tool (see [chapter 5.2, page 111](#)).

The Setup Tool is easy to use, and you will soon find your way around. Nevertheless, you should first familiarize yourself with the facilities offered by the Setup Tool. By way of introduction, we would first like to point out a few things you should be aware of when using the **X1000** Setup Tool.

Menu layout Every Setup Tool menu consists of three parts:

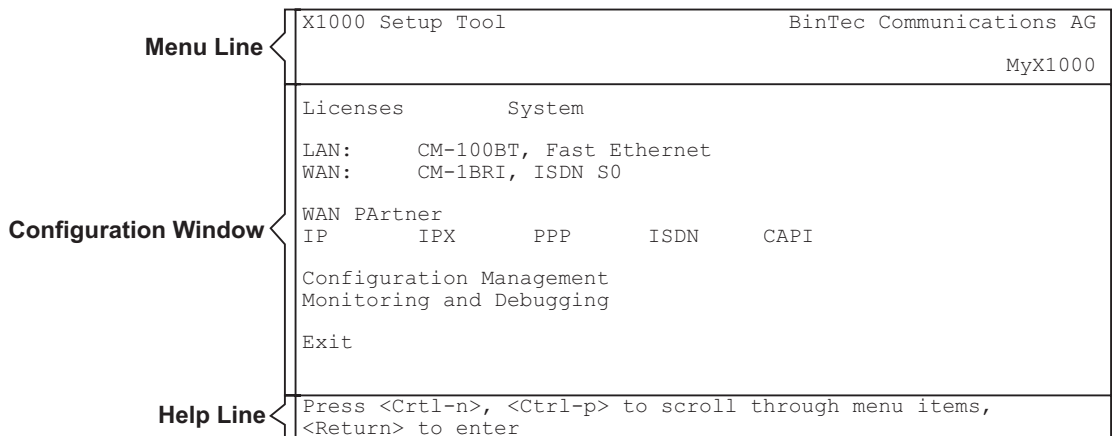


Figure 5-3: Setup Tool menu layout

The menu line contains a navigation aid to show you where you currently are in the Setup Tool menu system. The system name of **X1000** 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 displayed. The field in which the cursor is currently located is also marked.

The help line at the bottom of the window tells you how to move around or how to change entries in the menu currently being displayed.

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	To move forwards or backwards between menu fields (functions with VT 100 emulation when using a terminal program).
left or right	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 D. 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 without saving.

Table 5-2: Navigation in the Setup Tool

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**. The meaning of the respective commands is explained below:

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 pressed 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 5-3: Buttons in the Setup Tool

List search function Some Setup Tool menus contain lists of items, e.g. the **WAN PARTNER** menu, which lists all **➤➤ WAN partners** currently configured.

```

X1000 Setup Tool                               BinTec Communications AG
[WAN]: WAN Partners                             MyX1000

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 an 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 5-4: Search results

Changing the password

The procedure described below for changing the password applies to all **X1000** passwords: the access passwords for the user names `admin`, `read` and `write`, the HTTP password, the PPP password and the provider password.

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 **X1000** Setup Tool in a mode in which the passwords are displayed in plain language and can be changed once by editing, you must enter the command `setup -p`. This option only exists if you have logged in on **X1000** under the user name `admin`.

To change a password, proceed as follows:



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

- Select the password field and enter the new password.
The field changes to the change mode and the message `Change Password` appears in the help line.
- 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.
- Enter the password again and confirm with **Return**, **Tabulator** or a **Cursor key**.
If you have entered the repeat password correctly, 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.

Convention To ensure you always know which Setup Tool menu we are talking about in this manual or how you get there, we have devised the following convention (the starting point is always the main menu):

MENU ➤ **SUBMENU** ➤ **SUBMENU**

Examples:

- "Go to the submenu Routing from the menu IP" is represented as follows:
Go to **IP** ➤ **ROUTING**.
- "Go to the submenu Advanced Settings from the submenu WAN Numbers. To do this you must press ADD in the menu WAN Partner and submenu WAN Numbers." This is shown thus:
Go to **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** ➤ **ADD** ➤ **ADVANCED SETTINGS**.
- "Go to the submenu WAN Numbers of an entered WAN partner to change an existing entry. Mark the relevant WAN partner in the menu WAN Partner and press Return." This is shown thus:
Go to **WAN PARTNER** ➤ **EDIT** ➤ **WAN NUMBERS**.

Menu Architecture The menu architecture of the Setup Tool looks like this:

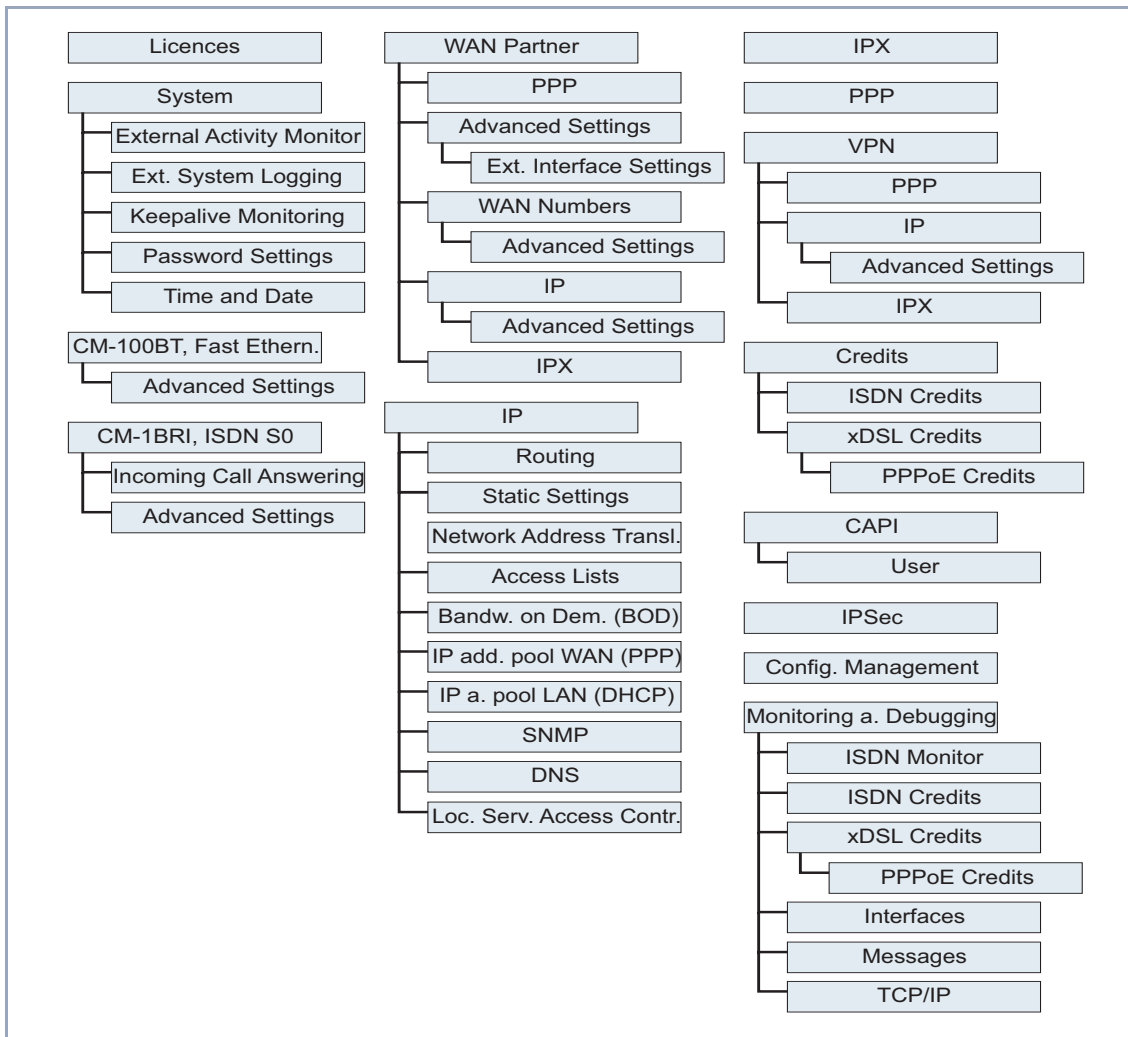


Figure 5-4: Setup Tool menu architecture

All menus of the Setup Tool available to **X1000** are illustrated in [figure 5-4, page 122](#). Not all functions are available on all routers (e.g. VPN). To use them, an extra license is necessary, which you can acquire from BinTec Communications AG. When you activate the necessary license, **X1000** detects this and dis-

plays the corresponding menus (for entering license, see [chapter 6.1.1, page 130](#)).

Summary To help you find your way around during configuration, the menus are briefly explained below. A more detailed description of the individual configuration steps necessary for the required settings is given in the following chapters.

Menu	Function
LICENSES	This menu is for entering the license information printed on the license card supplied with the equipment. This menu is also used for activating extra licenses.
SYSTEM	In this menu, you enter the basic system settings of X1000 , e.g. system name and passwords.
CM-100BT, FAST ETHER-NET	This menu is for configuring the LAN interface of X1000 . Here you enter data such as the IP address and netmask of X1000 .
CM-1BRI, ISDN S0	This menu is for configuring the WAN interface of X1000 . Here you enter data such as the type of ISDN connection to which X1000 is connected. The submenu WAN INTERFACE INCOMING CALL ANSWERING is for assigning the available ISDN extensions 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 X1000's IP routing table. Here you enter routes to your partners (e.g. default routes, network routes), which ensure that your X1000 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 X1000, 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 X1000 from establishing unintended connections to the ISDN.</p> <p>IP ► IP ADDRESS POOL WAN (PPP) is for setting up a pool of IP addresses that X1000 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 X1000 as a ►► DHCP server. As a DHCP server, X1000 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 ► DNS is for defining the procedure for name resolution in X1000.</p> <p>IP ► TOKEN AUTHENTICATION FIREWALL is for personal authentication of IP connection partners.</p> <p>IP ► LOCAL SERVICES ACCESS CONTROL is for controlling access to the local UDP and TCP services in X1000.</p>
IPX	<p>Here you make the entries for the IPX protocol. ►► IPX is used especially in Novell networks.</p>

Menu	Function
PPP	Includes generally valid ►► PPP settings, e.g. authentication protocol, that do not just refer to particular WAN partners. The router can use these settings to perform an authentication procedure for incoming calls 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).
VPN	Here the necessary settings for Virtual Private Networking (VPN) are made. This menu only appears if you have entered the relevant valid license. The license can be purchased as an option. You will find more detailed explanations and instructions on configuration in the Software Reference .
CREDITS	Here you administrate the Credits Based Accounting System of X1000 .
CAPI	Includes the settings for BinTec's ►► CAPI user concept. You can use this to assign user names and passwords to users of X1000 's CAPI applications. This makes sure that only authorized users can receive incoming calls and make outgoing calls via CAPI.
IPSEC	This menu is for making the necessary settings for Internet Protocol Security (IPSec). This menu only appears if you have entered the relevant valid license. The license can be purchased as an option. You will find more detailed explanations and instructions on configuration in the IPSec Reference Manual , which is supplied together with the license, or in the Software Reference .
CONFIGURATION MANAGEMENT	Here you can administrate X1000 's configuration files. You can save them either locally on X1000 or on your PC, for example.
MONITORING AND DEBUGGING	Contains submenus that enable you to locate problems in your network and monitor activities in X1000 .
EXIT	Quit the Setup Tool with Exit . You can save the configuration file to the flash memory with Exit ► Save as boot configuration and exit ; this file is loaded after X1000 is restarted. If you select Exit ► Exit without saving , all the changes will be lost the next time X1000 is started.

Table 5-5: Setup Tool menus

6 Basic Configuration with the Setup Tool

This chapter explains the basic configuration of **X1000** with the **Setup Tool**, which covers the same subjects as configuration with the **Configuration Wizard** as explained in [chapter 3.5, page 50](#). However, the Setup Tool is independent of the operating system and also enables you to make additional settings.

Basic configuration The basic configuration of **X1000** includes:

- The basic **router** settings
- The configuration of **WAN partner(s)**
 - for Internet access
 - for a LAN-LAN connection (e.g. corporate network connection)
- Saving the configuration file

The basic router settings are essential for the operation of **X1000**. Depending on your needs, you can configure Internet access and corporate network access right away or later.

Extending existing configuration If you do not carry out basic configuration, but want to modify your existing configuration, you will still find lots of useful tips in this chapter, for example:

- How to add additional **WAN partners**
- How to change passwords
- How to enter extra licenses
- How to organize Incoming Call Answering
- How to setup **X1000** as a **DHCP** server
- How to define a simple **NetBIOS** filter
- How to make routing entries

How to supplement and improve your configuration after finishing the basic configuration is explained in [chapter 7, page 201](#).

How to configure security mechanisms according to SAFERNET is explained in [chapter 8, page 289](#).



Use the Credits Based Accounting System (see [chapter 8.1.3, page 299](#)). This enables you to set a limit for connections to **X1000** to prevent unnecessary charges accumulating as a result of mistakes made during configuration.

6.1 Basic Router Settings

The configuration of the basic router settings concerns only your **X1000** and your local network. The relevant detail from [figure 6-4, page 157](#) is illustrated in [figure 6-1, page 129](#). There you will find examples of names, **IP addresses**, extensions, etc. If you are setting up a new Local Area Network (LAN) together with **X1000** 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.

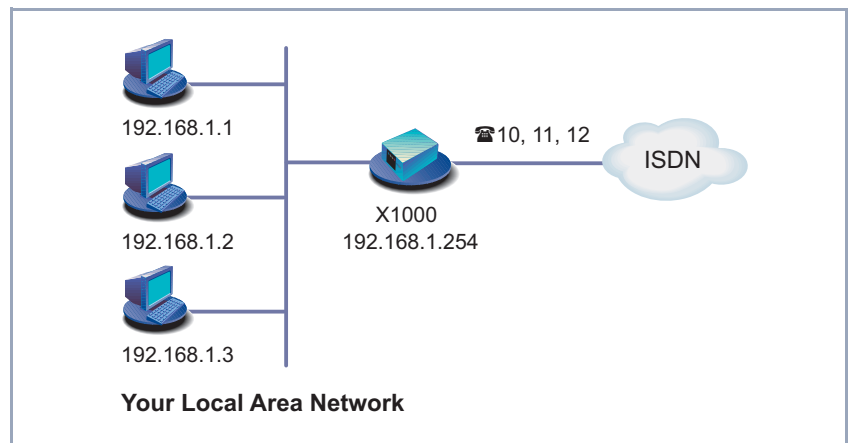


Figure 6-1: Basic router settings

The following steps are necessary:

- Entering licenses
- Entering system data (e.g. passwords)
- Configuring the LAN Interface
- Configuring the **WAN Interface**
- **X1000** as a DHCP **server** (optional)
- Setting **filters** (optional, explained in detail in [chapter 8.2.8, page 317](#))

Off we go!

6.1.1 Entering Licenses

License card After you have logged in to your **X1000** with the user name `admin` and called up the Setup Tool with `setup`, as described in [chapter 5.2, page 111](#), enter the license information. This information is printed on the license card supplied. Entering this information activates the functions of **X1000**.

➤ Go to **LICENSES**:

```

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

Available Licenses:

IP (builtin), STAC (valid), CAPI (valid), IPX (valid)

Serialnumber      Mask      Key      State
101546            5134     88PNUPZ  ok

ADD                DELETE                EXIT

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

```

Listed under **Available Licenses** are all subsystems available on **X1000** and their current state (*builtin* - always available, *valid* - activated).

The license entries are shown under (**Serialnumber, Mask, Key**).

If you have not yet entered any licenses, only **IP** is entered in the subsystem list, i.e. ➤➤ **IP** routing is available (*builtin*).

Subsystems The following subsystems can be activated on your **X1000**:

Subsystems	Meaning
IP	IP routing
TUNNEL	Virtual Private Networking VPN (only with extra license)
LEASED LINE	Leased line (only with extra license)
STAC	➤➤ STAC ➤➤ data compression
CAPI	➤➤ Remote CAPI interface, permits communications applications on your PC, e.g. sending and receiving faxes.
IPX	➤➤ IPX routing
IPSEC	Internet Protocol Security (only with extra licence)

Table 6-1: Subsystems

To do To enter your license, proceed as follows:

- Add a new entry with **ADD**.
Another menu window opens.
- Type in the **Serial Number**.
- Type in the **Mask**.
- Type in the **Key**.
- Press **SAVE**.

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 shown as the state, you have probably made a typing error.

- Try again.

6.1.2 Entering System Data

System name, ... Next you should enter the basic system data for identification of your **X1000**.

➤ Go to **SYSTEM**:

X1000 Setup Tool	BinTec Communications AG
[SYSTEM]: Change System Parameters	MyX1000
System Name	MyX1000
Local PPP ID (default)	LittleIndian
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 X1000 , is also used as PPP host name. Appears as input prompt when logging in to X1000 . 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 X1000 , if PPP authentication (e.g. PAP or CHAP) is carried out that is not specific to a partner (see chapter 7.1.3, page 208).
Location	Indicates where X1000 is located (optional).
Contact	States the contact person responsible (optional). If the person is to be reached from X1000 's HTTP status page, a valid e-mail address must be entered here.

Table 6-2: **SYSTEM**

Passwords Enter the passwords for **X1000** in the submenu **SYSTEM ► PASSWORD SETTINGS**:

Field	Meaning
admin Login Password	Password for user name <code>admin</code> .
read Login Password	Password for user name <code>read</code> .
write Login Password	Password for user name <code>write</code> .
HTTP Server Password	Password for the HTTP status page of X1000 .

Table 6-3: **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 "[Changing the password](#)", page 120.

➤ Change the passwords to prevent unauthorized access to **X1000**.

The permission rights of the possible user names and passwords can be found in [chapter 5.2](#), page 111.

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

- Enter **System Name** of **X1000**, e.g. *MyX1000*.
- 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**.
- Enter **read Login Password**.
- Enter **write Login Password**.
- Enter **HTTP Server Password**.
- Press **SAVE**.
- Press **SAVE**.

You have returned to the main menu and the entries have been saved.

Advanced configuration

The menu **SYSTEM** ➤ **EXTERNAL ACTIVITY MONITOR** contains the settings necessary for monitoring **X1000** with the Windows **Activity Monitor** (see [chapter 8.1.5](#), page 305 and **BRICKware** for Windows).

The menu **SYSTEM** ➤ **EXTERNAL SYSTEM LOGGING** contains the settings for syslog messages (see [chapter 8.1.1](#), page 290).

The menu **SYSTEM** ➤ **KEEPLIVE MONITORING** contains the settings for the keepalive monitoring function (see [chapter 7.2.11](#), page 249).

The menu **SYSTEM** ► **TIME AND DATE** contains the settings for manually entering the time and date in **X1000** (see [chapter 7.3.1, page 255](#)).

6.1.3 Configuring the LAN Interface

- IP address,
- netmask,
- encapsulation

The next step is to configure **X1000**'s LAN interface. The LAN interface is the physical interface to the local network. In the following menu, 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.

If your **X1000** 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:

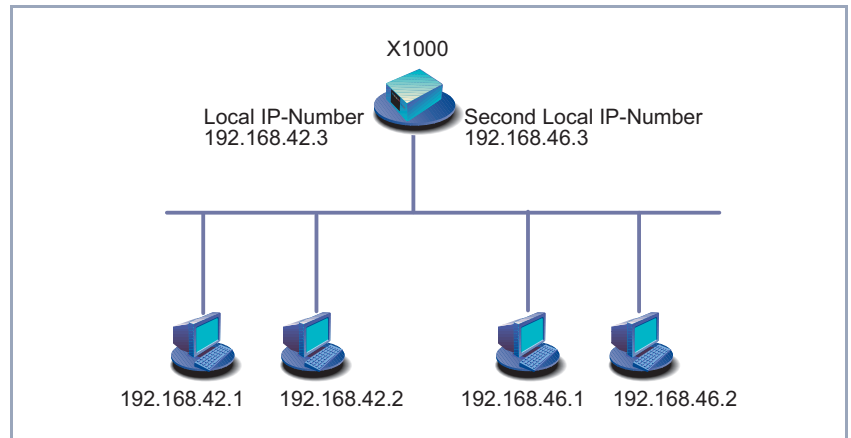


Figure 6-2: **X1000** with two different local IP addresses

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, **X1000** 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.



You may have already assigned your **X1000** its IP address and netmask before the basic configuration, e.g. with the help of the **▶▶ BootP** server of **▶▶ DIME Tools**. Even if you have, you should still check the entries in the following menu.

▶ Go to **CM-100BT, FAST ETHERNET**.

X1000 Setup Tool	BinTec Communications AG
[LAN]: Configure Ethernet Interface	MyX1000
IP Configuration 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	
IPX Configuration Local IPX Netnumber 0 Encapsulation none	
Bridging disabled	
Advanced Settings>	
SAVE	CANCEL
Enter IP address (a.b.c.d or resolvable host name)	

Entries for IP and **▶▶ IPX** configuration are possible in the menu. This chapter explains only the configuration of the **▶▶ IP**. Retain the preset values under **IPX Configuration**.

If you wish to use the IPX **▶▶ protocol**, you will find an explanation of how to configure the LAN interface for IPX in [chapter 7.4, page 281](#).

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

Field	Meaning
Local IP Number	IP address of X1000 in the LAN.
Local Netmask	Netmask of the network where X1000 is located.
Second Local IP Number	Second IP address of X1000 in the LAN.
Second Local Netmask	Netmask of the subnetwork in which X1000 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 keep the default value <i>Ethernet II</i>. The LAN interface is called <i>en1</i> for <i>Ethernet II</i> and <i>en1-snap</i> 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 Mbps Half Duplex</i> ■ <i>10 Mbps Full Duplex</i> ■ <i>100 Mbps Half Duplex</i> ■ <i>100 Mbps Full Duplex</i>

Table 6-4: **CM-BNC/TP, ETHERNET**

To do Proceed as follows to configure **X1000**'s LAN interface:

- Enter **Local IP Number** of **X1000**, 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**.
- Press **SAVE**.

You have returned to the main menu and the entries have been saved.

6.1.4 Configuring the WAN Interface

Interface to ISDN The next step involves configuring your **X1000**'s ➤➤ **WAN interface**. The WAN interface is the physical interface to the ➤➤ **ISDN**. You can use it for dialup connections and with an extra license for leased lines as well. Its configuration for dialup connections involves two steps:

- 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 your ➤➤ **router** how it should react to incoming calls from the WAN.

Autoconfiguration, First enter the settings for your ISDN connection.

ISDN Switch Type,

➤ Go to **CM-1BRI, ISDN S0**:

X1000 Setup Tool	BinTec Communications AG
[WAN]: WAN Interface	MyX1000
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	

The menu contains the following fields:

Field	Meaning
Result of Autoconfiguration	<p>Status of ISDN autoconfiguration. Automatic ►► D-channel protocol detection runs until a setting is found or until the ISDN protocol is entered manually under ISDN Switch Type.</p> <p>Leased lines must always be entered manually under ISDN Switch Type.</p>
ISDN Switch Type	<p>Defines the ISDN ►► protocol supplied by your ISDN provider.</p> <p>The following settings are possible:</p> <ul style="list-style-type: none"> ■ <i>autodetect on bootup</i>: automatic D-channel protocol 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 ■ <i>none</i>: ISDN connection deactivated ■ <i>leased line B1 channel (64S)</i>: leased line over B-channel 1 ■ <i>leased line B1 + B2 channel (64S2)</i>: leased line over both B-channels ■ <i>leased line D + B1 + B2 channel (TS02)</i>: leased line over D-channel and both B-channels ■ <i>leased line B1 + B2 different endpoints (digital 64S with dual connection)</i>: leased line to two different endpoints <p>The settings for leased lines appear only if you have entered a relevant license.</p>

Field	Meaning
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"> <input type="checkbox"/> <i>leased dte</i> (default value) <input type="checkbox"/> <i>leased dce</i>
B-Channel 1	<p>Configuration of first B-channel. Possible values:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>dialup</i> (default setting) <input type="checkbox"/> <i>not used</i> <input type="checkbox"/> <i>leased dte</i> <input type="checkbox"/> <i>leased dce</i> <p>The settings for leased lines appear only if you have entered a relevant license.</p>
B-Channel 2	<p>Configuration of second B-channel. Possible values:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>dialup</i> (default setting) <input type="checkbox"/> <i>not used</i> <input type="checkbox"/> <i>leased dte</i> <input type="checkbox"/> <i>leased dce</i> <p>The settings for leased lines appear only if you have entered a relevant license.</p>

Table 6-5: **CM-1BRI, ISDN S0**

Do not use the setting *not used* for dialup connections under **B-Channel 1** and **B-Channel 2**, as this mode can cause undesirable side effects.

To do To enter the settings of your ISDN connection, proceed as follows:

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

This setting enables **X1000** 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 set up!

- Select **B-Channel 1**: *dialup*.
- Select **B-Channel 2**: *dialup*.



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 (see [chapter 7.5.3, page 288](#)) 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).

- Press **SAVE**.

You have returned to the main menu. and the entries have been saved.

Incoming Call Answering

If you use the WAN interface for dialup connections, you must now tell **X1000** how it should respond to incoming calls from the ISDN and how it is to handle outgoing calls. (These settings are not necessary for leased lines.) **X1000** distributes the incoming calls to the appropriate internal services according to the settings in the following menus.

X1000 supports the following services:

- PPP (routing)

The ➤➤ **PPP** service is **X1000**'s general routing service. It 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.

■ ISDN Login

The >>> **ISDN Login** service allows incoming data calls access to the >>> **SNMP shell** of your **X1000**. This is how **X1000** is remotely configured and administrated.

■ CAPI

The >>> **CAPI** service allows connection of incoming data and voice calls to communications applications on hosts in the LAN that access the >>> **Remote CAPI** interface of **X1000**. This enables hosts connected to **X1000** to receive faxes, for example.

When a call is received, **X1000** 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 **X1000**. Then the call is forwarded to the corresponding service (see [figure 6-3, page 143](#)).

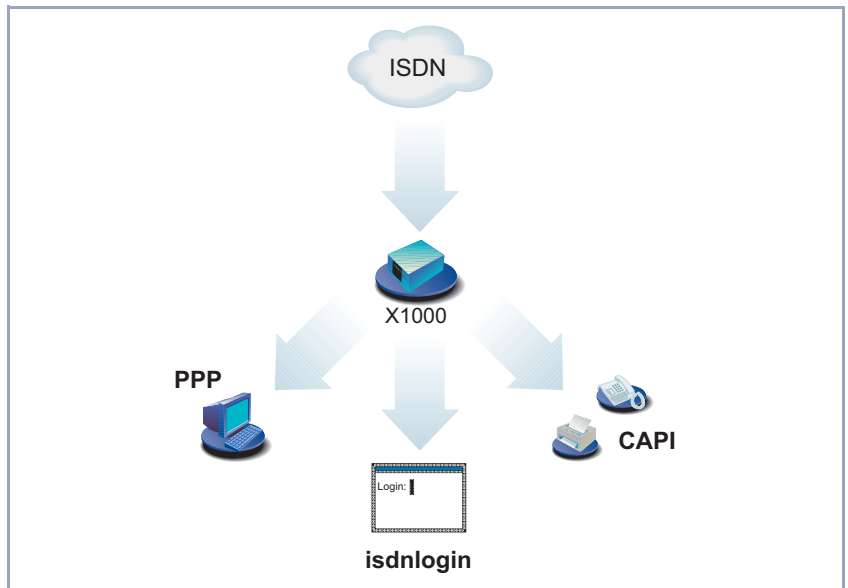


Figure 6-3: Distribution of incoming calls to services

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 6-6: Distribution of extensions to services



If you make no entries in the following menu, every incoming 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.



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



Assign your own numbers to the various services. Enter your own numbers under **Number**.

Now set the entries for Incoming Call Answering:

➤ Go to **CM-1BRI, ISDN S0** ➤ **INCOMING CALL ANSWERING**.

The following menu window opens:

X1000 Setup Tool		BinTec Communications AG	
[WAN][INCOMING]: Incoming Call Answering		MyX1000	
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/untag DELETE, <Return> to edit			

This menu lists the allocation of services to extensions.

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:

X1000 Setup Tool		BinTec Communications AG	
[WAN][INCOMING][ADD]:Incoming Call Answering		MyX1000	
Item	PPP (routing)		
Number	10		
Mode	right to left		
Bearer	data		
	SAVE	CANCEL	
Use <Space> to select			

The menu contains the following fields:

Field	Meaning
Item	Service which shall accept a call to the Number below.
Number	Phone number under which the service (Item) entered above can be reached.
Mode	Mode in which X1000 compares the digits of Number with the called party number of the incoming call: <ul style="list-style-type: none"> <input type="checkbox"/> <i>right to left</i> (default value) <input type="checkbox"/> <i>left to right (DDI)</i>: Always select if X1000 is connected to a point-to-point connection.
User name	CAPI user name. Only necessary if you want to use the CAPI user concept (see chapter 7.1.2, page 204).
Bearer	Type of incoming call. Possible values: <ul style="list-style-type: none"> <input type="checkbox"/> <i>data</i>: data call <input type="checkbox"/> <i>voice</i>: voice call <input type="checkbox"/> <i>any</i>: both data and voice calls

Table 6-7: **CM-1BRI, ISDN S0** ► **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.
<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>	Not available in X1000 .
<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>	Permits PPP connections to V.110 at bit rates of 1200 bps, 2400 bps,..., 38400 bps.
<i>Pots</i>	Not available in X1000 .
<i>PPP Modem Profile 1...8</i>	Not available in X1000 .
<i>CAPI 1.1 EAZ 0...9 Mapping</i>	Enables connections with Remote CAPI applications. Required for CAPI 1.1 applications only.
<i>X.25 PAD</i>	Not available in X1000 .

Table 6-8: **Item**

To do 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**.

- Press **SAVE**.

You have returned to the menu **CM-1BRI, ISDN S0** ➤ **INCOMING CALL ANSWERING**. The entries are saved and displayed in the list.

You have now assigned one of your extensions (**10**) to a possible service (**PPP (routing)**). That is, if a data call is received by called party number 10, it is forwarded to the PPP (routing) service.



As **X1000** forwards all incoming calls that do not match an entry in this menu to the ➤➤ **CAPI** service, it is not necessary to enter CAPI (except for CAPI 1.1 applications)!

- Repeat these steps until you have assigned to all phone numbers the services to be reached under these numbers.

This concludes the configuration of Incoming Call Answering. **X1000** now distributes the incoming calls to the internal services. These numbers and the assigned services are also used for outgoing calls



Make sure you enter the right number under **Number**, i.e. the number that actually arrives at **X1000**! For example, if **X1000** is connected to a ➤➤ **PABX**, only the PABX extension number arrives at **X1000**.

If you are not sure which number arrives at **X1000**, proceed as follows:

- Call **X1000** 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 **X1000**.
- Type in this part of the number in **CM-1BRI, ISDN S0** ➤ **INCOMING CALL ANSWERING** ➤ **ADD** under **Number**.



With the CAPI user concept (see [chapter 7.1.2, page 204](#)), you can reserve access to the CAPI services for certain users with their own passwords.

Advanced configuration *CM-1BRI, ISDN S0* ► **ADVANCED SETTINGS** contains settings for X.31 TEI (see [chapter 7.2.4, page 220](#)).

If you use an X.31 leased line (see [chapter 7.5.3, page 288](#)), you can also implement a backup solution using the Bandwidth on Demand feature ([chapter 7.2.3, page 214](#)). If you use this facility, a dialup connection is set up to the connection partner if the leased line fails.

6.1.5 Configuring X1000 as DHCP Server

IP addresses in the LAN

Each PC in your ►► LAN and X1000 requires its own IP address. If you configure X1000 as a ►► DHCP (Dynamic Host Configuration Protocol) server, it automatically assigns those PCs in the LAN ►► IP addresses from a pre-defined IP address pool. A PC sends out an address request and in turn receives its IP address assigned by X1000. 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 X1000 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.

► Go to **IP** ► **IP ADDRESS POOL LAN (DHCP)** ► **ADD:**

X1000 Setup Tool		BinTec Communications AG
[IP][DHCP][ADD]: Add Range of IP Addresses		MyX1000
Interface	en1	
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 .
Gateway	Defines which IP address is assigned to the DHCP client as gateway. If no IP address is entered here, the IP address of X1000 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 6-9: **IP** ➤ **IP ADDRESS POOL LAN (DHCP)** ➤ **ADD**

To do Make the following entries to configure **X1000** as a DHCP server:

- Select **Interface**, e.g. **en1**.
- 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**.
- Press **SAVE**.

You have returned to **IP ➤ IP ADDRESS POOL LAN (DHCP)**, where the IP address pools are listed and the entries have been saved.



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**, etc.

6.1.6 Setting Filters

NetBIOS filters

If you are working with Windows in your local network, you should set ➤➤ **NetBIOS** filters in order to reduce charges. This prevents **X1000** setting up connections, e.g. to the Internet Service Provider (➤➤ **ISP**), in order to forward WINS requests from PCs in your network. That is, **X1000** asks the ISP which ➤➤ **host name** can be assigned to an IP address. These connections are unnecessary because the ISP cannot resolve WINS names, but still cost money.

A more detailed explanation of ➤➤ **filters** can be found in [chapter 8.2.8, page 317](#).

To prevent these unnecessary connections, proceed as follows:



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

- Use the serial interface or ISDN login to access **X1000** for filter configuration.
- If you access **X1000** over telnet, select **IP ➤ ACCESS LISTS ➤ INTERFACES ➤ EDIT: First rule = none**.
- Go to **IP ➤ ACCESS LISTS ➤ FILTER ➤ ADD**.

The following menu window opens:

X1000 Setup Tool		BinTec Communications AG
[IP][ACCESS][FILTER][ADD]: Configure IP Access Filter		MyX1000
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	
	SAVE	CANCEL
Enter string, max length = 48 chars		

To do 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*.
- Press **SAVE**.

You have returned to **IP** ➤ **ACCESS LISTS** ➤ **FILTER**, and the entries have been 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*.

➤ Press **SAVE**.

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

To define rules for these filters, proceed as follows:

➤ Go to **IP** ➤ **ACCESS LISTS** ➤ **RULES** ➤ **ADD**:

X1000 Setup Tool		BinTec Communications AG	
[IP][ACCESS][RULE][ADD]: Configure IP Access Rules		MyX1000	
Action	deny M		
Filter	wrong_dns (1)		
	SAVE		CANCEL
Use <Space> to select			

To do Make the following entries to define a rule:

➤ Select **Action**: *deny M*.

➤ Select **Filter**: *wrong_dns (1)*.

➤ Press **SAVE**.

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

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)*.

➤ Press **SAVE**.

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

The following menu window displays all entries saved:

```

X1000 Setup Tool                               BinTec Communications AG
[IP][ACCESS][RULE]: Configure IP Access Rules   MyX1000

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/untag DELETE, <Return>
to edit

```

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

```

X1000 Setup Tool                               BinTec Communications AG
[IP][ACCESS][INTERFACES]: Configure First Rule  MyX1000

Configure first rules for interfaces

Interface      First Rule      First Filter
en1            1               1 (wrong_dns)
en1-snap      1               1 (wrong_dns)

EXIT

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

```

To do Make the following entries:

- Select the LAN interface of **X1000** (**en1** or **en1-snap**) and confirm with **Return**.
- Select **First Rule**: *RI 1 FI 1 (wrong_dns)*.
- Press **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.

➤ Leave the main menu via **EXIT** and save the configuration you have created with **Save as boot configuration and exit**.

The settings are then saved to the flash memory and will not be lost when **X1000** is switched off ([chapter 6.3, page 199](#)).

6.2 X1000 and the WAN

If you have carried out the configuration steps in [chapter 6.1, page 129](#), **X1000** is set up for your **LAN**. If you also want to access hosts outside your LAN, e.g. to surf the **Internet**, then this chapter will be of interest to you.

The following points are considered:

■ General configuration of **WAN partners**:

To enable **X1000** to make connections to networks outside your LAN, you must configure the desired connection partners as WAN partners on your **X1000**. This applies to outgoing connections (**X1000** dials its WAN partner), incoming connections (a WAN partner dials the number of your **X1000**) and leased lines (see [chapter 7.5.3, page 288](#)). If you want to access the Internet, you must configure your Internet Service Provider (**ISP**) as a WAN partner. If you wish to establish a LAN-LAN connection, e.g. between your LAN and the LAN of your head office (corporate network connection), you must configure the LAN of your head office as a WAN partner.

How to configure a WAN partner on your **X1000** is explained in general terms in [chapter 6.2.1, page 158](#).

If you configured one or two leased lines at the S_0 connection (see [chapter 6.1.4, page 138](#)) during configuration of **X1000**'s WAN interface, a WAN partner entry for each leased line appears automatically in the WAN Partner menu. Edit this entry to suit your requirements.

■ Examples of configuring a WAN partner for Internet access:

You will find examples of how to set up an ISP as a WAN partner in [chapter 6.2.2, page 184](#). Here you will find a quick procedure if you want to access the Internet with **X1000** via one of the following providers:

- T-Online
- Compuserve

■ Examples of configuring a WAN partner for a corporate network connection:

You will find two examples of how to configure a corporate network connection in [chapter 6.2.3, page 190](#). The first example explains how to connect a branch office to a head office. This example will be sufficient in most cases. The second example shows you how you can dial in to the head office

as a field service or home office employee if you don't have a router, i.e. how **X1000** must be configured in the head office and what you must do on your PC.

A basic scenario is illustrated in [figure 6-4, page 157](#) and gives you an idea of what connections from **X1000** to the WAN partners, ISP and head office could look like.

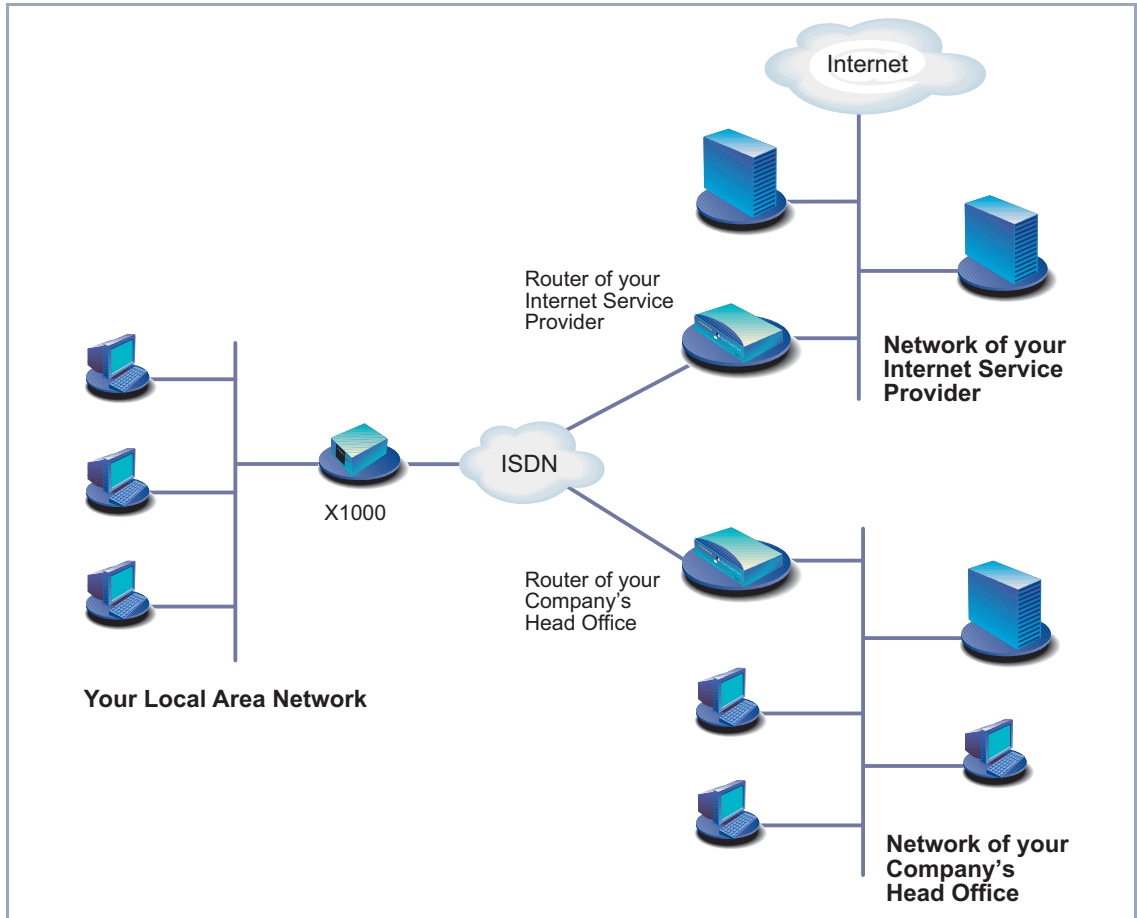


Figure 6-4: Basic scenario

6.2.1 Configuring WAN Partners

Configuring a WAN partner generally involves the following steps:

- Entering a WAN partner:
 - Defining a >> **protocol**.
 - Entering extension(s).
 - Defining >> **PPP** settings for authentication.
 - Defining >> **short hold**.
 - Carrying out IP configuration.
- Creating routing entry
- Activating Network Address Translation (>> **NAT**) (optional).

Off we go!

Entering a WAN Partner

Configuring WAN partners

Here you are going to configure access to your chosen WAN partner, e.g. your Internet Service Provider (ISP). Before you get down to it, you should collect the necessary access information that you received from your ISP or system administrator (see [chapter 3.2.1, page 36](#)). The terms used may vary slightly from provider to provider.

To enter a WAN partner, proceed as follows:

- Go to **WAN PARTNER**.

The following menu window opens:

```

X1000 Setup Tool                               BinTec Communications AG
[WAN]: WAN Partners                             MyX1000

Current WAN Partner Configuration

  Partnername          Protocol          State
  T-Online             ppp             dormant

ADD                   DELETE                   EXIT

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

```

This is where all WAN partners currently configured are listed with the corresponding **Partner name**, **Protocol** and **State**.



If you have set up one or more leased lines (see [chapter 6.1.4, page 138](#)) on configuring the WAN interface of **X1000**, a WAN partner for each leased line is already created automatically in the WAN Partner menu. Edit this entry to suit your requirements.

State can have the following values:

- *up*: connected
- *dormant*: not connected
- *blocked*: not connected (an error occurred on establishing a connection, a renewed attempt is only possible after a specified number of seconds, see [chapter 7.2.1, page 211](#)).
- *down*: set to down by administration

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:

X1000 Setup Tool	BinTec Communications AG
[WAN][ADD]: Configure WAN Partner	MyX1000
Partner Name	T-Online
Encapsulation	PPP
Compression	none
Encryption	none
Calling Line Identification	no
PPP >	
Advanced settings >	
WAN Numbers	
IP >	
IPX>	
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.
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>X.25_PPP: not available on X1000</i> ■ <i>X.25: not available on X1000</i> ■ <i>HDLC Framing (IP only)</i> ■ <i>LAPB Framing (IP only)</i> ■ <i>X31 B-Channel: not available on X1000</i> ■ <i>X.25 No Signalling: not available on X1000</i> ■ <i>X.25 PAD: not available on X1000</i> ■ <i>X.25 No Configuration: not available on X1000</i> ■ <i>Frame Relay: not available on X1000</i> ■ <i>X.25 No Configuration, No Signalling: not available on X1000</i>

Field	Meaning
Compression	Defines the type of compression that should be used for data traffic to the WAN partner. Possible values: <ul style="list-style-type: none">■ <i>STAC</i>: only if Encapsulation = <i>PPP</i>■ <i>MS-STAC</i>: only if Encapsulation = <i>PPP</i>■ <i>none</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>Blowfish 56</i>: Blowfish with 56-bit key ■ <i>Blowfish 168</i>: Blowfish with 168-bit key ■ <i>DES 56</i>: DES with 56-bit key ■ <i>DES3 168</i>: Triple DES with 168-bit key ■ <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>
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 6-10: **WAN PARTNER** ▶ **ADD**

The following table illustrates which encapsulations support procedures for
 ➤➤ **data compression**:

Protocols		Encapsulation	Compression
IP	IPX		STAC, MS-STAC
X	X	<i>PPP</i>	X
X	X	<i>Async PPP over X.75</i>	X
X	X	<i>Async PPP over X.75/T.70/BTX</i>	X
X	X	<i>Multi-Protocol LAPB Framing</i>	
X	X	<i>Multi-Protocol HDLC Framing</i>	
X		<i>HDLC Framing (IP only)</i>	
X		<i>LAPB Framing (IP only)</i>	

Table 6-11: Encapsulation and compression

To do Make the following entries:

- Type in **Partner Name**, e.g. *BigBoss*.
- Select **Encapsulation**, e.g. *PPP*.
- Select **Compression**, e.g. *none*.
- Select **Encryption**, e.g. *none*.
- Go to submenu **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS**.

Entering extension numbers

X1000 Setup Tool	BinTec Communications AG				
[WAN][ADD][WAN Numbers]: WAN Numbers (BigBoss)	MyX1000				
<p>WAN Numbers for this partner:</p> <table> <tr> <td>WAN Number</td> <td>Direction</td> </tr> <tr> <td>0911987654321</td> <td>outgoing</td> </tr> </table>		WAN Number	Direction	0911987654321	outgoing
WAN Number	Direction				
0911987654321	outgoing				
ADD	DELETE	EXIT			
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit					

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

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:

X1000 Setup Tool	BinTec Communications AG
[WAN][ADD][WAN NUMBERS][ADD]:Add or Change WAN Numb.(BigBoss)	MyX1000
Number Direction Advanced settings >	0911987654321 outgoing
SAVE	Cancel
Enter string, max length = 40 chars	

The menu contains the following fields:

Field	Meaning
Number	Extension of WAN partner.
Direction	Defines whether Number should be used for incoming or outgoing calls or for both.

Table 6-12: **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 X1000 .

Table 6-13: **Direction**



When **X1000** 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 be the same as 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	X1000 accepts incoming calls, e.g. with:	Outgoing calls, i.e. X1000 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 6-14: 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**.

- Press **SAVE**.

The entries are saved and listed.

- Leave **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** with **EXIT**.

➤➤ **PPP 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 **X1000** 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 common password and two user names. You get 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 **X1000** matches the caller's data.

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

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

X1000 Setup Tool	BinTec Communications AG
[WAN][ADD][PPP]: PPP Settings (BigBoss)	MyX1000
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	X1000's ID
PPP Password	Password
Keepalives	Activates keepalive packets.
Link Quality Monitoring	PPP Link Quality Monitoring acc. to RFC 1989

Table 6-15: **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>CHAP + PAP</i>	Run primarily CHAP, otherwise PAP.
<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>none</i>	Run no PPP authentication protocol.

Table 6-16: **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 ["Changing the password", page 120](#).

- 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 **X1000** does not know which authentication protocol was set for this WAN partner. To enable the call to still be accepted, **X1000** falls back on general settings in the PPP, which you can change as necessary ([chapter 7.1.3, page 208](#)).

Defining short hold

Now set short hold so that **X1000** clears down the ISDN connection when there is no further data exchange to save money. The short hold setting can be either static or dynamic and tells **X1000** the duration of the idle time, after which it is to clear down 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 the idle timer 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, the idle timer 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 and shortly before the next charging unit starts.



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 **switched 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, **X1000** 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.

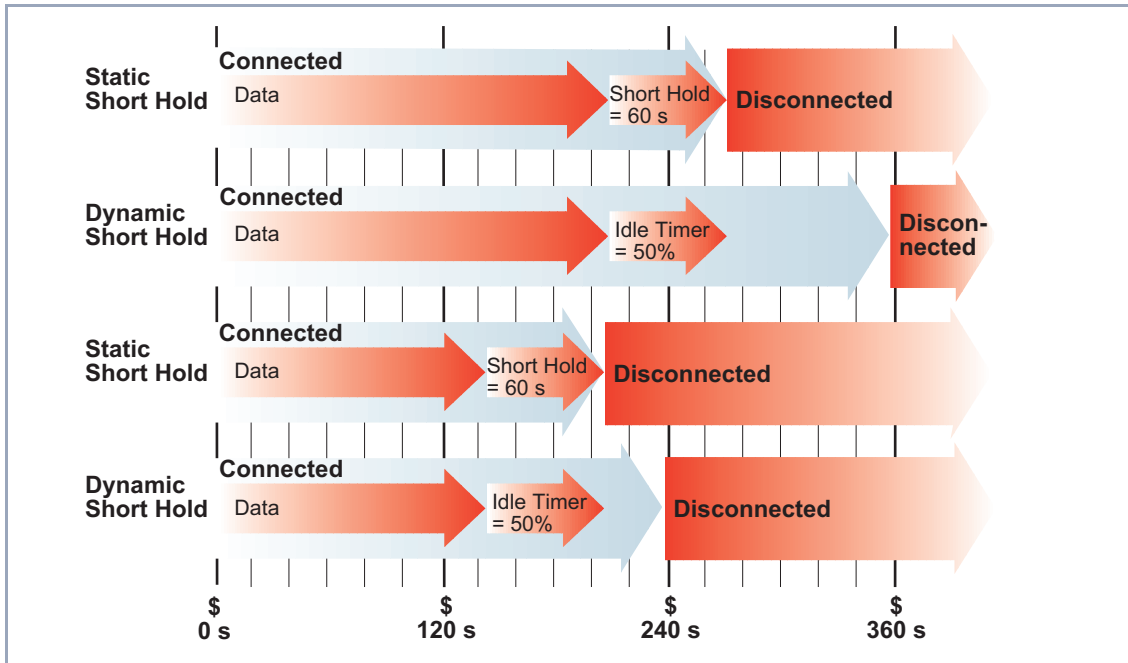


Figure 6-5: Dynamic and static short hold

Proceed as follows:

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

The following menu window opens:

X1000 Setup Tool		BinTec Communications AG
[WAN][ADD][ADVANCED]: Advanced Settings (BigBoss)		MyX1000
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) >		
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 6-17: **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

Now let's move on to the IP configuration of your WAN partner. Here you enter the >>> **IP address** and >>> **netmask** of your partner.

Proceed as follows:

- Go to **WAN PARTNER** ➤ **ADD** ➤ **IP**:

X1000 Setup Tool	BinTec Communications AG
[WAN][ADD][IP]: IP Configuration (BigBoss)	MyX1000
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	Defines whether X1000 uses a transit network to the WAN partner.
Local IP Address	IP address of X1000 . 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 7.2.6, page 235).
Local ISDN IP Address	ISDN IP address of X1000 in the transit network.
Partner's ISDN IP Address	ISDN IP address of WAN partner in the transit network.
Partner's LAN IP Address	WAN partner's LAN IP address.
Partner's LAN Netmask	Your WAN partner's LAN netmask. If you make no entry, X1000 enters a default netmask for the net class used under Partner's LAN IP Address .

Table 6-18: **WAN PARTNER** ► **ADD** ► **IP**

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*.
- Press **SAVE**.
- Press **SAVE** again.

You have returned to **WAN PARTNER** and your entries have been saved.



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 **X1000** 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**: **X1000**'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 **X1000**'s static IP address you get from your ISP.
 - No entries for **Partner's LAN IP Address** and **Partner's LAN Netmask**.

If you want to know more about what a transit network actually is, for example, and what you need it for, see [chapter 7.2.6, page 235](#).



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.

Creating a Routing Entry

Creating routing entry

You have just entered a WAN partner in your **X1000**. A routing entry is created automatically in the routing table of your **X1000** 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.

Proceed as follows:

➤ Go to **IP** ➤ **ROUTING**:

```

X1000 Setup Tool                               BinTec Communications AG
[IP][ROUTING]: IP Routing                       MyX1000

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      255.255.255.0US    0   en1         loc
10.1.1.0     255.255.255.0DI    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/untag DELETE, <Return>
to edit

```

All IP routes entered are listed here. **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 **X1000** has "learned" the routing entry is displayed under **Pro**.

To define a route, proceed as follows:

➤ 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, press the **ADDEXT** button to open the relevant menu. In this case, see [chapter 8.2.12, page 335](#).

The following menu window opens:

X1000 Setup Tool	BinTec Communications AG
[IP][ROUTING][ADD]: IP Routing	MyX1000
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).
Destination IP Address	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>).
Gateway IP Address	IP address of the host to which X1000 should forward the IP packets.
Metric	The lower the value, the higher the priority of the route (possible values 1...14).

Table 6-19: **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 X1000 '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 transit network.
<i>WAN with transit network</i>	Route to a destination host or LAN that can be reached via a WAN partner with transit network.
<i>Refuse</i>	X1000 discards data packets using this route and sends the sender a message saying the destination of the packet is unreachable.
<i>Ignore</i>	X1000 discards data packets using this route without sending a status message.

Table 6-20: **Network**



You can only configure one default route on your **X1000**. 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 **X1000**.

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. *GolInternet*.
- Enter **Metric**, e.g. *1*.

➤ Press **SAVE**.

You have returned to **IP** ➤ **ROUTING**. The entries have been saved and 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.

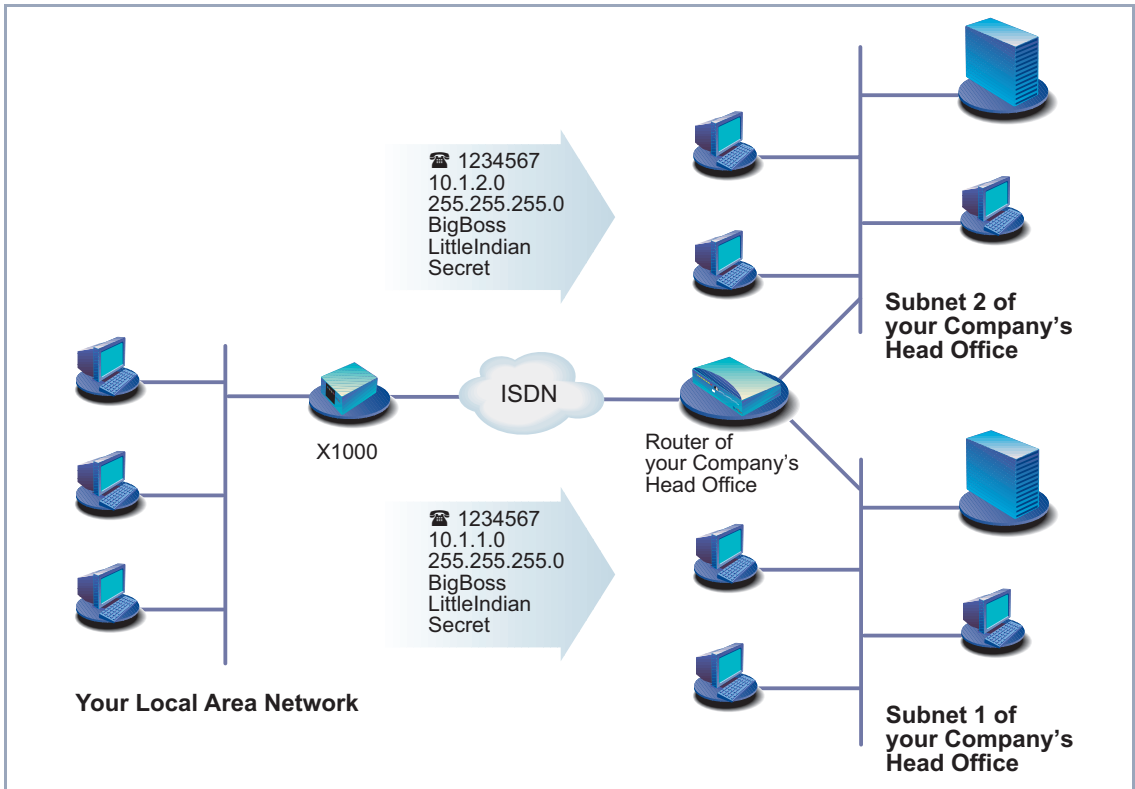


Figure 6-6: Corporate network with several connected LANs

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*.
- Press **SAVE**.

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

- Repeat these steps if you have to enter several routes.

Activating Network Address Translation (NAT)

Activating NAT 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. 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 8.2.7, page 313](#).

Proceed as follows to activate NAT:

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

```

X1000 Setup Tool                               BinTec Communications AG
[IP][NAT]: NAT Configuration                     MyX1000

Select IP Interface to be configured for NAT

Name          Nat      static mappings
GoInternet    off
BigBoss       off
enl           off
enl-snap      off

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 press **Return**.

Another menu window opens:

```

X1000 Setup Tool                               BinTec Communications AG
[IP][NAT][CONFIG]: NAT Configuration (GoInternet) MyX1000

Network Address Translation      on

Configuration for sessions requested from outside

Service      Destination      Source Dep.      Dest. Dep.      Port Remap

            ADD              DELETE           SAVE            CANCEL

Use <Space> to select

```

To do Make the following entries:

- Select **Network Address Translation: on**.

- Press **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 and have configured a WAN partner.

6.2.2 Internet Access with X1000

Examples A few examples are given here following the general procedure described in [chapter 6.2.1, page 158](#), which you can basically use for any Internet Service Provider (ISP). They show you how to set up Internet access to certain providers quickly and easily.

- Example 1: T-Online

- Example 2: Compuserve

Keep at hand the access information you received from your ISP (see [chapter 3.2.1, page 36](#)). The terms may vary slightly from provider to provider.

Off we go:

Example 1: T-Online

If you want to access the Internet with T-Online as provider, proceed as follows:

Configuring WAN partners

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

Entering extensions

- Select **WAN Numbers** and press **Return**.
 - Add a new entry with **ADD**.
 - Enter **Number** (= access number), e.g. **0191011**.
 - Select **Direction**: *outgoing*.
 - Press **SAVE**.
- The extension you use to call T-Online is now in the list.
- Leave **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** with **EXIT**.

Selecting PPP authentication

- Select **PPP** and confirm with **Return**.
- Select **Authentication**: *CHAP + PAP*.
- Enter your **Partner PPP ID** (= provider name): *T_Online*.
- Enter **Local PPP ID** (= your user name):
e.g. **000460004256091169386#0001**.



The T-Online user name comprises the following elements:

<user account><T-Online number>#<co-user number>

The user account is a 12-digit number, in this case: *000460004256*.

The T-Online number is the extension number, in this case: *091169386*.

The co-user number is a 4-digit number, in this case: *0001*.

The T-Online number and the co-user number must be separated by # if the T-Online number has less than 12 digits.

- 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. **minimum: 60**.
- Enter **Idle for Dynamic Short Hold (%)**, e.g. **0**.
- Enter **Delay after Connection Failure (sec)**, e.g. **300**.
- Leave out **Extended Interface Settings (optional)**.
- Select **Channel Bundling**: *no*.
- Select **Layer 1 Protocol**: *ISDN 64 kbps*.
- Confirm with **OK**.

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

Carrying out IP configuration

- Select **IP** and press **Return**.
- Select **IP Transit Network**: *dynamic client*.

- Select **Advanced Settings** and press **Return**.
- Select **RIP Send**: *none*.
- Select **RIP Receive**: *none*.
- Activate **Van Jacobson Header Compression**: *on*.
- Select **Dynamic Name Server Negotiation**: *client (receive)*.
- Deactivate **IP Accounting**: *off*.
- Deactivate **Back Route Verify**: *off*.
- Select **Route Announce**: *up or dormant*.
- Select **Proxy Arp**: *off*.
- Confirm with **OK**.
- Press **SAVE**.
- Press **SAVE** again.
- 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**: *T_Online*.
- Enter **Metric**, e.g. **1**.
- Press **SAVE**.
- Leave **IP** ➤ **ROUTING** with **EXIT**.

Activating NAT

- Go to **IP** ➤ **NETWORK ADDRESS TRANSLATION**.
- Select the IP Interface *T_Online* and press **Return**.
- Select **Network Address Translation**: *on*.
- Press **SAVE**.
- Leave **IP** ➤ **NETWORK ADDRESS TRANSLATION** with **EXIT**.

- Leave **IP** with **EXIT**.
- You have returned to the main menu.
- Configuration of Internet access over T-Online is complete.

Example 2: Compuserve

If you want to access the Internet with Compuserve as provider, proceed as follows:



Access to Compuserve by directly dialing in to a Compuserve network node is explained below.

If you want to reach Compuserve indirectly over T-Online's Compuserve gateway, replace with the following entries at the appropriate places in the configuration sequence:

- Select **Encapsulation**: *Async PPP over X.75/T.70/BTX*.
- Type in **Number**: *01910*.
- Select **Provider**: *Compuserve via T-Online*.

Configuring WAN partners

- Go to **WAN PARTNER** ➤ **ADD**.
- Enter your **Partner Name** (= provider name): *COMPUSERVE*.
- Select **Encapsulation**: *Async PPP over X.75*.
- Select **Compression**: *none*.
- Select **Encryption**: *none*.

Entering extensions

- Select **WAN Numbers** and press **Return**.
- Add a new entry with **ADD**.
- Enter the **Number** (access number).
- Select **Direction**: *outgoing*.
- Press **SAVE**.

The extension you use to call Compuserve is now in the list.

- Leave **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** with **EXIT**.

Selecting PPP authentication

- Select **PPP** and confirm with **Return**.
- Select **Authentication**: *none*.

- 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)**: *120* (the value entered here must be equal to or greater than 120).
- Enter **Idle for Dynamic Short Hold (%)**, e.g. *0*.
- Enter **Delay after Connection Failure (sec)**, e.g. *300*.
- Leave out **Extended Interface Settings (optional)**.
- Select **Channel Bundling**: *no*.
- Select **Layer 1 Protocol**: *ISDN 64 kbps*.

Setting authentication

- Select **Provider Configuration** and press **Return**.
 - Select **Provider**: *Compuserve Network*.
 - Enter **Host**: *CIS*.
 - Enter **User ID** (= your user name).
 - Enter **Password**.
 - Confirm with **OK**.
 - Press **OK** again.
- You have returned to the menu **WAN PARTNER** ➤ **ADD**.

Carrying out IP configuration

- Select **IP** and press **Return**.
- Select **IP Transit Network**: *dynamic client*.
- Select **Advanced Settings** and press **Return**.
- Select **RIP Send**: *none*.
- Select **RIP Receive**: *none*.
- Deactivate **Van Jacobson Header Compression**: *off*.

- Select **Dynamic Name Server Negotiation**: *client (receive)*.
- Deactivate **IP Accounting**: *off*.
- Deactivate **Back Route Verify**: *off*.
- Select **Route Announce**: *up or dormant*.
- Select **Proxy Arp**: *off*.
- Confirm with **OK**.
- Press **SAVE**.
- Press **SAVE** again.
- 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**: *COMPUSERVE*.
- Enter **Metric**, e.g. **1**.
- Press **SAVE**.
- Leave **IP** ➤ **ROUTING** with **EXIT**.

Activating NAT

- Go to **IP** ➤ **NETWORK ADDRESS TRANSLATION**.
- Select the IP Interface COMPUSERVE and press **Return**.
- Select **Network Address Translation**: *on*.
- Press **SAVE**.
- Leave **IP** ➤ **NETWORK ADDRESS TRANSLATION** with **EXIT**.
- Leave **IP** with **EXIT**.

You have returned to the main menu.

Configuration of Internet access over Compuserve is complete.

6.2.3 Dialing into Corporate Network

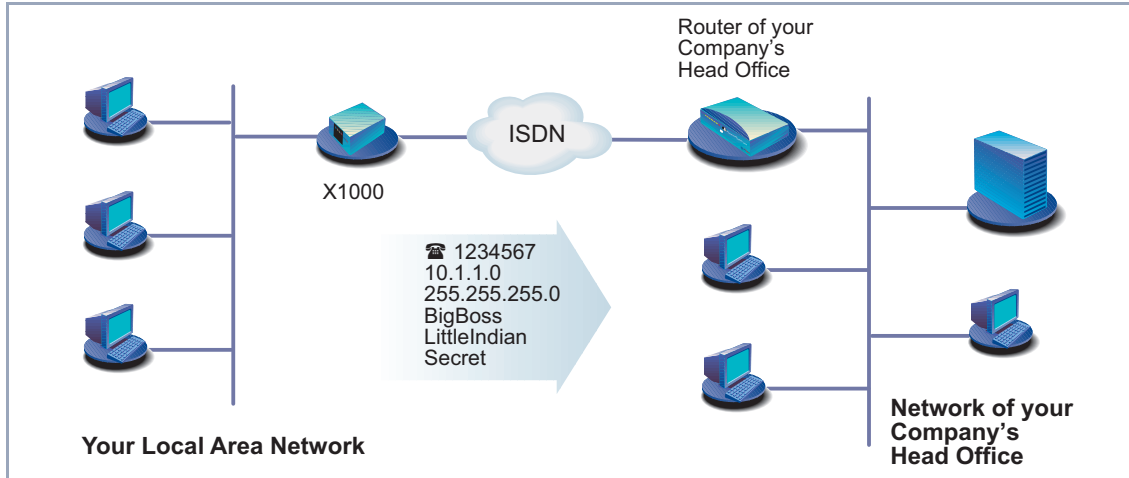


Figure 6-7: **X1000** and your head office

The first part of this chapter explains in quick and easy steps how to configure your **X1000** for a corporate network connection (LAN-LAN connection). The second part describes how to proceed if field staff or a home office staff want to dial in to the head office.

Corporate Network Connection: General Example

Keep at hand the data you have received from the system administrator of your head office (see [chapter 3.2.1, page 36](#)). If you are not sure about some points, refer to [chapter 6.2.1, page 158](#).

Proceed as follows:

- Configuring WAN partners**
- Go to **WAN PARTNER** ➤ **ADD**.
 - Enter **Partner Name** (= user ID of head office), e.g. **BigBoss**.
 - Select **Encapsulation**: *PPP*.
 - Select **Compression**: *STAC*.
 - Select **Encryption**: *none*.

- Entering extensions**
- Select **WAN Numbers** and press **Return**.
 - Add a new entry with **ADD**.
 - Enter the **Number** (= the extension of your head office's router), e.g. **0911987654321**.
 - Select **Direction**: *outgoing*.
 - Press **SAVE**.
The number you use to dial your head office is now in the list.
 - Leave **WAN PARTNER** ➤ **ADD** ➤ **WAN NUMBERS** with **EXIT**.
- Selecting PPP authentication**
- Select **PPP** and confirm with **Return**.
 - Select **Authentication**: *CHAP + PAP*.
 - Enter **Partner PPP ID** (= user ID of head office), e.g. **BigBoss**.
 - Enter **Local PPP ID** (= your own ID), e.g. **LittleIndian**.
 - Enter **PPP Password** (= common password for this connection).
 - 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. **20**.
 - Enter **Idle for Dynamic Short Hold (%)**, e.g. **0**.
 - Enter **Delay after Connection Failure (sec)**, e.g. **300**.
 - Leave out **Extended Interface Settings (optional)**.
 - Select **Channel Bundling**: *no*.
 - Select **Layer 1 Protocol**: *ISDN 64 kbps*.
 - Confirm with **OK**.
You have returned to the menu **WAN PARTNER** ➤ **ADD**.

Carrying out IP configuration

- Select **IP** and press **Return**.
- Select **IP Transit Network**: *no*.
- Enter **Partner's LAN IP Address** (= network address of head office): e.g. **10.1.1.0**.
- Enter **Partner's LAN Netmask** (= netmask of head office), e.g. **255.255.255.0**.
- Select **Advanced Settings** and press **Return**.
- Select **RIP Send**: *none*.
- Select **RIP Receive**: *none*.
- Activate **Van Jacobson Header Compression**: *off*.
- Select **Dynamic Name Server Negotiation**: *yes* (if you have configured Internet access) or *off* (if you have not configured Internet access).
- Activate **IP Accounting**: *on*.
- Activate **Back Route Verify**: *on*.
- Select **Route Announce**: *up or dormant*.
- Select **Proxy Arp**: *off*.
- Confirm with **OK**.
- Press **SAVE**.
- Press **SAVE** again.
- Leave **WAN PARTNER** with **EXIT**.
You have returned to the main menu.
Configuration of access to the corporate network is complete.

Creating routing entry



If you have not configured any Internet access, then you can configure a default route for access to your head office (see [chapter 6.2.1, page 158](#)):

- Make the following entries in **IP** ➤ **ROUTING** ➤ **ADD**:
 - **Route Type**: *Default route*
 - **Network**: *WAN without transit network*
 - **Partner / Interface**, e.g. **BigBoss**
 - **Metric**, e.g. **1**



If the corporate network comprises several LANs (subnets) and you do not configure a default route to head office, then you must create a separate routing entry for each LAN you want to reach. See instructions in [chapter 6.2.1, page 158](#) and [figure 6-6, page 181](#).

- Repeat the steps for creating a routing entry until you have entered all the necessary routes.
- Press **SAVE**.
- Leave **IP** ➤ **ROUTING** with **EXIT**.
- Leave **IP** with **EXIT**.

