XCENTRIC

User's Guide

Installation and Configuration

Copyright © 2001 BinTec Communications AG, all rights reserved.

Version 1.3
Document # 71000J
April 2001

Purpose

This manual explains the installation and initial configuration of **XCENTRIC** with software release 5.2.1. 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 **XCENTRIC**, can be found at www.bintec.net.

As a multiprotocol router, **XCENTRIC** sets up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. BinTec Communications AG accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks

BinTec and the BinTec logo are registered trademarks of BinTec Communications AG.

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.

Bestimmungen der Telefongesellschaft

Beachten Sie bei der Installation externer ISDN-Basisanschlüsse die jeweils gültigen Rahmenbedingungen Ihres Landes. Gegebenenfalls ist ein Techniker erforderlich, der über die entsprechende Zulassung verfügt. Informieren Sie sich über die Besonderheiten nationaler Verordnungen und beachten Sie deren rechtliche Grundlagen bei der Installation.

Guidelines and standards used

XCENTRICcomplies with the following guidelines and standards:

- Low voltage directive 73/23/EEC according to EN60950, complies with German equipment safety regulations (certificate no. S 9918045, tested to EN 60950).
- Interference immunity according to EN50082 1/1.32
- Class B interference emissions according to EN55022 /8.94, electromagnetic compatibility according to EU directive 89/336/EEC.
- CE marking for all EC countries (EC type test certificate, registration number D810362L).

Registration:

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

How to reach BinTec

BinTec Communications AG
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 911 96 73 0

Fax: +49 911 688 07 25

Internet: www.bintec.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.de/fr

Table of Contents 5

1 Welcome to the Office

Congratulations on deciding to buy **XCENTRIC**, a new-generation modular telecommunication server. **XCENTRIC** offers you all the advantages of a multiprotocol router from the BIANCA/BRICK range of BinTec Communications AG. **XCENTRIC** is also a modular extendible private automatic branch exchange for digital and analog extensions.

Figure 1-1: **XCENTRIC** "Office in a Box"

The "Office in a Box" handles Internet access, corporate networking, telephony, fax and e-mail all in a single unit. This means your work group, office or branch is connected to all modern means of communication. The integration of telecommunication, computer and Internet in your working environment opens up possibilities such as Unified Messaging and CTI (Computer Telephone Integration).

BinTec's security package SAFERNET^{TM}, which is included in the scope of features for **XCENTRIC**, meets the latest data security requirements.

1.1 XCENTRIC – The Platform for Present and Future Technologies

XCENTRIC's modular design makes you flexible.

Basic unit The pre-installed main module has an input for external music for music on hold, a slot for a flash card, an Ethernet/LAN interface and a serial interface. The basic unit is also equipped with the door intercom module.

Communication module Slots are available for up to four communication modules. BinTec Communications AG offers you two different communication modules: XCM-5S0 and XCM-S04AB. The XCM-5S0 has five S_0 interfaces configured as internal or external interfaces. The internal interfaces are used for connecting ISDN terminals (e.g. ISDN telephones). The XCM-S04AB has one external S_0 socket and four analog terminals can be connected (analog telephones, G3 fax machines).

Hub module **XCENTRIC** has two slots for hub modules (XCM-HUB). The hub module enables direct connection of PCs and servers to **XCENTRIC**. The dual-speed hub has an auto sensing function for 10-Mbps or 100-Mbps connections.

Fax modem module You can extend the features of your **XCENTRIC** by installing the fax modem module XFM-Fax.

ISDN **XCENTRIC** supports Euro ISDN at its point-to-point and/or point-to-multipoint connection as an interface to the ISDN (D-channel protocol: ➤➤ **DSS1**). The internal interfaces of the private automatic branch exchange are point-to-multipoint connections (also Euro ISDN). **XCENTRIC** also supports leased lines.

PABX **XCENTRIC** is a private automatic branch exchange (PABX) with integrated router and application interfaces for network-wide use of communication applications (fax, CTI, Unified Messaging).

System telephones BinTec's CS300 ISDN system telephone is available together with **XCENTRIC**. BinTec CS300 is designed for use with **XCENTRIC** and offers a range of convenient features.

Multiprotocol router The integrated multiprotocol router for the ➤➤ **TCP/IP** and ➤➤ **IPX** protocols also supports bridging using the spanning tree method. The routing software offers a whole range of features (e.g. data compression) that can be used on the router.

Security

BinTec's SAFERNET^{TM} security technology includes features such as encryption procedures, access lists, ➤➤ **NAT** and access passwords. The security features protect **XCENTRIC** and therefore the PABX against unauthorized access.

➤➤ **VPN** can be used as an optional feature, which is obtainable via a license.

Configuration

If you work with Windows, you will be offered the easy-to-use BinTec Configuration Wizard as one of several tools for configuring the router and PABX parts of **XCENTRIC**. Various other configuration programs are also available and can be used for Windows, Unix and Macintosh environments. **XCENTRIC** can also be configured and administrated completely ➤➤ **remote** (e.g. by a system administrator in a remote head office). **XCENTRIC**'s configuration data can be managed with SNMP.

The future

New technologies and developments are vital for BinTec Communications AG. The control software for **XCENTRIC** is constantly being improved and extended so that future technologies can be implemented on **XCENTRIC**.

You can download BinTec's current software via the World Wide Web.

You can find detailed information about the individual subjects in the relevant parts of this manual and in the more detailed documentation.

1.2 Scope of Supply

1.2.1 Basic Unit

The **XCENTRIC** basic unit comprises a metal housing with integrated mains unit, pre-installed main module and door intercom module. All except one of the unused slots are protected by dummy covers. A device for hanging the unit on the wall is located at the rear of the unit. The unit is provided with a plastic cover.

Basic unit

The **XCENTRIC** basic unit is supplied with the following parts:

- Cable sets
  - serial cable with adaptor
  - 100BT Ethernet cable of category 5 STP type (shielded twisted pair, 5 meters long)
  - IEC AC power cord
- BinTec ISDN Companion CD
- Documentation
  - User's Guide (English)
  - Quick Install Guide (English)
  - Release Notes (English)
- Additional material
  - License card with license information

Expansion modules

You will find a description of the installation of the modules in a later chapter of this manual. The description of the installation of the XFM-Fax module is supplied together with the module.

➤ Before you install modules and make connections, make sure you read the hardware installation instructions in chapter 6, page 57.

The following modules are available separately:

- XCM-5S0 (5 x S_0 module)
- XCM-S04AB (ab module)

- XCM-HUB (hub module)
- XFM-Fax (fax modem module)

1.2.2 Expansion Modules

- 5 x S_0 module (XCM-5S0)
  The XCM-5S0 communication module has five ➤➤ **S_0 connections**.
  Each S_0 connection can be configured individually
  – as an external connection for connecting an ISDN exchange line or
  – as an internal connection for connecting to an ISDN terminal or ➤➤ **S_0 bus**.
  by inserting jumpers.
  The interfaces on each module are 4-pole screw terminal connectors.

- ab module (XCM-S04AB)
  The XCM-S04AB communication module is used for connecting four analog terminals such as analog telephones, G3 fax machines or modems. It also has an external S_0 connection (RJ45 socket) for connecting to an ISDN exchange line.
  Each of the four ab connections are 3-pole screw terminal connectors.
  An ISDN cable (RJ45 – RJ45) is also supplied with the module.

- Hub module (XCM-HUB)
  The hub module is used for direct connection of PCs and servers. **XCENTRIC** can be extended by up to two hub modules.
  Each hub module is equipped with eight ports (RJ45 sockets) for the connection of data terminals.
  The module is supplied with a 100BT Ethernet cable of the category 5 STP type (shielded twisted pair), length one meter.

- Fax modem module (XFM-Fax)
  The fax modem module extends the **XCENTRIC** basic unit by adding a fax modem functionality.
  The fax modem module is supplied together with various parts for installing the module and an installation guide.

1.3 BinTec ISDN Companion CD

You will find all the programs you need for the installation, configuration and administration of **XCENTRIC** on your BinTec Companion CD. The CD also contains communication software and drivers (CAPI, TAPI) for application interfaces.

BRICKware

- DIME Tools are for monitoring and administration of your **XCENTRIC**.
- The Configuration Wizard leads you step by step through the basic configuration of **XCENTRIC**.
- You gain access to **XCENTRIC** via the serial interface using the terminal program BRICK at COM1 or BRICK at COM2.
- The Configuration Manager contains a Windows-based SNMP Manager and also offers you a graphical interface for conveniently viewing and setting the configuration of the extension numbers.
- The Java Status Monitor allows you to request all relevant system information over an Internet browser.
- The Activity Monitor enables you to monitor the utilization of **XCENTRIC** at a glance.
- Application interfaces
  The Remote CAPI Client and Remote TAPI Client allow you to use communication applications based on the standard ➤➤ **CAPI** or ➤➤ **TAPI** interface.
- BinTec CTI Software

More detailed descriptions of all software programs can be found in our online manual **BRICKware for Windows**. The documentation for BinTec's CTI phone can be found on the BinTec ISDN Companion CD.

What else?

If you scan through the Companion CD, you will find a range of other useful directories in which you can find the following, for example:

- The documentation in electronic form
- UNIX tools

- Adobe's Acrobat Reader

1.4 BinTec Documentation

Together with **XCENTRIC**, 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 (English, PDF and printed)
  This manual.
- Leaflet with a Quick Install Guide for initial configuration of **XCENTRIC** (English, PDF and printed).
- Reference manuals (English, PDF/HTML).
  - Software Reference (PDF)
    Online reference with more detailed information about the functions described here and 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 **XCENTRIC**.
- 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 Logic Release Notes, 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

XCENTRIC can be configured from all conventional platforms. **XCENTRIC** is a stand-alone device that is independent of the PC or operating system to which it is connected. It communicates with the PC over a LAN interface 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 **XCENTRIC**, 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.

Configuration Wizard

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

- PC with serial interface (V.24)
- Windows 95 or 98 or Windows NT 4.0
- 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.

Telephones

You can connect the following telephones internally to **XCENTRIC**:

- Analog telephones
  Telephones that are connected to the ab connections must support ➤➤ **DTMF** (dual-tone multifrequency) dialing and be set to this dialing mode. We recommend that you use analog telephones equipped with an R-key with flash function.

- ISDN equipment
  Digital telephones that are operated on the internal S_0 connections must be approved for use with Euro ISDN (DSS1).
  Up to eight digital terminals can be connected and administrated for each internal S_0 bus (S_0 unit). A power supply of maximum 2 W per S_0 unit is available for digital telephones without their own power supply. A maximum supply of 20 W is available for the system in its maximum size.

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

- Windows 95 or 98 or Windows NT 4.0
- Novell Netware 3.1x and 4.0x

Remote TAPI TAPI support for CTI applications is available in

- Windows 95 or 98 or Windows NT 4.0

1.6 Guarantee Terms

XCENTRIC is guaranteed for 12 months from the date of purchase.

Simply register as BinTec **XCENTRIC** customer with the enclosed registration card or online at www.bintec.de/XCENTRIC/ within 14 days of the date of purchase.

Guarantee

1. BinTec hereby guarantees this equipment against failure due to faulty material and workmanship for a period of 12 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.

1.7 About this Manual

1.7.1 Contents

This manual is structured as follows:

Chapter	Contents
1: "Welcome to the Office"	General introduction, scope of supply, table of contents.
2: "General Safety Precautions"	General safety precautions.
3: "Operation of ISDN Telephones"	Description of the operation of ISDN telephones connected to **XCENTRIC**.
4: "Operation of Analog Telephones"	Describes the operation of analog telephones connected to **XCENTRIC**.
5: "Operation of Door Intercom"	Describes the operation of the door intercom.
6: "Hardware Installation"	Describes the installation of the **XCENTRIC** hardware.
7: "LEDs"	Describes the LED displays for the various operational states of **XCENTRIC**.
8: "Software Configuration Requirements"	What you should know before starting software configuration and installation instructions for BinTec's BRICKware for Windows.
9: "Quick Configuration with the Configuration Wizard"	Describes the quick configuration of **XCENTRIC** using the Configuration Wizard Windows tool.
10: "Basic Configuration of Router with Setup Tool"	Describes the basic configuration of the router part of **XCENTRIC** using the Setup Tool.
11: "Configuration of PABX"	Describes the configuration of the PABX part of **XCENTRIC** using the Setup Tool.

Chapter	Contents
12: "Configuring PCs in your LAN"	Describes the configuration of the PCs in the LAN (application interfaces, additional configuration for data transmission).
13: "BinTec CTI Phone (Server and Standalone Version)"	Describes the CTI application, BinTec's CTI phone.
14: "Advanced Router Configuration"	Describes more advanced configuration steps than those needed for basic configuration of the **XCENTRIC** router.
15: "Security Mechanisms"	Describes how to configure security mechanisms using SAFERNET, e.g. NAT (Network Address Translation) or CLID (Calling Line Identification).
16: "Configuration Management and Flash Card"	Describes how to administrate configuration files and how to perform software updates.
17: "Trouble Shooting"	Important tips on fault clearance.
18: "Important Commands"	A brief overview of the most important commands of the SNMP shell and BRICKtools for Unix.
19: "Technical Data"	**XCENTRIC** technical data.

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:

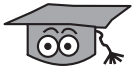
Symbol	Meaning
	Points out useful and relevant tips and tricks.
	Predicts potential pitfalls and explains how to avoid them.
	Brings to your attention general and important points.
	Explains additional background information.
	Brings your attention to important safety precautions. Levels of danger are in accordance with ANSI: ■ 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. ■ Used to display the Setup Tool.
`<IP address>`	Indicates inputs in which you enter a value for the term shown in the brackets. Do not enter the pointed brackets.
bold, italics, e.g. BigBoss	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.
italics, e.g. none	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

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

Transport and storage

- Only transport and store **XCENTRIC** 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 **XCENTRIC**.
- Please comply with the general conditions applicable in your country when installing external ISDN basic rate accesses. In some cases, you may have to consult a technician who possesses the relevant approval. Obtain information about the special requirements of national regulations and make sure that your installation complies with these legal requirements.
- Electrostatic charges may cause damage to the equipment. Wear an antistatic wrist strap or touch a grounded surface before you touch the open equipment or one of the modules. Only grip printed circuit boards at the edges and do not touch cables or components.
- Install the modules only in the intended slots. Fitting modules in the wrong slots may damage the module or the complete equipment.
- When installing the hub modules, ensure that a module is always fitted in slot 6. A single hub module must never be fitted in slot 7, as this may damage the module or the complete equipment.
- Close unused module slots with the dummy covers to prevent objects getting inside the equipment. Foreign bodies located in the equipment during operation create a danger of electric shock and short-circuits.
- A 5-S_0 module may be damaged on taking into operation if the jumpers are set incorrectly. The modules are equipped to a certain extent with protective measures to prevent such damage, but you should still insert jumpers very carefully. Make sure that suitably configured (internal or external) units are also connected correctly.
- Make sure the cables do not cover the ventilation slots of the equipment or interfere with ventilation. Obstructing the ventilation of **XCENTRIC** may

cause damage to the equipment. Damage caused by lack of ventilation invalidates the guarantee.

- Never open the mains unit or the basic unit (including door intercom module) and do not tamper with the mains unit in any way, as this can create a lethal danger through electric shock. Do not remove any screws used for fixing the mains unit and basic unit.
- 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 local mains voltage is the same as the nominal voltages of the mains unit. The equipment may only be operated under the following conditions.
  - 230 - 240 V AC
  - 50/60 Hz
- Make sure the safety mains socket in the building is freely accessible. You must remove the mains plug to disconnect the equipment completely from the mains.
- Make sure you follow the correct cabling sequence, as described in the manual. Use only the cables supplied with the equipment or cables that meet the specifications in this manual. If you use other cables, BinTec Communications AG cannot accept liability for any damage occurring or for any adverse effects on operation. The equipment guarantee is invalidated in such cases.
- Connect the equipment as described in the manual. When plugging in the terminal blocks, make sure you do not bend the pins and that the screws of the terminal block point to the right when it is plugged in. If not, the interface will not function and may be damaged.
- Arrange the cables so that they are not in the way and cannot be tripped over or damaged.
- Do not connect, disconnect or touch the data lines during lightning storms.

- Only connect terminals to **XCENTRIC** that meet the general safety requirements for telecommunications equipment. Terminals approved by CETECON (formerly BZT) meet these requirements. ISDN terminals connected to **XCENTRIC** must be approved for use with Euro ISDN (DSS1). Analog terminals must support DTMF (Dual Tone Multifrequency) dialing and be set to this mode.

Operation according to the regulations

- **XCENTRIC** is intended for use in offices. As an ISDN multiprotocol router, **XCENTRIC** establishes WAN connections depending on the system configuration. To avoid extra charges, you should carefully monitor the product.
- **XCENTRIC** meets the relevant safety standards for information technology equipment for use in offices.
- **XCENTRIC** is designed for wall mounting and must only be operated in a hanging position. Ventilation must not be obstructed.
- 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 40 °C. Avoid exposure to direct sunlight.
- Make sure no foreign objects (e.g. paper clips) or liquids get into the equipment (risk of electric shock, short-circuit). Make sure the equipment is sufficiently cooled.
- In an emergency (e.g. damaged housing or operating element, entry of liquid or foreign bodies), immediately disconnect the power supply and notify customer service.

Cleaning and repair

- The equipment should only be opened by trained personnel. Always disconnect the power cord before opening the equipment. Unauthorized opening and improper repairs can result in serious danger for the user (e.g. electric shock). Ensure that repairs are only carried out by service centers authorized by BinTec. Your dealer will tell you where the service centers are situated.

- 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 Operation of ISDN Telephones

XCENTRIC supports the following features for ISDN telephones:

- Call waiting
- Inquiry call
- Brokering
- Three-party conference
- Call transfer
- Call pickup
- Calling Line Identification Restriction
- Call forwarding

Call charging data and information are also displayed.

You will find information about the installation and configuration of BinTec CS300 system telephones in chapter 11.14, page 320.

The features available on ISDN telephones depend on the scope of features offered by the telephone you are using (user guide, display). Please refer to the product description of your ISDN telephone. An exception is "call pickup", which must also be controlled on ISDN telephones via the given codes (see chapter 3.1.1, page 37 and chapter 3.1.2, page 37).

You must configure the relevant assigned ➤➤ **extensions** on ISDN telephones.

It is sufficient if the last digits of an ➤➤ **extension** are configured on the ISDN telephone. The numbers configured on a unit must be unique. If, for example, two ISDN telephones with extension numbers 129 and 139 are connected to an S_0 bus on an internal S_0 unit, at least the 29 and 39 must be configured on the relevant telephone, as the 9 would not be unique.

The user concept of **XCENTRIC**'s PABX makes it possible to show the name of the called party and calling party on the display of an ISDN telephone for calls within **XCENTRIC**, provided the ISDN telephones used support "DISPLAY" INFO messages. The names are displayed as configured for **XCENTRIC** in the Configuration Wizard (see chapter 9.1.1, page 142) or in the Setup Tool (see chapter 11.5.1, page 241 and chapter 11.7, page 272).

When entering external extensions for configuring call forwarding, you must always enter the trunk prefix before the external extension.

The trunk prefix is either the number you dial before you make an external call or – with automatic trunk prefix – the number you have configured as **Auto Dialout Number** for your telephone (see chapter 11.11, page 289).

3.1 Call Pickup on ISDN Telephones

The "call pickup" feature transfers a call for any or a certain extension (within your call group only) to your telephone. Call groups must be created by your system administrator (see chapter 11.8, page 276).

The "call pickup" feature corresponds to accepting a call. You must therefore hold any call already in progress before you can use this feature. Please refer to the operating manual of your ISDN telephone for information on holding a call.

3.1.1 Group Call Pickup on ISDN Telephones

You can use the "group call pickup" feature to accept a call for any extension in your call group. Call groups must be created by your system administrator (see chapter 11.8, page 276).

A telephone in your call group rings.

- Lift the receiver.
- Press * , 9 , 0 and # in succession.
  You are connected to the caller.

3.1.2 Directed Call Pickup on ISDN Telephones

The "directed call pickup" feature enables you to accept a call for a certain extension in your call group. Call groups must be created by your system administrator (see chapter 11.8, page 276).

- Lift the receiver.
- Press * , 9 , 0 and * in succession.
- Enter the internal extension of the telephone ringing.

If you normally use "#" as a prefix for internal extensions, do not enter the initial "#" before you dial internal extensions for directed call pickup.

➤ Press # .

You are connected to the caller.

4 Operation of Analog Telephones

Analog telephones with Dual Tone Multifrequency (DTMF) dialing that are connected to **XCENTRIC** have the following features:

- Call waiting
- Inquiry call
- Brokering
- Three-party conference
- Call transfer
- Call pickup
- Calling Line Identification Restriction
- Call forwarding

These features are described below.

For analog telephones connected to **XCENTRIC** that are equipped with a display and CLIP detector, it is possible to display the number of the calling party.

The calling party number is transferred to the analog telephone of the called party between the first and second ringing tone. If the calling party has activated the Calling Line Identification Restriction (CLIR) function, the number is not displayed.

Analog telephones that do not meet the requirements described above can be equipped retrospectively with a suitable additional unit to display the calling party number.

The asterisk key starts the configuration mode, which is switched off again automatically if no other keys are pressed within two seconds.

The last page of this user's guide contains an abbreviated guide to telephone operation, which you can cut out and keep near your telephone.

The R key of DTMF telephones usually has the option of selecting a long or short flash signal. **XCENTRIC** detects a flash signal length of approx. 75 to 330 milliseconds. Please select "long flash" as the setting for the R key.

The R key can be replaced by the key combination

* , 0 and # .

4.1 Call Waiting

If a second call is received while you are phoning, this is indicated by a waiting tone in your receiver. You can switch the "call waiting" feature on and off. The default setting for "call waiting" is on and this value is therefore set after a restart of **XCENTRIC**.

4.1.1 Switching Off Call Waiting

- Lift the receiver.
- Press * , 3 and # in succession.
  The feature is switched off.

If call waiting occurs when a call is in progress, this key combination only rejects the waiting call. See chapter 4.1.4, page 42.

4.1.2 Switching On Call Waiting

To switch on this feature:

- Lift the receiver.
- Press * , 2 and # in succession.
  "Call waiting" is switched on.

4.1.3 Accepting a Waiting Call

You are making a call and would like to accept a "waiting call".

➤ Press R .

The waiting call is connected through to you. The call in progress is held for the meantime. You can broker, i.e. switch between the two calls (see chapter 4.2.2, page 43).

Accepting "waiting call" without R key

If your telephone is not equipped with an R key:

➤ Press * , 0 and # in succession.

The waiting call is connected through to you. The call in progress is held for the meantime.

4.1.4 Rejecting a Waiting Call

You are making a call and a second call is indicated by a waiting tone. To reject the second call:

➤ Press * , 3 and # in succession.

The second call is rejected.

4.2 Inquiry Call and Brokering

You are making a call and would like to call another person to make an inquiry. This is done by holding the first call and calling the second subscriber. You can then broker between both calls, connect the two calls or set up a three-party conference (see chapter 4.3, page 45).

4.2.1 Inquiry Call

➤ Press R.

The call is now held. The waiting subscriber hears music – if music-on-hold is configured – or the announcement "Your call is on hold".

➤ Dial the required extension.

You can now make your inquiry call.

Inquiry call without R key

If your telephone is not equipped with an R key:

➤ Press *, 0 and # in succession.

The call is now held. The waiting subscriber hears music – if music-on-hold is configured – or the announcement "Your call is on hold".

➤ Dial the required extension.

You can now make your inquiry call.

4.2.2 Brokering

You can also continue the first call:

➤ Press R again.

You can now continue the first call.

Brokering without R key

If your telephone is not equipped with an R key:

➤ Press *, 0 and # in succession.

You can now continue the first call.

Brokering - alternately speaking to both subscribers - is now possible by pressing the R key or the key combination described.

4.2.3 Ending Brokering Call

You are holding one call with another call in progress. You would now like to end the call in progress.

➤ Press * , 1 and # in succession.

The call in progress is ended. You are connected to the call being held.

4.3 Three-Party Conference

You are making a call, holding a second call and would now like to set up a three-party conference.

4.3.1 Setting Up a Three-Party Conference

To set up a three-party conference with an active call and a call on hold:

➤ Press * , 5 and # in succession.
You are now connected to a three-party conference.

4.3.2 Ending a Three-Party Conference

To end the three-party conference:

➤ Press * , 6 and # in succession.
The calls are restored to their status before the three-party conference. You have one active call and one call on hold.

4.4 Call Transfer

You are making a call and would like to connect the caller to another subscriber:

- Press R .
  The first call is held.
- Dial the number of the second subscriber.
  The second subscriber lifts the receiver.
- Tell the second subscriber the call is being transferred.
- Replace the receiver or press * , 8 and # .
  The two subscribers are interconnected.

Call transfer without R key

If your telephone is not equipped with an R key:

- Press * , 0 and # in succession.
  The first call is held.
- Dial the number of the second subscriber.
  The second subscriber lifts the receiver.
- Tell the second subscriber the call is being transferred.
- Replace the receiver or press * , 8 and # .
  The two subscribers are interconnected.

You can also interconnect the two subscribers without talking to the second subscriber by replacing the receiver or pressing * , 8 and # as soon as you hear the ringing tone after dialing the extension of the second subscriber.

Both external and internal calls can be transferred internally. Transferring calls externally is only possible for internal subscribers.

4.5 Call Pickup

The "call pickup" feature transfers a call for any or a certain extension (within your call group only) to your telephone. Call groups must be created by your system administrator (see chapter 11.8, page 276).

The "call pickup" feature corresponds to accepting a call. You must therefore hold any call already in progress (see chapter 4.2.1, page 43) before you can use this feature.

4.5.1 Group Call Pickup

You can use the "group call pickup" feature to accept a call for any extension in your call group.

A telephone in your call group rings.

- Lift the receiver.
- Press * , 9 , 0 and # in succession.
  You are connected to the caller.

4.5.2 Directed Call Pickup

The "directed call pickup" feature enables you to accept a call for a certain extension in your call group.

- Lift the receiver.
- Press * , 9 , 0 and * in succession.
- Enter the extension of the telephone ringing.

If you normally use "#" as a prefix for internal extensions, do not enter the initial "#" before you dial internal extensions for directed call pickup.

➤ Press # .

You are connected to the caller.

4.6 Calling Line Identification Restriction (CLIR)

You can use the "calling line identification restriction" feature to prevent your extension number being displayed to the called subscriber on your next call.

- Lift the receiver.
- Press * , 7 and # in succession.
- Dial the required extension.

  Your number is now no longer displayed to the called subscriber.

This key combination must be pressed every time you make a new call in which your number is not to be displayed to the other subscriber.

4.7 Call Forwarding

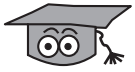
The "call forwarding" feature forwards incoming calls to another extension.

The "call forwarding on no reply" and "call forwarding on busy" features can be active at the same time.

It is necessary to use a special entry procedure to configure call forwarding for forwarding calls to external extensions.

When entering external extensions, you must always enter the trunk prefix before the external extension.

The trunk prefix is either the number you dial before you make an external call or – with automatic trunk prefix – the number you have configured as **Auto Dialout Number** for your telephone (see chapter 11.11, page 289).



The settings made are saved automatically in the relevant MIB tables in the flash ROM of **XCENTRIC**. They are also still available after a system restart. The default setting of 15 seconds for "Call forwarding on no reply" can be changed in the Setup Tool in the ***PABX*** ➧ ***CALL FORWARDING*** menu. This is done separately for each extension in the **NoReply Timer** field. Call forwarding can also be configured in this menu via the Setup Tool.

4.7.1 Immediate Call Forwarding

- Lift the receiver.
- Press * , 4 , * , 0 and * in succession.
- Enter the extension to which calls are to be forwarded.
- Press # .

  Call forwarding is effective immediately.

The setting for call forwarding can be deleted.

Deleting

- Lift the receiver.

➤ Press * , 4 , * , 0 , * and # .
"Immediate call forwarding" is switched off.

4.7.2 Call Forwarding on Busy

➤ Lift the receiver.
➤ Press * , 4 , * , 1 and * in succession.
➤ Enter the extension to which calls are to be forwarded.
➤ Press # .
The call will be forwarded to the extension entered if you are busy.

The setting for call forwarding can be deleted.

Deleting
➤ Lift the receiver.
➤ Press * , 4 , * , 1 , * and # .
"Call forwarding on busy" is switched off.

4.7.3 Call Forwarding on No Reply

➤ Lift the receiver.
➤ Press * , 4 , * , 2 and * in succession.
➤ Enter the extension to which calls are to be forwarded.
➤ Press # .
The call will be forwarded to the extension entered after 15 seconds.

The setting for call forwarding can be deleted.

Deleting
➤ Lift the receiver.
➤ Press * , 4 , * , 2 , * and # .
"Call forwarding on no reply" is switched off.

5 Operation of Door Intercom

The operation of the door intercom and door opener is described below.

The call extension can be configured in the **Door Intercom Call Extension** field of the ***PABX*** ➧ ***STATIC SETTINGS*** menu in the Setup Tool. The call extension is the extension called when the door bell is rung. This extension can be a group extension or a terminal.

The ***PABX*** ➧ ***STATIC SETTINGS*** menu (Setup Tool) also contains the **Door Intercom External Open** field for configuring whether or not the door may be opened by a call from an external telephone (see chapter 11.3, page 212).

5.1 Operation of Door Intercom with ISDN Telephones

The door bell rings.

- The telephones in the door intercom call group or the telephone that is called by the door intercom ring(s).
- A subscriber lifts the receiver. The call is set up to the door intercom.
- Talk to the person at the door.

➤ End the call.

➤ Lift the receiver and enter the extension of the door intercom.

The door opener is then operated for five seconds and you can talk to the person at the door.

➤ Replace the receiver.

The door opener can be operated with ISDN telephones exactly as with analog telephones, if the following requirement is fulfilled (see chapter 5.2, page 55):

The ISDN terminal generates keypad or information messages and not DTMF tones when keys are pressed during an active call.

This information can be found in the manual for your telephone.

5.2 Operation of Door Intercom with Analog Telephones

The door bell rings.

- The telephones in the door intercom call group or the telephone that is called by the door intercom ring(s).
- A subscriber lifts the receiver. The call is set up to the door intercom.
- Talk to the person at the door.

➤ Open the door during the call by pressing any number on the telephone keypad.

➤ End the call.

Just as with ISDN telephones, the door opener can also be operated by a call to the door intercom. The door opener is then operated for five seconds and you can talk to the person at the door.

5 Operation of Door Intercom

6 Hardware Installation

This chapter contains all the information you need for the installation of **XCENTRIC**.

Chapter 6.1: "Installation Requirements" contains items that you must consider before installation or wall mounting.

Chapter 6.2: "Wall Mounting of XCENTRIC" describes how to mount the equipment on the wall.

Chapter 6.3: "Basic Unit with Mains Unit" describes the connections of the basic unit.

Chapter 6.4: "Door Intercom Module in Basic Unit" describes the door intercom module integrated in the basic unit.

Chapter 6.5: "Installing and Removing Communication Modules and Connection Methods" shows the general installation of communication modules and describes the connection methods you will find during installation.

Chapter 6.6: "Cable Installation for Basic Unit and Communication Modules" provides instructions on cabling the basic unit and communication modules.

The chapters on the individual modules deal with the components and associated connections in detail. The chapter on the hub module also contains descriptions for installing and removing the hub module and instructions on cable routing.

Caution!

Electrostatic charges can damage electronic components. Please observe the following precautions to avoid damaging components:

- Ground yourself before unpacking components and before carrying out installation work on the equipment.
- Only grip boards at the edges and do not touch cables or components.

6.1 Installation Requirements

6.1.1 Network Planning

Prepare your network plan before carrying out the installation, especially the necessary external and internal ISDN connections.

6.1.2 Installation Position

The position you choose for mounting **XCENTRIC** on the wall must not be exposed to direct sunlight or near a heater. The ambient temperature must not exceed 40 °C.

Caution!

XCENTRIC must be hung in the correct position on a wall with ventilation on all sides. Inadequate ventilation can cause damage to the equipment.

- Operate **XCENTRIC** only in a hanging position on a wall. Make sure **XCENTRIC** is not tilted to one side or mounted upside down.
- The ambient conditions must fulfil the stated requirements. (see chapter 19, page 509).

6.1.3 Wer darf XCENTRIC installieren?

Beachten Sie bei der Installation externer ISDN-Basisanschlüsse die jeweils gültigen Rahmenbedingungen Ihres Landes. Gegebenenfalls ist ein Techniker erforderlich, der über die entsprechende Zulassung verfügt. Informieren Sie sich über die Besonderheiten nationaler Verordnungen und beachten Sie deren rechtliche Grundlagen bei der Installation.

6.1.4 Lengths and Types of Cable

You should prepare the necessary tools and materials before starting wall mounting, installation and connection of **XCENTRIC**.

See chapter 6.2, page 64 (Wall Mounting).

- Mains unit
  Use only the IEC AC power cord supplied with the equipment.
- Serial interface
  Use only the cable supplied with the equipment. The length of the connection must not exceed 2 m.
- Ethernet/LAN Interface
  To connect an external hub, use only the cable supplied with the basic unit (length 5 m).
  To connect the basic unit to the hub module (XCM-HUB), you must use the cable enclosed with the hub module (length 1 m).
- ISDN connections
  We recommend the following type of cable: J-2Y(ST)Y shielded twisted pair, Z=100 ohm.
  The maximum cable lengths are shown in the individual installation descriptions in chapter 6.7.4, page 91.
- ab connections
  We recommend the following type of cable: indoor telephone cable J-Y(ST)Y to VDE0815, shielded twisted pair.
- Door intercom interface
  We recommend the same cable as used for the ab connections.
- Music-on-Hold Interface
  You should use an audio cable with a 3.5 mm jack plug.

- Hub connections
  For connecting equipment to the hub ports of the hub module (XCM-HUB), Ethernet cable of category 5 STP type (shielded twisted pair) must be used to achieve CE conformity.
  The maximum cable length between the hub and data terminal equipment in 100-Mbps networks is always 100 meters.

6.1.5 Removing and Mounting the Plastic Cover

The plastic cover of the equipment must be removed before wall mounting and installation of modules.

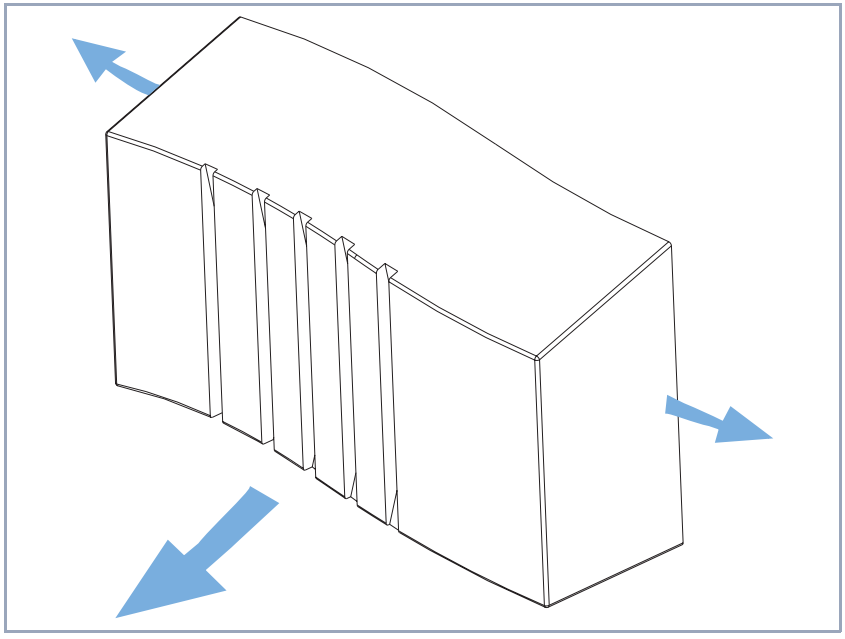


Figure 6-1: Removing the plastic cover

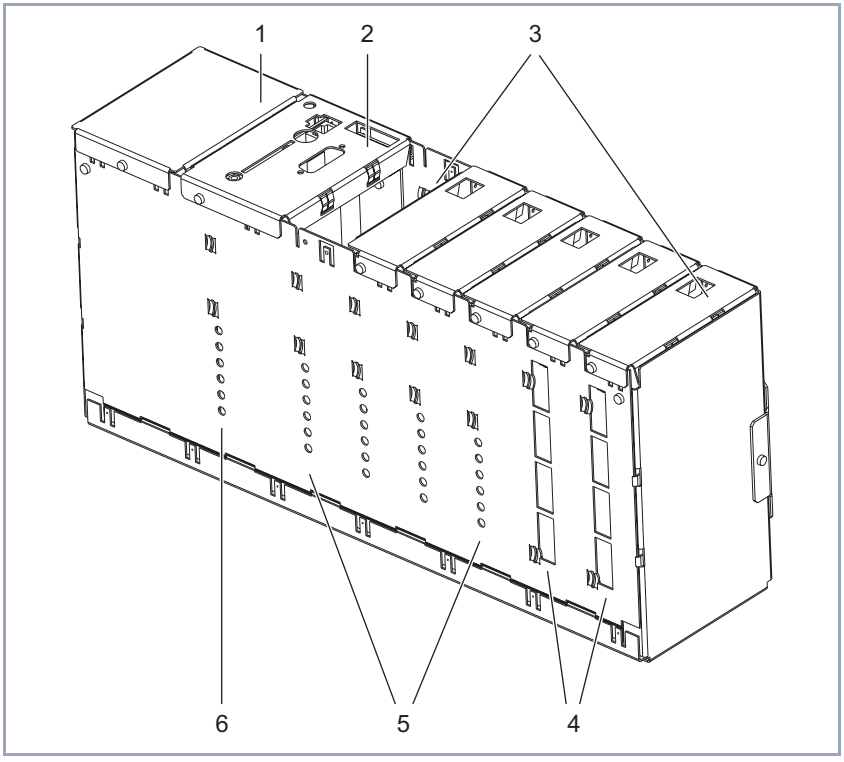
Removing the cover

Proceed as follows to remove the plastic cover from the metal housing:

- Grip both sides of the cover at the rear and pull the side panels apart.
- Remove the cover towards the front.