Corporate Network Connection Dial-in (without router)

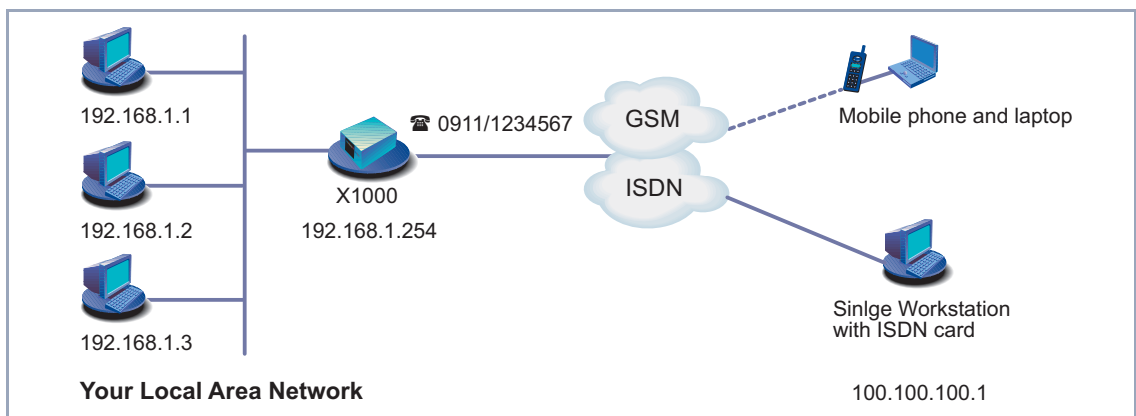


Figure 6-8: Scenario for dial-in

To access the data at head office, field service staff can dial in over laptop and mobile phone to the network at head office. If home office staff have no router, they need either an ISDN card in their PC or a modem. The configuration of **X1000** and the PC or laptop is basically identical in all these cases. Field service staff using a Nokia Communicator mobile phone must make additional settings, which are described at the end of the next section.

The configuration is made in two or three steps.

■ Configuration of **X1000**

- Configuration of the PC
- Configuration for Windows network (optional)

Configuration of X1000 After basic configuration of **X1000** (see [chapter 3.5.1, page 53](#) and [chapter 6.1, page 129](#)), configure the desired dial-in partners as WAN partners.

Configuring WAN partners

- Go to **WAN PARTNER** ➤ **ADD**.
- Type in **Partner Name**, e.g. *Client Dialin*.
- Select **Encapsulation**: *PPP*.
- Select **Compression**: *none*.
- Select **Encryption**: *none*.

Selecting PPP authentication

- Select **PPP** and confirm with **Return**.
- Select **Authentication**: *CHAP*.
- Enter **Partner PPP ID**, e.g. *clientdialin*.
- Leave **Local PPP ID** (= your own ID) empty (for dial-in only).
- Enter **PPP Password** (= common password for this connection).
- Deactivate **Keepalives**: *off*.
- Deactivate **Link Quality Monitoring**: *off*.
- Confirm with **OK**.

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

Carrying out IP configuration

Define the route to your dial-in partner:

- Select **IP** and press **Return**.
- Select **IP Transit Network**: *Dynamic Server*.

Defining address pool

- Select **Advanced Settings** and press **Return**.
- Select **RIP Send**: *none*.
- Select **RIP Receive**: *none*.
- Deactivate **Van Jacobson Header Compression**: *off*.
- Deactivate **Dynamic Name Server Negotiation**: *off*.
- Enter **IP Address Pool**: *1*.

- Deactivate **IP Accounting**: *off*.
 - Deactivate **Back Route Verify**: *off*.
 - Select **Route Announce**: *up or dormant*.
 - Select **Proxy Arp**: *off*.
 - Confirm with **OK**.
 - Press **SAVE**.
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. **300**, i.e. a high value.
 - Enter **Idle for Dynamic Short Hold (%)**, e.g. **0**.
 - Enter **Delay after Connection Failure (sec)**, e.g. **30**.
 - Leave out **Extended Interface Settings (optional)**.
 - Select **Channel Bundling**: *no*.
 - Select **Layer 1 Protocol**: *ISDN 64 kbps*.
 - Confirm with **OK**.
You have returned to the menu **WAN PARTNER** ➤ **ADD**.
 - Press **Save**.
 - Leave **WAN PARTNER** with **EXIT**.
- Entering IP address**
- Go to **IP** ➤ **IP ADDRESS POOL WAN (PPP)** ➤ **ADD**.
 - Enter **Pool ID**, e.g. **1**.
 - Enter **IP Address** (= IP address of your dial-in partner), e.g. **100.100.100.1**.
 - Enter **Number of Consecutive Addresses**, e.g. **1**.
 - Press **SAVE**.
 - Leave **IP** ➤ **IP ADDRESS POOL WAN (PPP)** with **EXIT**.
 - Leave **IP** with **EXIT**.
- Entering extensions**
- Go to **CM-1BRI, ISDN S0** ➤ **INCOMING CALL ANSWERING** ➤ **ADD**.

- Select **Item**: *PPP (routing)*.
The setting *PPP (routing)* automatically detects the protocol used (e.g. **ISDN 64 kbps** or **V110 (9600)**).
- Enter **Number**, e.g. **1234567** (= telephone number over which the dial-in partner is to dial in).



Enter only your extension without prefix under **Number**. If **X1000** is connected to a PABX, you must only enter the PABX extension number that **X1000** receives. (You should also refer to the information in [chapter 6.1.4, page 138](#)).

- Select **Mode**: *right to left*.
- You can leave **Username** empty.
- Select **Bearer**: *any*.
- Press **SAVE**.
- Leave **ICM-1BRI, ISDN S0** ➤ **INCOMING CALL ANSWERING** with **EXIT**.
- Confirm with **SAVE**.

Nokia Communicator

If you use a Nokia Communicator mobile phone, you must make the following additional entries to enable the mobile phone to set up a connection to the corporate network:

- Go to **PPP**.
- Activate **PPP Link Quality Monitoring**: *yes*.
- Go to **WAN PARTNER** ➤ **ADD** ➤ **PPP**.
- Activate **Link Quality Monitoring**: *on*.

Configuration of PC in Windows NT

The necessary steps for configuration of your PC or laptop if you use the Windows NT operating system are given below. If you use Windows 95 or 98, you must observe basically the same points to complete the configuration successfully using the list.

The following steps are necessary:

- Installing the ISDN/GSM card or modem together with the relevant data communications driver. (Refer to the documentation supplied with the card or modem and follow the instructions on the screen.)

- Check whether the TCP/IP protocol is installed (in the Windows Start menu under **Settings ▶ Control Panel ▶ Network**) or install this protocol if necessary (see [chapter 3.2.2, page 40](#)).
- Check the installed card (in the **Network Card** tab).
- Check whether the RAS service is installed and install if necessary (in the **Services** tab).
- Leave the **Network** menu with **OK**. The TCP/IP protocol is fixed on the dial-up adaptor. When the installation is successfully completed, the virtual modems are listed (**Settings ▶ Control Panel ▶ Modems**).
- Make a new entry for the connection in the directory (**Program ▶ Accessories ▶ DCN**). The telephone number must be entered under which **X1000** accepts routing calls.
- Check the directory entry (**Continue ▶ Edit Entry and Modem Parameters** in the **Entries** tab).
- Only **TCP/IP** is to be selected as network protocol in the **Server** tab.
- Create connection (**Select**).
- Entering user name and password (= **Partner PPP ID** and **PPP Password** under **WAN PARTNER ▶ ADD ▶ PPP** in **X1000**).
- The connection is set up on leaving the menu by pressing **OK**.



If you want to dial in to a Windows network, you must carry out a few additional configuration steps.

Configuration for Windows network

If you want to log in to a Windows NT server, you or the system administrator must carry out configuration steps at two points:

- at the Windows NT Domain Server
- at the Windows PC

Windows NT server The administrator must carry out the following configuration steps at the Windows NT server:

- configure a user in the User Manager
- configure the dial-in PC as a member of the domain
- name resolution should be carried out (WINS, DNS or LMHOSTS file).

Windows client The following configuration steps must be carried out at the Windows PC:

- Entering the NetBIOS name of the PC and the group name (i.e. in the Windows Start menu under **Settings ▶ Control Panel ▶ Network**, the group name and the name of the NT domain must be identical in the **Identification** tab).
- Installing the client for Microsoft networks and entering the domain of the server there (e.g. ***BINTECDOM***).

6.3 Saving the Configuration File

After creating a working configuration on your **X1000**, make sure you save it:

- In the Setup Tool main menu, select **Exit** and press **Return**.

Another menu window opens:

```
X1000 Setup Tool                               BinTec Communications AG
[EXIT]: Exit Setup                             MyX1000

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 a file in the flash memory.

The SNMP shell of **X1000** appears with the login prompt. All the changes you have made with the Setup Tool are saved. The next time you start your **X1000**, the configuration file you have just saved will be loaded.

- Select **Exit without saving** to quit the Setup Tool without saving the changes made.

The SNMP shell of **X1000** appears with the login prompt. All settings or changes you have made with the Setup Tool will be lost when you turn off your **X1000**.

7 Advanced Configuration

This chapter contains more **X1000** configuration options for the advanced user. This is the right chapter if you would like to make additional settings that are not covered by the **Configuration Wizard** or in [chapter 6, page 127](#).

The following configuration steps are described:

- General >> **WAN** Settings
- Settings Specific to WAN Partners
- Basic >> **IP** Settings
- >>> **IPX** Settings
- Extra License Functions



Use the Credits Based Accounting System (see [chapter 8.1.3, page 299](#)). This enables you to set a limit for connections to **X1000** to prevent unnecessary charges accumulating as a result of mistakes made during configuration.

7.1 General WAN Settings

General WAN functions:

- **X1000** as dynamic IP address >>> **server**
- >>> **CAPI** user concept
- General >>> **PPP** settings

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

7.1.1 Dynamic IP Address Server

IP address pools **X1000** 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, **X1000** first checks whether a host route is entered in the routing table for this caller. If not, **X1000** 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**

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 7-1: **IP** ► **IP ADDRESS POOL WAN (PPP)**

Field	Meaning
IP Transit Network	Defines whether a transit network is to be used between X1000 and the WAN partner. You must select <i>dynamic server</i> here if you assign an address pool.

Table 7-2: **WAN PARTNER** ► **EDIT** ► **IP**

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

Table 7-3: **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**.
- Press **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**.
- Press **SAVE**.

7.1.2 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 **X1000**'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 [chapter 6.1.4, page 138](#)), 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. So if Old Shatterhand is quicker off the mark ...

Configuration is made in:

- **CAPI** ➤ **USER**
- **CM-1BRI, ISDN S0** ➤ **INCOMING CALL ANSWERING**

The **CAPI** ► **USER** menu contains the following fields:

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 7-4: **CAPI** ► **USER**

The **CM-1BRI, ISDN S0** ► **INCOMING CALL ANSWERING** menu contains the following fields:

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 X1000 compares the digits of Number with the called party number of the incoming call: <i>right to left</i> : default mode. <i>left to right (DDI)</i> : always select this mode if X1000 is connected to a point-to-point ISDN access (system access).
User name	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: <input type="checkbox"/> <i>data</i> : data call <input type="checkbox"/> <i>voice</i> : voice call <input type="checkbox"/> <i>any</i> : random call

Table 7-5: **CM-1BRI, ISDN S0** ► **INCOMING CALL ANSWERING**



If there is no entry in **CAPI** ► **USER** on starting **X1000**, a standard entry is created automatically 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**.
- Select **CAPI: enabled**.
- Press **SAVE**.
- Repeat these steps for every user in the LAN.
- Go to **CM-1BRI, ISDN S0** ➤ **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: CAPI**.



If you use a communications application on your PC that is based on Remote CAPI 1.1 (current version: Remote CAPI 2.0), **X1000** 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**.

CAPI 2.0 evaluates the MSN directly and "translation" to EAZ is not necessary. You can use the same CAPI 1.1 EAZ x Mapping entry for each **Number** i.e. a single entry is sufficient.

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 **User Name**.
- Select **Bearer**.
- Press **SAVE**.

- Repeat these steps as often as necessary until you have created an entry for every user.

7.1.3 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 6.2.1, page 158](#)). If a call is received, **X1000** 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 some cases, it is not possible to identify an incoming call via CLID. This is the case, for example,

- if the call is made over an analog line (the caller dials into your router via a ➤➤ **modem**),
- if the caller suppresses the CLID facility.

In both cases, **X1000** receives no calling line number. The caller therefore cannot be identified by CLID, even if the caller is entered as a WAN partner. **X1000** 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, **X1000** 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, **X1000** 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 rejected then the protocol required by the caller ■ <i>none</i>: no PPP authentication
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 biboPPPLQMTable.

Table 7-6: **PPP**

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

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

7.1.4 X.31 TEI

The menu **CM-1BRI, ISDN S0 ► 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 autoconfiguration 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 autoconfiguration, but can also be entered manually.
X.31 TEI Service	Here you select the service for which you want to use X.31 TEI. Possible values: <ul style="list-style-type: none"> <input type="checkbox"/> <i>Capi</i> <input type="checkbox"/> <i>Capi Default</i> <input type="checkbox"/> <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 7-7: **CM-1BRI, ISDN S0 ► ADVANCED SETTINGS**

7.2 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 7.2.1, page 211](#))
- Channel Bundling - Basic Configuration for Dialup Connections ([chapter 7.2.2, page 212](#))
- Channel Bundling - Bandwidth on Demand (BOD) - Advance Configuration for PPP Connections ([chapter 7.2.3, page 214](#))
- Always On/Dynamic ISDN (AO/DI) ([chapter 7.2.4, page 220](#))
- Layer 1 Protocol ([chapter 7.2.5, page 233](#))
- IP Transit Network ([chapter 7.2.6, page 235](#))
- Transfer of DNS and WINS Server IP Addresses to WAN Partners ([chapter 7.2.7, page 238](#))
- **➤➤ RIP** ([chapter 7.2.8, page 242](#))
- Compression: **➤➤ VJHC**, **➤➤ STAC**, MS-STAC ([chapter 7.2.9, page 245](#))
- **➤➤ Proxy ARP** ([chapter 7.2.10, page 247](#))
- Keepalive Monitoring ([chapter 7.2.11, page 249](#))

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

7.2.1 Delay after Connection Failure

This function enables you to set the period of time **X1000** 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 wait time in seconds before X1000 tries again after an attempt to establish a connection has failed.

Table 7-8: **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**.
- Press **SAVE**.

7.2.2 Channel Bundling - Basic Configuration for Dialup Connections

X1000 supports dynamic and static ►► **channel bundling** for dialup connections over multilink PPP.

Dynamic In dynamic channel bundling, only one B-channel is initially opened on setting up a connection. If the data throughput is large enough, **X1000** adds the second ►► **ISDN** B-channel to increase the bandwidth for connections to the WAN partner. If the amount of data traffic drops, the second ►► **B-channel** is closed again.

Adding and dropping B-channels A B-channel is added if the current data throughput of the relevant interface to the connection partner is 90% or more of the maximum permissible throughput for at least 5 seconds.

The current throughput is not used as a basis for dropping a B-channel already connected. This is based on the calculated (i.e. fictitious) throughput of the channel group after switching out one B-channel. A B-channel is dropped if the calculated value stays below 80% of the maximum permissible throughput of the remaining channels for 10 seconds.

Static or dynamic short hold 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.

Static In static channel bundling, you specify right from the start that **X1000** is to use two B-channels for connections to the WAN partner, regardless of the amount of data transferred.

Both B-channels are initiated in a period of less than 1 second.

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.
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 connection. Possible values: 1, 2.

Table 7-9: **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 7-10: **Channel bundling**

To do Proceed as follows:

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS**.
- Select **Channel Bundling**: *dynamic* or *static*.
- Enter **Total Number of Channels**.
- Confirm with **OK**.
- Press **SAVE**.

Refer to the advanced configuration options (Bandwidth on Demand BOD), see [chapter 7.2.3, page 214](#).

7.2.3 Channel Bundling - Bandwidth on Demand (BOD) - Advanced Configuration for PPP Connections

Bandwidth management, subsequently called BOD (Bandwidth on Demand), offers advance configuration options for dialup connections compared with the basic configuration (see [chapter 7.2.2, page 212](#)). You can also use BOD to dynamically bundle leased lines with dialup connections to cope with a large data flow. You can also easily configure a backup mode for leased lines, so that a dialup connection is set up to the partner if the leased line fails.

You also have a facility for defining the possible use of the Bandwidth Allocation Control Protocol (BACP/BAP to RFC 2125).

Authentication PPP authentication of the connection partner is typically not necessary for setting up a leased line, but authentication is necessary for any dialup connections switched in.

BOD is configured in

- **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS** ➤ **EXTENDED INTERFACE SETTINGS (OPTIONAL)**
- **WAN PARTNER** ➤ **EDIT** ➤ **WAN NUMBERS** ➤ **ADD** (menu description in [chapter 6.2, page 156](#))
- **WAN PARTNER** ➤ **EDIT** ➤ **PPP** (menu description in [chapter 6.2, page 156](#))

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



The fields described below appear for dialup connections or leased lines only under certain conditions.

The fields only appear for dialup connections if **Channel Bundling** has been previously set to *dynamic* in menu **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** and **Mode** to *Bandwidth On Demand Enabled* in menu **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS**.

The fields only appear for leased lines if menu **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS** ► **EXTENDED INTERFACE SETTINGS** under **Mode** e.g. **has been previously set to** *Bandwidth On Demand Active*.



The default settings in the **Line Utilization Weighting**, **Line Utilization Sample (sec)**, **Gear Up Threshold** and **Gear Down Threshold** fields should only be changed for special applications. We recommend that you use the default values for standard applications; they correspond to those of the basic configuration (see [chapter 7.2.2, page 212](#)).

Field	Meaning
Mode	Defines which mode is used for BOD. Possible values: see table 7-12, page 219 .
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 values of data throughput measured are more heavily weighted for the calculation. That is, the calculation is most heavily influenced by the values measured last in the Line Utilization Sample (sec).
Line Utilization Sample (sec)	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).
Gear Up Threshold	Utilization threshold in percent at which another B-channel is added for a connection. A B-channel is added when the current throughput of the relevant interface to the connection partner equals or exceeds the Gear Up Threshold for at least 5 seconds.
Gear Down Threshold	B-channels are dropped until the remaining channels have at least the remaining percentage utilization. A B-channel is dropped if the calculated value is below the Gear Down Threshold of the remaining channels for 10 seconds.

Field	Meaning
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 7.2.4, page 220).</p>
Maximum Number of Dialup Channels	<p>Maximum permitted number of channels that are opened.</p> <p>The value is only displayed here for dialup connections; it is set under Total Number of Channels in the menu WAN PARTNER ► EDIT ► ADVANCED SETTINGS.</p> <p>The value can be set here for leased lines.</p>

Table 7-11: **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>	<p>BAP behaves as follows in Active Mode:</p> <ul style="list-style-type: none"> ■ Call Request: one of the two communication partners wants to add a B-channel; is initiated if applicable. ■ Callback Request: the remote terminal is requested to add a B-channel; is not initiated but accepted if applicable. ■ Link Drop Request: one communication partner wants to drop a B-channel; dropping is initiated or accepted if applicable. <p><i>BAP, Active Mode</i> is necessary for the AO/DI (Always On/Dynamic ISDN) function, see table 7-17, page 228</p>
<i>BAP, Passive Mode</i>	<p>BAP behaves as follows in Active Mode:</p> <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>
<i>Backup</i>	<p>(For leased lines only) Backup connection is activated if the leased line fails. The backup connection is cleared when the leased line is available again. BOD is also available for this mode, if a value > 1 is used for Maximum Number of Dialup Channels.</p>
<i>Bandwidth On Demand Active</i>	<p>(For leased lines only) Enables BOD and defines the active partner. Only one of the connection partners should be configured as active partner. This page activates adding and dropping additional B-channels on demand.</p>
<i>Bandwidth On Demand Passive</i>	<p>(For leased lines only) Enables BOD and defines the passive partner. This page does not activate adding and dropping additional channels.</p>

Table 7-12: **Mode**

To do Proceed as follows:

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS** ➤ **EXTENDED INTERFACE SETTINGS (OPTIONAL)**.
- Select **Mode** and **Line Utilization Weighting**.
- Enter **Line Utilization Sample (sec)** and for leased lines **Maximum Number of Dialup Channels**.
- Press **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*.

- Press **SAVE**.
- Go to **WAN PARTNER** ➤ **EDIT** ➤ **PPP**.
- Select **Authentication**.
- Enter **Partner PPP ID**, **Local PPP ID** and **PPP Password**, if applicable.
- Confirm with **OK**.
- Press **SAVE**.

7.2.4 Always On/Dynamic ISDN (AO/DI)

Always On/Dynamic ISDN (AO/DI) uses the existing ISDN infrastructure to configure a new 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 Internet Service Provider.

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 two B-channels are dynamically added (Dynamic ISDN). Data transmission in this case is only in the B-channel or B-channels, i.e. the B-channels remain reserved for bandwidth-intensive applications (B-channel Mode).

AO/DI offers the following advantages:

- three full communication channels, which can be independent if required
- 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
- in B-Channel Mode:
 - time-dependent connection charges only for bandwidth-intensive applications

How Does AO/DI Work?

AO/DI is implemented in **X1000** 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).

The use of the B-channels is controlled by the data throughput or by application-dependent bandwidth management (Bandwidth on Demand, BOD for IP-based applications). Both Bandwidth on Demand and BOD for IP-based applications uses the Bandwidth Allocation Control Protocol (BACP/BAP to RFC 2125) in order to agree with the remote terminal on the circumstances under which B-channels are to be added or dropped. The use of BACP/BAP is agreed during the initial connection setup. As the D-channel connection is normally no longer

ended after connection setup, 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 change to B-channel mode or the addition of another B-channel can be made on the basis of throughput measurement or triggered via packets of IP-based applications. This is implemented in **X1000** by an advanced configuration option in the IP subsystem. An interface is assigned filters, rules and rule chains similarly to the IP access lists (see [chapter 8.2.8, page 317](#)). 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 **X1000** for AO/DI:

- Carry out X.31 configuration, i.e. reserve the TEI (Terminal Endpoint Identifier) value for X.25 (Packet Switch) (see "[X.31 configuration](#)", [page 223](#))
- Carry out X.25 configuration (see "[X.25 configuration](#)", [page 223](#)):
 - Link configuration for Datex-P
 - Call routing
- Configure AO/DI partner as WAN partner (see "[Configuring AO/DI partner as WAN partner](#)", [page 225](#))
 - Select PPP parameters
 - Define the PPP interface as AO/DI interface
 - Enter X.25 destination address for initial connection setup
 - Control Bandwidth on Demand (dynamic B-channel bundling)
 - Control BOD for IP-based applications

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 using the Setup Tool.

For **X1000**, the X.25 software is designed as an X.25 switch. This switch must be appropriately configured for AO/DI (see "[X.25 configuration](#)", page 223).

You will find all the necessary steps below for configuring **X1000** for AO/DI with the Setup Tool.

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

- Go to **CM-1BRI, ISDN S0** ➤ **ADVANCED SETTINGS** (the menu is described in [chapter 7.1.4, page 210](#)).
- 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**: 1.
- Select **X.31 TEI Service**: *Packet Switch*.
- Press **SAVE**.
You have returned to the **CM-1BRI, ISDN S0** menu.
- Press **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. Information about the X.25 parameters can be found in the **Software Reference** at www.bintec.net.

X.25 configuration 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.

Table 7-13: X.25 ► LINK CONFIGURATION ► EDIT

- Select **L3 Packet Size max**: 256.
- Select **Windowsize/Packetsize Neg.**: *never*.
- Enter **Highest Two-Way-Channel (HTC)**: 1.
- Press **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 7-14: X.25 ► ROUTING ► ADD

- Select **Source Link**: *local*.
- Select **Destination Link**, e.g. *x31d2-0-1*.

- Enter **Destination X.25 Address**, e.g. **019011**.
 - Press **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 X1000 is to use. There is only one meaningful setting for AO/DI: <i>AO/DI</i> .
Channel Bundling	Defines whether or which type of channel bundling is to be used for connections to the WAN partner (see manual, chapter 7.2.2). 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 channels that may be opened for dynamic channel bundling. Possible values for X1000 : 1 or 2.
Remote X.25 Address	X.25 destination address. Appears only if <i>AO/DI</i> is selected under Layer 1 Protocol .

Table 7-15: **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**.

Control of Bandwidth On Demand

Proceed as follows to configure BACP/BAP for "AO/DI client" access:

- 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, 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 (see table 7-11, page 217).
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 .
Gear Up Threshold	Utilization threshold in percent at which another B-channel is added for a connection. A B-channel is switched in when the current throughput of the relevant interface to the connection partner equals or exceeds the Gear Up Threshold for at least 5 seconds.
Gear Down Threshold	B-channels are dropped until the remaining channels have at least the percentage utilization remaining here. A B-channel is dropped if the calculated value is below the Gear Down Threshold of the remaining channels for 10 seconds.
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.
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 7-16: **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 Active Mode:</p> <ul style="list-style-type: none"> ■ Call Request: one of the two communication partners wants to add a B-channel; is initiated if applicable. ■ Callback Request: the remote terminal is requested to add a B-channel; is not initiated but accepted if applicable. ■ Link Drop Request: one communication partner wants to drop a B-channel; dropping is initiated or accepted if applicable.

Table 7-17: **Mode** = *BAP, Active Mode*

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

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

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

For dynamic assignment of the IP address by the Internet Service Provider, proceed as follows:

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

You have returned to the main menu.

BOD for IP-Based Applications (Optional)

Filters and rules BOD for IP-based applications is configured by filters and rules in a similar way to Access Lists for IP packets (see [chapter 8.2.8, page 317](#)). First filters are defined that determine which IP packets (and thus applications) are to influence the available bandwidth. If several filters are defined, they can be interlinked using a rule chain.

Proceed as follows to define suitable filters:

- 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. *172.16.08.15*.
- Enter **Destination Mask**, e.g. *255.255.255.255*.
- Select **Destination Port**: e.g. *specify*.
- Enter **Specify Port**, e.g. *25* (port for SMTP).
- Press **SAVE**.

A list of all the previously defined filters appears.

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

A rule for BOD is defined in a similar way to a rule for IP packets (see [chapter 8.2.8, page 317](#)). Different rules normally consist of different filters and can be interlinked to form a rule chain. Each rule results in an action, but 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 8.2.8, page 317](#)), the menu contains the following fields:

Field	Meaning
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 added. Possible values for X1000 : 1 or 2.

Table 7-18: **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **RULES FOR BOD** ➤ **ADD**

The **Action** field, which indicates how a filtered out 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.
<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 7-19: **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*.
- Press **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, e.g. *adclient*, and press **Return**.
- Select the rule you wish to apply to this interface, e.g. *mail_smtp_out*.
- Press **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.

Configuration Examples for BOD (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 **X1000** 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*.
- Enter **Source Address**: *172.16.77.11*.
- Enter **Source Mask**: *255.255.255.255*.
- Select **Destination Port**: *specify*.
- Enter **Specify Port**: *80*.
Press **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)*.
- Press **SAVE**.
- Leave **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **RULES FOR BOD** with **Exit**.

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*.
- Enter **Destination Address**: *172.16.08.15*.
- Enter **Destination Mask**: *255.255.255.255*.
- Select **Destination Port**: *specify*.
- Enter **Specify Port**: *110*.
- Press **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*.
- Select **Direction**: *incoming*.
- Select **Number of Channels**: *1*.
- Select **Filter**: *mail_pop3_in (2)*.
- Press **SAVE**.
- Leave **IP** ➤ **BANDWIDTH ON DEMAND (BOD)** ➤ **RULES FOR BOD** with **Exit**.

7.2.5 Layer 1 Protocol (ISDN B-Channel)

ISDN B-channel You can define the Layer 1 Protocol of the ISDN ➤➤ **B-channel** that **X1000** 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 explicitly necessary.

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

Field	Meaning
Layer 1 Protocol	Defines which Layer 1 Protocol X1000 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 7-20: **WAN PARTNER** ► **EDIT** ► **ADVANCED SETTINGS**



For incoming calls that cannot be identified from the calling party number, **X1000** uses the settings under **Item** in menu **CM-1BRI, ISDN SO** ► **INCOMING CALL ANSWERING** as the Layer 1 Protocol (see [chapter 6.1.4, page 138](#)).

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.
<i>Modem</i>	Not available in X1000 .
<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 to V.110 at bit rates of 1200 bps, 2400 bps,..., 38400 bps.
<i>Modem Profile 1 ... 8</i>	Not available in X1000 .
<i>PPTP PNS</i>	For VPN interface.
<i>AO/DI</i>	For using Always On/Dynamic ISDN (AO/DI, see chapter 7.2.4, page 220).

Table 7-21: **Layer 1 Protocol**



Most of the entries for **Layer 1 Protocol** correspond to the entries for **Item** in **CM-1BRI, ISDN S0** ► **INCOMING CALL ANSWERING** (see [chapter 6.1.4, page 138](#)).

To do Proceed as follows:

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

7.2.6 IP Transit Network

When you enter a WAN partner in **X1000**, there are various options for indicating the IP address of the partner or 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 **X1000** and the WAN partner. You thus set up a virtual IP network during the connection, a so-called transit network. You do not need this setting normally, only 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.

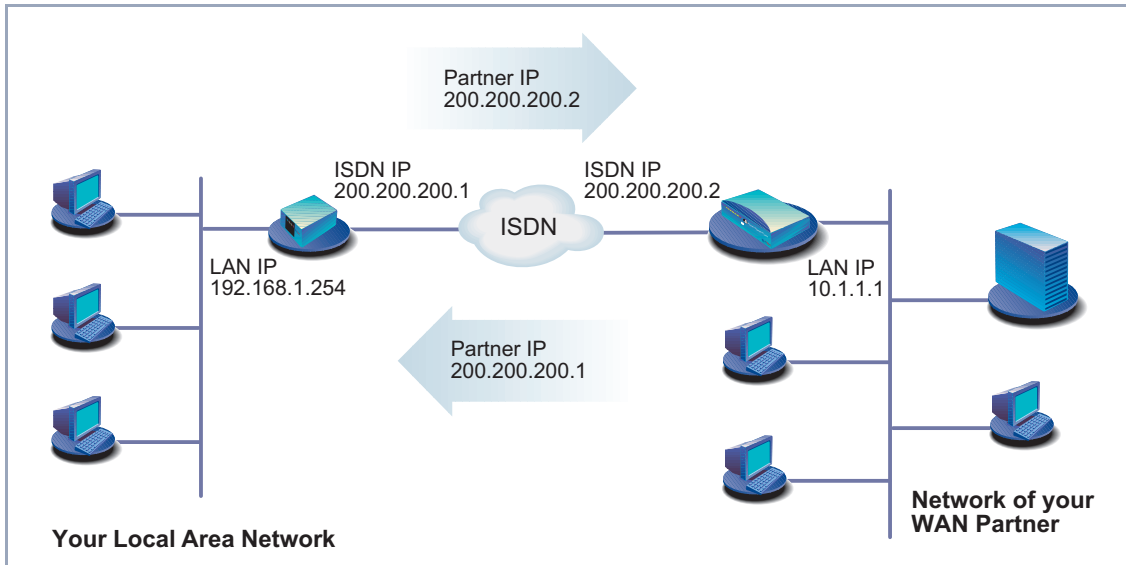


Figure 7-1: LAN-LAN link with transit network

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

Field	Meaning
IP Transit Network	Defines whether X1000 uses a transit network to the WAN partner.
Local IP Address	<p>IP address of X1000.</p> <p>Appears only for the following values of IP Transit Network: <i>no, dynamic client, dynamic server</i>.</p> <p>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.</p>
Local ISDN IP Address	ISDN IP address of X1000 in the transit network.
Partner's ISDN IP Address	WAN partner's ISDN IP address in the transit network.
Partner's LAN IP Address	IP address of LAN of your WAN partner or LAN IP address (host).
Partner's LAN Netmask	Your WAN partner's LAN netmask. If you make no entry, X1000 enters a default netmask for the net class used under Partner's LAN IP Address .

Table 7-22: **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>	X1000 receives its IP address from the WAN partner for the duration of the connection.
<i>dynamic server</i>	X1000 assigns the Remote WAN partner an IP address for the duration of the connection. In this case, X1000 must be configured as a dynamic IP address server, i.e. it has an IP address pool available (see chapter 7.1.1, page 202).
<i>no</i>	No transit network. This setting is adequate for most WAN partners.

Table 7-23: **IP Transit Network**

To do Proceed as follows:

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **IP**.
- Select **IP Transit Network**.
- Enter **Local IP Address**, if applicable (no transit network).
- Enter **Local ISDN IP Address** (transit network).
- Enter **Partner's ISDN IP Address**, if applicable (transit network).
- Enter **Partner's LAN IP Address**, if applicable.
- Enter **Partner's LAN Netmask**, if applicable.
- Press **SAVE**.

7.2.7 Transfer of DNS and WINS IP Addresses to WAN Partner

IP address = ? 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 your primary DNS, it tries to execute name resolution using its internal tables. If it cannot find the name, it asks a higher-level DNS that it knows.



If you use the DNS Proxy function, **X1000** can save previously resolved names and IP addresses in the 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 **X1000** itself. How to configure the DNS Proxy function is described in [chapter 7.3.2, page 259](#).

When you enter a WAN partner in **X1000**, you can define whether **X1000** sends or answers requests for WINS or DNS IP addresses.

Configuration is made in:

■ **IP ► STATIC SETTINGS**

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

Field	Meaning
Primary Domain Name Server	IP address of X1000 's first global Domain Name Server (DNS).
Secondary Domain Name Server	IP address of another global Domain Name Server.
Primary WINS	IP address of X1000 '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 7-24: **IP ► STATIC SETTINGS**

Field	Meaning
Dynamic Name Server Negotiation	In the event of dynamic name server negotiation, defines whether X1000 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 7-25: *WAN PARTNER* ➤ *EDIT* ➤ *IP* ➤ *ADVANCED SETTINGS*

The **Dynamic Name Server Negotiation** field contains the following selection options:

Possible Values	Meaning
<i>off</i>	X1000 does not send or answer requests for WINS or DNS IP 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"> ■ X1000 sends requests for name server addresses to the WAN partner if <i>dynamic client</i> is selected. ■ X1000 answers requests for name server addresses from the WAN partner if <i>dynamic server</i> is selected. ■ X1000 answers but does not send requests for name server addresses if <i>yes</i> or <i>no</i> is selected.
<i>client (receive)</i>	X1000 sends requests for name server addresses to the WAN partner.
<i>server (send)</i>	X1000 answers requests from the WAN partner for name server addresses.

Table 7-26: **Dynamic Name Server Negotiation**

WINS, DNS in the LAN If you have set up a DNS or WINS in your LAN, enter its IP address.

To do Proceed as follows if you have not made this entry already ([chapter 7.3.2, page 259](#)):

- Go to **IP** ► **STATIC SETTINGS**.
- Enter **Primary** or **Secondary Domain Name Server**, if applicable.
- Enter **Primary** or **Secondary WINS**, if applicable.
- Press **SAVE**.

Proceed as follows if you want **X1000** to report the DNS or WINS server IP addresses entered to the WAN partner (Server Mode) or if DNS/WINS addresses other than those in the LAN are to be used for connections to the WAN partner (Client Mode, e.g. for dialing into an Internet Service Provider).

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**.
- Select **Dynamic Name Server Negotiation**.
- Confirm with **OK**.
- Press **SAVE**.



If you do not have a Secondary DNS or 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.



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. Detailed information about this is given in [chapter 3.7.2, page 68](#).

7.2.8 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 [chapter 6.2.1, page 158](#)), 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. **X1000** 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. **X1000** can do both.

WAN partner If you negotiate to receive and/or send RIP packets from/to your WAN partner, **X1000** 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 **X1000**'s routing functionality.

RIP packets do not set up or hold ISDN connections.

Configuration is made in:

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

■ **CM-BNC/TP, ETHERNET ➤ 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 7-27: **WAN PARTNER ➤ EDIT ➤ IP ➤ ADVANCED SETTINGS** or **CM-BNC/TP, ETHERNET ➤ 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 7-28: **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**.
- Press **SAVE**.
- Press **SAVE**.
- Go to **CM-BNC/TP, ETHERNET** ➤ **ADVANCED SETTINGS**.
- Select **RIP Send**.
- Select **RIP Receive**.
- Press **SAVE**.

7.2.9 Compression

Data compression You can increase the data throughput and so reduce the connection costs by using **data compression**. **X1000** supports several options, depending on the **encapsulation** selected, e.g. **PPP** (see [chapter 6.2.1, page 158](#)):

■ **STAC**

The industry standard STAC data compression (Check Mode 3 in RFC 1974) implemented in **X1000** 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, **X1000** 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**

Field	Meaning
Compression	Defines the type of compression for connections to the WAN partner.

Table 7-29: **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).
<i>MPPC</i>	Not available in X1000 .

Table 7-30: **Compression**

Field	Meaning
Van Jacobson Header Compression	Enables VJHC.

Table 7-31: **WAN PARTNER ► EDIT ► IP ► ADVANCED SETTINGS**

STAC, MS-STAC Proceed as follows to set STAC or MS-STAC:

- Go to **WAN PARTNER ► EDIT**.
- Select **Compression**.
- Press **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**.
- Press **SAVE**.
- Press **SAVE**.

7.2.10 Proxy ARP (Address Resolution Protocol)

ARP requests The **Proxy ARP** function enables **X1000** to answer **ARP** requests from the LAN. That is, if a host in the LAN wants to set up a connection to another host in the LAN or to a WAN partner but doesn't know its hardware address, it sends a so-called ARP request into the network as a **broadcast**. This is actually a question to all those in the network: "What is the hardware address of host x?" If Proxy ARP is activated in **X1000** and the desired host can be reached over a defined WAN connection, **X1000** answers the ARP request with its own hardware address. This is sufficient for establishing the connection: The **data packets** are sent to **X1000**, which then forwards them to the desired host.

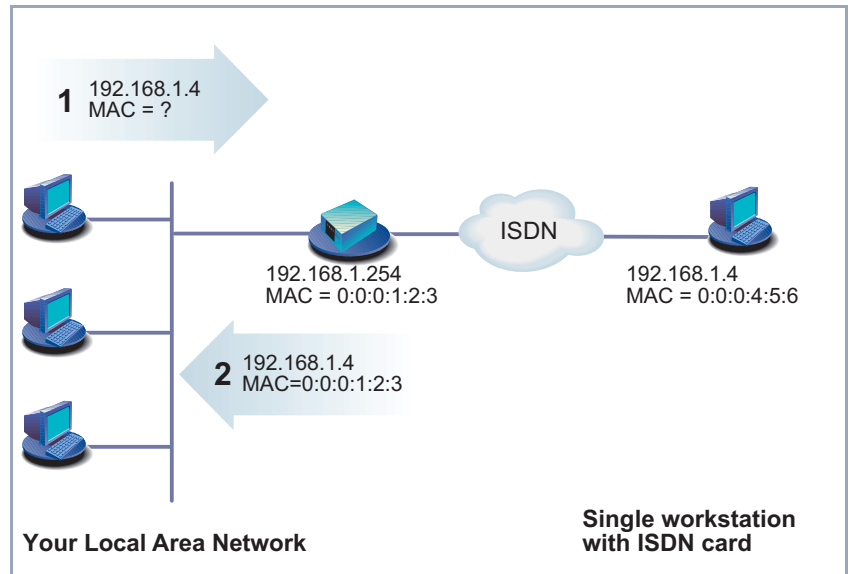


Figure 7-2: Proxy ARP

Configuration is made in:

- **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**
- **CM-BNC/TP, ETHERNET** ► **ADVANCED SETTINGS**

Field	Meaning
Proxy Arp	Enables X1000 to answer ARP requests.

Table 7-32: **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS** or **CM-BNC/TP, ETHERNET** ► **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 via the interface to the WAN partner.
<i>on (up or dormant)</i>	X1000 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). If this status is <i>dormant</i> , X1000 sets up a connection after the ARP request.
<i>on (up only)</i>	X1000 answers an ARP request only if the status of the connection to the WAN partner is up (active), i.e. a connection already exists to the WAN partner.

Table 7-33: **Proxy Arp**

Proxy ARP in **CM-BNC/TP, ETHERNET** ► **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 7-34: **Proxy Arp**

To do Proceed as follows:

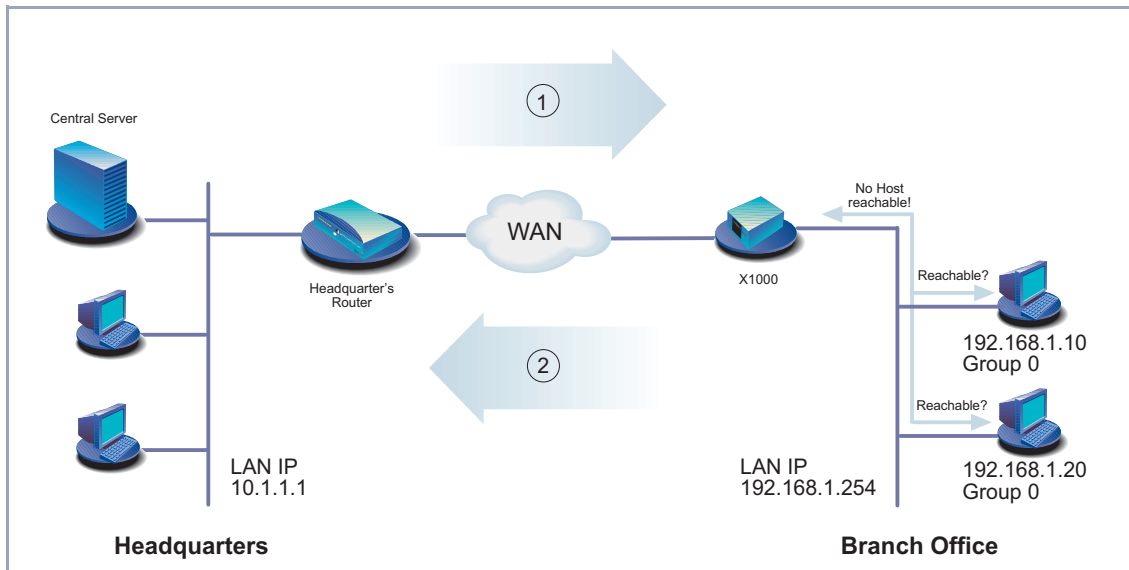
- Go to **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**.

- Select **Proxy Arp**.
- Confirm with **OK**.
- Press **SAVE**.
- Press **SAVE**.
- Leave **WAN PARTNER** with **EXIT**.
You have returned to the main menu.
- Go to **CM-BNC/TP, ETHERNET** ➤ **ADVANCED SETTINGS**.
- Select **Proxy Arp**.
- Press **SAVE**.
- Press **SAVE**.

7.2.11 Keepalive Monitoring

LAN-LAN connection If you have connected two (or more) LANs over a dialup connection, e.g. between the LAN of the head office and the LAN of a branch office as in [figure 7-3, page 250](#), a central server is frequently located in the LAN at the head office. If this central server is configured such that it regularly sets up WAN connections to **X1000** 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. the head office.

The following scenario illustrates Keepalive Monitoring:



1	Connection setup attempt	2	X1000 is "busy", no connection is possible
---	--------------------------	---	---

Figure 7-3: Keepalive Monitoring

Cutting costs The Keepalive Monitoring function enables you to configure **X1000** in the branch office so that unnecessary WAN connections from the head office to the branch office are avoided. **X1000** 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, connection setup by the central server is prevented by **X1000** deactivating the interface to the "head office" WAN partner. The result is that the line to the branch office appears to be busy if the central server at head office attempts to set up a connection. 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 the head office is not set up automatically as soon as one of the PCs to be monitored is switched on. The interface to the "head office" WAN partner is not activated, i.e. a connection cannot be set up to the head office, until **X1000** has registered that a PC can be reached. The amount of time that expires before **X1000** indicates that a PC can be reached again depends on the monitoring interval set (**Interval**).



The corresponding WAN partner, i.e. the head office, should be identifiable in **X1000** via CLID (Calling Line Identification). If this is not the case, Keepalive Monitoring may not function.

Configuration is made in **SYSTEM** ► **KEEPALIVE MONITORING** ► **ADD**:

Field	Meaning
Group	<p>Defines a group of hosts, whose reachability is to be monitored by X1000. 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 X1000.</p>
Interval	<p>Defines the time interval in seconds to be used for checking the reachability of hosts (default value: 300).</p> <p>The smallest time interval is used within a group, i.e. all the hosts in a group are checked by X1000 at the smallest time interval of the group.</p>
DownAction	<p>Defines how the status of the X1000 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>

Field	Meaning
FirstIndex	<p>Defines the first interface of an interface range in X1000, for which the action defined under DownAction is to be executed.</p> <p>Possible values: <i>10001 ... 15000</i> (default value: <i>10001</i>).</p> <p>Interfaces with indices from 10001 to 15000 are provided for dialup connections to WAN partners. The default value <i>10001</i> designates the interface to the first WAN partner configured in X1000 (dialup connection). The indices of other interfaces are given in the Software Reference.</p>
Range	<p>Defines the range of interfaces in X1000, for which the action defined under DownAction is to be executed.</p> <p>If you set FirstIndex = <i>10001</i> and Range = <i>0</i>, only the interface with the index 10001 is affected.</p> <p>If you set FirstIndex = <i>10001</i> and Range = <i>4999</i> (default value), the interfaces with indices 10001 to 15000 are affected.</p>

Table 7-35: **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 7-3, page 250](#):

- Go to **SYSTEM ► KEEPALIVE MONITORING**.
- Press **ADD** to add the first host that is to be monitored by **X1000** with Keepalive Monitoring.
- Enter **Group**: *0*.
- Enter **IPAddress**: *192.168.1.10*.

- Enter **Interval**, e.g. **300**.
- Select **DownAction**: **down**.
- Enter **FirstIfIndex**: **10001**.
- Enter **Range**, **4999**.
- Press **SAVE**.
- Press **ADD** to add the second host.
- Enter **Group**: **0**.
- Enter **IPAddress**: **192.168.1.20**.
- Enter **Interval**, e.g. **300**.
- Select **DownAction**: **down**.
- Enter **FirstIfIndex**: **10001**.
- Enter **Range**, **4999**.
- Press **SAVE**.

These settings ensure that **X1000** checks the reachability of hosts 192.168.1.10 and 192.168.1.20 at intervals of 300 s. If neither of the two hosts is reachable after three consecutive attempts, all **X1000** interfaces for dialup connections to WAN partners are deactivated. **X1000** continues to check the hosts at a time interval of 300 s and **X1000** activates the interfaces again as soon as at least one host is reachable again.