Due to stresses in the material used for the plastic cover, the cover may be a little difficult to remove and mount the first few times.

Housing of ex works basic unit after removal of the plastic cover:



1	Mains unit	4	Slot 6 and 7: Openings for the connections for a hub module
2	Slot 1: Main module	5	Slot 2 to 5: Openings for the LEDs of a communication module
3	Slot 2 to Slot 7	6	Slot 1: Openings for the LEDs of the main module

Figure 6-2: **XCENTRIC**Basic Unit

Danger! Electric shock!

There is a risk of electric shock on opening the mains unit.

- Never open the mains unit.
- Never interfere in any way with the mains unit.
- Never remove the cover of the mains unit or loosen the screws.

How to mount the plastic cover is shown in the diagram below:

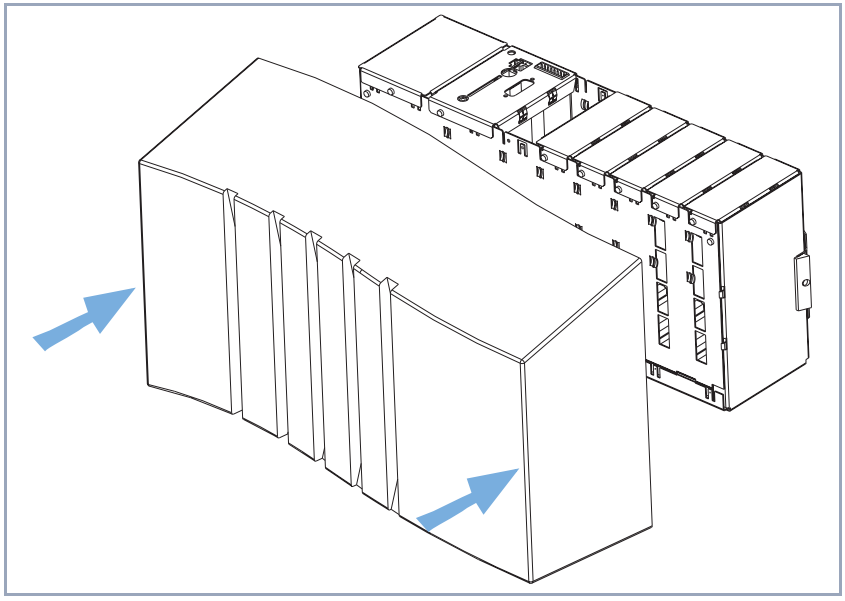


Figure 6-3: Mounting the plastic cover

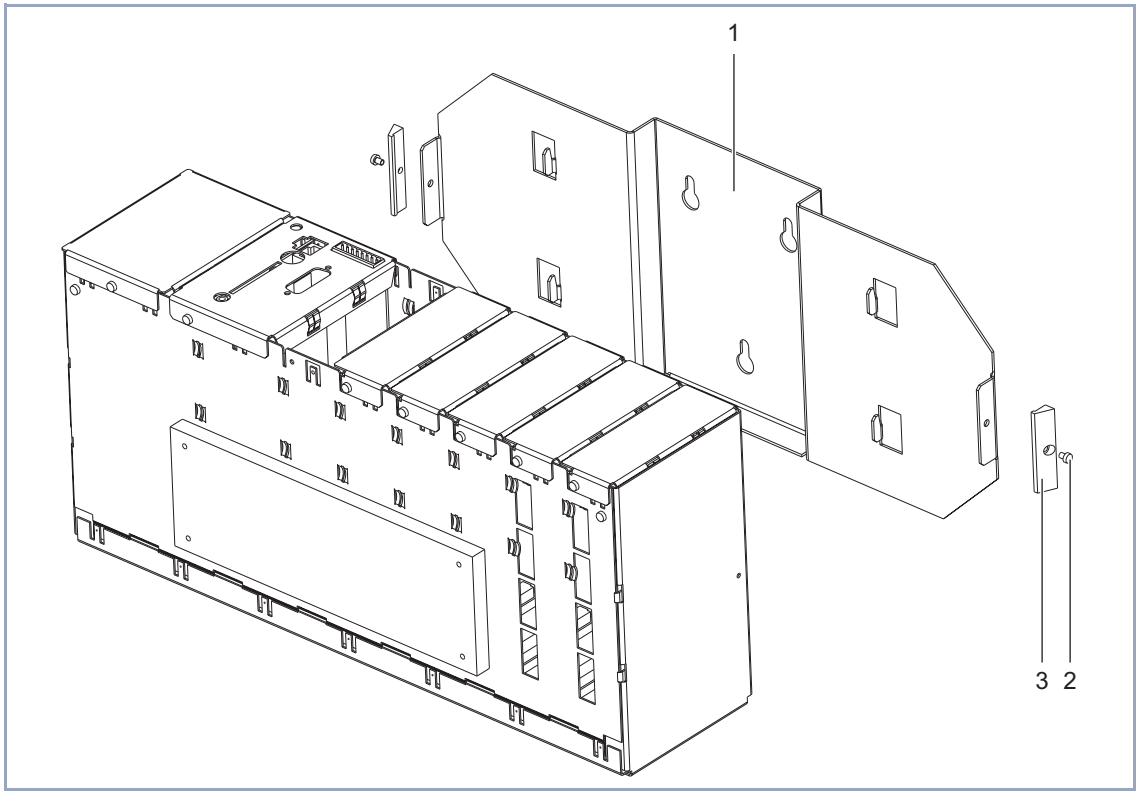
Mounting the cover

Proceed as follows to mount the plastic cover on the metal housing:

- Place the cover over the equipment from the front.
- Press the cover over the side fixing elements until it clicks into position.

6.2 Wall Mounting of XCENTRIC

A wall holder is located on the back of **XCENTRIC** for mounting it on the wall. The equipment is inserted into this holder.



1	Wall holder	3	Locking elements
2	Screws		

Figure 6-4: Components for wall mounting of **XCENTRIC**

Mounting XCENTRIC on the wall

Proceed as follows to mount **XCENTRIC** on the wall:

- Unscrew the wall holder from the equipment. Remove the screw located on each side of the equipment.
- Use the wall holder as a template for drilling.
- Fix the wall holder firmly to the wall using three wall plugs and screws to suit the type of foundation.
- Insert the equipment into the wall holder from above.
- Replace the screws on both sides to fix the equipment to the wall holder. Do not forget to fit the locking elements.

6.3 Basic Unit with Mains Unit

Detailed information (pin assignment) for the relevant interfaces can be found in chapter 19, page 509.

Danger! Electric shock!

There is a risk of electric shock on opening the basic unit (including door intercom module) or the mains unit!

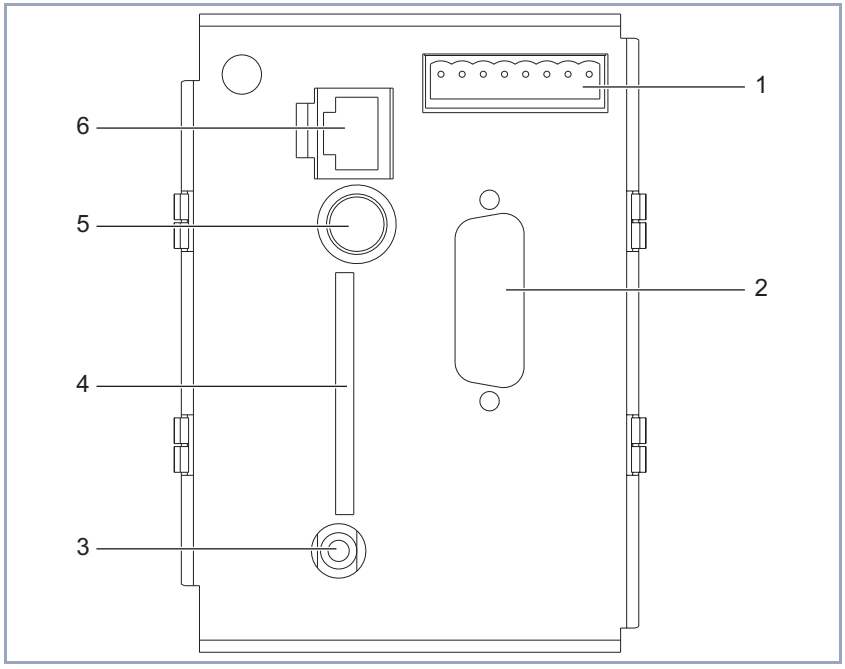
- Never open the mains unit or the basic unit.
- Never remove any fixing screws on the mains unit or basic unit (main module with door intercom module).

Caution!

Opening the basic unit (including door intercom module) or the mains unit can damage the equipment.

- Never open the mains unit or the basic unit.
- Never remove any fixing screws on the mains unit or basic unit (main module with door intercom module).

The top of the basic unit is shown in the diagram below:



1	Door intercom interface	4	Flash Card Slot
2	Interface (not currently used)	5	Serial interface
3	Music-on-Hold Interface	6	Ethernet/LAN Interface

Figure 6-5: Connections on basic unit

The basic unit with the mains unit has the following connections:

- Mains unit
  IEC AC socket on the bottom of **XCENTRIC**. See figure 6-6, page 69.
  The mains unit is only to be connected to the power supply using the power cord supplied with the equipment.

- Serial interface
  8-pole mini DIN socket
  The serial interface is used for connecting **XCENTRIC** to a computer. Use the serial cable supplied with the equipment for this connection, if necessary with an adapter.

- 10/100 Mbps Ethernet/LAN interface
  RJ45 socket
  The Ethernet/LAN interface is used for connecting to a hub.
  For connecting to an external hub, use only the 5-meter long 100BT cable of category 5 STP type (shielded twisted pair) supplied with the basic unit.
  For connecting the integrated hub module (XCM-HUB) to **XCENTRIC**, use only the 1-meter long 100BT cable of category 5 STP type (shielded twisted pair) supplied with the hub module.

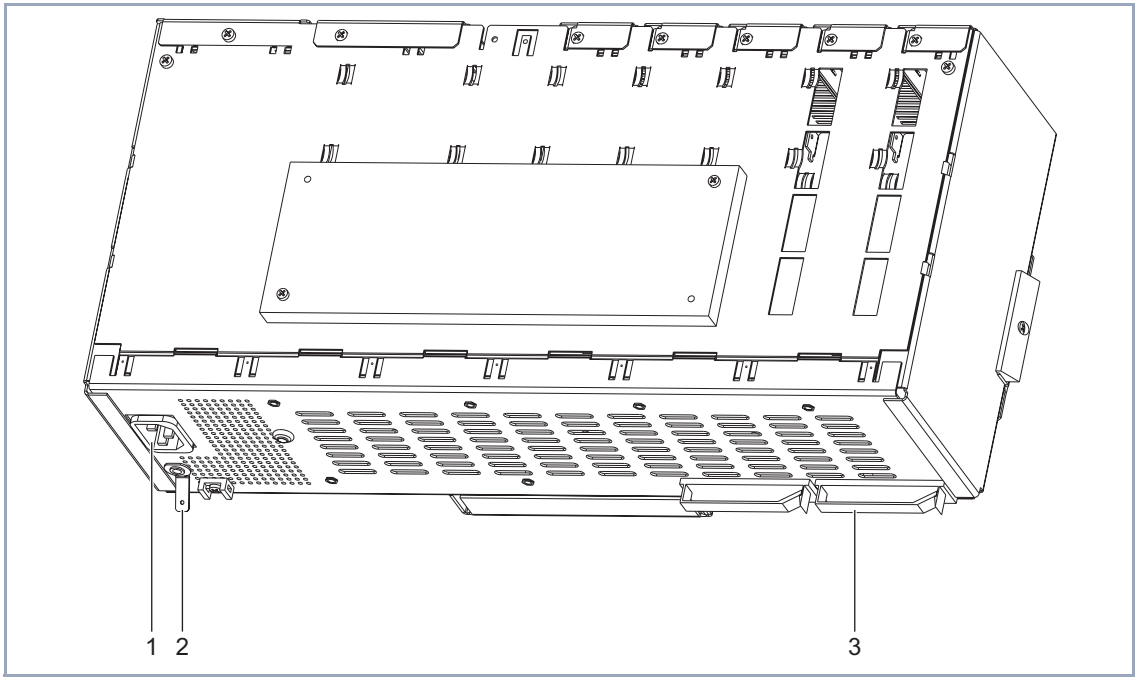
- Door intercom interface
  8-pole screw terminal connector.
  Description in chapter 6.4, page 70

- Flash card slot
  SmartMedia flash cards (such as obtainable from photo shops) can be used for saving configurations and different versions of **XCENTRIC**'s system software. Cards with 4 MB, 8 MB, 16 MB and 32 MB of memory (all 3.3 V only) are supported. You will find detailed information about the flash card in chapter 16.2, page 474.

- Music-on-Hold Interface
  Stereo jack.
  The music-on-hold interface is used for supplying **XCENTRIC** with external music from audio equipment (stereo system, cassette recorder, CD player) for the music-on-hold feature. Connect the stereo jack of **XCENTRIC** via a 3.5 mm jack plug to the headphone output of the external equipment.
  The volume is controlled via the external audio equipment.

- Ground terminal
  A ground terminal is located on the bottom of **XCENTRIC** beside the IEC AC socket on the outside of the housing. The ground terminal is used for connecting the ground wire of a telephone cable (6.3 x 0.8 mm spade connector). See figure 6-6, page 69.

A three-dimensional view of the bottom of **XCENTRIC**'s metal housing is shown below:



1	IEC AC socket of mains unit	3	Cable holder (provided for cables of hub modules)
2	Ground terminal		

Figure 6-6: Bottom view of metal housing

6.4 Door Intercom Module in Basic Unit

The basic unit of **XCENTRIC** contains a door intercom module (XCM-TFE) for connecting an external door intercom unit with amplifier. The external door intercom unit used must comply with the German FTZ 123 D 12 standard.

The door intercom module offers the following facilities:

- connection of a speech channel without DC component to an ab interface
- floating connection for switching the supply voltage of the external door intercom unit (amplifier)
- floating connection for an external door opener
- connection for a door bell button

The interface of the door intercom module is an 8-pole screw terminal connector with the following pin assignment:

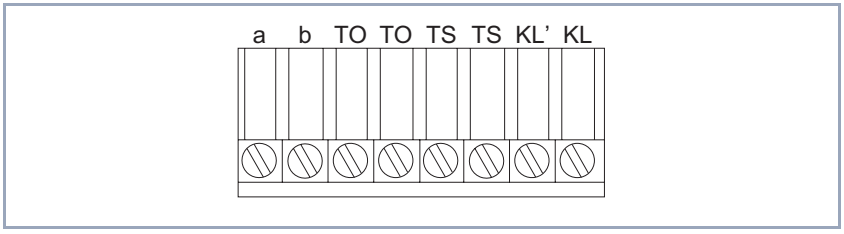


Figure 6-7: Pin assignment of door intercom module

A detailed description of the individual interfaces (e.g. contact rating) can be found in chapter 19.2.3, page 514.

Description of pin assignment of door intercom interface:

Pin	Remarks
a/b	ab interface for connecting a speech circuit without DC component.
TO/TO	Floating connection for the door opener.
TS/TS	Floating connection for the door intercom supply voltage.
KL'/KL	Connection for a door bell button

Table 6-1: Description of pin assignment of door intercom

It is assumed for the following connection examples that a simple standard door intercom to the German FTZ 123 D 12 standard is used. In the examples shown, a bell transformer (230 V AC/12 V AC) is required for the supply voltage for the door opener, door intercom and door bell button.

The following installation information represents examples of possible connections only.

Always follow the description of your own door intercom system when carrying out the installation!

Door intercom station Example connection for an external door intercom station:

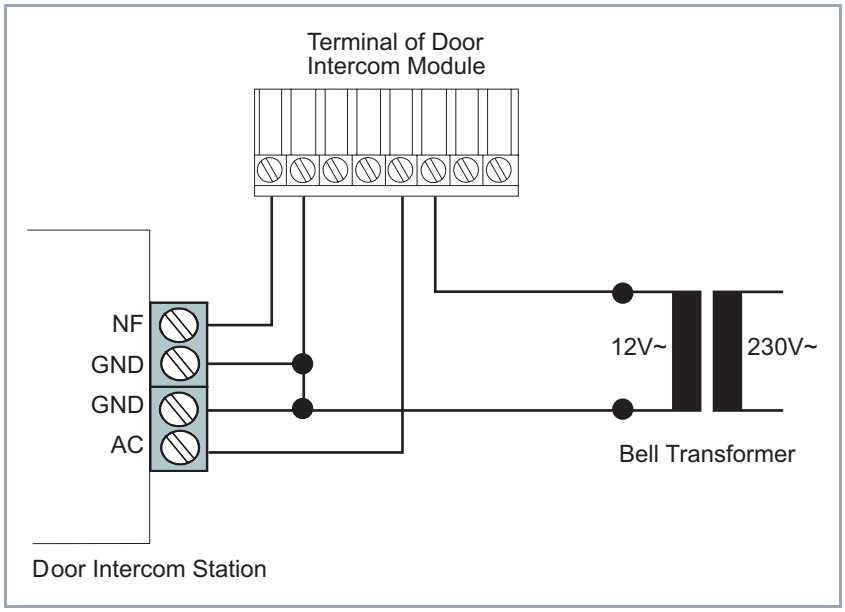


Figure 6-8: Example connection for door intercom station

Door bell button Example connection for a door bell button:

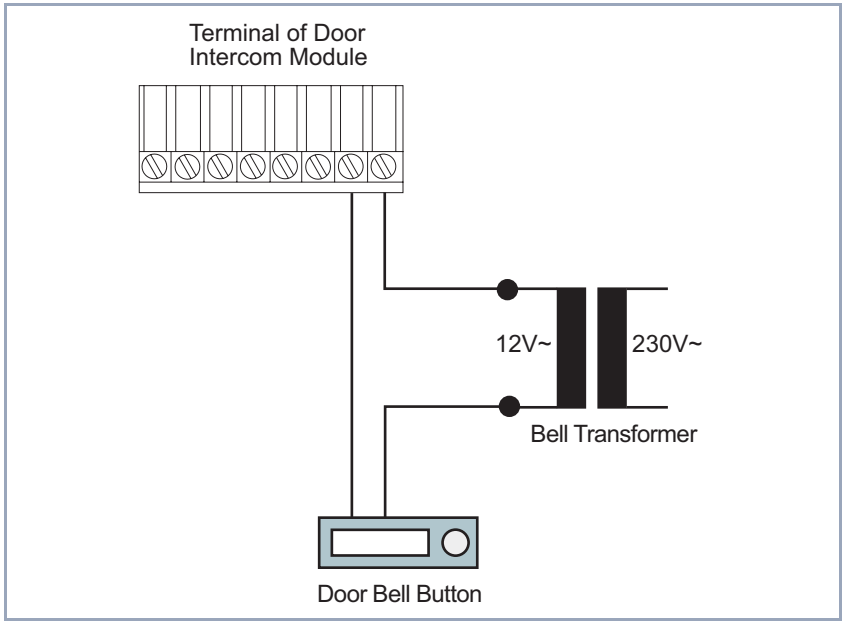


Figure 6-9: Example connection for a door bell button

Door opener Example connection for a door opener:

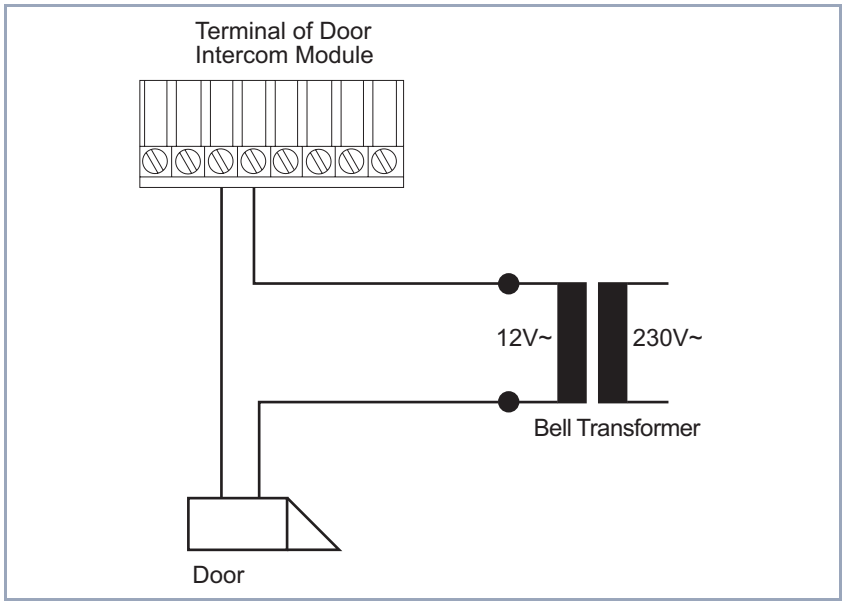


Figure 6-10: Example connection for a door opener

6.5 Installing and Removing Communication Modules and Connection Methods

Installing

As the XCM-S04AB and XCM-5S0 communication modules are installed in the same way, this description generally refers to the installation of one module.

Danger!

There is a risk of electric shock if installation work is carried out during operation.

- Always disconnect the power cord before carrying out installation work on **XCENTRIC**.
- You must also disconnect **XCENTRIC** from the power supply before installing modules, connecting and installing the screw terminal connectors or making any kind of connections. This is done by disconnecting the power cord of **XCENTRIC**.
- Do not connect **XCENTRIC** to the power supply until the equipment is completely installed and you have rechecked the installation.

Caution!

Electrostatic charges can damage electronic components. Please observe the following precautions to avoid damaging components:

- Ground yourself before unpacking components and before carrying out installation work on the equipment.
- Only grip boards at the edges and do not touch cables or components.

Danger!

Close unused module slots with the dummy covers to prevent objects getting inside the equipment. Foreign bodies located in the equipment during operation create a danger of electric shock and short-circuits.

- Always close unused module slots with the dummy covers.

Slot 1 is fitted with the main module with the door intercom module (basic unit), which must not be removed. Slots 2 to 5 are intended for mounting communi-

cation modules and Slots 6 and 7 are reserved for future extension with hub modules.

Caution!

Installing a module in the wrong slot can damage the module or the whole equipment.

- Make sure you install the modules in their correct slots:
  Slots 2 to 5: communication modules (XCM-S04AB and XCM-5S0)
  Slots 6 and 7: hub modules (XCM-HUB)

Note that slot 2 of **XCENTRIC** should always be equipped with a communication module, as this is necessary for the operation of the fax modem module (XFM-Fax).

This is shown in the diagram below:

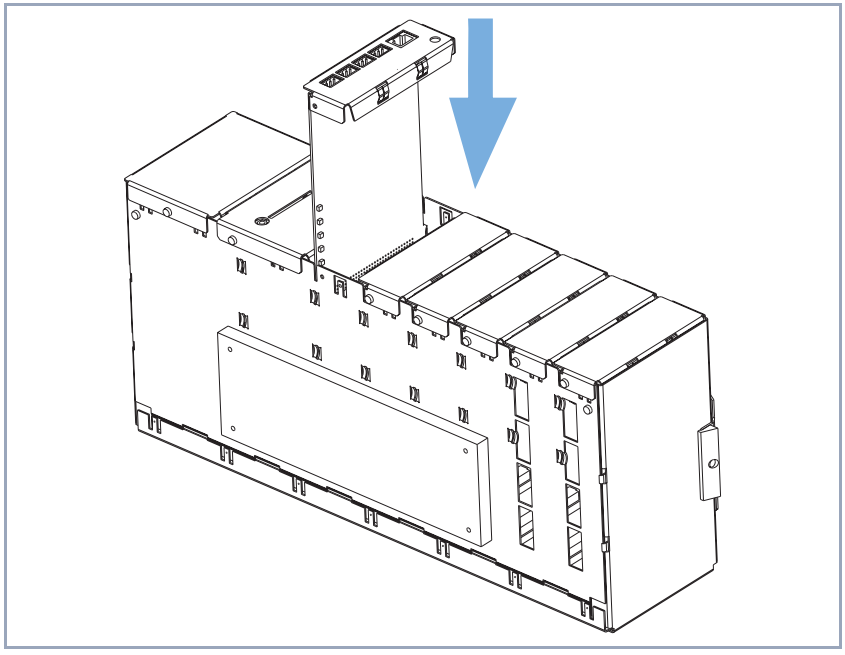


Figure 6-11: Installation of a communication module

Installing a module

Installation of a module:

- Read the description of the communication module before installing it (XCM-5S0 in chapter 6.7, page 81, XCM-S04AB in chapter 6.8, page 99). This is necessary, for example, for setting the jumpers before installing the module.
- If a dummy cover is fitted to the slot concerned, unscrew and remove this cover first.
- Insert the module into the housing from above with the top of the module pointing to the right. Card guides are fitted to the side plates of each slot to ensure that the modules are inserted safely. Push the module downwards until it engages in the slot sockets/connectors on the backplane.
- When the module engages in position, secure it to the housing using the enclosed screw.

Removing module

- To remove a module, carry out the steps described above for installing a module in the reverse order.

6.5.1 Connecting the Screw Terminal Connectors

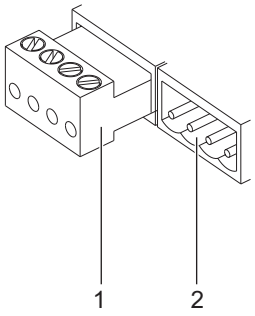
Screw terminal connectors are used for the **XCENTRIC** communication modules and the door intercom module. They are used for connecting the door intercom, for connecting terminals to ab connections and for connecting an external/internal S_0 connection to the ISDN exchange line and S_0 buses or digital terminals. The screw terminal connectors consist of two parts: the pins fixed to the boards and the detachable terminal blocks to which the wires are clamped.

Caution!

The interface will not work and can be damaged if the terminal blocks are connected incorrectly.

- Make sure the pins are not bent when plugging in the terminal block.
- Make sure the screws of the terminal block point to the right (when viewed from the front of **XCENTRIC**) when the block is plugged in; the direction for inserting is determined by notches on the terminal blocks.

Example of a screw terminal connector on XCM-5S0:



1	Terminal block plugged into the pins	2	Pins fixed to the module for the screw terminal connector, without terminal block

Figure 6-12: S_0 screw terminal connector

Danger!

There is a risk of electric shock if installation work is carried out during operation.

- You must also disconnect **XCENTRIC** from the power supply before installing modules, connecting and installing the screw terminal connectors or making any kind of connections. This is done by disconnecting the power cord of **XCENTRIC**.

Connecting wires

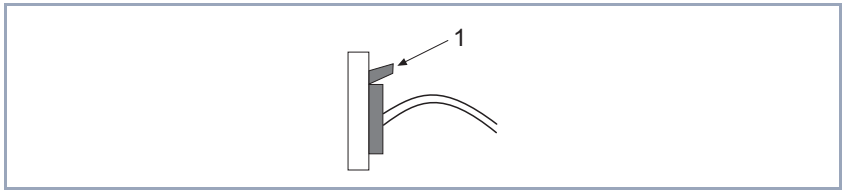
Proceed as follows to connect the wires:

- Remove a terminal block (1) from the pins (2) on the board.
- Strip back the insulation of the wires by 5 mm and fix the wires to the terminal block.
- Push the terminal block onto the pins again.

The screw terminal connector system makes it possible to exchange terminal connections without disconnecting the wires. The cables can also be prepared outside the equipment and then only need to be plugged in.

6.5.2 Connecting the Western Plug (RJ45)

After plugging into an ISDN socket, Western plugs (RJ45 plug, ISDN plug) are locked in position by the lever on the top of the plug.



1	Press here to remove the plug.		

Figure 6-13: Western plug (RJ45 plug)

RJ45 plug removal

➤ You must press down the small lever before the plug can be removed from the socket.

6.5.3 Connecting the RJ45 Sockets

You can use RJ45 sockets for the installation of internal S_0 buses.

IAE and UAE sockets can be purchased in Germany as RJ45 sockets. In other countries, please observe the descriptions and labeling of the RJ45 sockets obtainable.

Always observe the description and labeling of the sockets in each case!

RJ45 sockets are specially designed for ISDN installations and usually contain terminating resistors (two x 100 Ω). Carefully check the labeling on the sockets during installation, as it is possible that this may deviate from the standard pin assignment given in later examples in this manual.

RJ45 sockets can also be used for other applications than ISDN installation. Check whether the RJ45 sockets used contain terminating resistors. You should also check the sequence of numbering of RJ45 sockets.

6.6 Cable Installation for Basic Unit and Communication Modules

Strain relief devices are mounted on the basic unit and communication modules for fixing the cables securely.

Caution!

Make sure the cables do not cover the ventilation slots of the equipment or interfere with ventilation. Obstructing the ventilation of **XCENTRIC** may cause damage to the equipment.

➤ Install the cables so that the ventilation slots are kept clear and avoid obstructing the ventilation of **XCENTRIC**.

The cables from the main module and communication modules are routed from above, secured in the strain relief devices and then fed downwards to the rear between the wall and **XCENTRIC**. At the rear of **XCENTRIC**, the cables are routed downwards to the left and right of the centre part of the wall holder.

6.7 5 x S_0 Module (XCM-5S0)

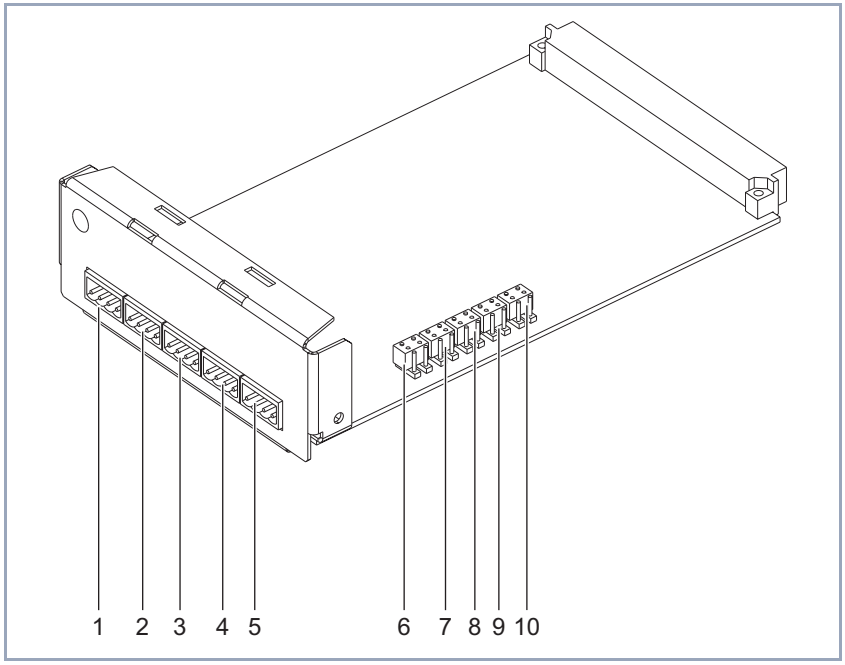
The XCM-5S0 communication module is equipped with five S_0 connections in the form of 4-pole screw terminal connectors. The S_0 interfaces can be configured individually as internal S_0 connections or external S_0 connections by inserting jumpers.

Internal S_0 connections are used for connecting an ISDN terminal or for installing an internal passive S_0 bus (series connection of several ISDN sockets). The connection to an internal S_0 connection is always point-to-multipoint. A short introduction to installing internal passive S_0 buses can be found at the end of the module description.

Installing the communication modules in the **XCENTRIC** housing is described in chapter 6.5, page 75. Please follow the instructions given there.

The use of Western plugs (RJ45) and making connections using screw terminal connectors are also described in chapter 6.5, page 75.

In the figure below, all S_0 connections are configured as internal S_0 connections by inserting the double jumpers.



1	Unit 0: S_0 connection	6	Jumper for Unit 4
2	Unit 1: S_0 connection	7	Jumper for Unit 3
3	Unit 2: S_0 connection	8	Jumper for Unit 2
4	Unit 3: S_0 connection	9	Jumper for Unit 1
5	Unit 4: S_0 connection	10	Jumper for Unit 0

Figure 6-14: XCM-5S0 module with S_0 connections (4-pole screw terminal connector) and double jumpers for configuration as internal or external S_0 connections

6.7.1 Jumpers for S_0 Connections

Besides the five double jumpers parallel to the long side of the module for changing between internal and external S_0 connection, you will also find another row of double jumpers behind the S_0 connections, parallel to the short side of the module. These jumpers are used for termination (terminating resistors).

The jumpers are already inserted in the ex works state. Change all the jumpers necessary for your network configuration before you install the module.

Warning!

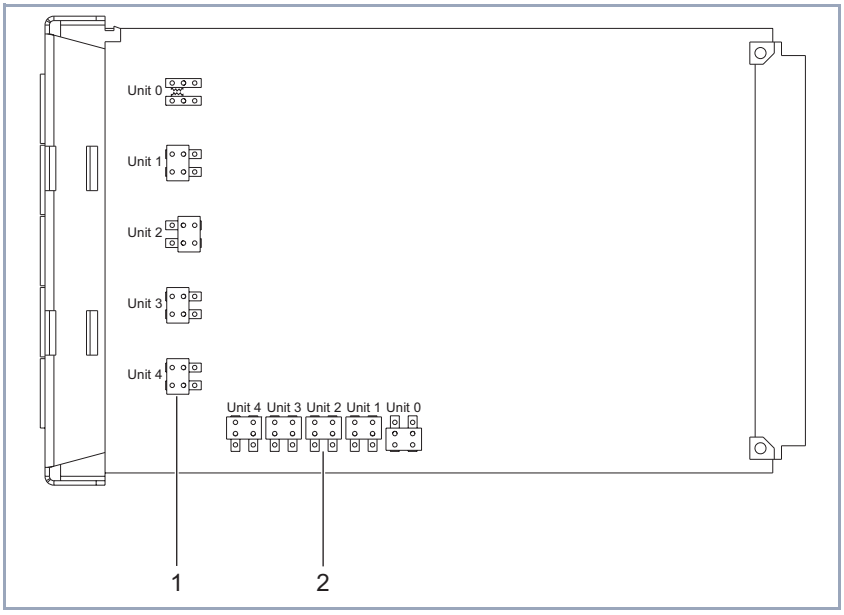
A module may be damaged on taking into operation if the jumpers are set incorrectly. The modules are equipped to a certain extent with protective measures to prevent such damage, but you should still insert jumpers very carefully.

➤ Make sure that suitably configured (internal or external) units are also connected correctly.

Each board also contains markings to simplify inserting the jumpers. The marking indicates the position in which the respective double jumper must be inserted for setting the relevant operating mode. The layout of the jumper posts largely prevents accidentally inserting the jumpers in the wrong position (twisting, offsetting).

The jumper posts for the jumpers for changing from internal to external S_0 are marked by a telephone handset for internal S_0 and a post office horn symbol for external S_0. The jumper posts for the termination jumpers are marked by a jagged line for a terminated S_0 connection (with terminating resistor: 2 x 100 Ω). See figure 6-16, page 85 and figure 6-17, page 86.

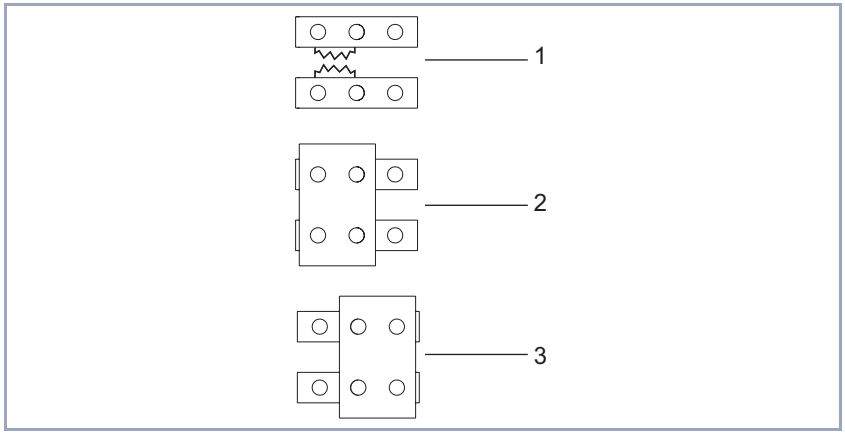
A diagram of the 5-S_0 module is shown below:



1	Jumpers for termination	2	Jumpers for configuration of external and internal S_0 connections

Figure 6-15: 5 x S_0 module with jumpers for termination and configuration of internal and external S_0 connections

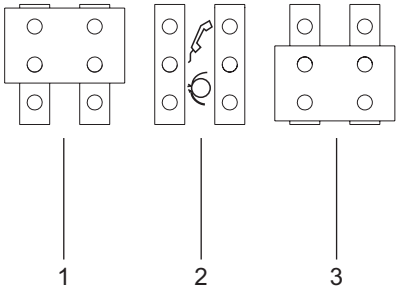
Jumpers for termination on XCM-5S0:



1	Associated jumper posts without double jumper inserted = not terminated	3	Double jumper inserted right = not terminated
2	Double jumper inserted left = terminated		

Figure 6-16: Enlarged view of three jumpers for termination

Jumpers for configuration of internal and external S_0 connections on XCM-5S0:



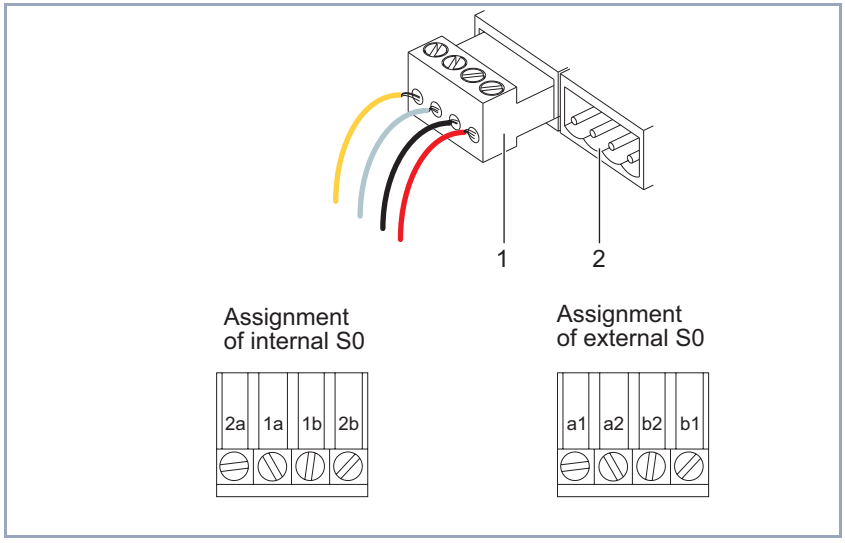
1	Double jumper inserted = internal S_0	3	Double jumper inserted = external S_0
2	Associated jumper posts without double jumper inserted (for illustration purposes only; a double jumper must always be inserted here)		

Figure 6-17: Enlarged view of three jumpers for configuration

6.7.2 Pin Assignment of XCM-5S0

Defining the S_0 connections as external or internal S_0 connections also determines the assignment of the individual pins. The cables must be connected to the terminal blocks according to this assignment.