7.3 Basic IP settings

Here you will find a number of basic settings you can define in **X1000**:

- Deriving system time
- Name resolution (➤➤ **DNS**) in **X1000**
- ➤➤ **port** numbers
- ➤➤ **BOOTP** Relay Agent

The necessary configuration steps are explained below.

7.3.1 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 256).
- by setting it manually in **X1000** (see "[Setting the System Time Manually](#)", page 258).

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, X1000 interprets the input as the number of hours and converts it to the corresponding number of seconds automatically after you press SAVE.</p> <p>Note: If you select <i>ISDN</i> as Time Protocol, you must set the Time Offset to 0. In this case, you do not need a Time Offset because you automatically receive the correct time for the respective time zone.</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, X1000 interprets the input as the number of hours and converts it to the corresponding number of seconds automatically after you press 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 X1000 . Time Server is not needed if you set <i>ISDN</i> as Time Protocol .

Table 7-36: **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 7-37: **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).
- Press **SAVE**.
X1000 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 the IP address or host name for **Time Server**.
- Press **SAVE**.

X1000 now derives the system time via a time server. **X1000** adjusts its system time to the time set on the time server every 24 hours.



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 **X1000**.



If your PC has no fixed IP address but is assigned its IP address dynamically via ➤➤ **DHCP**, you cannot use your PC as a time server.

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 X1000 (date and time).
New Time:	For entering the new time to be used by X1000 (hours:minutes).
New Date:	For entering the new date to be used by X1000 (month/day/year).

Table 7-38: **SYSTEM** ➤ **TIME AND DATE**

Proceed as follows to enter the system time in **X1000** manually:



If a method for automatically deriving the time is defined in **X1000**, the values obtained in this way automatically have higher priority. That is, if **X1000** 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 **X1000**.

7.3.2 Name Resolution in **X1000** 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 or ping) or enter the ➤➤ **URL** "http://www.bintec.de" 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 (see [chapter 3.7.2, page 68](#)):**
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 IP addresses. This means connections to DNS are no longer needed to resolve these names. As the

HOSTS files must be updated on every 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 X1000

X1000 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 **X1000**.

This is how it works:

DNS Proxy DNS Proxy makes the tedious updating of HOSTS files on PCs in the LAN unnecessary, as you can enter **X1000** as DNS on the relevant PCs. DNS requests are passed by the PC to **X1000** 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 **X1000** as DHCP server.

Forwarding entries enable **X1000** to decide which DNS is to be used for the resolution of certain names. If, for example, you have configured two WAN partners in **X1000**, 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 **X1000** 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 **X1000**. This means that once a name has been resolved and is required again, **X1000** 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 saved 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 **X1000**. If you save frequently needed IP addresses in this way, **X1000** 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 **X1000**. 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 easily change a dynamic entry to a static entry "at the press of a button" in **IP** ► **DNS** ► **DYNAMIC CACHE** (see [table 7-43, page 271](#)).

Filter function By using negative static entries, you can limit name resolution in **X1000** 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 **X1000** 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 **X1000** or another name server (see [chapter 12.1, page 384](#)). 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 first if **X1000** cannot answer requests itself or with forwarding entries.

For local applications, the IP address of **X1000** or the loopback address (127.0.0.1) can be entered as global name server.

If necessary, **X1000** 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 **X1000** 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 **X1000** can be sent or the address of **X1000** itself. In the latter case, DNS requests from the DHCP clients are sent to **X1000**, which either answers these itself or passes them on if necessary (proxy function).

Exchanging DNS Addresses with WAN Partners

IPCP The same applies if dynamic negotiation of name servers is activated for the IP configuration of a WAN partner and **X1000** 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 **X1000** itself can also be sent for name server negotiations via IPCP to the WAN partner, who is the IP address client.

If **X1000** 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 **X1000**. These can be entered as global name servers in **X1000** and are thus available for future name resolutions.

Strategy for Name Resolution in X1000

A DNS request is handled by **X1000** 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 **X1000** 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

The configuration and monitoring of name resolution in **X1000** is set in:

- **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**

IP ► **STATIC SETTINGS** contains the following fields:

Field	Meaning
Domain Name	Defines X1000 's Domain Name.
Primary Domain Name Server	IP address of X1000 's first global Domain Name Server (DNS).
Secondary Domain Name Server	IP address of another global Domain Name Server.
Primary WINS	IP address of X1000 '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 7-39: **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. ■ <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 X1000 (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>

Field	Meaning
Default Interface	Defines the WAN partner to which a connection is normally set up for name server negotiation if other name resolution attempts were not successful.
DHCP Assignment	<p>Defines which name server addresses are sent to the DHCP client if X1000 is configured as DHCP server. Possible values:</p> <ul style="list-style-type: none"> ■ <i>none</i>: No name server address is sent. ■ <i>self</i> (default value): The address of X1000 is sent as name server address. ■ <i>global</i>: The addresses of the global name servers entered in X1000 are sent.
IPCP Assignment	<p>Defines which name server addresses are sent by X1000 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 X1000 is sent as name server address. ■ <i>global</i> (default value): The addresses of the global name servers entered in X1000 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 7-40: IP ➤ DNS

IP ► **DNS** ► **STATIC HOSTS** ► **ADD** contains the following fields:

Field	Meaning
Default Domain	The Domain Name of X1000 entered in IP ► STATIC SETTINGS is displayed.
Name	Host name, which is assigned the Address with this static entry. May also contain wild-cards (*) (only at the start of Name , e.g. <i>*.bintec.de</i>). If an incomplete name is entered without a dot, this is completed with ". Default Domain " after confirming with SAVE .
Response	Defines the type of static entry. Possible values: <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	(Only for Response = <i>positive</i>) IP address, which is assigned to Name .
TTL	Period of validity in seconds for the assignment of Name to Address (only relevant if Response = <i>positive</i>). This value is displayed in the TTL field (Time To Live) if X1000 sends a corresponding DNS record. Default value: <i>86400</i> (= 24 h)

Table 7-41: **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.
Default Domain:	The Domain Name of X1000 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. <i>*.bintec.de</i>). 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 from X1000 for Name is answered with a DNS record, this contains a TTL field (= Time To Live in s), whose value is not normally changed by X1000 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 7-42: **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.
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.

Field	Meaning
STATIC	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.

Table 7-43: **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 TTL 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 7-44: **IP** ► **DNS** ► **ADVANCED SETTINGS...**

IP ► DNS ► GLOBAL STATISTICS... contains the following fields (the menu is updated every second):

Field	Meaning
Received DNS Packets	Displays the number of DNS packets received, including the answer packets for forwarded requests.
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 7-45: **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 X1000 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 7-46: **WAN PARTNER** ► **EDIT** ► **IP** ► **ADVANCED SETTINGS**

The **Dynamic Name Server Negotiation** field contains the following selection options:

Possible Values	Meaning
<i>off</i>	X1000 does not send or answer requests for name server addresses.
<i>yes</i>	The response is linked to the mode for issuing/receiving an IP address (setting in WAN PARTNER ► EDIT ► IP under IP Transit Network): <ul style="list-style-type: none"> ■ X1000 sends requests for name server addresses to the WAN partner if <i>dynamic client</i> is selected. ■ X1000 answers requests for name server addresses from the WAN partner if <i>dynamic server</i> is selected. ■ X1000 answers but does not send requests for name server addresses if <i>yes</i> or <i>no</i> is selected.
<i>client (receive)</i>	X1000 sends requests for name server addresses to the WAN partner.

Possible Values	Meaning
<i>server (send)</i>	X1000 answers requests from the WAN partner for name server addresses.

Table 7-47: Dynamic Name Server Negotiation

Configuration Procedure

To do Proceed as follows to configure name resolution with DNS Proxy in **X1000**:

Name resolution in X1000 If applicable, first enter the global name servers in **X1000**:

- 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.

- Press **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**.
- Press **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**.
- Press **SAVE**.

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**.
- Press **SAVE**.
- Select **EXIT**.
- Press **SAVE**.

X1000 ↔ **WAN partner**

Proceed as follows if you would like to configure a WAN partner so that the address of a name server is sent by **X1000** to the WAN partner or from the WAN partner to **X1000**, if applicable:

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **IP** ➤ **ADVANCED SETTINGS**.
- Select **Dynamic Name Server Negotiation**.
Make the required setting here.

- Confirm with **OK**.
- Press **SAVE**.

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.

7.3.3 Port Numbers

What is a ➤➤ port?

X1000 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 **X1000**. This addresses the relevant application. Ports are only used in the TCP and UDP protocols.

X1000 forwards incoming ➤➤ **data packets** for the desired application to the port with the corresponding number. This addresses the relevant **X1000** application and the incoming data can be processed.

You can define important port numbers in **IP ➤ STATIC SETTINGS**:



As the settings are normally correct, you should only make changes here if necessary.

Field	Meaning
Remote CAPI Server TCP Port	Port number for ►► Remote CAPI connections: 2662 (defined by IANA, www.iana.com).
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.
HTTP TCP Port	Port number for HTTP Requests. Default value: 80. HTTP TCP Port = 0 disables access to X1000 's HTTP status page (see chapter 8.1.4, page 302).

Table 7-48: **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**.
- Press **SAVE**.

7.3.4 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 Re-

lay Agent. The agent forwards all requests and responses between the client and server via a WAN connection to this server.

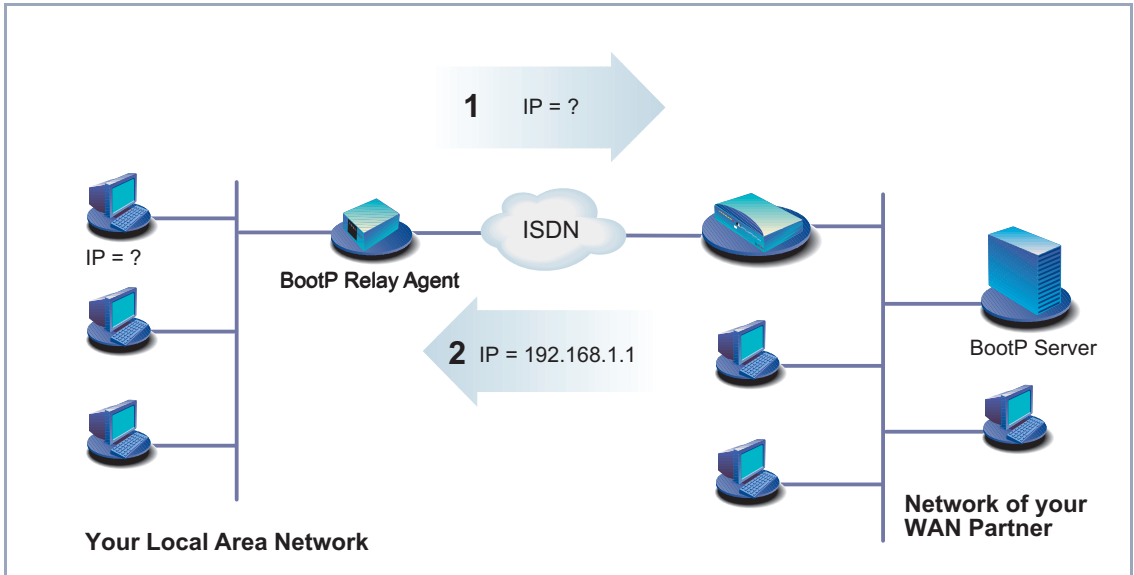


Figure 7-4: **X1000** as BOOTP Relay Agent

Configuration is made in **IP** ➤ **STATIC SETTINGS**:

Field	Meaning
BOOTP Relay Server	IP address of the BOOTP server.

Table 7-49: **IP** ➤ **STATIC SETTINGS**

To do Proceed as follows:

- Go to **IP** ➤ **STATIC SETTINGS**.
- Enter **BOOTP Relay Server**.
- Press **SAVE**.



If an ISDN connection is needed for the connection between the BOOTP server and BOOTP client, you must configure an appropriate WAN partner (see [chapter 6.2.1, page 158](#)).

7.4 IPX Settings

The >> **IPX** Protocol (Internet Packet Exchange Protocol) is a network protocol that is used mainly in Novell networks. Novell >> **clients** and Novell >> **servers** can use IPX to communicate via LAN/WAN connections.

The configuration steps necessary for IPX connections are explained below:

- General Settings
- Configuring the LAN Interface
- Configuring WAN Partners

7.4.1 General Settings

Here you will find the global parameters for IPX. These settings apply to all IPX connections of **X1000**.

The configuration is made in **IPX**:

Field	Meaning
Local System Name	IPX system name of X1000 . This name may comprise upper case letters, numbers and the characters : / -
Internal Network Number	X1000 's internal network number. This value must be unique among all the network numbers and normally comprises the last four bytes of X1000 's MAC address . Change this value only if it is already used somewhere else in the network.
Enable IPX Spoofing	Enables and disables NCP session watchdog spoofing and handling of "broadcast message waiting" packets. Possible values: <ul style="list-style-type: none"> <input type="checkbox"/> <i>yes</i>: low cost for IPX-WAN connections <input type="checkbox"/> <i>no</i>
Enable SPX Spoofing	Enables and disables spoofing of SPX session watchdog packets. Possible values: <ul style="list-style-type: none"> <input type="checkbox"/> <i>yes</i>: low cost for SPX sessions over WAN connections <input type="checkbox"/> <i>no</i>
NetBIOS Broadcast Replication	Defines how X1000 handles NetBIOS packets.

Table 7-50: **IPX**

NetBIOS Broadcast Replication contains the following selection options:

Possible Values	Meaning
<i>yes</i>	All NetBIOS hosts in the network can access each other, even if WAN connections must be set up frequently. Cost-intensive!
<i>no</i> <i>on LAN only</i>	NetBIOS hosts in the LAN can only access each other if they do not need WAN connections to be set up. Low cost.

Table 7-51: **NetBIOS Broadcast Replication**

To do Proceed as follows:

- Go to **IPX**.
- Enter **Local System Name**.
- Enter **Internal Network Number** (only if necessary!).
- Activate **Enable IPX Spoofing**, if applicable.
- Activate **Enable SPX Spoofing**, if applicable.
- Select **NetBIOS Broadcast Replication**, e.g. *on LAN only*.
- Press **SAVE**.

7.4.2 Configuring the LAN Interface

The next step is to configure **X1000**'s LAN interface to the IPX network. The LAN interface is the physical interface to the local network. In the next menu, you tell the router the network number of the IPX LAN to which it is connected. As long as **X1000** does not have this information, it cannot actively participate in its own IPX LAN.

The configuration is made in **CM-BNC/TP, ETHERNET**.

Field	Meaning
Local IPX NetNumber	The IPX network number of the LAN to which X1000 is connected.
Encapsulation	Defines the type of header to be used for IPX packets in the LAN connected. Possible values: <ul style="list-style-type: none"> <input type="checkbox"/> <i>none</i> <input type="checkbox"/> <i>Ethernet II</i> <input type="checkbox"/> <i>Ethernet 802.2 LLC</i> <input type="checkbox"/> <i>Ethernet SNAP</i> <input type="checkbox"/> <i>Ethernet NOVELL 802.3</i>

Table 7-52: **CM-BNC/TP, ETHERNET**

To do Proceed as follows:

- Go to **CM-BNC/TP, ETHERNET**.
- Enter **Local IPX NetNumber**.
- Select **Encapsulation**.
- Press **SAVE**.

7.4.3 Configuring WAN Partners

If the connection to one or more WAN partners is implemented with the IPX protocol, you must define a number of IPX-specific settings for the WAN partner.

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

Field	Meaning
Enable IPX	Enables IPX for the WAN partner. Possible values: <input type="checkbox"/> <i>yes</i> <input type="checkbox"/> <i>no</i>
IPX NetNumber	IPX network number of the WAN connection. This is required by some IPX routers. The zero is sufficient for connections between X1000s .
Send RIP/SAP Updates	Defines how often ►► RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) packets are sent by X1000 to the WAN partner. In IPX networks, RIP and SAP packets are sent as ►► broadcasts to connected networks to provide information about current routes and services. The data flow caused by this is acceptable in the LAN, but you must make a setting here to control the data flow for networks connected via WAN connections.
Update Time	Defines the time intervals at which periodic updates are sent.
Age Multiplier	If routes and services entered are not renewed during Update Time x Age Multiplier , they are deleted. This prevents accumulation of unnecessarily large numbers of routes and services that are not used.

Table 7-53: **WAN PARTNER** ► **EDIT** ► **IPX**

The **Send RIP/SAP Updates** field is for defining how often **RIP** and SAP packets are sent by **X1000** to the WAN partner. The field contains the following selection options, which are explained with the aid of a table:

Possible values for Send RIP/SAP Updates	New connection opened?	Update the existing tables?	Periodic update?	Remarks
<i>off</i>	never	no	no	All routes and services must be entered statically.
<i>triggered + piggyback (on changes, only if link active)</i>	only for changes	yes	yes	This is the default setting, which is sufficient in most cases.
<i>triggered (on changes)</i>	only for changes	yes	no	Less data traffic than <i>triggered + piggyback</i> , but also less reliable.
<i>piggyback (only if link active)</i>	never	yes	yes	At least 1 static route and 1 static service must be entered for the WAN partner.
<i>passive triggered (on changes only if link active)</i>	never	yes	no	At least 1 static route and 1 static service must be entered for the WAN partner.
<i>timed update (always)</i>	always	yes	yes	Cost-intensive!

Table 7-54: **Send RIP/SAP Updates**

To do Proceed as follows:

- Go to **WAN PARTNER** ➤ **EDIT** ➤ **IP**.
- Select **Enable IPX**: **yes**.
- Enter **IPX NetNumber**, e.g. **0**.
- Select **Send RIP/SAP Updates**.
- Enter **Update Time**, if applicable.

- Enter **Age Multiplier**, if applicable.
- Confirm with **OK**.
- Press **SAVE**.

7.5 Extra License Functions

This chapter briefly describes the **X1000** features you can activate with extra licenses.

7.5.1 Virtual Private Network (VPN) and Encryption

X1000 can provide a VPN using the PPTP (Point to Point Tunneling Protocol). This provides safe (encrypted) transmission of data over WAN connections, e.g. over the Internet. It could be used, for example, to provide field service staff with low-cost access to data in the company network via Internet and laptop (dialing in via a local Internet Service Provider).

A VPN license implicitly includes the DES and Blowfish encryption processes (see [chapter 8.3.1, page 336](#)).

You can find detailed information and configuration instructions (with examples) in the **Software Reference**.

7.5.2 IPSec (Internet Protocol Security)

The IPSec security standard enables you to exchange IP-based data securely over public networks (e.g. the Internet).

Detailed information and configuration instructions can be found in the **IPSec Reference Manual**, which you receive together with your IPSec license, or in the **Software Reference**.

7.5.3 Leased Lines

With an extra license, you can also use **X1000**'s ISDN BRI interface for leased lines and not just for dialup connections.

You will find configuration instructions in [chapter 6.1.4, page 138](#) and [chapter 6.2, page 156](#).

8 Security Mechanisms

SAFERNET The **X1000** 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
- Access security
- Line tapping security
- Special features
- Checklist

8.1 Activity Monitoring

A major requirement for a high degree of security is the possibility of monitoring all activities on and over the router. BinTec Communications AG provides a variety of facilities for this purpose.

8.1.1 Syslog Messages

All major events on **X1000**'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 information to debug). The logged data are saved by **X1000** 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 internally saved syslog messages are lost when you restart **X1000**.



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 distribute to various files depending on the contents (see **BRICKware for Windows**).

Settings for syslog messages are made in:

- **SYSTEM**
- **SYSTEM ▶ EXTERNAL SYSTEM LOGGING**
- **CM-BNC/TP ETHERNET ▶ ADVANCED SETTINGS**
- **WAN PARTNER ▶ EDIT ▶ IP ▶ ADVANCED SETTINGS**

The following tables list the fields contained in the relevant menus:

Field	Meaning
Syslog Output on Serial Console	<p>Enables the display of syslog messages on the PC connected to the serial interface of X1000. Use this setting only if you make a fault analysis, as a large output over the serial console adversely affects the throughput of the other interfaces. Possible values:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>yes</i> <input type="checkbox"/> <i>no</i>
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"> <input type="checkbox"/> <i>emerg</i>: emergency messages (highest priority) <input type="checkbox"/> <i>alert</i>: alert messages <input type="checkbox"/> <i>crit</i>: critical messages <input type="checkbox"/> <i>err</i>: error messages <input type="checkbox"/> <i>warning</i>: warning messages <input type="checkbox"/> <i>notice</i>: notice messages <input type="checkbox"/> <i>info</i>: info messages <input type="checkbox"/> <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	<p>Maximum number of syslog messages saved in X1000. (possible values: 0 - 1000).</p>

Table 8-1: **SYSTEM**

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.
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.

Table 8-2: **SYSTEM** ➤ **EXTERNAL SYSTEM LOGGING**

Field	Meaning
IP Accounting	For saving accounting messages for ➤➤ TCP , ➤➤ UDP and ICMP sessions. Possible values: <i>on</i> , <i>off</i> .

Table 8-3: **CM-BNC/TP ETHERNET** ➤ **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 8-4: **WAN PARTNER** ➤ **ADD** ➤ **IP** ➤ **ADVANCED SETTINGS**

To do Make the desired settings for syslog messages as follows:

- Go to **SYSTEM**.
- Select **Syslog Output on Serial Console**.
- Select **Message Level for Syslog Table**.
- Enter **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 **Level**.
- Select **Facility**.
- Select **Type**.

IP accounting at LAN Proceed as follows to activate IP accounting for a LAN partner. **X1000** then generates and records accounting messages for the selected LAN partner from TCP, UDP and ICMP sessions:

- Go to **CM-BNC/TP ETHERNET** ➤ **ADVANCED SETTINGS**.
- Activate **IP Accounting** with *on*.

IP accounting at WAN Proceed as follows to activate extended IP accounting. This saves accounting messages from TCP, UDP and ICMP sessions in **X1000**:

- 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 in **X1000**:

X1000 Setup Tool		BinTec Communications AG
[MONITOR][MESSAGE]: Syslog Messages		MyX1000
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 **X1000**.

For interpretation of syslog messages: see the **Software Reference**.

8.1.2 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 (Credits)
- Interface statistics (comparative display of several interfaces)
- ➤➤ **TCP/IP** statistics
- Syslog messages (see [chapter 8.1.1, page 290](#))

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.

X1000 Setup Tool		BinTec Communications AG				
[MONITOR][ISDN CALLS]: ISDN Monitor - Calls		MyX1000				
Dir	Remote Name/Number	Charge	Duration	Stack	Channel	State
in	2		2910	0	B1	active
out	3		106	0	B2	active
(c)alls		(h)istory		(d)etails		(s)tatistics
						(r)elease

This menu also offers you other options:

- 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.
- Select **c** to display the list of existing ISDN connections again.

Credits Based Accounting System (Credits)

You can display the credits status for ISDN connections or PPPoE connections.

ISDN connections

Proceed as follows for ISDN connections:

- 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.

X1000 Setup Tool		BinTec Communications AG	
[MONITOR][ISDN CREDITS][STAT]: Monitor isdnlogin Credits		MyX1000	
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 8.1.3, page 299](#).

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 **X1000**'s interfaces:

➤ Go to **MONITORING AND DEBUGGING** ➤ **INTERFACES**.

The values for two interfaces are displayed side by side.

X1000 Setup Tool		BinTec Communications AG			
[MONITOR][INTERFACE]: Interface Monitoring		MyX1000			
Interface Name	en1	PROVIDER		dormant	
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. You can find the meaning of the MIB variables in the **MIB Reference**.

X1000 Setup Tool		BinTec Communications AG	
[MONITOR][IP]: IP Statistics		MyX1000	
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			

- 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.

8.1.3 Credits Based Accounting System

Credits **X1000's** Credits Based Accounting System enables you to control the charges billed. This means you can keep the effects of possible configuration errors within limits. The system also enables you to define the maximum number of connections allowed in a certain period of time. You can make settings for certain subsystems (➤➤ **PPP**, ➤➤ **CAPI**, ➤➤ **ISDN Login**) to define the number of connections, the connection time and the ISDN charges billed. If the defined limit is exceeded, **X1000** 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 **X1000** off and then switch it on again (i.e. reboot).

Configuration is made in **CREDITS** ▶ **ISDN CREDITS** or **CREDITS** ▶ **xDSL CREDITS** ▶ **PPPoE CREDITS**.

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.
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.

Field	Meaning
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 8-5: **CREDITS** ► **ISDN CREDITS** resp. **CREDITS** ► **xDSL CREDITS** ► **PPPoE CREDITS**

To do Proceed as follows to configure a Credits Based Accounting System for ISDN connections:

- Go to **CREDITS** ► **ISDN CREDITS**.
- Select a 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.
- Press **SAVE**.

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**.

8.1.4 HTTP Status Page


Every BinTec router is equipped with an internal home page, the so-called HTTP status page. You can use this together with an Internet browser (e.g. Netscape Navigator, Internet Explorer) to display the status of **X1000**. This enables all users of the **X1000** LAN to take a look at the status of the router, provided they know the password for the user name `http`.



Please note: HTTP pages are usually stored in the cache memory of the browser. This means they can possibly be read by other users at the same workspace and may also be visible at proxy ➤➤ **servers** involved.

- Enter the ➤➤ **URL** `http://<System Name>` in your browser. (You can also enter **X1000's** IP address instead of the name.)

The HTTP status page of the BinTec router with the system name <System Name> or with the IP address entered is displayed.

System Information: MyX1000 

System description

Type of System	X1000
System Name	MyX1000
Location	Germany
Contact	BINTEC
Software	V.5.1 Rev.4 from 2000/02/29 00:00:00
System state	up and running for 0d 0h 16min

Software options

ip	tunneling	stac	capi	ipx
o.k.	o.k.	o.k.	o.k.	o.k.

Hardware Interfaces

Slot 1	Fast Ethernet	o.k.	
Slot 2	ISDN S0	o.k.	used 0, available 2

You can [update](#) this page, see a list of [system tables](#), or [login](#) to the router.

For more information about BinTec products see <http://www.bintec.de>

Figure 8-1: HTTP status page

The HTTP status page contains three tables:

- **System description**
In addition to the version of the system software, this also lists information from the MIB table **system**, such as **System name** and **Contact**. If a valid e-mail address is given under **Contact**, this is shown underlined.
- **Software options**
This table lists information from the MIB table **biboAdmLicInfoTable** and displays the status of **X1000**'s subsystems.
- **Hardware interfaces**
This table displays the LAN and WAN interface of **X1000**. The third column of the table provides information on the current status of the physical interfaces with the following possible values:

Interface	State	Possible cause
LAN (Slot 1)	o.k.	Normal operation.
	inactive	LAN cable is not connected.
WAN (Slot 2)	o.k.	Displays the number of available B-channels and currently used B-channels.
	unconfigured	ISDN cable is not connected or a wrong ▶▶ D-channel protocol is entered.

Table 8-6: Interface states

The HTTP status page contains a number of links:

- **update**
Click update to update the status page.
- **login**
Click login to log in to the associated BinTec router via **▶▶ telnet**.
- **www.bintec.net**
Use this link to access BinTec's WWW server with the latest information on products and the current system software and documentation for **X1000**.

- system tables

Click system tables to display a list with all the **X1000** MIB tables. Clicking a table name lists the variables contained in the table.



If you don't want to display **X1000**'s HTTP status page, enter 0 as the port number of the http port:

- Go to **IP** ➤ **STATIC SETTINGS**.
- Enter **HTTP TCP port: 0**.
- Press **SAVE**.

8.1.5 Activity Monitor

What do you need it for? The **Activity Monitor** enables Windows users to monitor the activities of **X1000**. 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 **X1000**'s interfaces is possible.

How does it work? A Status Demon collects information on **X1000** 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 time interval, which can be adjusted individually to values from 1 - 60 seconds. All physical interfaces and up to 100 virtual interfaces can be monitored, provided the packet size of 4096 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 5.1.1 and higher.

Activate the **Activity Monitor** as follows:

- Appropriately configure the **X1000(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 X1000 sends the UDP packets.</p> <p>The default value <i>255.255.255.255</i> 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 usually sent every 5 seconds).</p>
Client UDP Port	<p>Port number for Activity Monitor (default value: <i>2107</i>, registered by IANA - Internet Assigned Numbers Authority).</p>
Type	<p>Type of information sent in the UDP packets to the Windows application. Possible values:</p> <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)	<p>Update interval in seconds. Possible values: <i>0</i> to <i>60</i> (default value: <i>5</i>).</p>

Table 8-7: **SYSTEM ► EXTERNAL ACTIVITY MONITOR**

To do Proceed as follows:

- Go to **SYSTEM ► EXTERNAL ACTIVITY MONITOR**.
- Enter **Client IP Address**, e.g. the IP address of your PC.
- Enter **Client UDP Port**: *2107*.

- Select **Type**, e.g. *physical_virt*.
- Enter **Update Interval (sec)**, e.g. *5*.
- Press **SAVE**.

8.2 Access Security

There are several ways of restricting logging in and access to **X1000** to authorized users only.

8.2.1 Logging In

Password Logging in to **X1000** can be done in several ways as described in [chapter 5, page 105](#), 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 "[Changing the password](#)", [page 120](#).

- Change the passwords to prevent unauthorized access to **X1000**.
- Also make sure that unauthorized persons do not have access to the **X1000** power supply, serial console and ➤➤ **Ethernet** connection.

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 **X1000** 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 12.1, page 384](#)).



If you carry out a software update (see [chapter 9.3, page 355](#)), 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.

8.2.2 Checking the Calling Party Number

CLID **X1000** 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**). **X1000** 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).

If you want **X1000** 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**.

8.2.3 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 6.2.1, page 158](#) and [chapter 7.1.3, page 208](#).

8.2.4 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. **X1000** 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 8-8: **WAN PARTNER** ➤ **EDIT** ➤ **ADVANCED SETTINGS**

Callback offers the following selection options:

Possible Values	Meaning
<i>no</i>	X1000 does not call back.
<i>expected (awaiting call-back)</i>	X1000 calls the WAN partner to initiate call-back.
<i>yes (PPP negotiation)</i>	X1000 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)</i>	X1000 calls back after approximately four seconds, if requested to by the WAN partner.
<i>yes (PPP negotiation, callback optional)</i>	Corresponds to the value <i>yes (PPP negotiation)</i> , but contains an abort option. The Microsoft client has the option of aborting callback and maintaining the initial connection to X1000 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 X1000 .
<i>yes</i>	X1000 calls back immediately, if requested to by the WAN partner.

Table 8-9: **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 **Callback**.
- Confirm with **OK**.

8.2.5 Closed User Group

X1000 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.
- Confirm with **OK**.

8.2.6 Access to Remote CAPI

The special features offered by BinTec routers include implementation of the ➤➤ **Remote CAPI** and Remote TAPI programming interfaces (only for PABX devices). 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.

CAPI user concept By using BinTec's ➤➤ **CAPI** user concept, you can make sure that only users authenticated by user name and password can access **X1000**'s Remote CAPI interface (see [chapter 7.1.2, page 204](#)).

Filters You can also prevent unauthorized access by defining filters (see [chapter 8.2.8, page 317](#)) and local filters (see [chapter 8.2.9, page 330](#)).

8.2.7 NAT (Network Address Translation)

➤➤ **NAT** is a simple-to-operate procedure that can be used for three purposes:

- 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.

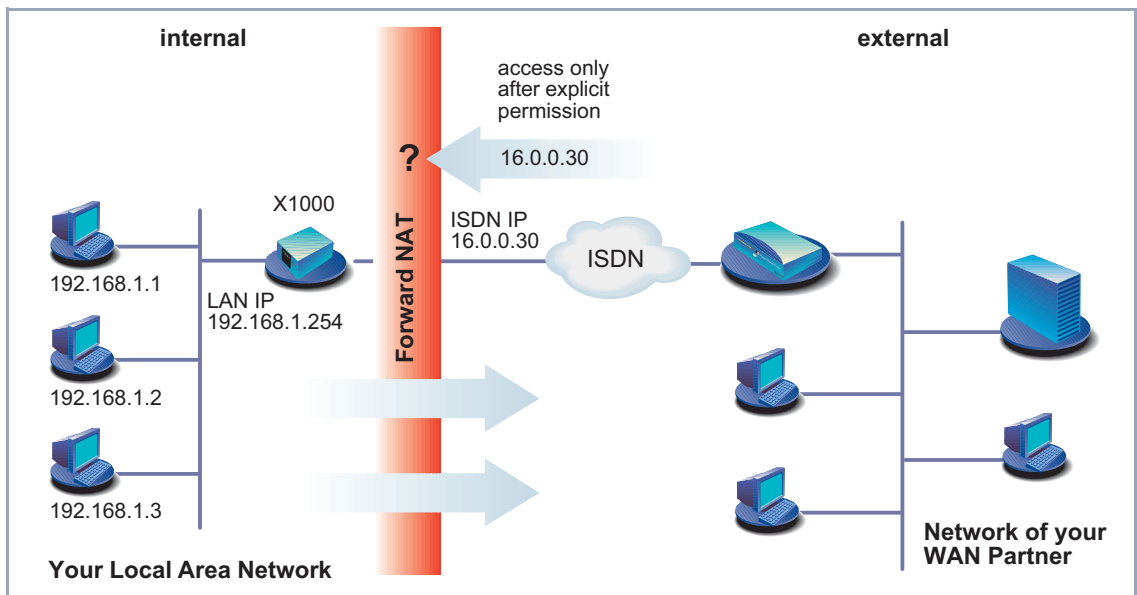


Figure 8-2: Forward NAT

- 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!

NAT always refers to an interface. **X1000**'s LAN side is always referred to as "internal", the WAN partner as "external".

You will find more information on NAT in the **Software Reference**.

Configuration is made in **IP ► NETWORK ADDRESS TRANSLATION**.

Activate NAT for an **X1000** interface with **IP ► NETWORK ADDRESS TRANSLATION ► EDIT**.

Field	Meaning
Network Address Translation	Defines the type of NAT for the selected interface. Possible values: <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.

Table 8-10: **IP ► NETWORK ADDRESS TRANSLATION ► EDIT**

You can explicitly allow a NAT interface certain IP connections to a certain internal host in **IP** ➤ **NETWORK ADDRESS TRANSLATION** ➤ **EDIT** ➤ **ADD**:

Field	Meaning
Service	<p>Service allowed for connections to the host defined under Destination. Possible values:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>ftp</i> <input type="checkbox"/> <i>telnet</i> <input type="checkbox"/> <i>smtp</i> <input type="checkbox"/> <i>domain/udp</i> <input type="checkbox"/> <i>domain/tcp</i> <input type="checkbox"/> <i>http</i> <input type="checkbox"/> <i>nntp</i> <input type="checkbox"/> <i>user defined</i>: If you do not use any of the predefined services. Enter the required values under Protocol and Port to define a service.
Protocol	<p>Only for Service = <i>user defined</i>. Defines the protocol allowed. Possible values:</p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>icmp</i> <input type="checkbox"/> <i>tcp</i> <input type="checkbox"/> <i>udp</i> <input type="checkbox"/> <i>gre</i> <input type="checkbox"/> <i>esp</i> <input type="checkbox"/> <i>ah</i> <input type="checkbox"/> <i>l2tp</i>

Field	Meaning
Port (-1 for any)	Only for Service = user defined . Defines the port allowed. Entering -1 allows any port for the protocol . If you specify the port, the entry must agree with the port number of the destination host in the LAN.
Destination	IP address of the host in the LAN.

Table 8-11: **IP ► NETWORK ADDRESS TRANSLATION ► EDIT ► ADD**

To do 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**.
- Select **Network Address Translation**, e.g. **on**.
This activates NAT for the selected interface.
- Press **SAVE**.



An entry takes effect as soon as you confirm it here with **SAVE**. Never forget this, especially if you are configuring NAT from a remote host, e.g. with telnet!

Proceed as follows to allow certain connections for a NAT interface to a certain host in the LAN:

- Go to **IP ► NETWORK ADDRESS TRANSLATION ► EDIT**.
- Add an entry with **ADD** or select an existing entry and confirm with **Return**.
- Select **Service**.
- Select **Protocol**, if applicable.
- Enter **Port (-1 for any)**, if applicable.
- Enter **Destination**.
- Press **SAVE**.

- Repeat these steps to define several entries for the selected NAT interface.

8.2.8 Filters (Access Lists)

IP filters (➤➤ **Access Lists**) in **X1000** are based on a concept of ➤➤ **filters**, rules and so-called chains. IP filters respond to incoming data packets, which means they can allow or deny access to **X1000** 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 are telling **X1000**: "Watch out for all data packets that match the following: ...".

Rule You use a rule to tell **X1000** what to do with the data packets it has 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 shared use of filters is possible and practicable.

Interface You can also assign a rule chain individually to each **X1000** interface.

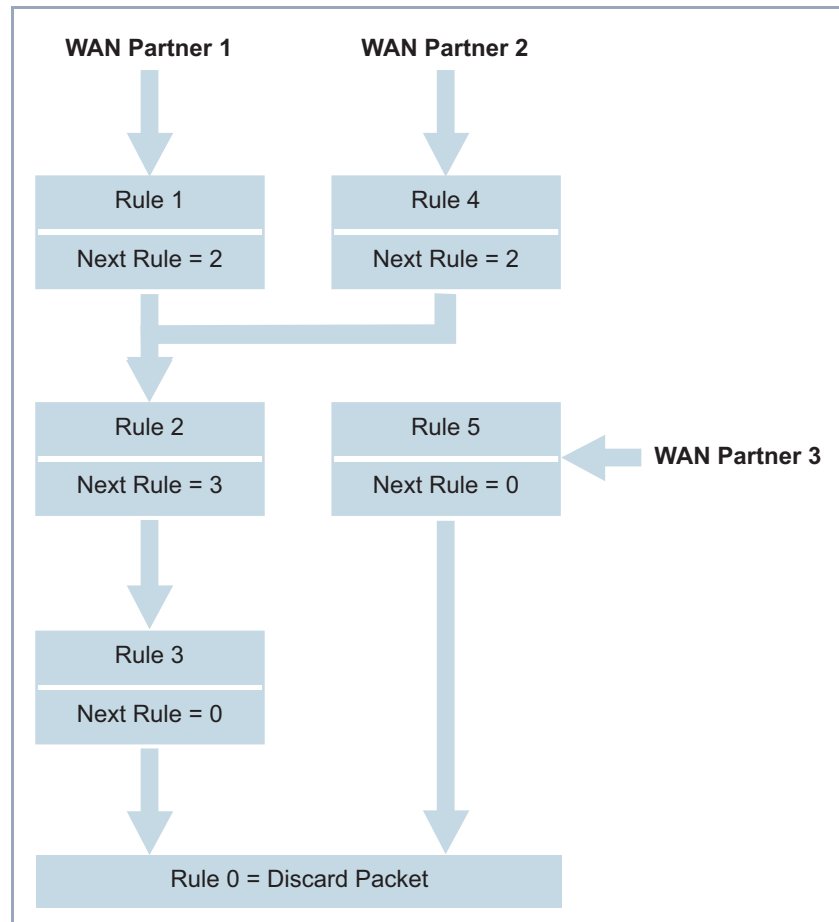


Figure 8-3: Rule chains for various interfaces

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. X1000 automatically issues a number to newly defined filters.
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.
Connection State	If Protocol = <i>tcp</i> , you can define a filter based on the status of the TCP connection. Possible values: <i>established</i> : All TCP packets that would not open any new TCP connection on routing over X1000 match the filter. <i>any</i> : All TCP packets match the filter.
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.
Source / Destination Address	Source and destination IP address of the data packets that match the filter.
Source / Destination Mask	The combination of Address and Mask defines a range of IP addresses that match the filter.
Source / Destination Port	Range of port numbers that match the filter.

Field	Meaning
Specify Port	If Source / Destination Port = <i>specify</i> or <i>specify range</i> : Enter port numbers or range of port numbers.
Type of Service (TOS)	Type of Service
TOS Mask	Mask for Type of Service

Table 8-12: 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.
<i>clients 2 (32768..65535)</i>	Port numbers: 32768 ... 65535.
<i>unpriv (1024..65535)</i>	Port numbers: 1024 ... 65535.

Table 8-13: **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 dynamically by ►► clients and ►► servers and have no permanent meaning (with the exception of 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 8-14: Port number ranges

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
➤➤ 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 8-15: 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:

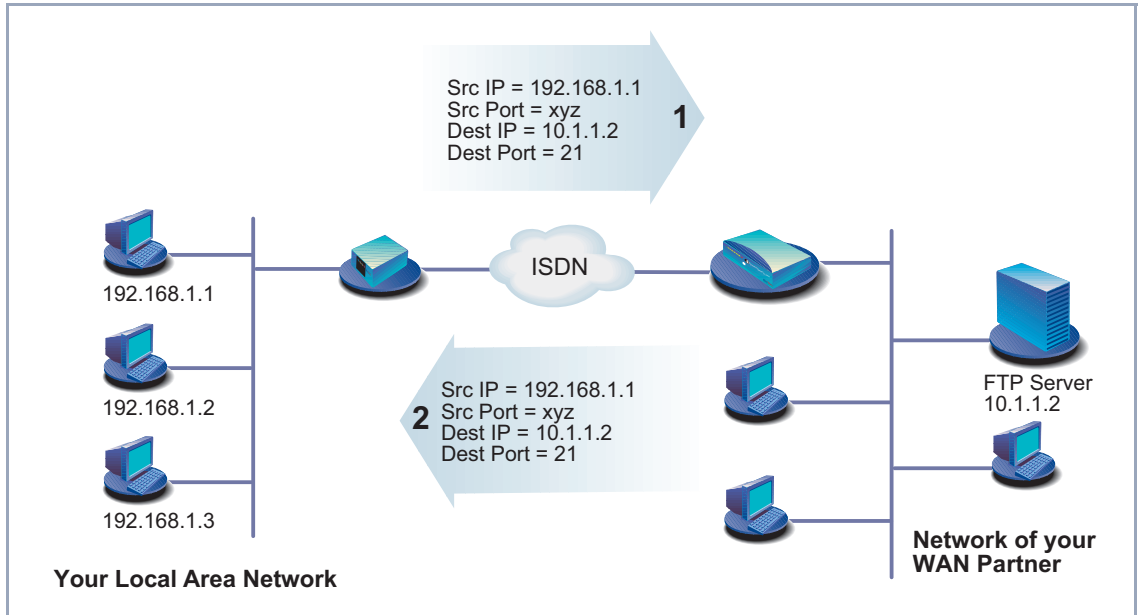


Figure 8-4: Example: FTP connection

You can define rules in **IP** ► **ACCESS LISTS** ► **RULES**:

Field	Meaning
Index	Cannot be changed. X1000 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 8-16: **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 8-17: **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 8-18: **IP** ▶ **ACCESS LISTS** ▶ **RULES** ▶ **REORG**

If you reorganize such a chain, **X1000** renumbers the remaining rules according to the selection in **Index of Rule that gets Index 1**:

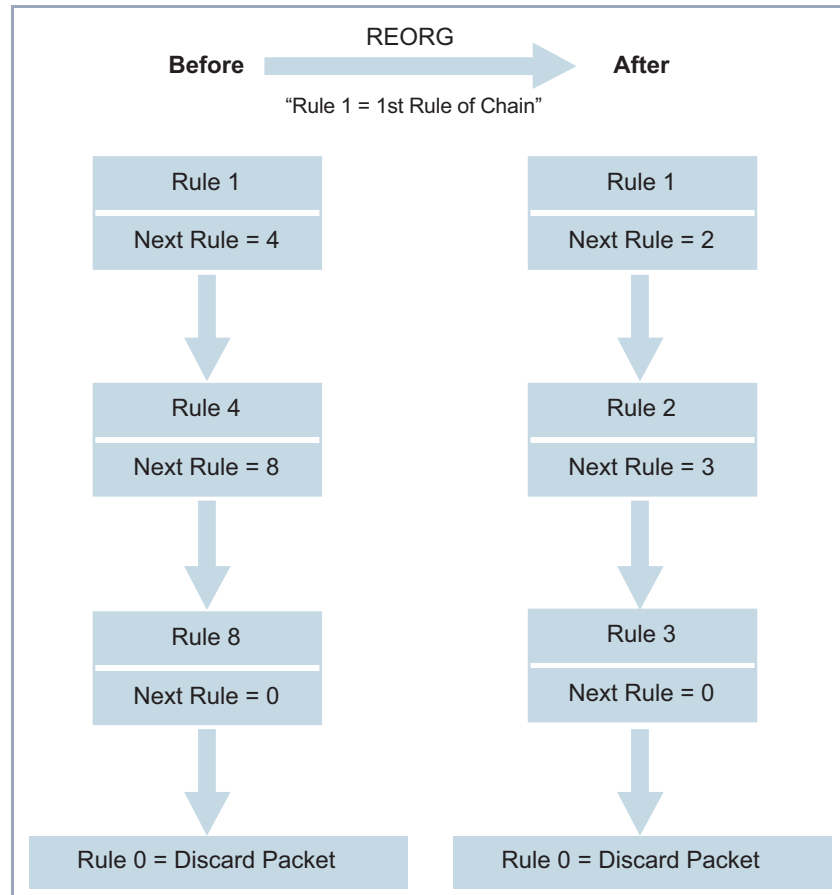


Figure 8-5: Example of chain reorganization

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 **X1000** due to a filter violation:



The rule with **Index = 1** is normally always used as the first rule for a newly created interface (e.g. to a WAN partner).

Field	Meaning
Interface	X1000 interface
First Rule	Defines which rule is used first for data packets that reach X1000 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 data 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 8-19: 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 **X1000** is no longer allowed as soon as you enter the rule and confirm with **SAVE**.

- Do not use filters in the LAN interface (**IP** ► **ACCESS LISTS** ► **INTERFACES** ► **EDIT First Rule = none**) if you access **X1000** from the LAN over telnet.
- If you access **X1000** via the serial interface or ISDN login, at least nothing can happen to you during configuration.

- Filters**
- Go to **IP** ► **ACCESS LISTS** ► **FILTERS**.
 - Add a new entry with **ADD** or select an existing entry and confirm with **Return** to change it.
 - Enter **Description**.
 - Select **Protocol**.
 - Enter **Source Address**, if applicable.
 - Enter **Source Mask**, if applicable.
 - Select **Source Port**.
 - Enter **Specify Port**, if applicable.
 - Enter **Destination Address**, if applicable.
 - Enter **Destination Mask**, if applicable.
 - Select **Destination Port**.
 - Enter **Specify Port**, if applicable.
 - Press **SAVE**.
 - Repeat these steps until you have defined all the 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 **Action**.
- Select **Filter**.
- Select **Next Rule** if you change an existing rule.
- Press **SAVE**.
- Repeat these steps until you have defined all the 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 **Deny Silent**.
- Select **Reporting Method**.
- Press **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 6.1.6, page 151](#).

8.2.9 Local Filters

Access to the local UDP and TCP services on **X1000** (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 8.2.7, page 313](#)) or global filters (see [chapter 8.2.8, page 317](#)).

Strategy As soon as at least one entry for local filters exists in **X1000**, incoming requests for the corresponding local services of **X1000** are only allowed if

1. the source address is 127.0.0.1 (loopback address), or
2. no entry exists for the corresponding service, or
3. 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.

Configuration is made in **IP** ► **LOCAL SERVICES ACCESS CONTROL** ► **ADD**:

Field	Meaning
Service	<p>Defines the local X1000 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>
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>

Field	Meaning
IP Address	(Only if Verify IP Address = <i>verify</i>) 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.
Mask	(Only if Verify IP Address = <i>verify</i>) 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. 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.
Verify Interface	Defines if a check is to be made to determine which X1000 interface is used for an incoming call received for the service selected under Service . Possible values: ■ <i>verify</i> ■ <i>don't verify</i>
Interface	(Only if Verify Interface = <i>verify</i>) Defines an interface of X1000 . If X1000 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 8-20: **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 **X1000** accepts this call.

- Go to **IP** ➤ **LOCAL SERVICES ACCESS CONTROL**.
All the entries made until now are listed here.
- Press **ADD** to add a new entry.
- Select **Service**.
- Select **Verify IP Address**, e.g. *verify*.
- Enter **IP Address**, if applicable.
- Enter **Mask**, if applicable.
- Select **Verify Interface**, e.g. *verify*.
- Select **Interface**, if applicable.
- Press **SAVE**.
The entry is listed.

8.2.10 Back Route Verification

This term conceals a simple but very effective **X1000** function. 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. 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**.

8.2.11 TAF Client

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 on BinTec's corporate access routers and configure the router as TAF server. You can configure the **X1000** personal access router as TAF **client** to obtain access on a TAF server and the connected LAN (if the TAF server has been configured appropriately). A detailed description of operation and the necessary configuration steps are contained in **BRICKware for Windows**.

8.2.12 Extended IP Routing (XIPR)

In addition to the normal routing table, **X1000** can also make routing decisions based on an additional table called the Extended Routing Table (Extended IP Routing). Apart from the destination address, **X1000** 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 switched 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** and in the MIB table **ipExtRtTable**.

A detailed description (including configuration using the MIB variables) can be found in the **Software Reference**. For configuration with the Setup Tool, please see the relevant additions in the next version of the **User's Guide**.

8.3 Line Tapping Security

You can use an encryption mechanism to obtain data security for critical PPP connections, provided both connection partners support this mechanism. The following functions are possible:

- Encryption ([chapter 8.3.1, page 336](#))
- VPN (with extra license, [chapter 8.3.2, page 339](#))

8.3.1 Encryption

X1000 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 and are only available with a VPN license.

MPPE V2 The MPPE version 2 encryption protocol, the successor to MPPE, has been developed by Microsoft and like version 1 also uses a 40-bit, 56-bit or 128-bit key.

If a larger key length is set in **X1000** than in the dial-in client, the connection is not set up.

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 **X1000** 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 **X1000**.

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. 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>Blowfish 56</i>: Blowfish with 56-bit key ■ <i>Blowfish 168</i>: Blowfish with 168-bit key ■ <i>DES 56</i>: DES with 56-bit key ■ <i>DES3 168</i>: Triple DES with 168-bit key ■ <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 8-21: **WAN PARTNER** ► **EDIT**

If DES or Blowfish are used, the key can be generated dynamically on 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 dynamically by X1000. ■ <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 8-22: **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 the WAN partner with whom encrypted data are to be exchanged 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. **1A35EFC17B56**.
- Enter **Encryption Key (RX)**, if applicable, e.g. **89A1288CD131**.
- Press **SAVE**.
- Confirm with **OK**.
- Press **SAVE**.

8.3.2 VPN (with extra license)

X1000 can set up a VPN (Virtual Private Network) using the PPTP (Point-to-Point Tunneling Protocol). This provides safe (encrypted) 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**.

8.3.3 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).



Detailed information and configuration instructions can be found in the **IPSec Reference Manual**, which you receive together with your IPSec license, or in the **Software Reference**.

8.4 Special Features

8.4.1 Startup Procedure

X1000 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.

8.4.2 Auto Logout

Connections to **X1000** via telnet, **ISDN Login** 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 12.1, page 384](#)).

8.4.3 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 **X1000** 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 8.2.10, page 334](#)).

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.

8.5 Checklist

The following list indicates the most important critical security points that you should observe when configuring **X1000**:

- Have you changed all four passwords for system access (admin, read, write, http)? See [chapter 6.1.2, page 132](#).
- Are the activities of your **X1000** sufficiently accurately logged on at least one external computer and do you check the syslog messages regularly? See [chapter 8.1.1, page 290](#).
- 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, HTTP, 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 8.2.7, page 313](#).
- 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 8.2.8, page 317](#).
- Have you restricted remote maintenance access via ISDN Login? Have you made a suitable entry under **CM-1BRI, ISDN S0** **INCOMING CALL ANSWERING**? See [chapter 6.1.4, page 138](#).

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 8.2.4, page 310](#).
- Do you use an encryption protocol for line tapping security on connections with critical security? See [chapter 8.3.1, page 336](#).
- 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 7.2.8, page 242](#).
- 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 the CAPI user concept?
- Are any additional user accounts created trouble-free?
- Have you prevented the interception of connections on the Ethernet by a suitable LAN infrastructure?

9 Configuration Management

In this chapter, you will find instructions on the administration of your configuration files and on updating the **X1000** software. The following areas are covered:

- Administration of Configuration Files
 - Where are the configuration files?
 - What is flash and memory?
 - How do I handle configuration files?
- Resetting **X1000** to the ex works state
 - How can I reset **X1000** to the ex works state without deleting the existing configuration?
- Updating software
 - How do I keep my **X1000** up to date with the latest developments?
 - How do I load new system software?

9.1 Administration of Configuration Files

Flash **X1000** reads its configuration information from configuration files. These configuration files are stored in the flash EEPROM (electronically erasable, programmable read-only memory) of **X1000**. Several different configuration files can be stored in the flash memory. The data also remains stored in the flash when **X1000** is switched off.

Memory The current configuration and all changes you set during the operation of **X1000** are stored in the working memory (RAM). The contents of the RAM are lost when **X1000** is switched off. So if you modify your configuration and want to retain these changes for the next time you start **X1000**, you have to save the modified configuration to the flash before switching off: **Exit** ► **Save as boot configuration and exit** (see [chapter 6.3, page 199](#)). This file is then saved in the flash as a boot configuration file under the name "boot". When **X1000** is started again, this very file, the configuration file with the name "boot", is loaded in the RAM and becomes operative.

Ex works state If you reset **X1000** to the ex works state and want to keep the stored configuration, this is possible by switching the equipment off and on (see [chapter 9.2, page 353](#)). You can also reset **X1000** to the ex works state and delete all the configuration files (see [chapter 11.5, page 380](#) and [chapter 9.2, page 353](#)).

Operations Imagine the flash memory as a directory of configuration files. The files in this directory can be copied, moved, erased and newly filed. It is also possible to transfer configuration files between **X1000** and a remote host by TFTP.

Windows In Windows, you can use the TFTP server of **DIME Tools** for this (see **BRICKware for Windows**). You can then, for example, save a configuration file from **X1000** on your local PC.



The files to be transferred with the TFTP server of **DIME Tools** may have maximum eight characters for the file name, plus maximum three characters as file extension, e.g. **X1000.cf**.

Unix A TFTP server is part of the system under Unix. Please observe the instructions included in the **Software Reference**.

You can perform the various operations with the help of the Setup Tool:

- Go to the **CONFIGURATION MANAGEMENT** menu.

X1000 Setup Tool	BinTec Communications AG MyX1000
Operation	get (TFTP --> FLASH)
TFTP Server IP Address	192.168.1.1
TFTP File Name	brick.cf
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.
TFTP Server IP Address	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.
TFTP File Name	Name of the configuration file on the TFTP server (without path data).
Name in Flash	Name of the configuration file in the flash.
New Name in Flash	Name of the configuration file to be newly created in the flash (with Operation = <i>move</i> or <i>copy</i>).
Type of Last Operation	Type of previous operation (since the last X1000 start).
State of last operation	The state of the last operation executed.

Table 9-1: **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 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 <Name in Flash> to <New Name in Flash>.
<i>copy</i> (FLASH --> FLASH)	Copy configuration file <Name in Flash> as <New Name in Flash>.
<i>delete</i> (FLASH)	Delete configuration file <Name in Flash>.
<i>put</i> (FLASH --> TFTP)	Transfer configuration file <Name in Flash> from flash 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. Make sure that the TFTP Demon of the destination system has write access to the TFTP directory.
<i>get</i> (TFTP --> FLASH)	Transfer configuration file <TFTP File Name> from TFTP host with the IP address <TFTP Server IP Address> to flash. <Name in Flash> is then overwritten and recreated with the contents of <TFTP File Name>. As the configuration file is transferred to flash and not to memory, the file must then be loaded (FLASH --> MEMORY), so that the settings can take effect on X1000 .

Possible Values	Meaning
<i>state</i> (<i>MEMORY --> TFTP</i>)	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 X1000 . All settings in the memory are replaced by boot settings from the flash.

Table 9-2: **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, cf. chapter 8.1.1, page 290).

Table 9-3: **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 is deleted. So if you transfer a "boot" file, **X1000**'s boot file will be deleted and **X1000** 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 which you want to transfer a configuration file to or from. Make sure that the TFTP Demon of the destination system has write access to the TFTP directory.

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:

- 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:

- 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 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 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 to indicate the cause.

- Leave **CONFIGURATION MANAGEMENT** with **EXIT**.

Example You have created the configuration file `brick.cf`, e.g. with the help of the **Configuration Wizard**. You have not transferred the file to **X1000** over the serial interface; `brick.cf` can be found in the directory `C:\BRICK` on your PC. Your PC has the IP address `192.168.1.1`. If you want to transfer `brick.cf` from your PC to **X1000**, 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 active.
- Activate a TFTP server under Unix: see the **Software Reference**.
- Go to **CONFIGURATION MANAGEMENT**.
- Select **Operation**: *get (TFTP --> FLASH)*.
- Type in **TFTP Server IP Address**, e.g. ***192.168.1.1***.

TFTP host --> flash

- Type in **TFTP File Name**: *brick.cf*.
- 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 and **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 *brick.cf* is saved, for example, in **X1000**'s flash under the name *boot*.

To make the settings of *brick.cf* take immediate effect in **X1000**, proceed as follows:

- Flash --> memory**
- Reselect **Operation**: *load (FLASH --> MEMORY)*.
 - 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 and **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 **X1000**'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**.

9.2 Resetting X1000 to the Ex Works State

You can reset **X1000** to the "factory reset" (ex works) state with a special reset sequence (switching on and off). This state corresponds to a booted **X1000** in the ex works state. You can then dial in to the equipment from another location using ISDN Login (see [chapter 5.1.3, page 110](#)).

In the "factory reset" state, the default configuration is used and any existing boot configuration is ignored but not deleted.

Proceed as follows to reset **X1000** to the "factory reset" state:

- If the **X1000** is in operation, switch it off.
- Switch your **X1000** on so that it runs through the boot sequence (see [chapter 11.5, page 380](#)).
- Observe the LEDs on the front of **X1000**.
After running through the start mode (approximately 8 seconds; see [chapter 11.2, page 373](#)), all yellow LEDs light simultaneously. (If **X1000** is connected to your PC over the serial interface and **HyperTerminal** is started (see [chapter 5.1.1, page 107](#)), the message `Press <sp>` now appears on the screen.)
- Switch off the equipment while the yellow LEDs light. You have about 4 seconds for this.
- Repeat the on/off operation twice.
X1000 has now been switched on and off three times altogether.
- Switch on **X1000** for the fourth time.
If you do not interrupt the boot sequence this time, the equipment starts in the "factory reset" state.
This state is indicated by all yellow LEDs flashing three times.

To protect **X1000** against unauthorized access in the "factory reset" state, you need the password of the previously active boot configuration for dialing.

You can log in with ISDN Login and this password, e.g. for loading, modifying and saving the boot configuration.

As an option, you can enter `erase bootconfig` after the login prompt. This command deletes all the existing configurations and **X1000** is rebooted.

If you switch the equipment off and on again, it starts with the saved boot configuration.

9.3 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 **X1000**, this chapter tells you how to update your software.

www.bintec.net

If you want to update your software, load new system software in **X1000**. 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 (boot image) 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**, **Quick Install Guides**) and general product information (**Software Reference**, **BRICKware for Windows**).



Make sure you read the corresponding **Release Notes** before you update your software. The **Release Notes** describe the changes provided by the new system software.

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** and in [chapter 11.5, page 380](#).



An update of the BOOTmonitor and or Firmware Logic is recommended in a few cases. If this should be necessary with a new release, it is clearly noted in the corresponding **Release Notes**. The procedure and recommendations can then be found in the **Release Notes** BOOTmonitor and Firmware Logic Update.

You should only update BOOTmonitor or Firmware Logic if this is expressly recommended by BinTec Communications AG!

To do

To update the software (boot image), proceed as follows:



Do not turn **X1000** off during the update!

- Enter the ➤➤ **URL** `www.bintec.de` in your browser (e.g. Internet Explorer or Netscape Navigator).

The BinTec home page opens. Here you will find the latest software and documentation for **X1000**.
- Click the current system software (boot image, software image) with the right mouse button, e.g. Boot Image Release 5.1 Rev.4.
- In the context menu, click **Save link as...**
- Enter the directory and name under which the new system software should be saved on your PC. The directory is normally `C:\BRICK` for Windows PCs and `/ftptboot` for Unix workstations. As name, you can use ***b5104b02.x1x***, for example.
- Press **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 3.3, page 43](#)). Activate the TFTP server.
For a Unix computer: Follow the instructions in the **Software Reference**.
- Log in to **X1000**, if you have not already done so.
- Deactivate auto logout with `t 0`.
- In the SNMP shell, type in `update <IP address> <file name>`. Do not enter the pointed brackets.

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 system software you have saved on your PC (e.g. ***b5104b02.x1x***).

The file `<file name>` is first transferred to the memory of **X1000** and checked.

The following appears in the SNMP shell: Perform update (y or n)?

- Enter `y` and confirm with **Return**.

The software update is executed and the new system software is loaded in the flash memory.



X1000 requires a connected block of free working memory that is somewhat larger than the new system software. If insufficient memory is available on **X1000**, **X1000** offers an incremental update, in which the software is loaded directly in "chunks" to the flash memory without checking. Proceed as follows:

If insufficient memory is available, a query will appear in the SNMP shell: Do you want to perform an incremental update (y or n)?

- First enter `n`.
- Type in `update -v <IP address> <file name>`.
The image is checked, but not yet loaded.
- Type in `update <IP address> <file name>`.
The following appears in the SNMP shell: Perform update (y or n)?
- Enter `y` and confirm with **Return**.

X1000 performs an incremental update and the software is loaded to the flash memory. This procedure takes longer than a normal update!

The following appears in the SNMP shell: Reboot now (y or n)?

- Enter `y` and confirm with **Return**.

X1000 starts with the new system software. The existing configuration is transferred.

10 Troubleshooting

Tips If you are having problems with **X1000**, the following tips should help you to overcome some of the more usual stumbling blocks:

- Log in to **X1000** 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 **X1000** (see [chapter 8.1.1, page 290](#)). 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
- Typical Errors

10.1 Aids to Troubleshooting

Here you can find methods to help narrow down the possible causes of your problem:

- Local SNMP Shell Commands
- External Aids

10.1.1 Local SNMP Shell Commands

These commands are entered directly in **X1000**'s SNMP shell:

debug

You can use the `debug` command for troubleshooting in one or more sub-systems of **X1000**. A detailed explanation of the syntax and options can be found in [chapter 12.1, page 384](#).

Examples:

- Enter `debug all` to display debugging information for all subsystems.
- Enter `debug config &` for tracking down configuration management problems (see [chapter 9, page 345](#)).



If you add `&` to an SNMP shell command, the program runs in the background.

isdnlogin

You can use the `isdnlogin` command to verify that an ISDN connection can be made. This is explained in [chapter 12.1, page 384](#).

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

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 12.1, page 384](#).

Examples:

- Enter `trace -ip next` to display data packets that are to run over the next B-channel to be opened.
- Enter `trace -x -s me -d 0:a0:f9:d:5:a 0 0 1` to output data packets sent from **X1000**'s MAC address over the LAN to the host with the MAC address 0:a0:f9:d:5:a.

10.1.2 External Aids

You can analyze connections to **X1000** using the following utility programs on a Windows PC or Unix workstation.

DIME Tracer (Windows)

The DIME Tracer enables you to trace **X1000**'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 **X1000**'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 12.2, page 391](#).

10.2 Typical Errors

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. These situations are broken down into the following categories:

- System errors
- ISDN connections
- IPX routing

10.2.1 System Errors

I have forgotten my password.

You must reset **X1000** to the unconfigured initial state (ex works state):

- Connect your router over the serial interface to **X1000** as explained in [chapter 5.1.3, page 110](#).
- Switch **X1000** 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 **X1000** are deleted.
- Select (1) Boot System.
X1000 is restarted.
- Reconfigure **X1000**.

I can't reach X1000 in the LAN.

Try to establish a serial connection:

- Connect your PC to **X1000** 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 the IP address under **CM-100BT, FAST ETHERNET**?
 - Have you entered a filter under **IP ▶ ACCESS LISTS** that is locking you out?
 - Have you activated NAT for an Ethernet interface (`en1` or `en1-snap`) under **IP ▶ NETWORK ADDRESS TRANSLATION ▶ EDIT** and forgotten to allow the required IP connections for this interface under **IP ▶ NETWORK ADDRESS TRANSLATION ▶ EDIT ▶ ADD**.If so, make the required corrections.

If a serial connection does not work either:

- Check the settings of the terminal program (see [chapter 5.1.1, page 107](#)). If you have changed the default settings in `BOOTmonitor`, adjust your terminal settings accordingly.
- If this does not succeed, proceed as explained under "I have forgotten my password".

10.2.2 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 8.1.3, page 299](#)). This enables you to set a limit for connections to **X1000** to prevent unnecessary charges accumulating as a result of mistakes made during configuration.

In case of ISDN connections on **X1000** remaining open or unwanted ISDN connections being established:

- Use `debug all` or `trace` to check if a PC in the LAN is using a different netmask from the one entered on **X1000**.
- 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 **X1000** is configured so that syslog messages are sent to a host outside the LAN (destination port 514).
- Check the MIB table **biboAdmTrapHostTable** to determine if **X1000** is configured so that SNMP traps (messages) 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). Configure a local HOSTS file in the Windows directory that can carry out name resolution (see [chapter 4.5, page 95](#)).
- 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. Switch off NetBIOS over IP or set filters (configuration of the corresponding filters can be found in [chapter 6.1.6, page 151](#). You can also use the simple NetBIOS filter of the **Configuration Wizard**, see [chapter 4.7, page 101](#)).
- Check if you have configured callback (see [chapter 8.2.4, page 310](#)) 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.

- Check the LEDs on the front of **X1000** to determine if a connection is made (see [chapter 11.2, page 373](#)).
- 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*.
- In **CM-1BRI, ISDN S0** ➤ **INCOMING CALL ANSWERING**, check if your own extension number is entered correctly. This also applies to outgoing calls.

Incoming calls cannot be made.

- Check the LEDs on the front of **X1000** (see [chapter 11.2, page 373](#)) to determine if an incoming call is received at all.
- 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 **CM-1BRI, ISDN S0** ➤ **INCOMING CALL ANSWERING** to see 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.

10.2.3 IPX Routing

Here you will find some problems that could crop up with IPX routing together with suggestions on how they can be solved.

Check the following using the Setup Tool:

- Have you entered the correct license under *LICENSES*?
- Is the entry under **Internal Network Number** in *IPX* unique in the LAN?

A server exists in a remote LAN (LAN-LAN connection over ISDN), but is "invisible" for clients in the local LAN.

The server could be invisible for clients because SAP packets are not received from the server:

- Check the entries in **Update Time** and **Age Multiplier** in *WAN PARTNER* ➤ *EDIT* ➤ *IPX*. The settings must be compatible with the settings on the servers in *X1000*'s LAN.
- Check if a router between them filters out the SAP packets.
- Check with *isdnlogin* if an ISDN connection can be made between client and server.
- Check if you have made the correct entries in **Local IPX NetNumber** and **Encapsulation** under *CM-100BT*, *FAST ETHERNET* and if the server can receive them.

When the client tries to reach a server in a remote network over a PPP connection, he must wait a long time and the connection is possibly terminated.

In some cases, the local router erroneously tells the client that a server can be reached.

- Check if the server has crashed and that the aging interval has not yet expired. If necessary, change the setting of **Send RIP/SAP Updates** under **WAN PARTNER** ➤ **EDIT** ➤ **IPX**.
- Check if the server and the router in the remote network are simultaneously inactive (e.g. because of a power cut). Briefly set the WAN interface of the corresponding WAN partner with the command `ifconfig` to *down* and then back to *dialup*, in order to delete the routes and services learned by the WAN partner.

I can't change to a network drive on the client's station.

- The file server may be "invisible" to the client. Proceed as described under "A server exists in a remote LAN ...".
- Check if all the licenses available on the server are in use.

ISDN connections are constantly reconnected.

It is not only RIP/SAP packets that cause ISDN connections to be set up.

- Check if there is an entry in the MIB table **ipxDenyTable** that is preventing Novell serialization packets from being sent over the dialup connection.
- Check under **IPX** if you have activated **enable IPX spoofing** and **enable SPX spoofing** with *yes*.
- Check if any RCONSOLE is running with a constantly changing screen (e.g. MONITOR, IPXCON, TCPCON, screensaver, etc.).
- Check if NetBIOS over IPX is used in the LAN (Windows for Workgroups, NT, Win 95). If necessary, select *no* or *on LAN only* under **IPX** for **NetBIOS Broadcast replication**.
- Check if NDS Replica Synchronization is active (for Netware 4.1 servers and higher).

- Evaluate the syslog messages (**Level** = *debug*) and, if applicable, filter out the IPX packets indicated in the messages as causing unwanted connections to be set up.

The MIB variable `ipxAdmSpxConns` shows more connections than are actually active.

X1000 may not be receiving SPX disconnect messages from the server:

- Enter the command `reset router` on the console of the respective server.
All inactive connections between the server and **X1000** are cleared.
- If the disconnect for the client is lost, SPX connections could remain until timeout. These connections would then be displayed in **`ipxAdmSpxConns`** until timeout.

11 Technical Data

This chapter presents the technical data of **X1000**. The following areas are covered:

- General Product Features
- **X1000** Front Panel and LED Displays
- **X1000** Rear Panel and Connections
- Pin Assignment
- BOOTmonitor

11.1 General Product Features

The general product features cover **X1000**'s performance features and the technical requirements for installation and operation.

Feature	Value
Product name:	X1000
Dimensions and weight (B x H x D): Dimensions without cables Space for installation/maintenance Weight Transport weight (incl. documentation, cabling, packaging)	141 mm x 50 mm x 145 mm 150 mm x 60 mm x 210 mm 420 g approx. 2 kg
Memory:	8 MB DRAM, 2 MB flash ROM
LEDs:	5 (1 power, 3 function, 1 error)
Power consumption of equipment:	3 W (typical)
Voltage supply:	AC/DC adaptor Input: 230 V~50 Hz / 70 mA Output: 5 V - 800 mA 4 VA
Ambient requirements: Storage temperature Operating temperature Relative humidity Room classification	-20 to +85 °C 0 to 50 °C 20 to 90% non-condensing in operation 5 to 95% non-condensing in storage Operate only in dry rooms
MTBF:	100 000 hours

Feature	Value
Available interfaces: Serial interface V.24 Ethernet IEEE 802.3 LAN ISDN-WAN S ₀	built-in, supports the following baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bauds built-in (twisted-pair only), 10/100 Mbps, auto sensing built-in
Plugs used: Serial interface Ethernet interface ISDN interface	8-pole mini DIN RJ45 RJ45
Applications interface:	Dual Remote CAPI (v1.1 and 2.0), R-CAPI driver for Windows 95/98/2000/NT and Novell Netware. Source code library for other systems (e.g. Unix, AS400).
Data compression:	PPP LZS STAC compression rate up to 4:1
SAFERNET™ security technology:	Community passwords, PAP, CHAP, MS-CHAP, Callback, Access Control Lists, Allow Lists, CLID, NAT, TAF, MPPE Encryption.
Required licenses:	Licenses included for CAPI, IP, IPX and STAC. Extra licenses obtainable for VPN, IPSec and leased lines.
Software included:	RVS-COM Lite (communications application) BRICKware for Windows BRICKtools for Unix

Feature	Value
Printed documentation included:	User's Guide Quick Install Guide
Online documentation:	BRICKware for Windows Software Reference User's Guide

Table 11-1: General product features of **X1000**

11.2 Front Panel LEDs

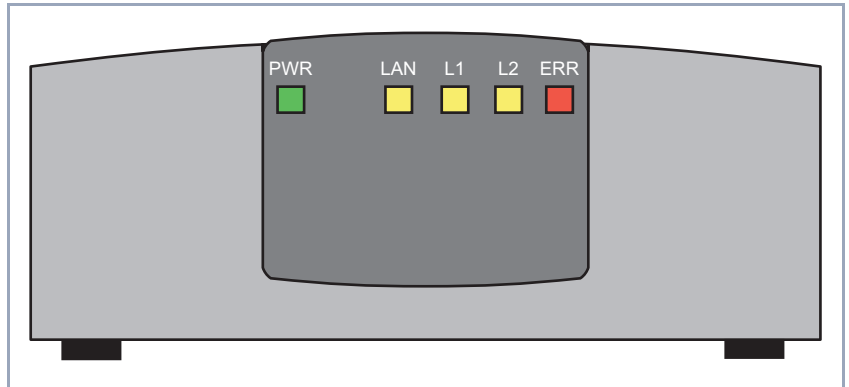


Figure 11-1: **X1000** front panel

There are five LEDs on the front panel for indicating the current status of your **X1000**. Each LED can convey different information according to which mode **X1000** is in. All LEDs light for half a second after the equipment is switched on to show that they are working. When **X1000** starts up, it changes between different functional states:

- Start Mode
- BOOTmonitor Mode (see [chapter 11.5, page 380](#))
- Normal Mode

The meanings of the LEDs in their different states is described in the following tables.

Start Mode

LED	State	Meaning
PWR	On	Power supply connected.
LAN	On	LAN (100BT) test is in progress.
L1	On	ISDN test is in progress.
L2	On	Memory test is in progress.
ERR	On	An error has occurred during a test.

Table 11-2: LEDs in start mode

The corresponding function LED lights as long as a test is in progress and goes out when the test is completed. If an error occurs during the test, the Error LED lights together with the corresponding function LED.

BOOTmonitor Mode

LED	State	Meaning
PWR	On	Power supply connected.
LAN, L1, L2	On	Switching X1000 off and on three times resets the equipment to the ex works state.
LAN	Blinking	TFTP transfer being carried out.
L1, L2	On	BOOTmonitor is active (or waiting for a keyboard entry).
L1, L2	Blinking	BOOTmonitor is compressing system software.
ERR	On	An error has occurred during the boot operation, which means X1000 cannot boot.

Table 11-3: LEDs in BOOTmonitor mode

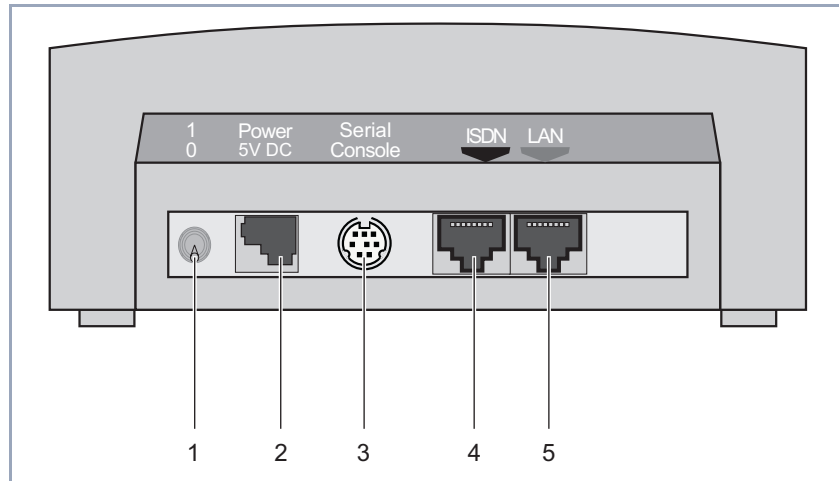
Normal Mode

LED	State	Meaning
PWR	On	Power supply connected.
LAN, L1, L2	Blinking (three times)	Resetting X1000 to the ex works state was successful.
LAN	On	Data packet passing through the LAN interface.
L1	Blinking	ISDN B1-channel: Connection is being set up.
L1	On	ISDN B1-channel: connection is active. (1)
L2	Blinking	ISDN B2-channel: Connection is being set up.
L2	On	ISDN B2-channel: connection is active. (1)
ERR	On (intermittently)	LAN error or collision has occurred.
ERR	On (permanently)	System stopped, restart is necessary.

Table 11-4: LEDs in normal mode

(1) Charges are incurred.

11.3 Rear Panel Connections



1	On/off switch	4	ISDN S ₀ port
2	Power supply connection	5	LAN interface (10/100 Base-T Ethernet), marked red on the equipment
3	Serial interface		

Figure 11-2: **X1000** rear panel

X1000's main board contains an Ethernet interface and an ISDN interface. These interfaces are reached via the connections on the rear panel (see [chapter 11.4, page 377](#)).



Caution!

The use of the wrong mains adaptor may damage your router!

- Use only the mains unit supplied (5 V DC).
- Make sure the rated voltage marked on the mains unit conforms with the local voltage supply.

11.4 Pin Assignment

Serial port

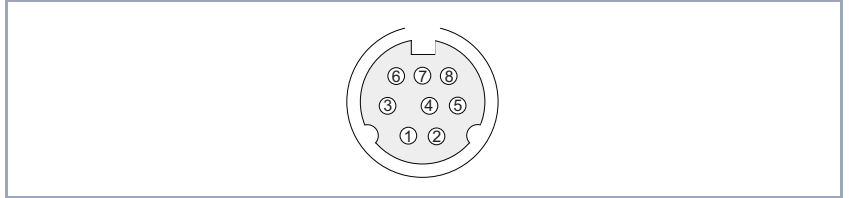


Figure 11-3: 8-pole mini DIN socket

As console port, **X1000** has a serial port with an 8-pole mini DIN socket. The equipment supports baud rates between 1200 and 115200.

The pin assignment for the 8-pole mini DIN socket is as follows:

Pin	Function
1	For future applications.
2	For future applications.
3	T
4	GND
5	R
6	NC
7	NC
8	NC

Table 11-5: Pin assignment for mini DIN socket

ISDN S₀ port

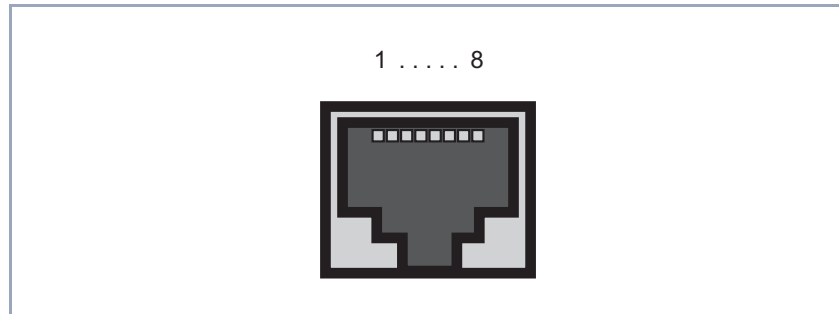


Figure 11-4: ISDN S₀ BRI port (RJ45 socket)

The pin assignment for the ISDN S₀ BRI interface (RJ45 socket) (4) is as follows:

Pin	Function
1	Not used
2	Not used
3	Send (+)
4	Receive (+)
5	Receive (-)
6	Send (-)
7	Not used
8	Not used

Table 11-6: Pin assignment for ISDN BRI interface

LAN interface

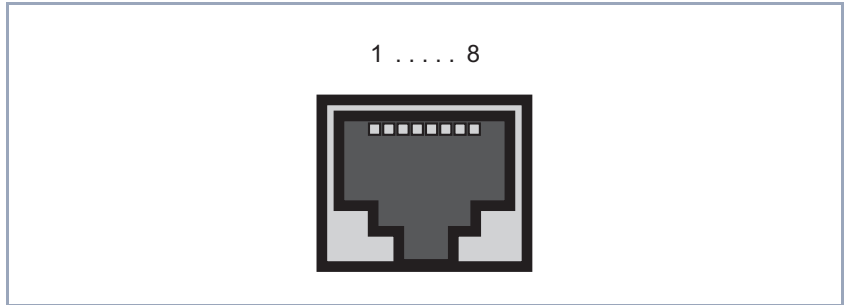


Figure 11-5: Ethernet 10/100Base-T interface (RJ45 socket)

The pin assignment for the Ethernet 10/100Base-T interface (RJ45 socket) is as follows:

Pin	Function
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

Table 11-7: Pin assignment for Ethernet 10/100Base-T interface



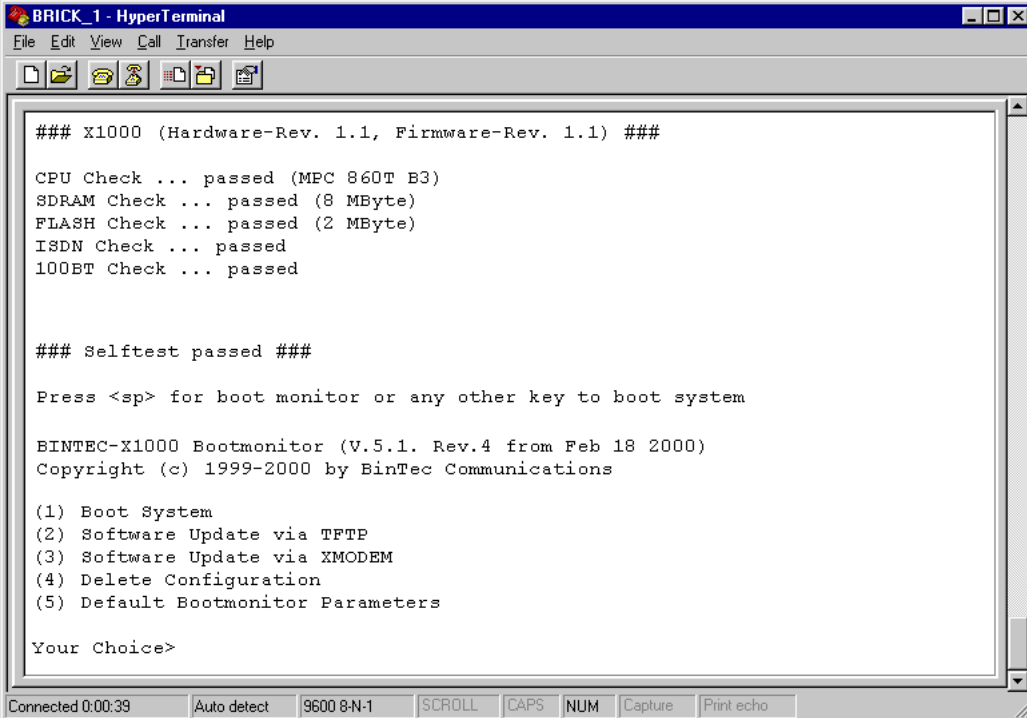
If you want to connect **X1000**'s LAN interface directly to the Ethernet card of your PC and not to an external hub, you need the adaptor cable in addition to the red LAN cable.

11.5 BOOT Sequence

X1000 passes through various functional states on starting (see also [chapter 11.2, page 373](#)):

- Start Mode
- BOOTmonitor Mode
- Normal Mode

After several selftests have been performed successfully in Start Mode, **X1000** changes to the BOOTmonitor Mode. The BOOTmonitor prompt is displayed if you are connected to **X1000** via a terminal program.