The assignments are shown in the following figure:



1	Terminal block pushed onto pins, cables secured to terminal block	2	Pins fixed to the module for the screw terminal connector, without terminal block

Figure 6-18: Assignment of S_0 connections

In Großbritannien werden in der Regel die in der folgenden Tabelle aufgeführten Kabelfarben bei der ISDN-Verkabelung benutzt:

In anderen Ländern können die Kabelfarben bei der ISDN-Verkabelung variieren. Beachten Sie bei der Verkabelung die Gegebenheiten des Einzelfalls.

a2	gelb	a1	grau
b1	schwarz	b2	rot

Table 6-2: Vorwiegend benutzte Kabelfarben in Großbritannien

6.7.3 External S_0 Connection

There are various options for connecting an external S_0 connection to the ISDN exchange line.

Here we assume that an ISDN cable (RJ45, single wires) is used, with the single wires being connected to the external S_0 connection of the 5 x S_0 module and the RJ45 plug acting as connection to the ISDN.

If you make the connection to the NTU (Network Termination Unit for ISDN Basic Rate Interface) via the terminal for the S_0 interface, connect the wires according to the labeling of the terminal on the NTU. See chapter 6.7.2, page 86 for the pin assignment of an external S_0 connection on XCM-5S0.

Point-to-point

A point-to-point connection can be made in two ways:

1. directly terminated on ➤➤ **NT**U (relevant unit of **XCENTRIC,**) or
2. to an RJ45 socket connected in series with the NTU (figure 6-20, page 89).

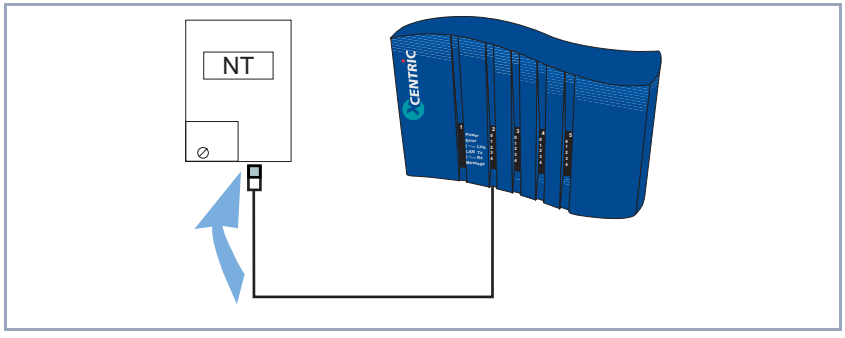


Figure 6-19: Direct connection to NTU

In the second option, connection to an RJ45 socket, check if the socket already contains a termination. If so, the relevant S_0 connection must no longer be terminated on the XCM-5S0. If the socket contains no termination, the relevant S_0 connection must be terminated on the XCM-5S0 using a double jumper.

XCENTRIC on an RJ45 socket connected in series with the NTU:

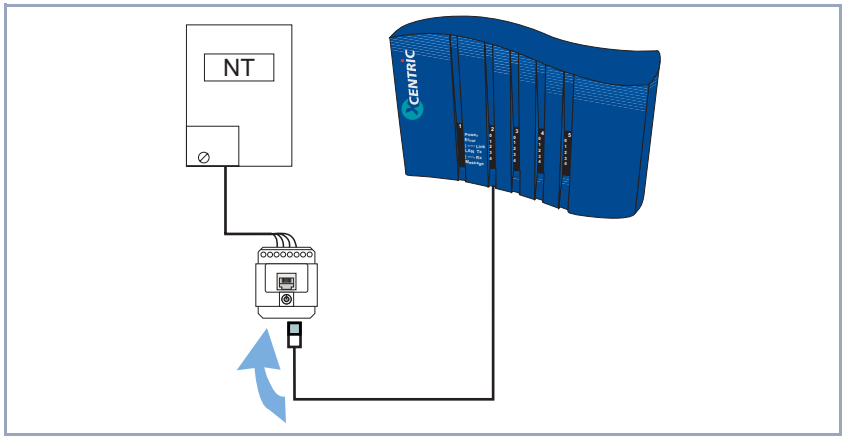


Figure 6-20: Connection to an RJ45 socket

Point-to-multipoint

For a point-to-multipoint connection, there are two additional options:

3. at the end of an external S_0 bus (RJ45 sockets)
4. in the middle of an external S_0 bus (RJ45 sockets)

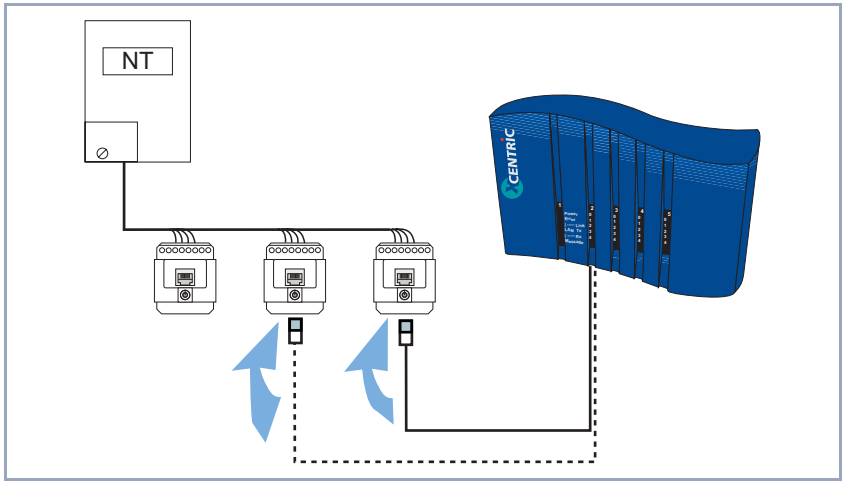


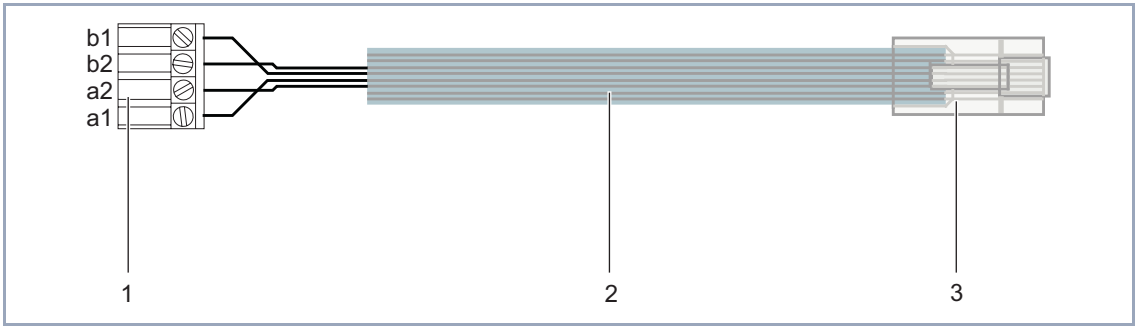
Figure 6-21: Connection to an external S_0 bus for point-to-multipoint connection

You must comply with the following when connecting to an external S_0 bus:

- Connection to the end of the bus (figure 6-21, page 89: continuous line)
  As an S_0 bus is usually terminated at both ends, the external S_0 connection of the XCM-5S0 must be terminated here; in this case, the last RJ45 socket (to which **XCENTRIC** is connected) must not be terminated. If this last socket is terminated, the relevant S_0 connection of the XCM-5S0 must not be terminated.
- Connection to the middle of the bus (figure 6-21, page 89: dotted line)
  As an S_0 bus is usually terminated at both ends, the external S_0 connection of the XCM-5S0 must not be terminated in this variant. Insert the double jumper of the S_0 connection concerned so that the interface is not terminated. See also chapter 6.7.1, page 83.

Wiring an RJ45 plug

To connect a cable (RJ45, single wires) to an external S_0 connection, connect the wires as shown in the diagram below:



1	Screw terminal of a 5 x S0 module (configured as external)	3	RJ45 plug (plan view, lever at top)
2	ISDN cable		

Figure 6-22: Connecting an ISDN cable to an external S_0 interface

A diagram of the RJ45 plug is shown below:

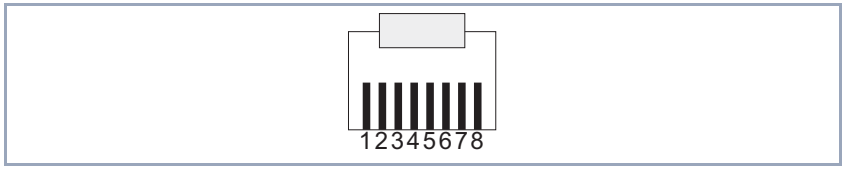


Figure 6-23: RJ45 plug

The pin assignment for connecting an external S_0 connection to an RJ45 plug is illustrated below in tabular form:

External S_0 connection	RJ45 plug
a2	3
a1	4
b1	5
b2	6

If a typical 8-wire ribbon cable is used, wires 3, 4, 5 and 6 are connected to the 4-pole screw terminal connector.

6.7.4 Internal S_0 Connection - Possible Connections

There are four possible ways of connecting to an internal S_0 screw terminal connector on the XCM-5S0 module:

- Short passive bus – **XCENTRIC** at the start or end of the bus
- Short passive bus – **XCENTRIC** in the middle of the bus
- Extended passive bus
- point-to-point connection

The maximum permissible length of the connecting cable from a terminal to the corresponding RJ45 socket is 10 m for all types of connection.

Short passive bus

A short passive S_0 bus can be 100 to 180 m long, depending on the type of cable.

Up to eight digital terminals can be connected to each short passive bus and administrated. A power supply of maximum 2 W per S_0 interface is available for digital telephones without their own power supply. A maximum total of 20 W is available for the equipment when fully equipped.

Not more than two of the terminals connected to an S_0 interface can operate at the same time. For example, you can receive a fax and make a phone call at the same time on one bus, or internal or external calls are possible on two telephones at the same time.

This is shown in the diagram below:

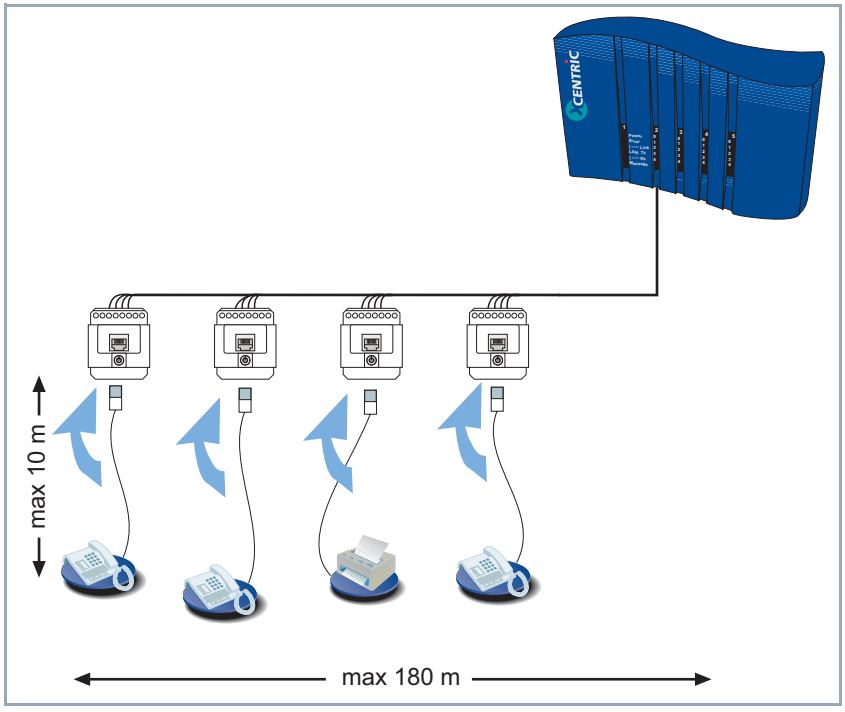


Figure 6-24: Internal S_0 connection: short passive bus with **XCENTRIC** connected to the start of bus

The termination (terminating resistors) must comply with the following:

- Short passive bus – **XCENTRIC** at the start or end of the bus
  If the S_0 bus is installed with **XCENTRIC** at one end, both the relevant **XCENTRIC** unit and the RJ45 socket at the other end of the S_0 bus must be terminated.
  See figure 6-24, page 93.

- Short passive bus – **XCENTRIC** in the middle of the bus
  If **XCENTRIC** is connected to the middle of the bus, the double jumpers must be inserted so that the relevant S_0 interface on the XCM-5S0 is not terminated. (See chapter 6.7.1, page 83 for inserting the jumpers.)
  In this case, the RJ45 sockets at both ends of the S_0 bus must have terminating resistors.

See figure 6-25, page 94:

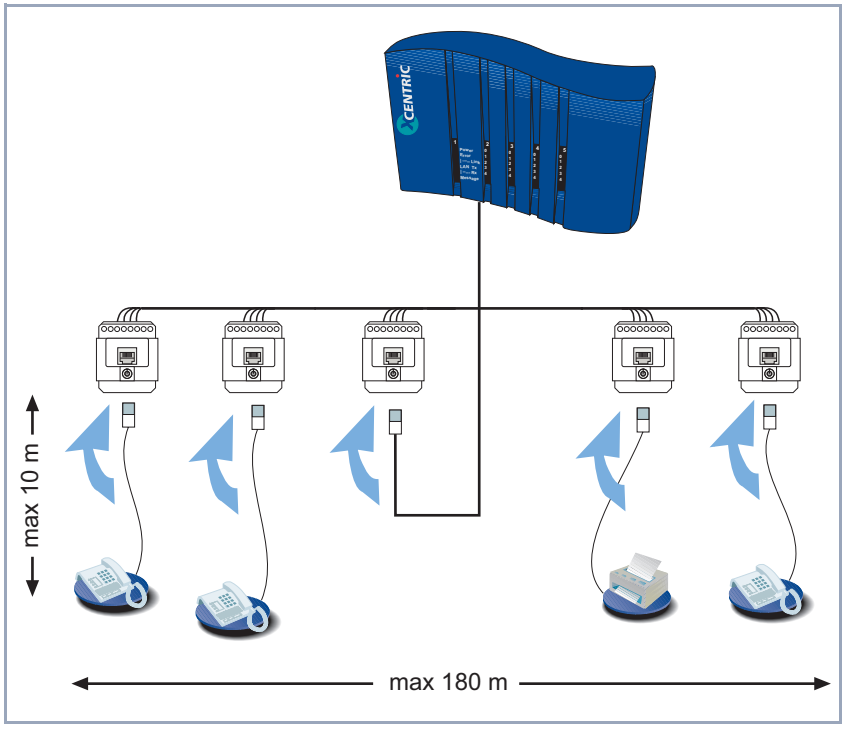


Figure 6-25: Internal S_0 connection: short passive bus with **XCENTRIC** connected to the middle of bus

Extended passive bus

If you connect an extended passive bus to the internal S_0 interface, we recommend a maximum cable length of 450 m to the distributor and maximum 10 m from the distributor to the RJ45 sockets.

Not more than three terminals should be connected to the distributor.

The relevant unit on the 5 x S_0 module and the distributor must be terminated; the RJ45 sockets connected to the distributor must not be fitted with terminating resistors.

The description given above for the short passive bus applies to feeding power to the terminals without their own power supply and using several terminals at the same time.

See figure 6-26, page 95:

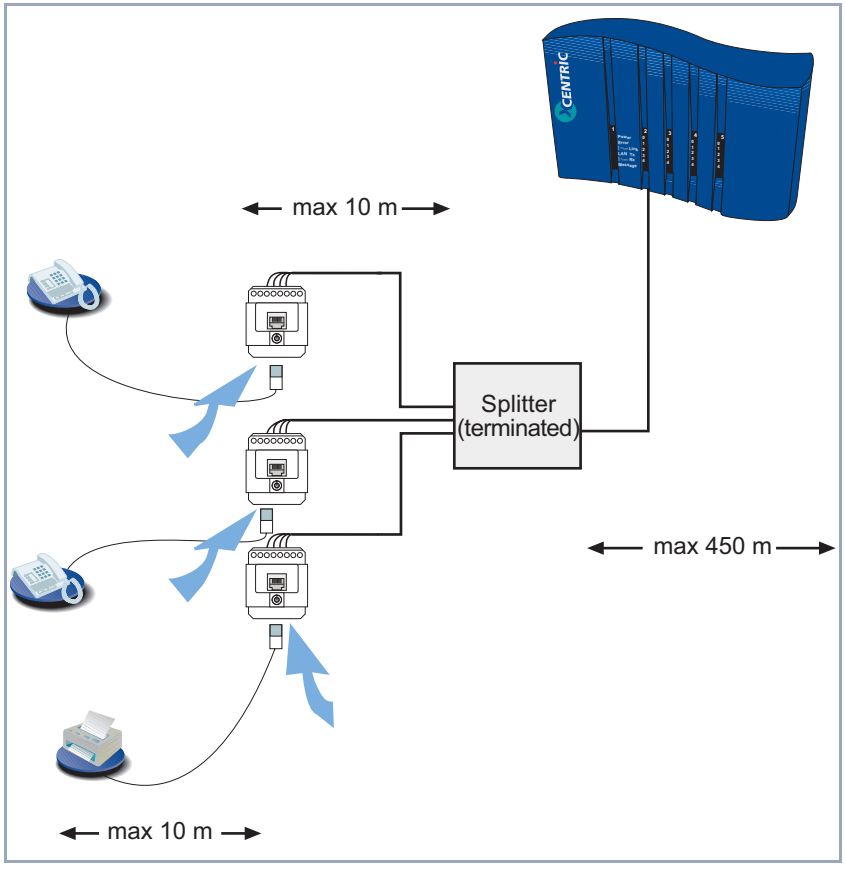


Figure 6-26: Internal S_0 connection: extended passive bus

Point-to-point

The maximum distance for connecting a digital terminal to an internal S_0 interface is 1000 m.

The relevant unit on the 5 x S_0 module and the RJ45 socket must be terminated.