```
BRICK_1 - HyperTerminal
File Edit View Call Transfer Help

### X1000 (Hardware-Rev. 1.1, Firmware-Rev. 1.1) ###

CPU Check ... passed (MPC 860T B3)
SDRAM Check ... passed (8 MByte)
FLASH Check ... passed (2 MByte)
ISDN Check ... passed
100BT Check ... passed

### Selftest passed ###

Press <sp> for boot monitor or any other key to boot system

BINTEC-X1000 Bootmonitor (V.5.1. Rev.4 from Feb 18 2000)
Copyright (c) 1999-2000 by BinTec Communications

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

Your Choice>
```

Figure 11-6: BOOTmonitor

BOOTmonitor If you want to use the BOOTmonitor functions, press the **Space** bar within 4 seconds of the BOOTmonitor prompt appearing (figure 11-6, page 380). If you do not make an entry within 4 seconds, **X1000** changes back to Normal Mode.

Functions The BOOTmonitor provides the following functions, which you can select by entering the relevant digit (for more detailed information, refer to the **Software Reference**):

- (1) Boot system:
X1000 loads the compressed boot file from the flash memory to the RAM memory. This happens automatically when started.
- (2) Software update via TFTP:
X1000 performs a software update via a TFTP server.
- (3) Software update via XMODEM:
X1000 performs a software update over a serial interface with XMODEM.
- (4) Delete configuration:
X1000 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 **X1000**'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 **X1000**!

12 Important Commands

This chapter describes the following commands:

- SNMP shell commands:
 - telnet
 - ping
 - trace
 - isdnlogin
 - debug
 - ifconfig
 - ifstat
 - netstat
 - date
 - t
 - nslookup
- **BRICKtools** for Unix commands:
 - bricktrace
 - capitrace

12.1 SNMP Shell Commands

X1000 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 **X1000**.



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 echo_request 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.

trace

For WAN interfaces:

```
trace [-h23aFADtpiNxX] [-T <tei>] [-c <cref>]
[<channel> <unit> <slot> | next | <ifcname>]
```

For LAN interfaces:

```
trace [-h23iNxX1] [-d <destination MAC filter>] [-o]
[-s <source MAC filter>] 0 0 <slot>
```

Is used to display and interpret data packets sent and received over ISDN (D- and B-channels) or the LAN.

- -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)
- -N: Novell IPX 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 ... 1. selects the physical interface for modules with two interfaces
- slot: 1 ... 2. indicates the slot in which the module is installed
- next: only display information for the next B-channel opened
- <ifcname>: name or index of the interface (see "ifstat", page 388)
- -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 = **X1000**'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] [-s <service>]
[-a <addinfo>] [-b <bits>] isdn-number [isdn-service]
layer1-protocol]
```

Is used to open a remote login shell on **X1000** over ISDN.

- -c <stknumber>: defines the ISDN stack (if several ISDN cards are used).
- -C: tries to use compression.

- `-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 **X1000**'s subsystems.

- `show`: displays all possible subsystems that can be debugged.
- `-q`: do not print a timestamp 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**).
- `destination <destaddr>`: destination IP address of a host. This adds a host route for this host in the routing table (**ipRouteDest**).

- address: **X1000**'s IP address for the interface (**ipRouteNextHop**).
- netmask <mask>: netmask of the interface (**ipRouteMask**).
- up: sets the interface to the up status.
- 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 en1` will display information on the interfaces `en1`, `en1-llc` and `en1-snap`).