See figure 6-27, page 96:

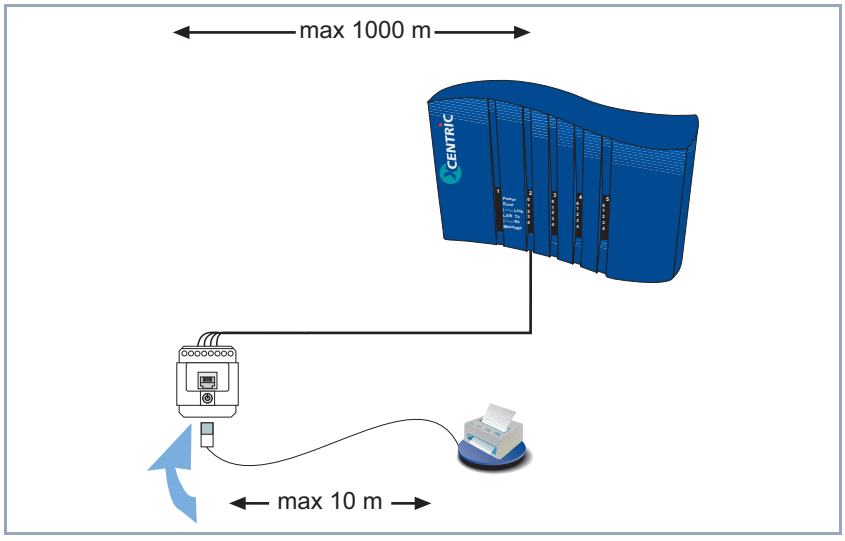


Figure 6-27: Internal S_0 connection: point-to-point connection

6.7.5 Internal S_0 Connection – Wiring

IAE and UAE sockets can be purchased in Germany as RJ45 sockets. In other countries, please observe the descriptions and labeling of the RJ45 sockets obtainable.

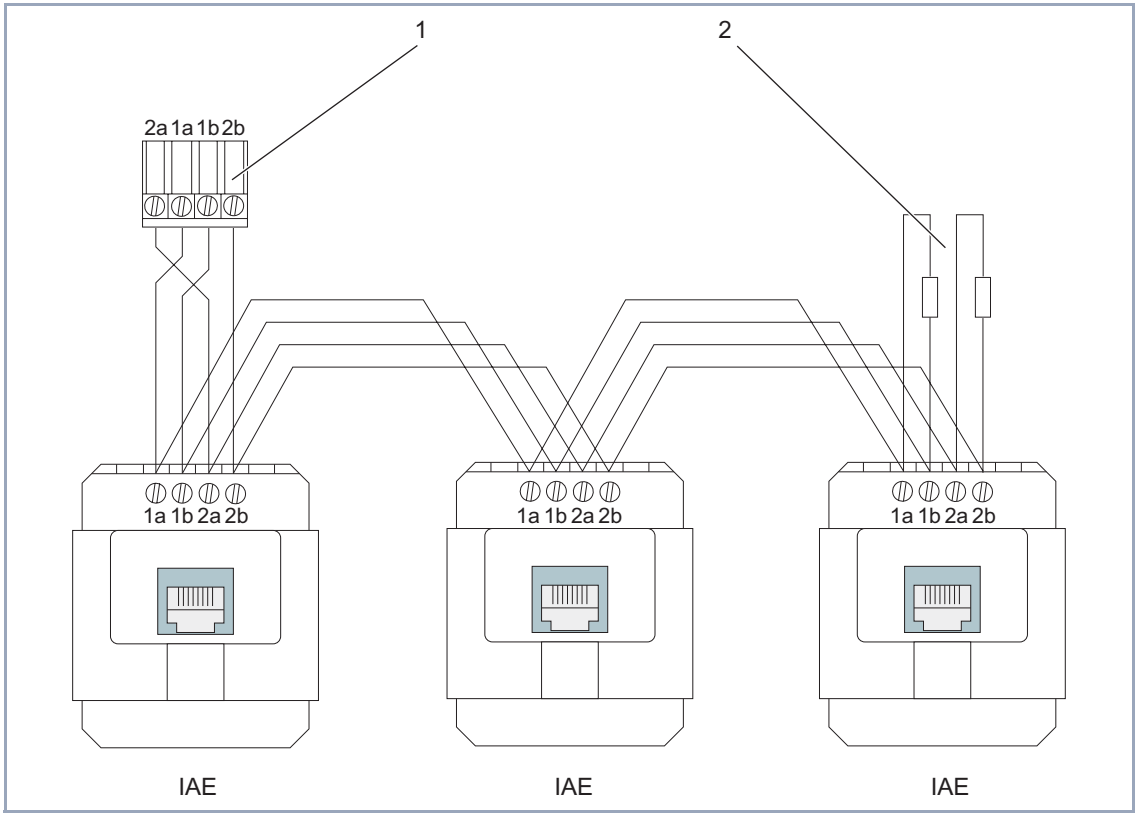
Always observe the description and labeling of the sockets in each case!

Make sure you take the different wiring and installation of terminating resistors in RJ45 sockets into account during the installation of internal S_0 buses.

The necessary information is given in the following figures.

The wiring of RJ45 sockets shown in figure 6-28, page 97 applies to standard RJ45 sockets. The labeling of RJ45 sockets can differ in practice. Make sure you check the labeling of the RJ45 sockets carefully and connect the wires accordingly.

Wiring and terminating resistors of RJ45 sockets in an internal S_0 bus:

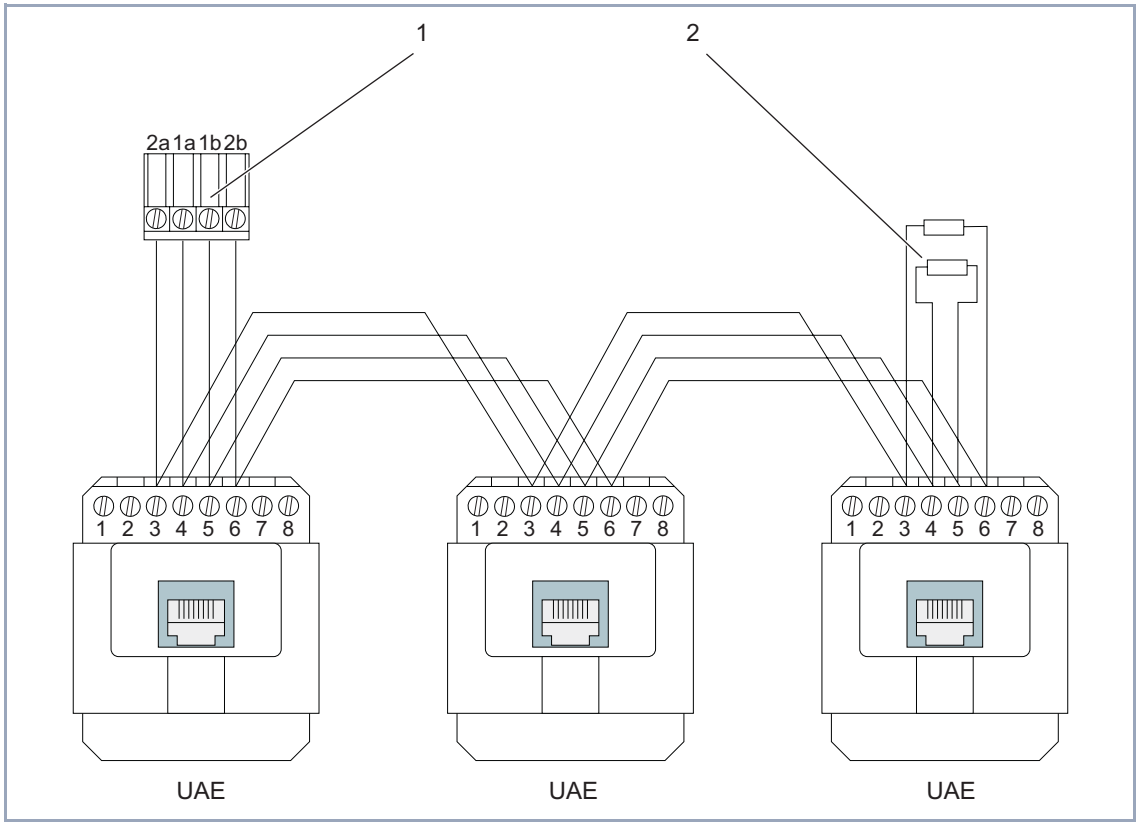


1	Screw terminal of 5 x S_0 module (configured as internal)	2	Terminating resistors at the last RJ45 socket (2 x 100 Ω)

Figure 6-28: Internal S_0 bus with RJ45 sockets

The wiring of RJ45 sockets shown in figure 6-29, page 98 applies to standard RJ45 sockets. The sequence of numbering for RJ45 sockets can differ in practice. Make sure you check the labeling of the RJ45 sockets carefully and connect the wires accordingly.

Wiring and terminating resistors of RJ45 sockets in an internal S_0 bus:



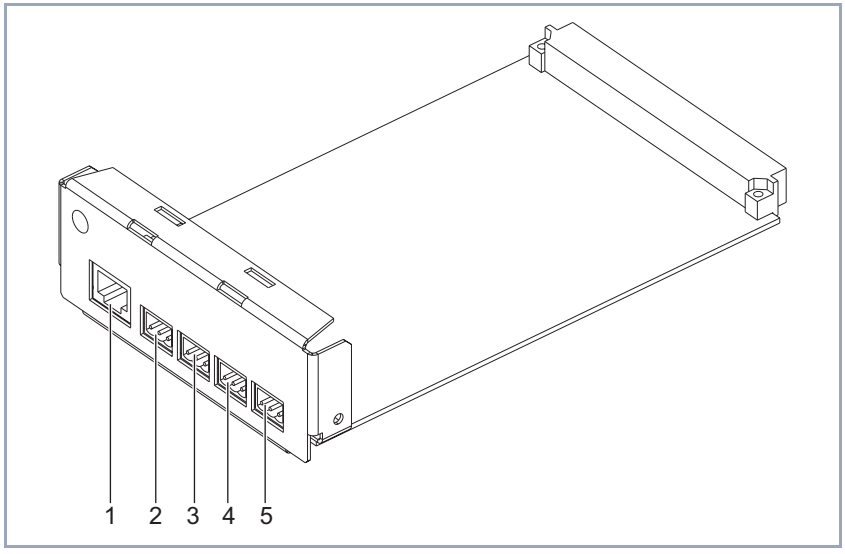
1	Screw terminal of 5 x S_0 module (configured as internal)	2	Terminating resistors at the last RJ45 socket (2 x 100 Ω)

Figure 6-29: Internal S_0 bus with RJ45 sockets

6.8 ab Module (XCM-S04AB)

The XCM-S04AB communication module is used for connecting four analog terminals such as analog telephones, G3 fax machines or modems. It also has an external S_0 connection (RJ45 socket) for connecting to an ISDN exchange line.

Each of the four ab connections are 3-pole screw terminal connectors.



1	Unit 0: External S_0 connection (RJ45 socket)	4	Unit 3: ab connection (3-pole screw terminal connector)
2	Unit 1: ab connection (3-pole screw terminal connector)	5	Unit 4: ab connection (3-pole screw terminal connector)
3	Unit 2: ab connection (3-pole screw terminal connector)		

Figure 6-30: XCM-S04AB module

Installing the communication modules in the **XCENTRIC** housing is described in chapter 6.5, page 75. Please follow the instructions given there.

The use of Western plugs (RJ45) and making connections using screw terminal connectors are also described in chapter 6.5, page 75.

6.8.1 Jumpers for S_0 Connections

The XCM-S04AB has two jumpers for terminating the external S_0 connection. The two jumpers are inserted in the default setting, i.e. the connection is terminated.

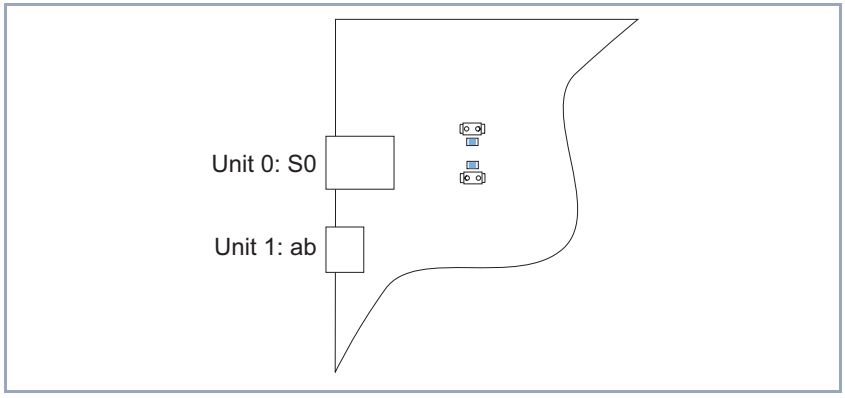


Figure 6-31: Part of XCM-S04AB with jumpers inserted (terminated)

If the S_0 connection for a point-to-multipoint connection is connected to an RJ45 socket in the middle of an external S_0 bus, both jumpers must be removed so that this connection is no longer terminated. See chapter 6.8.3, page 101 for connecting external S_0 interfaces.

6.8.2 Pin Assignment of XCM-S04AB

The pin assignment of the ab interfaces is shown in the drawing below and in the associated table.

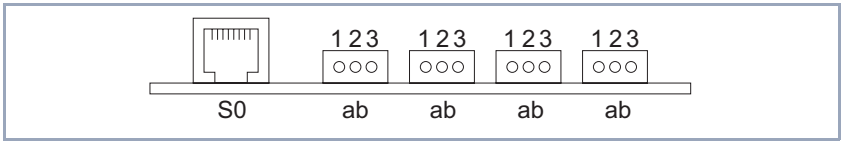


Figure 6-32: Pin assignment of XCM-S04AB

Pins of ab connections	Assignment
1	B (RING)
2	A (TIP)
3	Ringing capacitor (British Telecom)

Table 6-3: Pin assignment of ab connections (3-pole screw terminal connectors)

The last pin (pin 3) of an ab connection is only used for British Telecom analog terminals and is not used for standard German equipment.

6.8.3 External S_0 Connection

The RJ45 socket of the XCM-S04AB is connected to an ISDN exchange line using an ISDN cable.

Use an RJ45 plug for connecting the cable to **XCENTRIC**. For connecting the ISDN cable to the NTU, you can use either an RJ45 plug or a terminal connection.

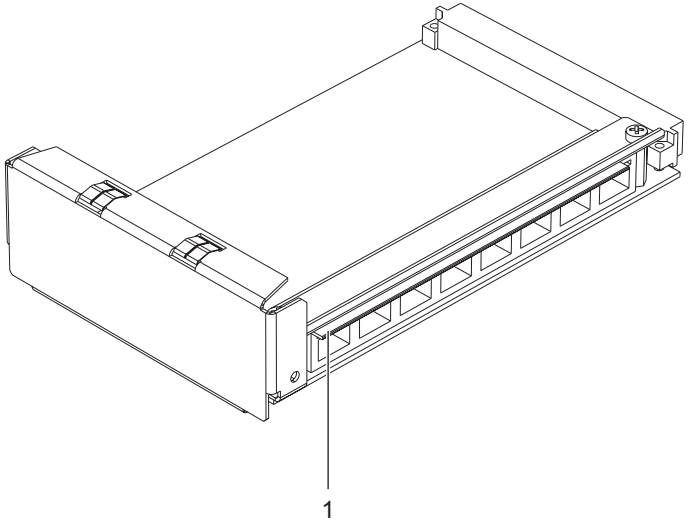
If you make the connection to the NTU (Network Termination Unit for ISDN Basic Rate Interface) via the terminal for the S_0 interface, connect the wires according to the labeling of the terminal on the NTU.

For the various possible connections to the ISDN, please read the description of the types of connection for the XCM-5S0 module (chapter 6.7.3, page 88), which also apply to the external S_0 connection of the XCM-S04AB module.

6.9 Hub Module (XCM-HUB)

The hub module (XCM-HUB) obtainable for **XCENTRIC** permits direct connection of PCs and servers. This integrated hub is a dual-speed hub with auto sensing function for 10 Mbps or 100 Mbps LANs. The hub has an integrated switching part.

The hub supports 10Base-T category 3-5 and 100Base-T category 5 operating modes.



1	Textile tape (radio-frequency seal)		

Figure 6-33: Hub module for **XCENTRIC** (XCM-HUB)

Up to two hub modules can be integrated in **XCENTRIC**. Eight ports are available for each module, with one port of the first module being used for the connection to the **XCENTRIC** basic unit. Each module has two ports, which support full-duplex transmission.

For EMC (electromagnetic compatibility) reasons, a textile tape is attached the length of the module alongside the LEDs.

6.9.1 Installation and Removal of Hub Module

Installing

The two slots (6 and 7) provided for the installation of the hub modules are assigned as master and slave slot; Slot 6 is the master slot and Slot 7 the slave slot. The first hub module or a single hub module must therefore always be installed in Slot 6 of the basic unit. See figure 6-2, page 62.

Slot 1 is fitted with the main module with the door intercom module (basic unit), which must not be removed. Slots 2 to 5 are intended for mounting communication modules and Slots 6 and 7 are reserved for future extension with hub modules.

Danger!

There is a risk of electric shock if installation work is carried out during operation.

- Always disconnect the power cord before carrying out installation work on **XCENTRIC**.
- You must disconnect **XCENTRIC** from the power supply before installing modules or connecting and installing any kind of connections. This is done by disconnecting the power cord of **XCENTRIC**.
- Do not connect **XCENTRIC** to the power supply until the equipment is completely installed and you have rechecked the installation.

Caution!

Electrostatic charges can damage electronic components. Please observe the following precautions to avoid damaging components:

- Ground yourself before unpacking components and before carrying out installation work on the equipment.
- Only grip boards at the edges and do not touch cables or components.

Danger!

Close unused module slots with the dummy covers to prevent objects getting inside the equipment. Foreign bodies located in the equipment during operation create a danger of electric shock and short-circuits.

- Always close unused module slots with the dummy covers.

Caution!

Installing a module in the wrong slot can damage the module or the whole equipment.

- Make sure you install the modules in their correct slots:
  Slots 2 to 5: communication modules (XCM-S04AB and XCM-5S0)
  Slots 6 and 7: hub modules (XCM-HUB)

Caution!

When installing the hub modules, make sure a module is always fitted in Slot 6. A single hub module must never be fitted in Slot 7, as this may damage the module or the complete equipment.

- Always install the first hub module or a single hub module in Slot 6.
- If you equip **XCENTRIC** with two hub modules and then remove a hub module, make sure the remaining module is always mounted in Slot 6.

This is shown in the diagram below:

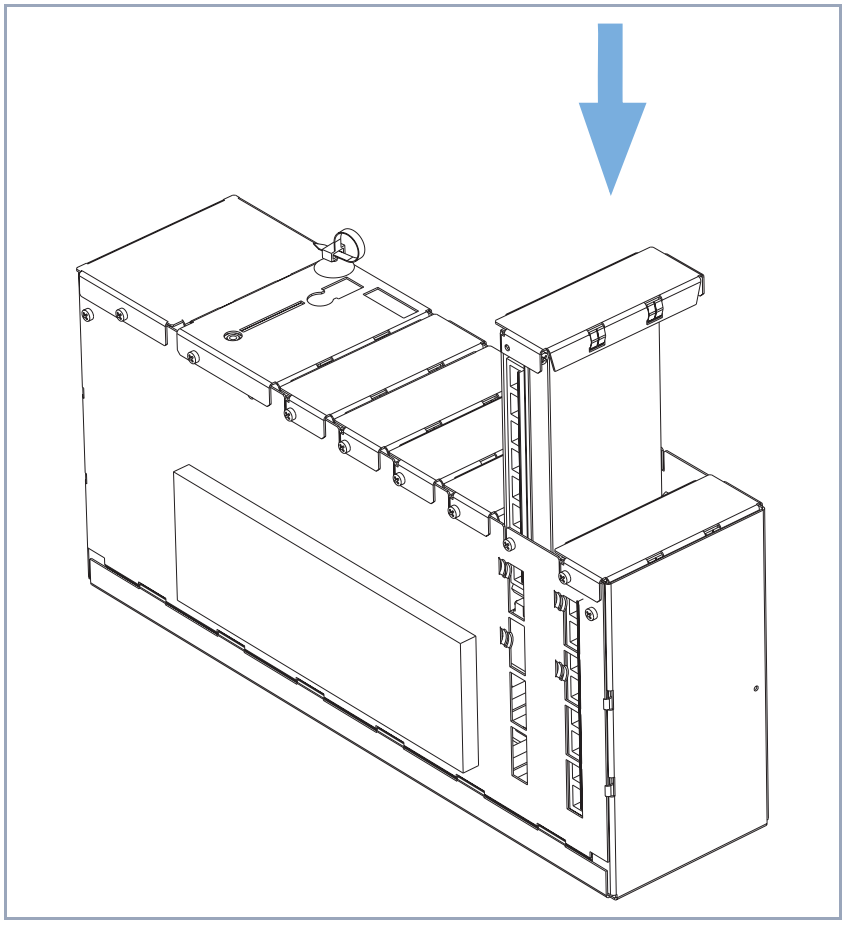


Figure 6-34: Installing a hub module

Installing a hub module

Installation of a hub module:

- If a dummy cover is fitted to the slot concerned, unscrew and remove this cover first.
- Insert the module into the housing from above with the top of the module pointing to the right, i.e. the ports are facing towards the front. Card guides are fitted to the side plates of each slot to ensure that the modules are inserted safely.

Make sure you press the textile tape to the right when sliding in the hub module. The textile tape (radio-frequency seal) must rest on the inside of the metal housing so that the LEDs remain visible.

- Push the module downwards until it engages in the slot sockets/connectors on the backplane.
- When the module engages in position, secure it to the housing using the enclosed screw.

Removing a hub module

Caution!

When removing one of two hub modules, make sure a module is always fitted in Slot 6. A single hub module must never be fitted in Slot 7, as this may damage the module or the complete equipment.

- If **XCENTRIC** is equipped with two hub modules and a hub module is later removed, make sure the remaining module is always mounted in Slot 6.
- To remove a module, carry out the steps described above for installing a module in the reverse order.

6.9.2 Ports of Hub Modules

Each hub module has eight ports, which are all equipped with an auto sensing function for 10 Mbps or 100 Mbps Ethernet/LAN connections.

The two top ports (Ports 1 and 2 and Ports 9 and 10, see figure 6-35, page 107) are also full-duplex ports. This means terminals connected to these ports that also support 100 Mbps and full-duplex can use this connection accordingly.

As the decision on whether a connection is operated in full-duplex or half-duplex mode is negotiated on setting up the connection (auto negotiation as per 802.3), a data terminal (e.g. a server) connected to Port 1 or 2 or Port 9 or 10 must be set so that the transmission method can be negotiated. This means that full-duplex must not be preset at the far end of the port.

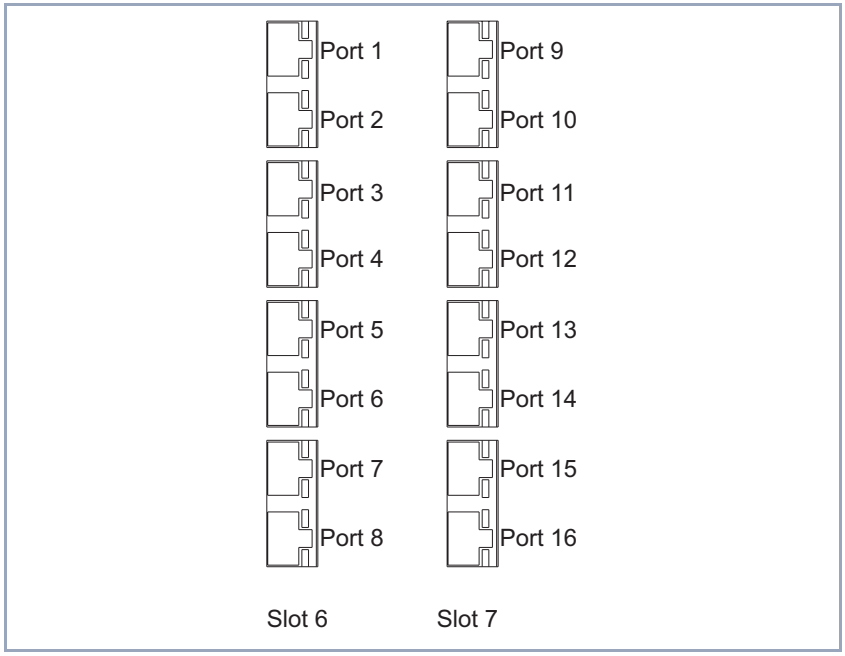


Figure 6-35: Ports for **XCENTRIC** equipped with two hub modules

We recommend you use Ports 1 and 2 and, if available, Ports 9 and 10 for connecting servers or hubs (see chapter 6.9.6, page 109), as these have separate LAN segments.

Make sure you use the correct cables for connecting hosts (e.g. PCs or servers) and hubs. Hosts have an MDI interface, hubs an MDIX interface. Crossed cables are used to interconnect two MDI interfaces or two MDIX interfaces. A 1:1 cable is used to connect an MDI interface to an MDIX interface.

6.9.3 Connection of Basic Unit and Hub Modules

To connect one or two hub modules to the basic unit of **XCENTRIC**, the Ethernet/LAN interface of the basic unit must be connected to Port 8 (the bottom port) of the hub module in Slot 6 (the master slot). Use the 100BT Ethernet category 5 STP cable (length 1 m) supplied with the hub module for this purpose.

The cable for this connection is routed from the Ethernet/LAN interface of the basic unit over the back of **XCENTRIC** and downwards. From here the cable is fed through the cable holders of the hub module to the front and connected to Port 8 of the hub module in Slot 6.

If **XCENTRIC** is equipped with two hub modules in Slot 6 and Slot 7, the connection between Slot 6 and Slot 7 is via the backplane of the basic unit, so that no additional connection is necessary between the two hub modules.

6.9.4 Cable Installation for Hub Module

Cable guides are mounted on the bottom of the basic unit for securely fixing the cables to the ports of the hub module.

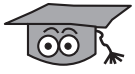
Caution!

Make sure the cables do not cover the ventilation slots of the equipment or interfere with ventilation. Obstructing the ventilation of **XCENTRIC** may cause damage to the equipment.

➤ Install the cables so that the ventilation slots are kept clear and avoid obstructing the ventilation of **XCENTRIC**.

The cables from the hub module are routed down the front and fixed by the folding cable guides.

6.9.5 Functionality of Hub Module



The hub module (XCM-HUB) of **XCENTRIC** is a dual-speed hub or switching hub with two switched ports.

A module has eight ports. If **XCENTRIC** is equipped with two hub modules, then the hub module can be said to have a total of 16 ports.

The integrated switching part enables several LAN segments to be formed. Ports 1 and 2 and Ports 9 and 10, which support both 10/100 Mbps auto sensing and full-duplex transmission, each form one switch internally. Each device connected to these ports is therefore located in its own LAN segment, a collision domain.

The remaining six ports together can form two further LAN segments. In a heterogeneous network in which both 10 Mbps connections and 100 Mbps connections exist, all 10 Mbps ports and all 100 Mbps ports are combined dynamically into two further LAN segments via the internal switching part.

If **XCENTRIC** is equipped with two hub modules, it is possible to form up to eight LAN segments, each of which forms its own collision domain, as the connection of the two hub modules is in turn implemented via a switch.

6.9.6 Cascading Other External Hubs

If the number of Ethernet ports of **XCENTRIC** when fully equipped with two hub module is not sufficient, other cascading options exist.

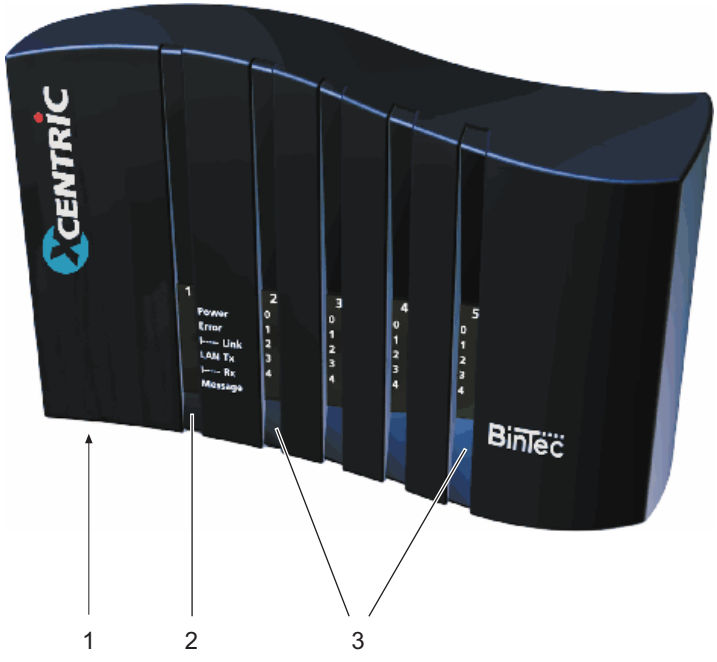
A 100 Mbps LAN is subject to a restriction of 200 meters on the maximum separation between two data terminals. In addition, not more than one hub is to be installed between the two terminals. The maximum cable length in these 100 Mbps networks is always 100 meters between the hub and terminal.

The above restrictions and the functionality of the hub module described in chapter 6.9.5, page 108 result in the following additional cascading options:

- Dual-speed/full-duplex ports (Ports 1 and 2 and Ports 9 and 10)
  Another hub can be connected to these ports.
- Dual Speed Port -10 Mbps (Ports 3 to 8 and Ports 11 to 16)
  These ports have no restrictions on further cascading.
- Dual Speed Port – 100 Mbps (Ports 3 to 8 and Ports 11 to 16)
  No more hubs are to be connected to these ports.

7 LEDs

XCENTRIC is enclosed in a plastic cover, which protects the internal metal housing. The individual LEDs of the basic unit and modules are visible through openings in the plastic cover.



1	Mains connection on the bottom	3	Slot 2 to 5: Labeled LEDs of communication modules
2	Slot 1: Labeled LEDs of main module		

Figure 7-1: **XCENTRIC** unit with plastic cover mounted

You can see the six LEDs of the main module (labeled on the plastic cover) and the LEDs of the communication modules on the front of the equipment. The LEDs of the communication modules are labeled inside on the metal housing and can also be read from outside through the lengthwise openings.

7.1 LEDs of Basic Unit

The LEDs of the basic unit are visible on the front of **XCENTRIC** through the lengthwise openings of the plastic cover.

The LEDs on the basic unit are shown in the figure below. This is followed by a description of the individual LEDs for the respective states.

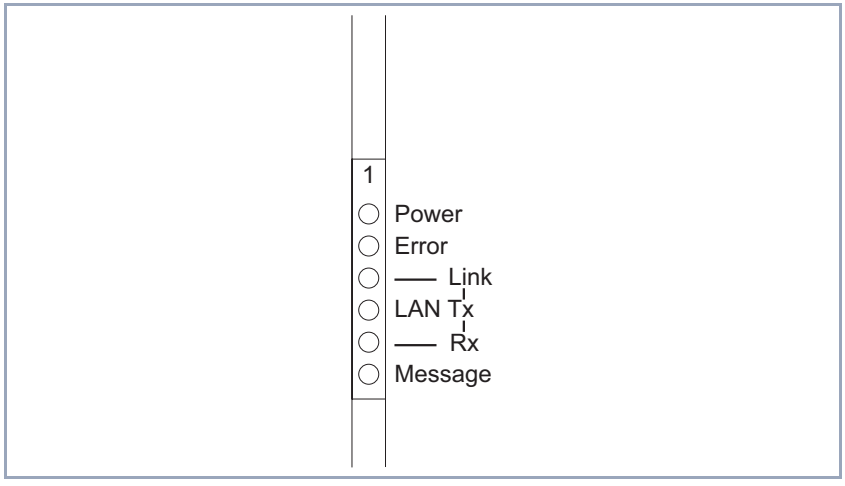


Figure 7-2: LEDs of basic unit

Selftest mode

LED	Color	State	Meaning
Power	green	on	Power supply connected.
Error	red	on	Error has occurred in the selftest.
LAN link	green	on	Ethernet test is being carried out.
LAN Tx	orange	on	Ethernet test is being carried out.
LAN Rx	orange	on	Ethernet test is being carried out.
Message			Not used.

Table 7-1: Meaning of LEDs on basic unit in selftest mode

BOOTmonitor Mode

LED	Color	State	Meaning
Power	green	on	Power supply connected.
Error	red	on flashing	BOOTmonitor Mode Firmware start.
LAN link	green	on	BOOTmonitor Mode
LAN Tx	orange	on	BOOTmonitor Mode
LAN Rx	orange	on	BOOTmonitor Mode
Message			Not used.

Table 7-2: Meaning of LEDs on basic unit in BOOTmonitor mode

Normal Mode

LED	Color	State	Meaning
Power	green	on	Power supply connected.
Error	red	on	Fault has occurred.
LAN link	green	off on flashing	LAN interface is not active. 10 Mbps Mode 100 Mbps Mode
LAN Tx	orange	on	Transmission of packets.
LAN Rx	orange	on	Reception of packets.
Message			Not used.

Table 7-3: Meaning of LEDs on basic unit in normal mode

7.2 LEDs of XCM-5S0

The LEDs of the XCM-5S0 are visible on the front of **XCENTRIC** through the lengthwise openings of the plastic cover. You can see the LEDs in the slot in which the module is inserted (possible slots 2 to 5).

This is shown in the diagram below:

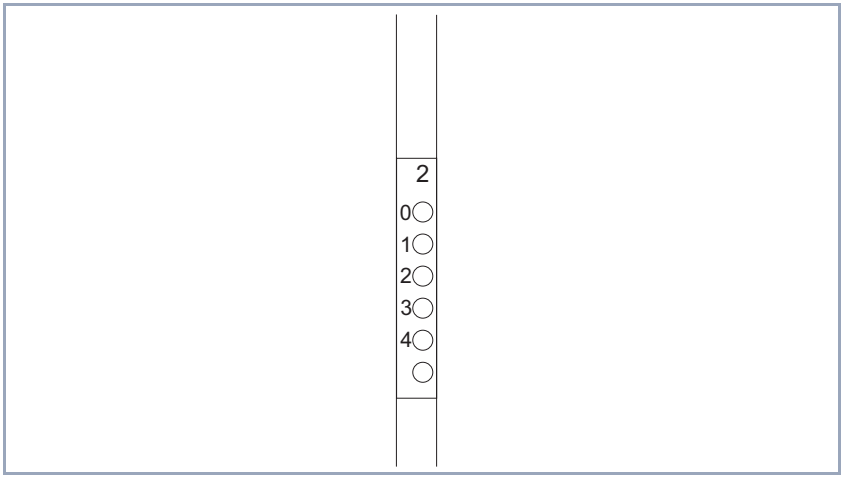


Figure 7-3: XCM-5S0: assignment of LEDs

The LEDs are assigned to the connections as follows:

LED	Assignment
0	Unit 0: external/internal S_0 connection
1	Unit 1: external/internal S_0 connection
2	Unit 2: external/internal S_0 connection
3	Unit 3: external/internal S_0 connection
4	Unit 4: external/internal S_0 connection

Table 7-4: Assignment of LEDs on XCM-5S0

The LED of an S_0 connection (Unit 0 - 4) lights green if layer 1 is active. This LED lights orange if one connection is active and flashes orange if two connections are active.

7.3 LEDs of XCM-S04AB

The LEDs of the XCM-S04AB are visible on the front of **XCENTRIC** through the lengthwise openings of the plastic cover. You can see the LEDs in the slot in which the module is inserted (possible slots 2 to 5).

The LEDs are assigned to the connections as follows:

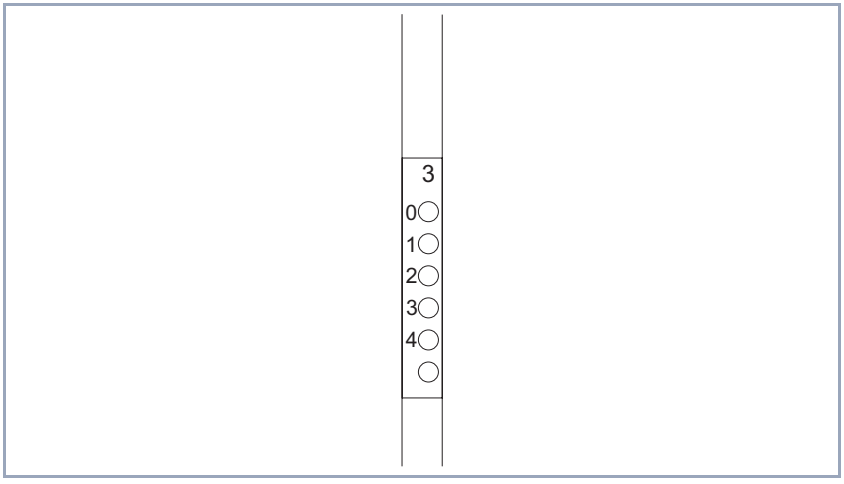


Figure 7-4: XCM-S04AB: assignment of LEDs

LED	Assignment
0	Unit 0: external S_0 connection
1	Unit 1: ab connection
2	Unit 2: ab connection
3	Unit 3: ab connection
4	Unit 4: ab connection

Table 7-5: Assignment of LEDs on XCM-S04AB

The LEDs of the ab connections (Unit 1 to 4) always light yellow if the handset is lifted on a telephone connected to the equipment. If a fax machine or answer-

ing machine is connected to the ab connection, the LED lights during the time a connection exists to the equipment.

The LED of an S_0 connection (Unit 0 - 4) lights green if layer 1 is active. This LED lights orange if one connection is active and flashes orange if two connections are active.

7.4 LEDs of XCM-HUB

The ports of the hub module (XCM-HUB) are each equipped with two LEDs to indicate the state of the interface.

These LEDs are only visible if the plastic cover of **XCENTRIC** is removed.

1	yellow LED (collision)	2	green LED (link/traffic)

Figure 7-5: LEDs on XCM-HUB

The top yellow LED lights if a collision has occurred in the associated LAN segment.