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]
```

X1000 has a software 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 **X1000** over telnet, ISDN login 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 **X1000** 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 `-?` (e.g. `netstat -?`) usually provides syntax help.

The `update` command can be found in [chapter 9.3, page 355](#).

Further SNMP commands can be found in the **Software Reference**.

12.2 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 [-h23aeFpiNtxs] [-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)
- -N: Novell IPX output (B-channel only)
- -t: output in ASCII text (B-channel only)
- -x: raw dump mode
- -s: check **X1000** 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 ... 1. selects the physical interface for modules with two interfaces
- slot: 1 ... 2. indicates the slot in which the module is installed

capitrace

```
capitrace [-h] [-s] [-l]
```

Is used to trace and evaluate CAPI messages. All CAPI messages sent or received by **X1000** are displayed. The IP address of **X1000** 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>)

13 General Safety Precautions in 15 Different Languages

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 **X1000** 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 **X1000** die Hinweise für die Umgebungsbedingungen (vgl. Technische Daten). Verwenden Sie eine feste und ebene Unterlage.
 - 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 temperaturangepasst und absolut trocken ist, bevor Sie es in Betrieb nehmen. Beachten Sie die Umweltbedingungen in den Technischen Daten.
 - Überprüfen Sie, ob die auf dem Typenschild des Netzteils angegebene Nennspannung mit der örtlichen Netzspannung übereinstimmt. **X1000** darf nur mit dem original BinTec-Steckernetzteil (5 V DC) betrieben werden. BinTec Communications AG haftet nicht für Schäden, die durch die Verwendung eines anderen Steckernetzteils hervorgerufen werden.
 - Beachten Sie beim Verkabeln die Reihenfolge, wie im Handbuch beschrieben. Verkabeln Sie zuerst LAN-, ISDN- und serielle Anschlüsse, schließen Sie dann die Stromversorgung an, und schalten Sie zum Schluß **X1000** ein.
 - Überprüfen Sie, ob Sie die Verkabelung – insbesondere die ISDN- und LAN-Verkabelung – richtig durchgeführt haben, bevor Sie **X1000** in Betrieb nehmen. Der ISDN-Anschluß von **X1000** darf nicht mit dem Ethernet-Anschluß Ihres Rechners oder Hubs verbunden werden, der LAN-Anschluß von **X1000** nicht mit Ihrem ISDN-Anschluß.

- Verwenden Sie für die Verkabelung nur die beigelegten Kabel. Falls Sie andere Kabel verwenden, übernimmt BinTec Communications AG für auftretende Schäden oder Beeinträchtigung der Funktionalität keine Haftung.
- 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.

Bestimmungsgemäße Verwendung, Betrieb

- **X1000** ist für den Einsatz in einer Büroumgebung bestimmt. Als Multiprotokoll-Router baut **X1000** in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen.
- **X1000** entspricht den einschlägigen Sicherheitsbestimmungen für Einrichtungen der Informationstechnik für den Einsatz in einer Büroumgebung.
- Der bestimmungsgemäße Betrieb gemäß IEC 950/EN 60950 des Systems ist nur bei montiertem Gehäusedeckel gewährleistet (Kühlung, Brandschutz, Funkentstörung).
- Die Umgebungstemperatur sollte 50°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 nur durch geschultes Fachpersonal geöffnet werden. Lassen Sie daher Reparaturen am Gerät nur von einer BinTec-autorisierten Servicestelle durchführen. Wo sich die Servicestelle befindet, erfahren Sie von Ihrem Händler. Durch unbefugtes Öffnen und unsachgemäße Reparaturen können erhebliche Gefahren für den Benutzer entstehen (z. B. Stromschlag). Unerlaubtes Öffnen der Geräte hat den Garantie- und Haftungsausschluß der BinTec Communications AG zur Folge.

- 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.

Yleiset turvallisuusmääräykset

Seuraavista kappaleista löydät turvallisuusmääräykset, joita on ehdottomasti noudatettava reittivalitsinta käytettäessä.

Kuljetus ja varastointi

- Kuljeta ja varastoi **X1000** vain alkuperäispakkauksessaan tai muussa sopivassa pakkauksessa, joka suojaa töytäisyltä ja iskuilta.

Asennus ja käyttöönotto

- Tarkista ennen **X1000** -laitteen asennusta ja käyttöä, että ympäristöolosuhteista annettuja ohjeita (kts. lukua Tekniset tiedot) on noudatettu. Aseta laite tukevalle, tasaiselle alustalle.
- Kun laite tuodaan kylmästä ympäristöstä käyttötiloihin, sen ulko- sekä sisäpinnoille voi syntyä kastetta. Odota, että laitteen lämpötila on asettunut ja laite on ehdottoman kuiva, ennen kuin otat sen käyttöön. Huomioi ympäristövaatimukset, jotka on esitetty teknisissä tiedoissa.
- Tarkasta, että verkkolaitteen tyyppikilvessä annettu verkkojännite on sama kuin paikallinen verkkojännite. **X1000** -laitetta saa käyttää vain alkuperäisen BinTec Communications-pistokeverkkolaitteen (5 V DC) kanssa. BinTec Communications AG ei vastaa vahingoista, jotka ovat aiheutuneet muun pistokeverkkolaitteen käytöstä.
- Käsikirjassa kuvattua kaapelien liitäntäjärjestystä on ehdottomasti noudatettava. Yhdistä ensin LAN-, ISDN- ja sarjaliitännät, liitä laite sitten virtaverkkoon ja kytke lopuksi **X1000** päälle.
- Tarkasta, että olet liittänyt kaapelit oikein, erityisesti ISDN- ja LAN-kaapelit, ennen kuin käynnistät **X1000** -laitteen. **X1000** -laitteen ISDN-liitäntää ei saa liittää laskimen tai jakajan Ethernet-liitäntään eikä **X1000** -laitteen LAN -liitäntää saa yhdistää ISDN-liitäntääsi.
- Käytä laitteiden yhdistämiseen vain mukana toimitettuja kaapeleita. Jos käytät muita kaapeleita, ei BinTec Communications AG vastaa tästä aiheutuvista vahingoista.
- Vedä kaapelit sellaisiin paikkoihin, että ne eivät aiheuta vaaratilanteita (kompastumisia) eivätkä vahingoitu.
- Älä liitä, irrota tai kosketa tiedonsiirtokaapeleita ukonilman aikana.

Määräystenmukainen käyttö, käyttö

- **X1000** on tarkoitettu käytettäväksi toimistoympäristössä. **X1000** on moniprotokollareititin, jonka avulla voidaan luoda järjestelmäkonfiguraatiosta riippuen WAN-yhteyksiä. Jotta ei-toivotuilta maksuilta vältytään, laitetta tulee ehdottomasti valvoa.
- **X1000** vastaa toimistotiloissa käytettäville tietotekniikan laitteistoille asetettuja asiaankuuluvia turvallisuusmääräyksiä.
- Järjestelmän määräystenmukainen käyttö standardin IEC 950/EN 60950 mukaan on mahdollista vain kun kotelon kansi on asennettu paikalleen (jäähdytys, palosuojelu, häirintäsuojaus)
- Ympäristön lämpötila ei saisi nousta yli 50°C. Älä aseta laitetta alttiiksi suoralle auringonpaisteelle.
- Varo, ettei mitään vieraita esineitä (esim. paperiliittimiä) tai nesteitä pääse laitteen sisäpuolelle (sähköisku, lyhytsulku). Huolehdi siitä, että laitteen jäähdytys on riittävä.
- Keskeytä hätätilanteessa (esim. särkynyt kotelo tai käyttölaite, nesteen tai vieraiden esineiden joutuminen laitteen sisään) virransyöttö välittömästi ja ota yhteyttä huoltopalveluun.

Puhdistus ja korjaus

- Vain koulutettu ammattihenkilöstö saa avata laitteen. Anna sen vuoksi kaikki korjaustyöt vain BinTec-valtuutetun huoltokorjaamon tehtäväksi. Kauppi-aasi voi kertoa, missä on lähin valtuutettu huoltokorjaamo. Luvaton aukaiseminen ja asiantuntemattomat korjaukset saattavat aiheuttaa käyttäjälle vakavia vaaratilanteita (esim. sähköisku). Laitteiden luvaton aukaiseminen aiheuttaa BinTec Communications AG -takuun raukeamisen sekä kaikkinaisen vastuun epäämisen.
- Älä missään tapauksessa puhdistu laitetta runsaalla vedellä. Sen sisään tunkeutunut vesi saattaisi aiheuttaa vakavia vaaroja (esim. sähköisku) käyttäjälle ja vaurioittaa laitetta pahasti.
- Älä koskaan käytä puhdistamiseen hankausaineita, alkalisia puhdistusaineita taikka syövyttäviä tai hankaavia tehoaineita.

Consignes de sécurité générales en français

Vous trouverez, dans les paragraphes suivants, les consignes de sécurité que vous devez absolument respecter lors de l'utilisation de votre router.

- Transport et entreposage**
- Transportez et entreposez **X1000** uniquement dans son emballage d'origine ou un autre emballage approprié lui garantissant une bonne protection contre les chocs et les coups.
- Installation et mise en service**
- Avant de procéder à l'installation et à la mise en service de **X1000**, veuillez vous référer aux indications concernant les conditions d'environnement (cf. Caractéristiques techniques). Utilisez un support stable et plat.
 - Si l'appareil est transporté dans une pièce où la température est plus élevée que celle de l'endroit d'où il provient, de la condensation risque de se former à l'extérieur comme à l'intérieur de l'appareil. Avant de mettre votre appareil en service, attendez qu'il soit à la même température que celle de la pièce et qu'il soit absolument sec. Veuillez respecter les indications concernant les conditions d'environnement (cf. Caractéristiques techniques).
 - Vérifiez si la tension nominale indiquée sur la plaque signalétique du bloc d'alimentation correspond bien à la tension de l'endroit en question. **X1000** doit uniquement fonctionner avec la fiche du bloc d'alimentation BinTec Communications originale (5 V cc). BinTec Communications AG décline toute responsabilité pour les dommages dus à l'utilisation d'une autre fiche de bloc d'alimentation.
 - Lors du câblage, respectez les étapes indiquées dans le manuel. Câblez tout d'abord les raccordements LAN, RNIS et sériels, puis connectez l'alimentation électrique et mettez finalement **X1000** en service.
 - Vérifiez si vous avez effectué un câblage correct, en particulier celui des réseaux RNIS et LAN, avant de mettre **X1000** en service. Le raccordement RNIS de **X1000** ne doit pas être relié au raccordement Ethernet de votre ordinateur ou de votre borne, le raccordement LAN de **X1000** ne doit pas être relié à votre raccordement RNIS.
 - Utilisez uniquement les câbles joints à la livraison pour effectuer le câblage. Dans le cas où vous utiliseriez d'autres câbles que ces derniers, la société

BinTec Communications AG décline toute responsabilité pour les dommages éventuels ou pour tout défaut de fonctionnement pouvant en résulter.

Utilisation conforme, fonctionnement

- Posez les câbles de telle sorte qu'ils ne puissent pas être à l'origine de risques (risques de trébuchement) ou être endommagés.
- Pendant un orage, ne connectez pas les lignes de transmission des données, ne les débranchez pas et ne les touchez pas.
- **X1000** est conçu pour l'utilisation dans les bureaux. En tant que router multiprotocole, **X1000** établit les connexions WAN en fonction de la configuration existante. Pour éviter des frais de taxation indésirables, il est impératif de placer ce produit sous contrôle.
- **X1000** est conforme aux prescriptions de sécurité relatives aux équipements de la technique de l'information pour l'utilisation dans les bureaux.
- L'emploi de ce système conformément aux normes IEC 950/EN 60950 ne peut être garanti que si le couvercle du boîtier est monté (refroidissement, protections anti-incendie et antiparasite)
- La température ambiante ne doit pas dépasser 50°C. Evitez le rayonnement direct du soleil sur l'appareil.
- Veillez à ce qu'aucun objet (des agrafes par exemple) ni aucun liquide ne s'introduise à l'intérieur de l'appareil (risque d'électrocution ou de court-circuit). Veillez à ce que l'appareil ait suffisamment refroidi.
- Dans les cas d'urgence extrême (si le boîtier ou des éléments de commande sont endommagés, lorsque du liquide ou des corps étrangers se sont introduits dans l'appareil, par exemple), déconnectez immédiatement l'alimentation en courant et contactez le service après-vente.

Nettoyage et réparations

- L'appareil doit être ouvert uniquement par un personnel spécialisé dûment instruit. Ne faites donc réaliser les réparations de l'appareil que par un point de service après-vente agréé par BinTec. Votre concessionnaire vous fera part de l'adresse à laquelle vous pourrez contacter le service après-vente. Une ouverture non autorisée et des réparations non conformes aux règles de l'art exposent l'opérateur à des risques très graves (risque d'électrocution par ex.). L'ouverture non autorisée de l'appareil annule tout droit à la

garantie et décharge la société BinTec Communications AG de toute responsabilité.

- L'appareil ne doit être en aucun cas nettoyé à l'eau. Une pénétration d'eau dans l'appareil pourrait entraîner des risques graves pour l'opérateur (risque d'électrocution par exemple) et des dommages importants de l'appareil.
- Ne jamais utiliser de produits récurants, de produits de nettoyage alcalins, ni d'outils tranchants ou grattants.

Γενικές οδηγίες ασφαλείας στα Ελληνικά

Στις ακόλουθες παραγράφους θα βρείτε τις οδηγίες ασφαλείας, τις οποίες θα πρέπει να λάβετε οπωσδήποτε υπ' όψιν σας κατά τη χρήση του Router.

- Μεταφορά και αποθήκευση**
- Να μεταφέρετε και να αποθηκεύετε το **X1000** μόνο στη γνήσια συσκευασία ή σε μία άλλη κατάλληλη συσκευασία, η οποία να εξασφαλίζει προστασία από τις κρούσεις και τα χτυπήματα.
- Εγκατάσταση και έναρξη της λειτουργίας**
- Πριν την εγκατάσταση και την έναρξη της λειτουργίας του **X1000** να λάβετε υπ' όψιν σας τις οδηγίες σχετικά με τις συνθήκες περιβάλλοντος (βλέπε Τεχνικά στοιχεία). Χρησιμοποιήστε ένα σταθερό και επίπεδο υπόβαθρο.
 - Όταν η συσκευή μεταφέρεται από ψυχρό περιβάλλον στον χώρο λειτουργίας μπορεί να παρουσιασθεί τήξη τόσο στο εξωτερικό όσο και στο εσωτερικό της συσκευής. Πριν την θέσετε σε λειτουργία περιμένετε μέχρι που η συσκευή να αποκτήσει την ίδια θερμοκρασία και να είναι τελείως στεγνή. Προσέξτε τις συνθήκες περιβάλλοντος στο Τεχνικά στοιχεία.
 - Επανελέγξτε εάν η ονομαστική τάση που αναφέρεται στην πλακέτα τύπου του φικς αντιστοιχεί στην τάση του τοπικού δικτύου. Το **X1000** επιτρέπεται να λειτουργεί μόνο με το γνήσιο φικς BinTec Communications AG (5 V DC). Η BinTec Communications AG δεν ευθύνεται για ζημιές που ενδέχεται να προκληθούν από τη χρήση ενός άλλου φικς.
 - Προσέξτε κατά την καλωδίωση, ώστε να τηρηθεί η σωστή σειρά που περιγράφεται στο εγχειρίδιο. Καλωδιώστε κατ' αρχήν το LAN, το ISDN και τη σειριακή διεπαφή. Στη συνέχεια να γίνεται η σύνδεση με το ηλεκτρικό ρεύμα και στο τέλος θέστε το **X1000** σε λειτουργία.
 - Επανελέγξτε εάν καλωδιώσατε κατά τον προβλεπόμενο τρόπο ιδίως το ISDN και το LAN, προτού να θέσετε το **X1000** σε λειτουργία. Η σύνδεση ISDN του **X1000** δεν επιτρέπεται να συνδεθεί με τη σύνδεση Ethernet του υπολογιστή ή της υποδοχής σας, και η σύνδεση LAN του **X1000** δεν επιτρέπεται να συνδεθεί με τη σύνδεση ISDN.

- Χρησιμοποιήστε για την καλωδίωση μόνον τα συνημμένα καλώδια. Σε περίπτωση που χρησιμοποιήσετε άλλα καλώδια, η BinTec Communications AG δεν αναλαμβάνει καμία ευθύνη για ενδεχόμενες ζημιές.
 - Διαστρώστε τα καλώδια κατά τέτοιον τρόπο, ώστε να μην προκύψουν σημεία κινδύνου (κίνδυνος παραπατήματος) και ώστε να μη μπορούν να υποστούν ζημιά.
 - Κατά την διάρκεια μιας καταιγίδας ούτε να συνδέετε ούτε να βγάξετε τα καλώδια μεταφοράς δεδομένων, ούτε να τα ακουμπάτε.
- Προβλεπόμενη χρήση, λειτουργία**
- Το **X1000** προορίζεται για χρήση σε περιβάλλον γραφείου. Σαν Router πολλαπλών πρωτοκόλλων (Multi-Protokoll) το **X1000** σε εξάρτηση από την διαμόρφωση του συστήματος δημιουργεί συνδέσεις WAN. Για να αποφύγετε πρόσθετα τέλη θα πρέπει οπωσδήποτε να επιτηρείτε την συσκευή.
 - Το **X1000** ανταποκρίνεται στις σχετικές διατάξεις ασφαλείας για εγκαταστάσεις τεχνολογίας πληροφοριών κατά τη χρήση σε περιβάλλον γραφείου.
 - Η προβλεπόμενη λειτουργία του συστήματος σύμφωνα με την IEC 950/EN 60950 διασφαλίζεται μόνον, όταν το καπάκι του κελύφους είναι μονταρισμένο (ψύξη, αντιπυρική προστασία, παρεμβολή σπινθήρων).
 - Η θερμοκρασία περιβάλλοντος δε θα πρέπει να υπερβαίνει τους 50°C. Αποφύγετε την έκθεση σε άμεση ηλιακή ακτινοβολία.
 - Να προσέχετε, ώστε να μην εισέλθουν αντικείμενα (π.χ. συνδετήρες) ή υγρά στο εσωτερικό της συσκευής (κίνδυνος ηλεκτροπληξίας, βραχυκυκλώματος). Θα πρέπει να εξασφαλίζεται η επαρκής ψύξη.
 - Σε έκτακτες περιπτώσεις (π.χ. όταν έχει προκληθεί βλάβη στο κέλυφος ή στη μονάδα χειρισμού ή όταν έχουν εισέλθει υγρά ή αντικείμενα) να διακόπτετε αμέσως την παροχή ρεύματος και να έρχεστε σε επαφή με το κατάλληλο συνεργείο.
- Καθαρισμός και επισκευή**
- Η συσκευή επιτρέπεται να ανοιχτεί μόνον από ειδικά εκπαιδευμένο τεχνικό προσωπικό. Γι' αυτόν το λόγο να επιτρέπεται τη διεξαγωγή

εργασιών επισκευής μόνο σε συνεργεία που έχουν εξουσιοδοτηθεί από την BinTec. Σχετικά με την έδρα των σχετικών συνεργείων μπορείτε να ζητήσετε πληροφορίες από τον εμπορικό σας αντιπρόσωπο. Το άνοιγμα της συσκευής από αναρμόδια άτομα καθώς και ακατάλληλες εργασίες επισκευής μπορούν να θέσουν το χρήστη σε σοβαρούς κινδύνους (π.χ. ηλεκτροπληξία). Το ανεπίτρεπτο άνοιγμα της συσκευής έχει σαν αποτέλεσμα την ανάκληση κάθε εγγύησης και ευθύνης από μέρος της BinTec Communications AG.

- Η συσκευή δεν επιτρέπεται σε καμία περίπτωση να καθαριστεί. Από την ενδεχόμενη είσοδο νερού μπορεί να προκύψουν σημαντικοί κίνδυνοι για το χρήστη (π.χ. ηλεκτροπληξία) και σοβαρές ζημιές στη συσκευή.
- Να μη χρησιμοποιείτε ποτέ συρμάτινα σφουγγαράκια και αιχμηρά ή αδρά βοηθητικά μέσα καθαρισμού.

Istruzioni generali di sicurezza

Nei seguenti paragrafi si trovano elencate le istruzioni generali di sicurezza da osservare rigorosamente nell'uso del Router.

Trasporto e immagazzinaggio

- Trasportare ed immagazzinare **X1000** soltanto nell'imballaggio originale o in altro imballaggio adeguato a garantire protezione da urti e colpi.

Installazione e azionamento

- Prima di installare ed usare **X1000** fare attenzione alle istruzioni sulle condizioni ambientali (cfr. Dati tecnici). Utilizzare un ripiano stabile e piano.
- Quando l'apparecchio viene trasferito da un ambiente freddo nel locale di esercizio, l'involucro esterno e l'interno dell'apparecchio possono presentare tracce di condensazione. Attendere finché l'apparecchio ha superato lo sbalzo di temperatura ed è assolutamente asciutto, prima di metterlo in funzione. Attenersi alle condizioni ambientali riportate nei dati tecnici
- Controllare che la tensione nominale indicata sulla targhetta dell'alimentatore corrisponda alla tensione di rete locale. **X1000** deve essere usato soltanto con la spina originale BinTec Communications (5 V c. c.). La BinTec Communications AG non risponde dei danni causati dall'utilizzo di una spina diversa.
- Per il cablaggio osservare l'ordine di successione descritto nel manuale. Cablare prima i collegamenti LAN, ISDN e quelli seriali, collegare poi il cavo di alimentazione ed alla fine inserire **X1000** .
- Accertarsi di aver eseguito il cablaggio correttamente – in particolare quello per ISDN e LAN prima di mettere in funzione **X1000** . Il collegamento ISDN di **X1000** non deve essere collegato all'attacco Ethernet del computer o dell'Hub, il collegamento LAN di **X1000** non deve essere collegato all'attacco per ISDN.
- Utilizzare per il cablaggio soltanto i cavi allegati. Nel caso in cui si utilizzino cavi diversi, la BinTec Communications AG non risponde per i danni o la riduzione della funzionalità che ne derivano.
- Disporre i collegamenti in modo che non costituiscano fonte di pericolo (pericolo d'inciampo) e che non possano essere danneggiati.
- Non collegare né disconnettere, né toccare i cavi di trasferimento dati durante un temporale.

**Utilizzazione conforme
alla destinazione,
funzionamento**

- **X1000** è concepito per l'impiego negli uffici. Come Router per reti multiprotocollo **X1000** stabilisce collegamenti WAN in rapporto alla configurazione del sistema. Per evitare canoni indesiderati, si consiglia di controllare assolutamente il prodotto.
- **X1000** è conforme alle relative disposizioni di sicurezza per impianti della tecnica informatica impiegati in ambiente d'ufficio.
- Il funzionamento conforme alla destinazione del sistema secondo IEC 950/EN 60950 è garantito soltanto se è montato il coperchio dell'involucro (raffreddamento, protezione antincendio, schermatura contro radiodisturbi)
- La temperatura ambiente non dovrebbe superare i 50°C. Evitare l'esposizione diretta alla luce solare.
- Fare attenzione che nessun oggetto (p. es. fermagli) o liquido penetri all'interno dell'apparecchio (scossa elettrica, corto circuito). Provvedere ad un sufficiente raffreddamento.
- In casi d'emergenza (p. es. danneggiamento dell'involucro o dell'elemento di comando, infiltrazione di liquido o di corpi estranei) staccare immediatamente la corrente ed informare il servizio assistenza.

**Pulizia e
riparazione**

- L'apparecchio deve essere aperto soltanto da personale competente ed addestrato. Si consiglia pertanto di far riparare l'apparecchio soltanto presso un centro assistenza autorizzato BinTec. Gli indirizzi dei servizi assistenza sono a Sua disposizione presso il rivenditore. Apertura non autorizzata e riparazioni inappropriate possono essere fonte di gravi pericoli per l'utente (p. es. scossa elettrica). Un'apertura non autorizzata degli apparecchi comporta l'esclusione della garanzia e della responsabilità della BinTec Communications AG .
- L'apparecchio non deve assolutamente essere pulito con acqua. L'infiltrazione di acqua può causare gravi pericoli per l'utente (p. es. scossa elettrica) nonché gravi danni all'apparecchio.
- Non utilizzare in nessun caso abrasivi, detersivi a base alcalina, attrezzatura affilata o abrasiva.

Algemene veiligheidsinstructies in het Nederlands

In de volgende paragrafen vindt u veiligheidsinstructies, die u bij de omgang met uw router absoluut moet in acht nemen.

- Transport en bewaring** ■ Transporteer en bewaar **X1000** alleen in de originele verpakking of in een andere geschikte verpakking, die bescherming biedt tegen schokken en stoten.
- Opstellen en in bedrijf nemen** ■ Let voor het opstellen en het bedrijf van **X1000** op de instructies voor de omgevingsvoorwaarden (vergelijk technische gegevens). Gebruik een harde en vlakke ondergrond.
- Als het toestel vanuit een koude omgeving in de bedrijfsruimte gebracht wordt, kan er aan de buiten- en binnenkant van het toestel condensatie optreden. Wacht tot uw toestel zich aan de temperatuur heeft aangepast en helemaal droog is vooraleer u het in gebruik neemt. Neem de milieuvorschriften in de technische gegevens in acht.
- Controleer of de op het typeplaatje aangegeven nominale spanning overeenstemt met de plaatselijke netspanning. **X1000** mag alleen met de originele BinTec Communications elektrische stekkervoeding (5 V DC) worden gebruikt. BinTec Communications AG is niet aansprakelijk voor beschadigingen, die ontstaan door gebruik van een andere elektrische voeding.
- Let bij de aansluiting van de kabels op de volgorde, zoals in het handboek wordt beschreven. Eerst sluit u de LAN-, ISDN- en de seriële aansluitingen aan, sluit daarna de stroomvoorzorging aan, en tenslotte schakelt u **X1000** in.
- Controleer of u de aansluiting - in het bijzonder de ISDN- en LAN-aansluiting correct heeft uitgevoerd, alvorens u **X1000** in bedrijf neemt. De ISDN-aansluiting van **X1000** mag niet met de ethernet-aansluiting van uw computer of hub go-ahead worden verbonden, de LAN-aansluiting van **X1000** niet met uw ISDN-aansluiting.
- Gebruik voor de aansluiting slechts de bijgevoegde kabels. Indien u andere kabels gebruikt, is BinTec Communications AG niet aansprakelijk voor optredende schade.

- Leg de kabels zodanig, dat zij geen gevaarsbron (struikelgevaar) vormen en niet worden beschadigd.
 - Tijdens een onweer de datatransmissielijnen niet aansluiten, uittrekken of aanraken.
- Doelmatig gebruik, bedrijf**
- **X1000** is enkel voor het gebruik in een bureau-omgeving geschikt. Als multi-protocol-router bouwt **X1000** afhankelijk van de systeemconfiguratie WAN-verbindingen op. Om ongewenste kosten te vermijden, moet het product absoluut gecontroleerd worden.
 - **X1000** voldoet aan de gebruikelijke veiligheidsbepalingen voor inrichtingen van informatietechniek voor toepassing in een kantooromgeving.
 - Het doelmatig bedrijf, overeenkomstig IEC 950/EN 60950 van het systeem, is alleen bij gemonteerd huisdeksel gewaarborgd (koeling, brandveiligheid, vonkontstoring)
 - De omgevingstemperatuur mag niet hoger zijn dan 50°C. Vermijd direct zonlicht.
 - Let erop, dat er geen voorwerpen (bijv. paperclips) of vloeistoffen in het inwendige van het apparaat geraken (elektrische schok, kortsluiting). Let op voldoende koeling.
 - Onderbreek in noodgevallen (bijv. beschadigd huis, of bedienelement, binnendringen van vloeistof of vreemde voorwerpen) onmiddellijk de stroomvoorzorging en neemt u contact op met de service-dienst.
- Reiniging en reparatie**
- Het apparaat mag alleen door geschoold vakpersoneel worden geopend. Laat daarom reparaties aan het apparaat alleen uitvoeren door een door BinTec-geautoriseerde service-dienst. Waar zich deze service-dienst bevindt, ervaart u bij uw handelaar. Door het onbevoegde openen en ondeskundige reparaties kunnen aanzienlijke gevaren ontstaan voor de gebruiker (bijv. elektrische schok). Onbevoegd openen van de apparaten heeft verval van de garantie en uitsluiting van de aansprakelijkheid van de BinTec Communications AG tot gevolg.
 - Het apparaat mag in geen geval nat worden gereinigd. Door binnendringend water kunnen er aanzienlijke gevaren ontstaan voor de gebruiker

(bijv. elektrische schok) en kan er aanzienlijke schade ontstaan aan het apparaat.

- Gebruik nooit schuurmiddelen, alkalische reinigingsmiddelen, scherpe of schurende hulpmiddelen.

Generelle sikkerhetshenvisninger på norsk

I de følgende avsnittene finner du sikkerhetshenvisninger som du absolutt må ta hensyn til ved omgangen med din router.

- Transport og lagring** ■ Du må kun transportere og lagre **X1000** i originalemballasjen eller i en annen egnet emballasje som beskytter mot støt og slag.
- Oppstilling og ibruktaking** ■ Før oppstilling og drift av **X1000** må du ta hensyn til henvisningene når det gjelder omgivelsesbetingelsene (sml. tekniske data). Bruk et fast og jevnt underlag.
 - Dersom apparatet blir tatt fra en kald omgivelse og inn i rommet der det skal brukes, kan det oppstå kondens både på utsiden og på innsiden av apparatet. Vent til routeren har tilpasset seg temperaturen og er helt tørr før du tar den i bruk.
 - Kontroller om den spenningen som er oppgitt på typeskiltet på nettdelen stemmer overens med spenningen på stedet. **X1000** må kun brukes sammen det originale BinTec kommunikasjons-støpselet (5 V DC). BinTec Communications AG er ikke ansvarlig for skader som måtte oppstå på grunn av at det er blitt brukt en annen støpsel-nettdel.
 - Ved sammenkopling av kablene, må det tas hensyn til rekkefølgen som er beskrevet i håndboken. Sammenkople først kablene LAN-, ISDN- og serielle tilkoblinger, tilkople så strømforsyningen, og slå deretter til slutt på **X1000**.
 - Kontroller om du har foretatt sammenkoplingen av kablene korrekt– i særdeleshet ISDN- og LAN-sammenkoplingen, før du tar **X1000** i drift. ISDN-tilkoplingen fra **X1000** må ikke forbindes med Ethernet-tilkoplingene på datamaskinen eller med hubs, og LAN-tilkoplingen må ikke forbindes med **X1000** ISDN-tilkoplingen.
 - Bruk kun de vedlagte kablene for tilkoplingen. Dersom du bruker andre kabler, overtar BinTec Communications AG intet ansvar for skader som måtte oppstå av den grunn.
 - Legg opp ledningene slik at de ikke kan bli skadet og at de ikke danner farekilder (fare for å snuble).

- I tordenvær må du verken tilkople dataoverføringsledningene eller frakople eller berøre dem.
- Forskriftsmessig bruk, drift**
- **X1000** er beregnet på bruk i et kontorlandskap. I egenskap av multi-protokoll-router bygger **X1000** opp WAN-forbindelser, avhengig av systemkonfigurasjonen. Det er tvingende nødvendig å overvåke produktet for å unngå utilsiktede gebyrer..
 - **X1000** oppfyller gjeldende sikkerhetsbestemmelser for innretninger innen informasjonsteknikk for bruk i kontorlandskap.
 - Forskriftsmessig bruk i henhold til IEC 950/EN 60950 for systemet er kun gitt ved montert husdeksel (kjøling, brannbeskyttelse, radio-støydempning).
 - Omgivelsestemperaturen bør ikke overstige 50°C. Unngå direkte sollys.
 - Pass på at ingen gjenstander (f. eks. binders) eller væsker kan komme inn i apparatet (fare for elektrisk støt, kortslutning). Pass på tilstrekkelig avkjøling.
 - I nødstilfeller (f.eks. skadet hus eller betjenings-elementer, når væske eller fremmedlegemer er kommet inn) må du straks bryte strømforsyningen og tilkalle service.
- Rengjøring og reparasjon**
- Apparatet må kun åpnes av opplært fagpersonell. La derfor alltid reparasjoner på apparatet gjennomføres av et BinTec-autorisert serviceverksted. Din forhandler informerer deg om hvor du finner serviceverksteder. Dersom uvedkommende åpner eller reparerer apparatet, kan det oppstå alvorlige risikoer for brukeren (f. eks. elektrisk støt). Dersom apparatet blir ulovlig åpnet, kan det ha til følge at garantien tapes, og at BinTec Communications AG fraskriver seg ethvert ansvar.
 - Apparatet må under ingen omstendighet rengjøres med vann. Dersom vann trenger inn, kan det oppstå alvorlige risikoer for brukeren (f. eks. elektrisk støt) og alvorlige skader på apparatet.
 - Bruk aldri skuremidler, alkaliske rengjøringsmidler, skarpe eller skurende hjelpemidler.

Considerações genéricas em matéria de segurança em português

Nos parágrafos que se seguem, encontra considerações em matéria de segurança que terá de respeitar estritamente ao lidar com o Router.

Transporte e armazenamento

- Transporte e armazene o **X1000** apenas na embalagem original ou noutra adequada para o efeito que o proteja contra embates fortes e pancadas.

Instalação e colocação em funcionamento

- Antes de proceder à instalação e à colocação em funcionamento do **X1000** tenha em conta as indicações relativas às condições ambientais (cf. Dados técnicos). Utilize uma base consistente e lisa.
- Quando o aparelho é deslocado de um local frio para o local de funcionamento, poderá haver formação de condensação tanto no exterior como no interior do aparelho. Aguarde até o aparelho se encontrar à temperatura ambiente e completamente seco antes de o colocar em funcionamento. Tenha em atenção as indicações relativas às condições ambientais nos Dados técnicos.
- Verifique se a tensão nominal constante da placa de características da fonte de alimentação é a mesma da do local. O **X1000** só pode ser colocado em funcionamento com a ficha da fonte de alimentação BinTec Communications (5 V DC) original. A BinTec Communications AG não se responsabiliza por danos decorrentes da utilização de outra ficha da fonte de alimentação.
- Ao proceder à cablagem, respeite a sequência, tal como descrita no manual. Proceda primeiro à distribuição das ligações LAN, RDIS e em série, conecte depois a alimentação de corrente e, para terminar, ligue o **X1000**.
- Verifique se a cablagem, em especial da RDIS e da LAN, ficou bem feita, antes de pôr o **X1000** em funcionamento. A ligação RDIS do **X1000** não pode ser conectada à Ethernet do seu computador ou Hubs, a ligação LAN do **X1000** não pode ser conectada à sua ligação RDIS.
- Para o cableamento, utilize unicamente o cabo fornecido juntamente. Se usar outro cabo, a BinTec Communications AG não se responsabiliza por danos daí decorrentes.
- Instale os cabos de maneira a não constituírem uma fonte de perigo (perigo de tropeçar) nem se danificarem.

- Utilização conforme com as especificações, Operação**
- Em caso de trovoadas, não ligue, retire ou toque nos cabos de transmissão de dados.
 - O **X1000** destina-se à utilização em escritórios. Como Router de protocolos múltiplos, o **X1000** constrói ligações WAN de acordo com a configuração do sistema. Para evitar custos indesejados, controle o produto.
 - O **X1000** corresponde às normas de segurança habituais relativas a dispositivos de informática para utilização em escritórios.
 - O funcionamento conforme as especificações IEC 950/EN 60950 do sistema só é garantido com a tampa da caixa montada (refrigeração, protecção contra incêndios, desparasitação).
 - A temperatura ambiente não pode exceder os 50°C. Evite expor o aparelho à luz solar directa.
 - Tenha o cuidado de não deixar entrar objectos (por ex. cliques) ou líquidos para o interior do aparelho (choque eléctrico, curto-circuito). Verifique se a refrigeração é suficiente.
 - Em caso de emergência (por ex. caixa ou elemento de comando danificado, entrada de líquido ou de corpos estranhos), interrompa imediatamente a alimentação de corrente e recorra ao serviço de assistência técnica.
- Limpeza e reparação**
- O aparelho só pode ser aberto por pessoal especializado. Por isso, deixe as reparações do aparelho exclusivamente a cargo de um serviço de assistência técnica BinTec autorizado. Informe-se junto do seu agente para saber onde encontrar um ponto de assistência técnica. O utilizador pode colocar-se a si próprio em perigo caso abra o dispositivo sem qualquer autorização ou proceda a uma reparação imprópria (por ex. choque eléctrico). A abertura não autorizada do aparelho tem como consequência a perda da garantia e da responsabilidade da BinTec Communications AG.
 - O aparelho nunca pode ser limpo a húmido. A infiltração de água pode constituir perigo para o utilizador (por ex. choque eléctrico) e danos de monta no aparelho.
 - Nunca utilizar abrasivos, produtos de limpeza alcalinos, objectos afiados ou que risquem.

Ogólne zasady bezpieczeństwa w języku polskim

Poniżej podano zasady bezpieczeństwa, których należy bezwzględnie przestrzegać przy obchodzeniu się z routerem.

Transport i magazynowanie

- Urządzenie **X1000** należy transportować i magazynować wyłącznie w opakowaniu oryginalnym lub innym nadającym się do tego celu opakowaniu, zapewniającym ochronę przed obciami i uderzeniami.

Ustawianie i uruchamianie

- Przed ustawieniem i uruchomieniem urządzenia **X1000** należy zastosować się do wskazówek dotyczących warunków otoczenia (por. Parametry techniczne). Urządzenie należy ustawić na trwałym i równym podłożu.
- W momencie przemieszczenia urządzenia z zimnego otoczenia do pomieszczenia eksploatacyjnego, może wystąpić pokrycie parą zarówno części zewnętrznych jak i wewnętrznych. Należy odczekać aż urządzenie przejmie nową temperaturę i całkowicie wyschnie, dopiero wtedy możliwa jest jego eksploatacja. Należy przestrzegać warunków środowiskowych opisanych w danych technicznych urządzenia.
- Należy sprawdzić, czy podane na tabliczce typologicznej zasilacza napięcie znamionowe jest zgodne z lokalnym napięciem sieciowym. Urządzenie **X1000** można eksploatować wyłącznie w połączeniu z oryginalnym zasilaczem wtykowym produkcji firmy BinTec Communications (5 V DC). Firma BinTec Communications AG nie odpowiada za szkody wywołane stosowaniem zasilacza innego typu.
- Przy przyłączaniu przewodów należy przestrzegać kolejności opisanej w instrukcji obsługi. W pierwszej kolejności należy przyłączyć złącza LAN, ISDN oraz złącza seryjne, następnie włączyć zasilanie prądem elektrycznym, na koniec zaś włączyć router **X1000**.
- Przed uruchomieniem urządzenia **X1000** należy sprawdzić, czy przyłączenie przewodów - a w szczególności przewodów ISDN i LAN - jest prawidłowe. Złącze ISDN urządzenia **X1000** nie może być połączone ze złączem ethernetowym komputera lub koncentratora, zaś złącze LAN urządzenia **X1000** ze złączem ISDN.
- Do przyłączenia produktu należy zastosować wyłącznie dostarczone wraz z nim przewody. W przypadku zastosowania innych przewodów firma BinTec Communications AG nie ponosi odpowiedzialności za powstałe szkody.

- Przewody należy ułożyć tak, aby nie występowało niebezpieczeństwo potykania się o nie oraz ich uszkodzania.
 - Podczas burzy nie wolno podłączać przewodów przenoszenia danych, ani też dotykać ich lub wyłączać.
- Zgodne z przeznaczeniem stosowanie, eksploatacja**
- **X1000** przeznaczona jest do pracy w otoczeniu biurowym. Jako Multi-Protokoll-Router buduje **X1000** niezależnie od konfiguracji systemowej połączenia WAN. Aby zapobiec nieprzewidzianym opłatom, powinno się go strzec.
 - Urządzenie **X1000** spełnia obowiązujące zasady bezpieczeństwa dla urządzeń informatycznych przeznaczonych do stosowania w otoczeniu biurowym.
 - Zgodne z przeznaczeniem użytkowanie systemu według wymogów norm IEC 950/EN 60950 jest zagwarantowane tylko przy zamontowanej pokrywie obudowy (chłodzenie, zabezpieczenie przeciwpożarowe, eliminacja zakłóceń)
 - Temperatura otoczenia nie powinna przekraczać 50°C. Należy unikać bezpośredniego działania promieni słonecznych.
 - Należy uważać, aby do wnętrza urządzenia nie wniknęły żadnego rodzaju przedmioty (np. spinacze biurowe) bądź ciecze (udar prądowy, zwarcia). Zapewnić wystarczające chłodzenia urządzenia.
 - W sytuacjach awaryjnych (np. uszkodzona obudowa lub element obsługi, wniknięcie cieczy bądź ciał obcych) należy natychmiast przerwać zasilanie urządzenia prądem elektrycznym i zawiadomić serwis.
- Oczyszczanie i naprawa**
- Urządzenie może być otwierane tylko przez odpowiednio przeszkolony personel. Naprawy urządzenia należy w związku z tym zlecać wyłącznie autoryzowanym przez firmę BinTec punktom serwisowym. Informacji na temat lokalizacji tych punktów można zasięgnąć w punkcie sprzedaży. Otwieranie obudowy urządzenia bez upoważnienia lub jego niefachowe naprawy mogą wywoływać poważne zagrożenia dla użytkownika (np. porażenie prądem). Niedozwolone otwieranie urządzeń pociąga za sobą utratę gwarancji udzielanej przez firmę BinTec Communications AG oraz jej odpowiedzialności cywilnej za skutki użytkowania produktu.

- Urządzenia pod żadnym pozorem nie wolno czyścić na mokro. Dostanie się wody do wnętrza urządzenia może wywoływać poważne zagrożenia dla użytkownika (np. porażenie prądem) oraz poważne uszkodzenia produktu.
- Nigdy nie stosować środków do szorowania, zasadowych środków czyszczących, ostrych lub szorujących środków pomocniczych.

Instrucciones generales de seguridad

En los párrafos siguientes encontrará unas instrucciones de seguridad. Es imprescindible tener las mismas en cuenta a la hora de manejar su router.

Transporte y almacenamiento

- Transporte y almacene su **X1000** únicamente en su embalaje original o en otro embalaje adecuado que garantice su protección contra golpes y choques.

Colocación y puesta en servicio

- Antes de la colocación y puesta en servicio de **X1000**, observe las instrucciones acerca de las condiciones ambientales (ver Datos técnicos). Utilice una superficie firme y plana.
- Si el aparato proviene de un ambiente frío, al introducirlo en el local de trabajo se puede producir deshielo tanto en su exterior como en su interior. Por ello, antes de ponerlo en funcionamiento espere a que su temperatura se haya igualado y a que esté totalmente seco. Preste atención a las condiciones medioambientales expuestas en el apartado de Datos Técnicos.
- Asegúrese de que la tensión nominal indicada en la placa de características coincide con la tensión de la red local. **X1000** únicamente debe ponerse en funcionamiento con el bloque de alimentación original de BinTec Communications (5 V DC). BinTec Communications AG no se hace responsable de los daños y perjuicios causados por el uso de otro tipo de bloque de alimentación.
- A la hora de cablear, respete el orden descrito en el manual. Cablee primero las conexiones LAN, RSDI y de serie, conecte la alimentación de energía eléctrica y encienda finalmente el **X1000**.
- Asegúrese del cableado correcto -y sobre todo del cableado de las conexiones LAN y RSDI- antes de poner **X1000** en servicio. La conexión RSDI de **X1000** no debe conectarse a la conexión Ethernet de su ordenador o hub, ni la conexión LAN de **X1000** a su conexión RSDI.
- Realice el cableado únicamente con los cables suministrados. Si utiliza cables distintos, BinTec Communications AG no asumirá la responsabilidad de los daños y perjuicios que puedan producirse.
- Coloque los cables de manera que no constituyan un peligro (tropezones) y no puedan ser deteriorados.

Utilización prevista, servicio

- Durante una tormenta, no enchufe ni desenchufe los conductos de transmisión de datos, ni los toque.
- **X1000** está concebido para ser utilizado en oficinas. Como router multiprotocolo, **X1000** establece conexiones WAN dependiendo de la configuración del sistema. Para evitar que se produzcan gastos de conexiones indeseadas, es absolutamente necesario vigilar el producto.
- **X1000** corresponde a las disposiciones de seguridad pertinentes para equipos informáticos utilizados en oficinas y despachos.
- El servicio previsto del sistema de acuerdo con IEC 950/EN 60950 queda únicamente garantizado si la tapa permanece montada en la caja (refrigeración, prevención de incendios, supresión de interferencias).
- La temperatura ambiental no debe superar los 50°C. No exponga el aparato a la luz solar directa.
- Procure que ningún objeto (p. ej. clips) o líquido entre en el interior del aparato (descargas eléctricas, cortocircuitos) y que exista una refrigeración suficiente.
- En casos de emergencia (p. ej. caja o elemento de mando deteriorados, penetración de líquidos o de cuerpos extraños), interrumpa inmediatamente la alimentación de energía y avise al servicio técnico.

Limpieza y reparación

- El aparato debe ser abierto únicamente por personal técnico cualificado. Por lo tanto, realice las posibles reparaciones del aparato sólo a través de un servicio técnico autorizado por BinTec. Su vendedor le informará de la dirección del servicio técnico. El abrir y reparar el aparato sin autorización puede conllevar un peligro considerable para el usuario (descargas eléctricas). El abrir de los aparatos sin autorización tiene como consecuencia la exoneración de la responsabilidad y de la garantía de BinTec Communications AG.
- En ningún caso, el aparato debe limpiarse en húmedo. Al penetrar agua, puede existir un peligro considerable para el usuario (p. ej., descargas eléctricas) y pueden producirse daños considerables en el aparato.
- No utilizar jamás productos abrasivos, detergentes alcalinos, ni instrumentos afilados o abrasivos.

Allmänna säkerhetsanvisningar på svenska

Beakta alltid nedanstående säkerhetsanvisningar för användning av apparaten.

- Transport och förvaring** ■ **X1000** får endast transporteras och förvaras i originalförpackningen eller i en annan likvärdig förpackning som ger ett fullvärdigt skydd mot stötar och slag.
- Installation och start** ■ Beakta uppgifterna om omgivningsförhållanden (se Tekniska data) innan **X1000** installeras och startas. Installera den på ett stabilt och jämnt underlag.
- Om enheten flyttas från en kall till en varm omgivning kan det bildas kondensvatten på och i apparaten. Tag apparaten i drift först när den har nått rumstemperatur och har torkat helt. Beakta uppgifterna över omgivningsförhållanden i Tekniska data.
- Kontrollera att märkspänningen som anges på nätdelens typskylt överensstämmer med nätspänningen på platsen. **X1000** får endast användas tillsammans med en original BinTec Communications nätenhet (5 V DC). BinTec Communications AG ansvarar inte för skador som uppstår p g a att en annan nätenhet används.
- Utför kabeldragningen i den ordningsföljd som anges i handboken. Anslut först kablarna för LAN- och ISDN-anslutningar samt för serieanslutningar, anslut därefter strömförsörjningen och starta sedan **X1000**.
- Kontrollera att kabeldragningen har utförts rätt – speciellt för ISDN- och LAN-anslutningarna – innan **X1000** startas. ISDN-anslutningen på **X1000** får inte kopplas samman med en Ethernet-anslutning på en dator eller en anslutningsbox, LAN-anslutningen på **X1000** får inte kopplas samman med en ISDN-anslutning.
- Använd endast medlevererade kablar för kabeldragningen. BinTec Communications AG påtar sig inget ansvar för eventuella skador eller brister på apparaten om den används tillsammans med andra kablar.
- Drag kablarna så att de inte kan utgöra någon fara (de får inte ligga så att man kan snubbla över dem) och så att de inte kan skadas.
- Dataöverföringskabeln får inte anslutas, dras ut eller vidröras under ett åskväder.

Ändamålsenlig användning, drift

- **X1000** är avsedd för användning i kontorslokaler. **X1000** är en multi-protokoll-router som, beroende på systemkonfiguration, upprättar WAN-förbindelser. Produkten bör övervakas så att inte onödiga kostnader uppstår.
- **X1000** uppfyller kraven i alla relevanta säkerhetsbestämmelser för informationsteknikutrustning i kontorslokaler.
- Ändamålsenlig användning av systemet enligt IEC 950/EN 60950 säkerställs endast om plåthöljet är monterat (kylning, brandskydd, radioavstörning).
- Omgivningstemperaturen bör inte vara högre än 50°C . Undvik direkt solljus.
- Säkerställ att det inte kan komma in några föremål (t ex häftklammer) eller någon vätska i apparaten (strömstötter, kortslutning). Sörj för fullgod kylning.
- Koppla genast ifrån strömförsörjningen i nödsituationer (t ex skadat hölje eller skadade manöverelement, eller om vätska eller främmande föremål har kommit in i apparaten) och tag kontakt med serviceavdelningen.

Rengöring och reparation:

- Apparaten får endast öppnas av behörig fackpersonal. Reparationer får bara utföras av en av BinTec auktoriserad serviceverkstad. Återförsäljaren tillhandahåller information om närmaste serviceverkstad. Obehörigt öppnande resp ej sakkunniga reparationer på apparaten kan medföra fara för användaren (t ex elektriska stötar). Om apparaten öppnas utan tillstånd gäller inte längre garantiansvaret från BinTec Communications AG.
- Apparaten får aldrig våtrengöras. Vatten som kommer i enheten kan medföra fara för användaren (t ex elektriska stötar) och förorsaka skador på apparaten.
- Använd inget skurpulver, inga alkaliska rengöringsmedel, använd inga vassa resp repande hjälpmedel.

Genel güvenlik bilgileri türkçe

Müteakip bölümlerde cihazınızı kullanırken mutlaka dikkat etmeniz gereken genel güvenlik bilgilerini bulabilirsiniz.

- Taşıma ve Depolama** ■ **X1000** cihazı sadece orjinal ambalajı içinde veya çarpmaya ve darbeye karşı koruyan uygun başka bir ambalajla taşıyıp depolayınız.
- Kurulması ve Çalıştırılması** ■ **X1000** cihazını kurup çalıştırmadan önce çevre koşulları hakkındaki bilgileri dikkate alınız (bak. Teknik Bilgiler). Sağlam ve düz bir altlık kullanınız.
- Cihaz, çalıştırılacağı odaya soğuk bir ortamdan getirilmiş ise, cihazın dışında ve içinde çiylenme olabilir. Cihazınızı çalıştırmadan önce tamamen kurumasını ve oda sıcaklığına uyum sağlamasını bekleyiniz. Teknik Bilgiler'deki çevre koşullarını dikkate alınız.
- Trafonun model etiketinde verilen anma gerilimin yerel şebeke gerilimi ile eşit değerde olup olmadığını kontrol ediniz. **X1000** cihazı sadece orjinal Bin Tec Kommunikation fişli trafo (5 V DC) ile kullanılmalıdır. BinTec Communications AG başka bir trafo ile kullanımdan kaynaklanan hasarlar için sorumluluk üstlenmez.
- Kabloları takarken el kitapçığındaki sıralamaya dikkat ediniz. Önce LAN-, ISDN ve seri bağlantıları takınız, ondan sonra elektrik bağlantısını açın ve son olarak da **X1000** cihazını bağlayınız.
- **X1000** cihazını çalıştırmadan önce kablo bağlantılarının -özellikle ISDN ve LAN kablo bağlantıları- doğru olup olmadığını kontrol ediniz. **X1000** cihazının ISDN bağlantısı bilgisayarınızın veya sanızın ethernet bağlantısı ile; **X1000** cihazının LAN bağlantısında ISDN bağlantısı ile birleştirilmelidir.
- Kablo bağlantıları için, sadece cihazın yanında bulunan kabloları kullanınız. Başka kablo kullandığınız takdirde, BinTec Communications AG meydana gelen hasar veya fonksiyonlardaki olumsuz etkilerden dolayı sorumluluk üstlenmez.
- Kabloları, tehlike kaynağı olamayacak ve zarar görmeyecek şekilde (takılma tehlikesi) döşeyiniz.
- Fırtına esnasında veri iletişim hatlarını ne bağlayınız, ne çıkartınız, ne de bunlara dokununuz.

Belirlenmiş şekilde kullanım, işletim

- **X1000** cihazı büro ortamında kullanım için tasarlanmıştır. Multi-Protokol-Router olarak **X1000** cihazı sistem konfigürasyonuna bağlı olarak WAN-bağlantıları kurmaktadır. İstenmeyen masrafları önlemek için, ürünü mutlaka kontrol altında tutunuz.
- **X1000** cihazı, büro ortamında kullanılan enformasyon teknik donanımları için geçerli olan güvenlik talimatnamelerine kesinlikle uymaktadır.
- IEC 950/EN 60950 uyarınca, sistemin belirlenmiş şekilde kullanımı sadece saç kasası tamamiyle monte edildiğinde sağlanabilir (soğutma, yangın önleme, parazit giderme).
- Çevre sıcaklığı 50°C' yi aşmamalıdır. Cihazı direk gelen güneş ışınlarından koruyunuz
- Cihazın içine yabancı cisimlerin (örneğin ataç) veya sıvıların girmesini önleyiniz (elektrik çarpması, kısa devre). Cihazın yeterli oranda soğutulmasına dikkat ediniz.
- Acil durumlarda (örneğin hasarlı cihaz kasası veya kullanım parçası, cihazın içine sıvı veya yabancı maddelerin girmesi) derhal elektrik akımını kesip servise haber veriniz.

Temizlik ve Tamir

- Cihaz sadece eğitilmiş uzman personel tarafından açılabilir. Bu yüzden cihazın tamiratını sadece BinTec yetkili servisi tarafından yaptırınız. Yetkili servis yerlerini nerede bulabileceğinizi satıcınızdan öğrenebilirsiniz. Müsaade edilen işlemler dışında açılması ve uygun olmayan şekilde tamir edilmesi, kullanıcı için büyük tehlikeler doğurabilir (örneğin elektrik çarpması). ICihazın izinsiz açılması, BinTec Communications AG'nin garanti ve sorumluluk yükümlülüğünün ortadan kalkmasına neden olur.
- Cihazın su ile temizlenmesi kesinlikle yasaktır. Suyun cihaz içine kaçması, kullanıcı için büyük tehlikeler doğurabilir (örneğin elektrik çarpması) ve cihaza da ciddi zararlar verebilir.
- Kesinlikle temizleme tozları, alkalik temizlik maddeleri, keskin veya aşındırıcı yardımcı maddeler kullanmayınız.

Általános biztonsági útmutató

A következő fejezetekben olyan biztonsági útmutatásokat talál, amelyeket a készüléke alkalmazása során feltétlenül figyelembe kell vennie.

- Szállítás és tárolás** ■ Az **X1000** csak az eredeti vagy egy más, arra alkalmas csomagolásban szállítandó és tárolandó, amely lökések és ütések ellen védelmet biztosít.
- Felállítás és üzembe helyezés** ■ Az **X1000** felállítása és üzembe helyezése előtt vegye figyelembe a környezeti feltételekre vonatkozó utasításokat (v.ö. a műszaki adatokkal). A készüléket szilárd és sík alapon alkalmazza.
- Ha a készülék hideg környezetből kerül az üzemeltetési helyére, akkor a készülék külsején és belsejében lecsapódhat a nedvesség. Az üzembe helyezés előtt várja meg, amíg a készülék el nem éri a szobahőmérsékletet, és teljesen meg nem szárad. Vegye figyelembe a műszaki adatoknál megadott környezeti feltételeket.
- Ellenőrizze, hogy a tápegység típusábláján megadott névleges feszültség megegyezik-e a helyi hálózati feszültséggel. Az **X1000** csak az eredeti BinTec Communications csatlakozó tápegységgel (5 V DC) üzemeltethető. A BinTec Communications AG nem vállal felelősséget olyan károkért, amelyek egy másik csatlakozó tápegység alkalmazása révén keletkeztek.
- A vezetékezés során vegye figyelembe a kézikönyvben megadott sorrendet. Először az LAN-, ISDN- és a soros csatlakozásokat vezetékhez, azután csatlakoztassa az áramellátást, végül kapcsolja be az **X1000** készüléket.
- Ellenőrizze, hogy a vezetékezés – különösen az ISDN- és LAN-vezetékezés – helyesen lett-e kivitelezve, mielőtt az **X1000** készüléket üzembe helyezi. Az **X1000** ISDN-csatlakozója nem csatlakozhat az Ön számítógépének vagy a hubjának az Ethernet csatlakozójához, az **X1000** LAN-csatlakozója pedig nem csatlakozhat az Ön ISDN-csatlakozójához.
- Csak a mellékelt vezetékeket alkalmazza a vezetékezéshez. Amennyiben más vezetékeket alkalmaz, az emiatt fellépő károkért vagy a működésben fellépő változásokért a BinTec Communications AG nem vállal felelősséget.
- A vezetékeket úgy fektesse le, hogy azok ne lehessenek veszélyek forrásai (botlásveszély), azokban pedig kár ne keletkezhesen.

- Az adatátvivő vezetékeket vihar esetében ne csatlakoztassa, ne húzza le, ne érintse meg.
- Rendeltetésszerű alkalmazás, üzemeltetés**
- Az **X1000** irodai környezetben való alkalmazásra készült. Az **X1000**, mint multi-protokoll-router, a rendszerkonfigurációtól függően a WAN-összeköttetésekre épül. A nem kívánt telefondíjak elkerülése végett, a terméket feltétlenül tartsa megfigyelés alatt.
 - Az **X1000** megfelel az idevágó - irodai környezetben való használatra alkalmas információtechnikai berendezésekre vonatkozó - biztonsági előírásoknak.
 - A rendszer rendeltetésszerű üzemeltetése az IEC 950/EN 60950 szabályzatnak megfelelően csak a teljesen összeszerelt fémburkolattal biztosítható (hűtés, tűzvédelem, zavarcsökkentés).
 - A környezeti hőmérséklet nem haladhatja meg az 50 °C-t. Kerülje a közvetlen napsütést.
 - Ügyeljen arra, hogy semmilyen tárgy (pl. gémkapocs) vagy folyadék ne kerülhessen a készülék belsejébe (áramütés, rövidzárlat). Ügyeljen a megfelelő hűtésre.
 - Vészhelyzetben (pl. sérült burkolat vagy kezelőegység, folyadék vagy idegen test behatolása esetén) azonnal szakítsa meg az áramellátást, és értesítse a szervizt.
- Tisztítás és javítás**
- A készüléket csak erre iskolázott szakember nyithatja fel. A készüléken szükséges javításokat ezért csak a BinTec által feljogosított szervizekkel végeztesse. A szervizek címét érdeklődjön meg a szakkereskedőjénél. A készülék jogtalan felnyitása és a helytelen javítás révén a felhasználó számára jelentős veszélyforrások keletkezhetnek (pl. áramütés). A készülékek engedély nélkül történő felnyitása a BinTec Communications AG felelősségének és garanciális kötelezettségének megszűnését vonja maga után.
 - A készüléket semmi esetre sem szabad nedvesen tisztítani. A behatoló víz jelentős veszélyforrásokat jelenthet a felhasználó számára (pl. áramütés), és jelentős károkat okozhat a készüléken.

- Sohasem szabad súrolószereket, lúgos tisztítószereket, éles vagy karcoló segédeszközöket alkalmazni.

Všeobecné bezpečnostní pokyny

V následujících odstavcích jsou uvedeny bezpečnostní pokyny, které se při používání přístroje musí zásadně dodržovat.

- Doprava a uskladnění**
- **X1000** dopravujte a skladujte pouze v originálním obalu anebo v jiném vhodném obalu, který jej chrání proti nárazům.
- Instalace a uvedení do provozu.**
- Před instalací a provozem **X1000** přihlížejte k pokynům, které se týkají podmínek okolního prostředí (srovn. Technické údaje). Předpokládá se pevný a rovný podklad.
 - Pokud se přístroj přemístí z chladného prostředí do provozního prostoru, může se vyskytnout orosení jak na vnějších částech tak i uvnitř přístroje. Vyčkejte teplotní přizpůsobení přístroje a jeho absolutní vysušení, než jej uvedete do provozu. Přihlížejte k podmínkám okolního prostředí uvedeným v Technických údajích.
 - Zkontrolujte, zda se jmenovité napětí uvedené na typovém štítku síťového zdroje shoduje s napětím místní sítě. **X1000** se smí provozovat pouze s originálním síťovým zdrojem BinTec Communications (5 V DC). BinTec Communications AG neručí za škody vzniklé z důvodu použití jiného síťového napájecího zdroje.
 - Při propojování dbejte na pořadí tak, jak je popsáno v příručce. Propojte nejdříve přípojky LAN, ISDN a sériové přípojky, potom zapojte napájení ze sítě, a jako poslední zapněte **X1000**.
 - Zkontrolujte, zda bylo řádně provedeno propojení – zejména propojení ISDN a LAN – , než uvedete **X1000** do provozu. Přípojka ISDN u **X1000** se nesmí spojovat s přípojkou Ethernet Vašeho počítače anebo s huby, LAN přípojka u **X1000** se nesmí připojit na Vaši přípojku ISDN.
 - Na propojování použijte pouze přiložené kabely. Pokud použijete jiné kabely, odmítá BinTec Communications AG ručení za vzniklé škody nebo za omezenou funkčnost.
 - Vedení ukládejte tak, aby se nestala zdrojem nebezpečí (např. zakopnutí) a aby se nepoškodily.
 - Během bouřky nepřipojujte vedení na přenos dat, neodpojujte je a ani se jich nedotýkejte.

Použití, provoz podle stanoveného účelu

- **X1000** je určen pro použití v kancelářském prostředí. Jako MultiProtocol Router sestavuje **X1000** v závislosti na systémové konfiguraci spojení WAN. Chcete-li zabránit účtování nežádoucích poplatků, měli byste výrobek bezpodmínečně hlídat.
- **X1000** odpovídá příslušným bezpečnostním předpisům pro zařízení informační techniky používaná v kancelářském prostředí.
- Provoz systému odpovídající stanovenému účelu podle IEC 950/EN 60950 je zaručen pouze při namontovaném krytu skříně (chlazení, protipožární ochrana, odrušení).
- Teplota okolí by neměla překročit 50°C. Zabraňte přímému ozáření sluncem.
- Dbejte na to, aby do vnitřku přístroje nemohly vniknout žádné předměty (např. kancelářské svorky) nebo kapaliny (elektrický výboj, zkrat). Dbejte na dostatečné chlazení.
- V nouzových případech (např. poškozená skříň anebo ovládací prvek, vniknutí kapaliny nebo cizích těles) okamžitě přerušete přívod proudu a informujte servis.

Čištění a opravy

- Přístroj smí otvírat pouze školený odborný personál. Provedením oprav přístroje proto pověřte pouze autorizovaný servis firmy BinTec. Adresu servisu Vám sdělí Váš obchodník. Nepovolaným otevíráním a neodbornými opravami se uživatel vystavuje značnému ohrožení (např. zasažení elektrickým proudem). Nedovolené otevření přístrojů má za následek zánik záruky a ručení firmy BinTec Communications AG .
- Přístroj se zásadně nesmí čistit mokrým způsobem. Vnikající voda může uživatele vystavit značnému ohrožení (např. zasažení elektrickým proudem) a může způsobit značné poškození přístroje.
- Nikdy nepoužívejte prostředky na mechanické čištění, alkalické čisticí prostředky, agresivní a drhnoucí pomůcky.

Generelle sikkerhedsforskrifter på dansk

Nedenstående afsnit indeholder sikkerhedsforskrifter, som ubetinget skal overholdes ved brugen af apparatet.

- Transport og opbevaring** ■ Transportér og opbevar kun **X1000** i originalemballage eller i anden egnet emballage, der beskytter mod stød og slag.
- Opstilling og ibrugtagning** ■ Læs og overhold forskrifterne for de omgivende betingelser, før **X1000** opstilles og tages i brug (se Tekniske data). Brug et fast og jævnt underlag.
- Hvis apparatet bringes fra kolde omgivelser ind i det rum, hvor det skal bruges, kan der opstå kondensvand både udvendigt og indvendigt på apparatet. Vent, indtil apparatet har tilpasset sig temperaturen og er absolut tørt, før du tager det i brug. Overhold omgivelsesbetingelserne i Tekniske data.
- Kontrollér om spændingen på typeskiltet stemmer overens med spændingen på brugsstedet. **X1000** må kun benyttes med den originale stiknetdel fra BinTec Communications (5 V DC). BinTec Communications AG hæfter ikke for skader, som måtte opstå som følge af brug af en anden stiknetdel.
- Sørg for at kablerne forbindes i den rigtige rækkefølge (se beskrivelsen i manualen). Forbind først LAN-, ISDN- og serielle tilslutninger, tilslut derefter strømforsyningen og tænd til sidst for **X1000**.
- Kontrollér om kablerne - især ISDN- og LAN-kablerne - er forbundet rigtigt, før **X1000** tages i brug. ISDN-tilslutningen på **X1000** må ikke forbindes med Ethernet-tilslutningen på din computer eller hub og LAN-tilslutningen på **X1000** må ikke forbindes med din ISDN-tilslutning.
- Apparatet må kun tilsluttes med de vedlagte kabler. Hvis du benytter andre kabler, fraskriver BinTec Communications AG sig ansvaret for evt. skader og funktionsbegrænsninger.
- Ledningerne skal trækkes på en sådan måde, at de ikke beskadiges og at de ikke er til fare for omgivelserne (fare for at snuble).
- Undlad at tilslutte eller trække datatransmissionsledninger ud af apparatet, når det er tordennejr, og undlad at berøre dem.

**Bestemmelsesmæssig
anvendelse, brug**

- **X1000** er beregnet til anvendelse i kontormiljø. Som multiprotokolrouter etablerer **X1000** WAN-forbindelser afhængigt af systemkonfigurationen. For at forebygge uønskede afgiftsbetalinger bør du ubetinget overvåge produktet.
- **X1000** opfylder de gældende sikkerhedsbestemmelser for informationsteknisk udstyr til kontorer.
- Bestemmelsesmæssig anvendelse af systemet iht. IEC 950/EN 60950) er kun sikret, når kabinetlåget er monteret (køling, brandsikkerhed, radiostøjdæmpning).
- Omgivelsestemperaturen må ikke overstige 50°C. Undgå direkte sollys.
- Sørg for, at genstande (f.eks. klips) eller væske ikke trænger ind i apparatet (elektrisk stød, kortslutning). Sørg for tilstrækkelig køling.
- Afbryd straks strømforsyningen og kontakt serviceafdelingen i nødstilfælde (f.eks. beskadiget kabinet eller betjeningselement, indtrængning af væske eller fremmede genstande).

**Rengøring og
reparation**

- Apparatet må kun åbnes af uddannede fagfolk. Reparationer på apparatet skal derfor altid udføres på et autoriseret BinTec-serviceværksted. Din forhandler kan oplyse om det nærmeste serviceværksted. Uautoriseret åbning og ukorrekt udførte reparationer kan medføre betydelige farer for brugeren. BinTec Communications AG fraskriver sig ethvert ansvar og garanti bortfalder, hvis apparatet åbnes uden tilladelse.
- Apparatet må under ingen omstændigheder rengøres med væske. Indtrængende vand kan udsætte brugeren for alvorlige farer (f.eks. elektrisk stød) og forårsage alvorlige skader på apparatet.
- Benyt aldrig skuremidler, alkaliske rengøringsmidler, skrappe eller skurende hjælpemidler.

- 10Base-2** Thin Ethernet connection. Network connection for 10-Mbps networks with BNC connector. T-connectors are used for the connection of equipment with BNC sockets.
- 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**.
- a/b** Standard interface for analog terminals (telephone, fax group 2/3, analog modems). Only for BinTec routers with integrated >>> **PABX**.
- 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 **X1000** 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 (communications programs such as RVS-COM Lite) 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 **X1000**'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.

- Configuration Manager** Windows application (similar to the Windows Explorer), which uses SNMP commands to request and carry out the configuration of **X1000**. Before **BRICKware** Version 5.1.3, the application was named Dime Browser.
- 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
- Dialup connection** A connection is set up when required by dialing an extension number, in contrast to a **leased line**.
- 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. **X1000** can be used as a DHCP server.
- 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.
- DIME Browser** Former name for **Configuration Manager**.

- 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.

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. **X1000** 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).
- 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 **X1000**'s features. **X1000** 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.

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.

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 **X1000**. 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.

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-point** Feature of a connection between two data stations only. The connection can be permanently switched or set up via switching systems.
- 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 **X1000**).

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 **X1000** 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.

X1000 is supplied as standard with suitable software (RVS-COM Lite).

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 **X1000** 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 **X1000**. 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.

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	Access lists	317
	Access security	308
	Advanced configuration	201
	Always On/Dynamic ISDN	220
	AO/DI	220
	ARP	247
	Authentication	208, 310, 335
	Auto logout	340
B	Back route verification	334
	Bandwidth on Demand	214
	Basic router configuration	
	Configuration Wizard	53
	Setup Tool	129
	BinTec Companion CD	18
	Blowfish	336
	BOD	214
	BOOT sequence	380
	BOOTmonitor	380
	BOOTP relay agent	278
	Branch office	47
C	Callback	310
	CAPI	88
	CAPI user concept	204
	Channel bundling	84, 212, 214
	Advance configuration	214
	Basic configuration	212
	CHAP	208, 310
	Checking the calling party number	309
	Checking the TCP/IP protocol	40
	CLID	309
	Closed User Group	312
	Commands	
	SNMP shell	384

Communications applications	46
Compression	87
MS-STAC	245
STAC	87, 245
Van Jacobson Header Compression	87, 245
Compuserve	184, 187
Configuration	
Advanced	201
Configuration	78
Configuring a PC	66
Partner's network	68
Preparation	36
Remote	110
Remote CAPI	64
RVS-COM Lite	71
Saving	199
Sending and receiving e-mails	78
Sending and receiving faxes	71
Setup Tool	127
under Windows	50
Configuration file administration	346
Configuration options	
Overview	113
Configuring a PC	66
Configuring answering machine	71
Configuring fax	71
Configuring WAN partners	158
Connection methods	106
ISDN	110
LAN	109
Serial interface	107
Connections	376
Corporate network connection	
Configuration Wizard	59
Dial-in (without router)	193
General example	190
Setup Tool	190

	Credits Based Accounting System	299
D	Default route	176
	Delay after connection failure	211
	Denial-of-Service attacks	340
	DES	336
	DHCP server	92
	DNS	95, 238, 259
	Documentation	20
	Domain Name	259
	Dynamic IP address server	202
E	E-mails	78
	Encapsulation	135
	Encryption	336, 339
	Entering your license	130
	Ex works state	353
	Extended IP routing	335
	Extensions	84
	Extra license	288
F	Factory reset	353
	Field service staff	48
	Filters	101, 151, 317, 330
	Flash memory	346
G	General PPP settings	208
	General Safety Precautions	29
	Guarantee terms	22
H	HTTP status page	302
I	Incoming Call Answering	138
	Installing BRICKware	43
	Installing the TCP/IP protocol	41

Internet access	
Compuserve	184
Configuration Wizard	57
Setup Tool	184
T-Online	184
IP address	92, 135
Pool	202
IPSec	288, 339
IPX	281
LAN interface	283
WAN partner	284
ISDN	84, 138
K Keepalive monitoring	249
L LAN interface	135
LAN-LAN connection	
Configuration Wizard	59
Setup Tool	190
Layer 1 Protocol	233
Leased line	138, 288
LEDs	373
License card	36
Line tapping security	336
Local filters	330
Logging in	111, 308
M Memory	346
MIB	103
Monitoring functions in the Setup Tool	295
MPPE	336
MS-STAC	245
N Name resolution	95, 238, 259
NAT	182, 313
NetBIOS	95, 101, 238
Netmask	135

	Network Address Translation	182, 313
	Novell networks	281
O	Overview	83
P	PAP	208, 310
	Partner's network	68
	Password, changing	120
	Passwords, entering	132
	Pick-up Service	22
	Pin assignment	377
	Port	277, 317
	PPP settings	208
	PPTP	288, 339
	Product features	370
	Proxy ARP	247
R	RAM	346
	Receiving a fax	80
	Remote CAPI	64, 88, 312
	RIP	242
	Routing	98
	Routing entry	176
	Routing Information Protocol	242
	Rule	317
	RVS-COM Lite	71
S	SAFERNET	289
	Safety Precautions	29
	Scope of supply	17
	Security mechanisms	289
	Access security	308
	Activity monitoring	290
	Checklist	342
	Line tapping security	336
	Special features	340
	Sending a fax	78

Service	88, 277, 317
Setting up and connecting	33
Setup Tool	
Basic configuration	127
Menu architecture	122
Monitoring functions	295
Using	114
Short hold	84, 170
SNMP	103
Software update	355
Solution scenarios	45
STAC	245
Startup procedure	340
Syslog messages	290
System data, entering	132
System requirements	21
System time	255
T	
TAF	335
Technical data	369
Testing your Internet access	78
Time server	255
Token Authentication Firewall	335
T-Online	184
Transit Network	235
Troubleshooting	359
Aids	360
IPX routing	366
ISDN connections	363
System errors	362
U	
Update	355
V	
Van Jacobson Header Compression	245
Virtual Private Network (VPN)	288, 339
VPN	288, 339

W	WAN interface	138
	Windows networks, configuration	40
	WINS	95, 238, 259
X	X.31 TEI	210