The bottom green LED indicates the state of the port. This LED lights if a connection exists to the port. Slow flashing (three times per second) indicates data

transmission at 10 Mbps and fast flashing (twelve times per second) indicates data transmission at 100 Mbps.

7 LEDs

8 Software Configuration Requirements

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

It also contains installation instructions for the BRICKware Windows software.

Caution!

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

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

- Use filters to reject certain data packets. Note that ISDN connections can be set up by broadcasts, especially in Windows networks.
  Basic filters are already set during configuration with the Configuration Wizard. Further information on setting filters is contained in chapter 10.1.5, page 161 and chapter 15.2, page 435.
- Use the Credits Based Accounting System to define a maximum number/duration of ISDN connections or a maximum limit for charges within a certain time. This limits excessive charges in advance. See chapter 15.1.3, page 424.
- See chapter 17.2.2, page 493. This chapter lists most of the reasons for excessive charges.

8.1 Connection Methods

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

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

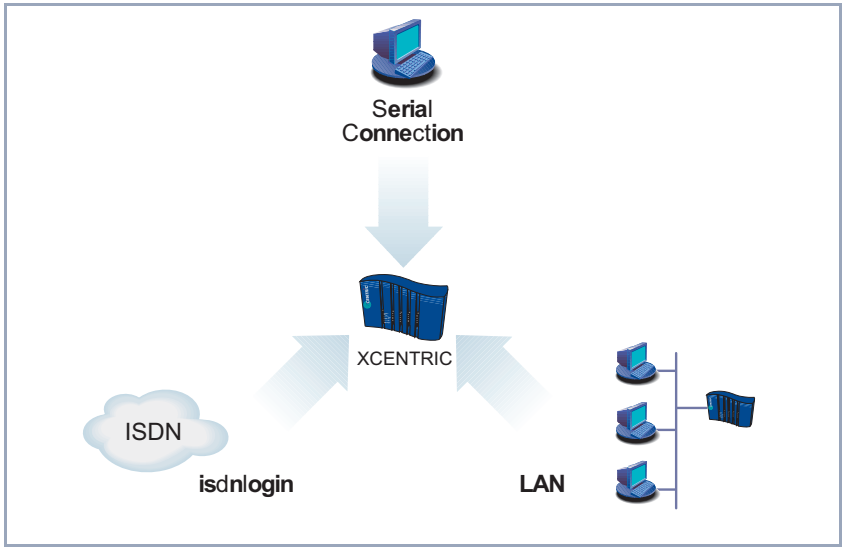


Figure 8-1: Possible connections to **XCENTRIC**

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 **XCENTRIC** over the LAN. If you use the Configuration Wizard, you connect to **XCENTRIC** over the serial interface.

8.1.1 Connecting Over the Serial Interface

Initial configuration

A serial interface connection is the most appropriate method if you are configuring your **XCENTRIC** for the first time. To connect **XCENTRIC** to your computer over the serial interface, connect the serial interface on the basic unit of **XCENTRIC** to the serial interface of your computer.

Windows

If you use a Windows PC, you need a terminal program for the serial connection, e.g. **HyperTerminal**. How to install this assistant and **BRICKware for Windows** is described in chapter 8.3, page 140.

- Click the Windows Start button and then **Programs** ➧ **BRICKware** ➧ **BRICK at COM1** (or **BRICK 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 **XCENTRIC.**
- Continue with chapter 8.1.4, page 127.

If the login prompt does not appear after pressing **Return** several times, the connection to **XCENTRIC** 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 **XCENTRIC** and set up the connection again.

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

Unix If you are using a Unix PC, you 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.

8.1.2 Connecting Over a LAN

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

- If you are working with Windows, you can assign **XCENTRIC** 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 8.3, page 140.
- If you are not working with Windows, use an alternative connection method for initial configuration (over the serial interface or ISDN).

➤ Connect **XCENTRIC** to the LAN.

Assigning IP addresses

To assign your **XCENTRIC** 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.

The BootP server window will appear after a short time if **XCENTRIC** is still unconfigured.

➤ Enter the name and IP address of your **XCENTRIC** in the window under **BRICK Parameter**.

➤ Click **OK**.

➤ Close **DIME Tools**.

Running telnet

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

Windows

➤ Click the Windows Start button and then **Run**....

➤ Type `telnet <IP address of XCENTRIC>`.

➤ Click **OK**.

A window with the login prompt appears. You are now in the SNMP shell of **XCENTRIC**. Continue with chapter 8.1.4, page 127.

Unix

➤ Type `telnet <IP address of XCENTRIC>` in a terminal.

A window with the login prompt appears. You are now in the SNMP shell of **XCENTRIC**. Continue with chapter 8.1.4, page 127.

Configuration Manager

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

8.1.3 Connection Over ISDN

Remote configuration

Connecting over ➤➤ **ISDN** with ➤➤ **ISDN login** is particularly useful when **XCENTRIC** is situated at a different location and you want to configure and administrate it from a distance. This is also possible even if **XCENTRIC** has not been initially configured, i.e. is still in the ex works state. You must, however, have an already configured BinTec router at your disposal in the remote LAN and know the telephone number of **XCENTRIC** in your own LAN. It is thus possible for the administrator of a head office to configure **XCENTRIC** in a home office which is hundreds of kilometers away. The **XCENTRIC** in the branch office merely has to be connected to an ISDN outlet and turned on.

If your equipment, e.g. **XCENTRIC** with built-in XFM-Fax module, is equipped with modem hardware, dialing in over a modem using a terminal program is also possible with the command `atd <telephone number of XCENTRIC>`. This dialing-in is not possible until access for ISDN login has been configured on **XCENTRIC**. To do this, the extension for ISDN login must be configured with **Type** *voice*. The default setting is *data*. See chapter 11.5.4, page 255.

You can also dial into **XCENTRIC** using an ISDN card.

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

➤ Connect **XCENTRIC** to the ISDN.

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

- Log in to your BinTec router in the remote LAN in the usual way.
- Type in `isdnlogin <telephone number of ISDN login of your` **XCENTRIC**> in the SNMP shell.

  The login prompt will appear in the window. You are now in the SNMP shell of **XCENTRIC**. Continue with chapter 8.1.4, page 127.

8.1.4 Logging In

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

In order to log in, you need to know the user name and password. In its ex works state, **XCENTRIC** 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 **XCENTRIC** is turned off).
`read`	public	Read system variables.
`http`	bintec	Call up HTTP status page and Java status monitor from **XCENTRIC**, read system variables, no login.

Table 8-1: 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

XCENTRIC 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. `xcentric:>`. The login was successful.

Caution!

To prevent unauthorized access to **XCENTRIC**, you should change the passwords right away. How to change the passwords is described in "Changing the password", page 135.

- Change the passwords.

Closing the SNMP shell

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

8.2 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 mainly describes the configuration of **XCENTRIC** using the Setup Tool.

8.2.1 Overview

Methods of configuring **XCENTRIC**:

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

Configuration Wizard

You will learn about configuration using the Configuration Wizard in chapter 9.1, page 142. It is useful for quick, initial configuration of **XCENTRIC** and can be used if you have a Windows PC. This usually covers most standard configurations of **XCENTRIC**. If you need further settings, you can use the other configuration options mentioned above. You could first configure **XCENTRIC** with the Configuration Wizard and subsequently extend or change this initial configuration with one of the other tools.

Configuration Manager

The Configuration Manager is a Windows application provided by BinTec Communications AG that contains an SNMP Manager.

The Configuration Manager contains a Windows-based SNMP Manager for configuration of **XCENTRIC** and offers you a clear overview of the configuration of the PABX part (extension numbers) of **XCENTRIC**.

Setup Tool

The Setup Tool is a menu-driven tool for the configuration and administration of **XCENTRIC**. 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. This manual mainly describes using the Setup Tool for configuration. The Setup Tool is independent of the operating system on your PC.

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 (a reference to the PABX MIB tables can be found in chapter 11.15, page 326).

Other SNMP managers

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 **XCENTRIC** 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.

8.2.2 Using the Setup Tool

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

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

Main menu

The main menu of the Setup Tool appears:

```
XCENTRIC Setup Tool                          BinTec Communications AG
                                                          MyXcentric

Licenses                System

Slot1:          CM-100BT, Fast Ethernet          Slot4:

Slot2:          XCM-5S0, ISDN 5S0                Slot5:

Slot3:          XCM-S04AB, 1xISDN 4xAB

WAN Partner
IP      IPX     PPP     PABX    ISDN    LCR

Configuration Management
Monitoring and Debugging
Exit

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

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 8.1.4, page 127).

The Setup Tool is easy to use. After a few minutes, you will have no problem finding 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 **XCENTRIC** Setup Tool.

Menu layout

Every Setup Tool menu consists of three parts:

Figure 8-2: 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 **XCENTRIC** 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 "∨" indicates more to come.
Ctrl - **b**	To scroll back a page in a long list. An "=" sign at the top right indicates the start of the list or a "∧" indicates more to come.
Ctrl - **c**	Leave the Setup Tool.

Table 8-2: 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 8-3: Buttons in the Setup Tool

Searching lists

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

```
XCENTRIC Setup Tool                              BinTec Communications AG
[WAN]: WAN Partners                                            MyXcentric

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 alphabetic or numeric 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**.

Changing the password

The procedure described below for changing the password applies to all **XCENTRIC** passwords: the access passwords for the user names `admin`, `read` and `write`, the HTTP password, the RADIUS password, the PPP password, the provider password, the PABX user passwords and PINS, the TAPIadmin password and the CAPIadmin 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 **XCENTRIC** 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 **XCENTRIC** 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 the **Return**, **Tabulator** or **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.

Menu structure The menu structure of the Setup Tool looks like this:

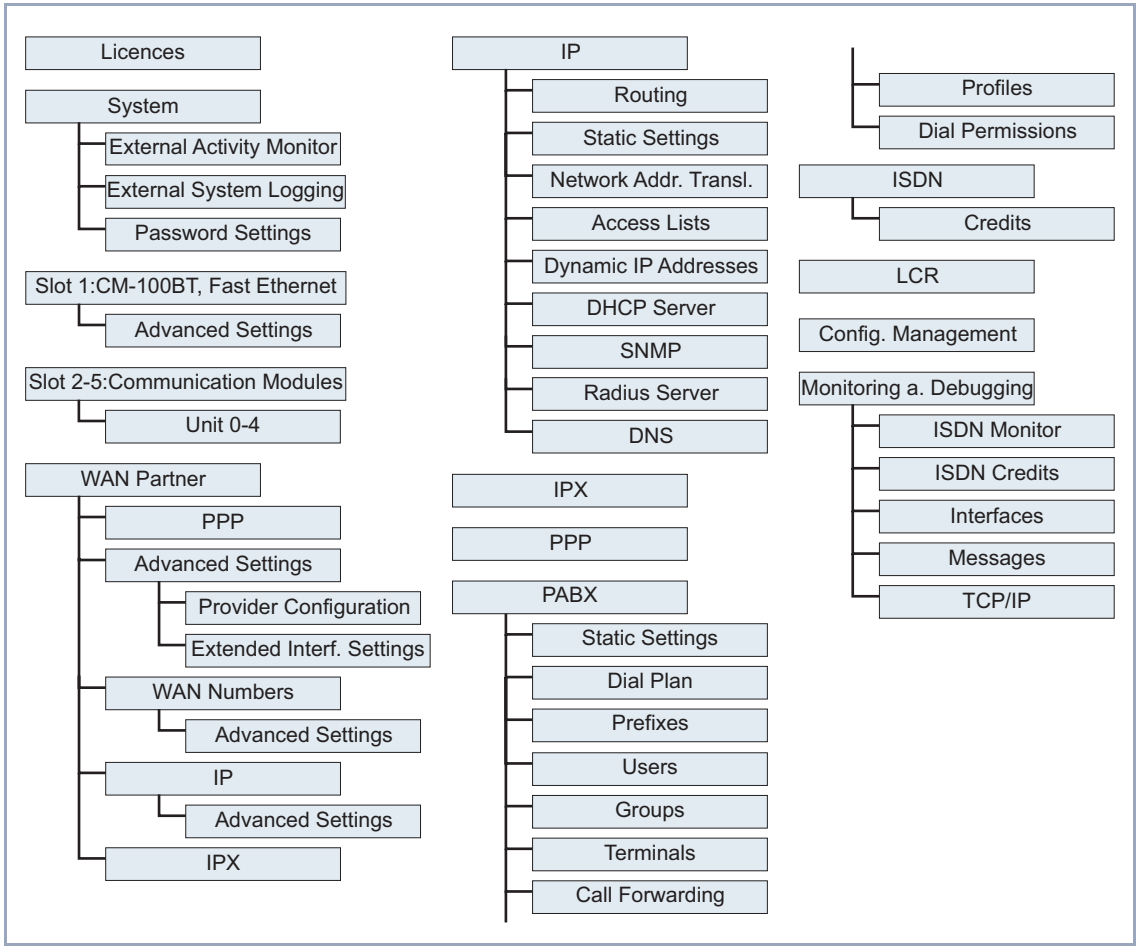


Figure 8-3: Setup Tool menu structure

figure 8-3, page 136 shows all the menus of the Setup Tool available as standard on **XCENTRIC**. When you activate your license, **XCENTRIC** recognizes this and displays the corresponding menus.

Summary To help you find your way around during configuration, the menus are briefly explained below.

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 **XCENTRIC** , e.g. system name and passwords.
SLOT 1: CM-100BT, FAST ETHERNET	This menu is for configuring the ➤➤ **LAN** interface of **XCENTRIC**. Here you enter data such as the IP address and netmask of **XCENTRIC**.
SLOT 2 -5:	In this menu you configure the external and internal S_0 interfaces and a/b interfaces of **XCENTRIC**'s communication modules. These slots contain the XCM-5S0 or XCM-S04AB modules, depending on the hardware installation.
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	Here you enter the settings for the ➤➤ **IP** protocol. This menu consists of several submenus: ***IP*** ➧ ***ROUTING*** includes **XCENTRIC**'s IP routing table. Here you enter routes to your partners (e.g. default routes, network routes), which ensure that your **XCENTRIC** sends all the ➤➤ **data packets** to the correct addresses. ***IP*** ➧ ***STATIC SETTINGS*** is for entering important settings, e.g. the domain name of **XCENTRIC**, the IP addresses of additional ➤➤ **servers** (e.g. Domain Name Server) and system time specifications. ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** is for configuring the interfaces to the partners for which you want to use the Network Address Translation function (➤➤ **NAT**). ***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 **XCENTRIC** from establishing unintended connections to the ISDN. ***IP*** ➧ ***DYNAMIC IP ADDRESSES*** is for setting up a pool of IP addresses that your **XCENTRIC** as a dynamic IP address server can assign to WAN partners, who can then dial in. ***IP*** ➧ ***DHCP SERVER*** is for configuring **XCENTRIC** as a ➤➤ **DHCP** server. As a DHCP server, **XCENTRIC** assigns the IP addresses to the hosts in the LAN dynamically. ***IP*** ➧ ***SNMP*** is for changing the basic ➤➤ **SNMP** settings. ***IP*** ➧ ***RADIUS SERVER*** is used for defining the settings for the Radius Server. ***IP*** ➧ ***DNS*** is for defining the procedure for name resolution in **XCENTRIC**.
IPX	Here you make the entries for the IPX protocol. ➤➤ **IPX** is used especially in Novell networks.

Menu	Function
PPP	Includes generally valid ➤➤ **PPP** settings, e.g. authentication protocol, that do not just refer to particular WAN partners. With these settings, the router can perform an authentication procedure for incoming calls, even if the calling line number cannot be identified (e.g. because the call is made from an analog line that does not transfer the calling line number).
PABX	This menu is for configuring the PABX part of **XCENTRIC**. You can define users and groups and assign extension numbers to the subsystems of **XCENTRIC**. You can also define the static PABX functionality.
ISDN	Here you administrate **XCENTRIC**'s Credits Based Accounting System.
LCR	This menu is used for configuring **XCENTRIC**'s LCR function (Least Cost Routing).
CONFIGURATION MANAGEMENT	Here you can administrate **XCENTRIC**'s configuration files. You can save them either locally on **XCENTRIC** or on your PC, for example.
MONITORING AND DEBUGGING	Includes submenus that enable you to locate problems in your network and monitor activities, e.g. at **XCENTRIC**'s WAN interface.
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 **XCENTRIC** is restarted. If you use **Exit** ➧ **Exit without saving**, the changes made in this Setup Tool session are lost the next time **XCENTRIC** is restarted. The configuration file is not saved in the flash memory.

Table 8-4: Setup Tool menus

8.3 Installing BRICKware

BRICKware for Windows is BinTec's Windows software for configuring **XCENTRIC** with a PC (Configuration Wizard and Configuration Manager). It also contains configuration programs for the Remote CAPI and Remote TAPI, which you may need on the PCs in your LAN.

To do For installing BRICKware:

- Close all Windows programs on your PC.
- Place your BinTec Companion CD in the CD-ROM drive of your PC. The Start window appears automatically after a short time. If the Start window does not open automatically, click your CD-ROM drive in Windows Explorer and double-click **setup.exe**.
- Click **BRICKware**. The setup program starts.
- Specify the directory in which BRICKware should be installed.
- Select your equipment.
- Select the software components you wish to install. Simply choose from the preset list.

The DIME Tools contain mainly assistants for configuration, maintenance and diagnosis of **XCENTRIC**. For the basic router function, it is not necessary to have DIME Tools started automatically by Windows. The Configuration Wizard starts after the installation.

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

9 Quick Configuration with the Configuration Wizard

The Configuration Wizard, which is part of BRICKware for Windows, offers a quick, convenient way to configure your **XCENTRIC** from a PC connected over a serial interface.

You can use the Configuration Wizard to create a basic configuration for **XCENTRIC**.

We recommend that you carry out the basic configuration of **XCENTRIC** with the Configuration Wizard and then make any necessary changes with the Setup Tool.

You will find descriptions of configuration with the Setup Tool in chapter 10, page 149 onwards.

9.1 Basic Configuration with the Configuration Wizard

With the Configuration Wizard included on your BinTec Companion CD, BinTec Communications AG offers you a quick and convenient way to start running your **XCENTRIC**. You can create a basic configuration via the serial interface of your Windows PC. This basic configuration includes all the important settings for **XCENTRIC**, access to the Internet via an Internet Service Provider (ISP), and connection to a WAN partner (e.g. a corporate headquarters). As the Configuration Wizard guides you step by step through the configuration, detailed knowledge of networking technologies is not necessary. Graphic illustrations and a detailed online help system you can access at any time during the configuration give you additional support.

The Configuration Wizard is one of several possible ways of configuring your **XCENTRIC**. Access to your **XCENTRIC** in this case is via the serial interface.

Other access possibilities are described in chapter 8.1, page 122. Additional configuration methods for fine tuning your configuration can be found in chapter 8.2, page 129.

Your system must meet the following requirements:

- Windows 95/98 or Windows NT 4.0
- Network card installed (Ethernet)
- Microsoft TCP/IP protocol installed (see chapter 9.1.1, page 142)
- High-color monitor (more than 256 colors) for correct display of graphics.

9.1.1 In Advance of Configuration

Basic settings

Before you start to configure your **XCENTRIC**, make sure you have the following information about your ISDN connections, network environment, telephones connected and users. A detailed description of the modules equipped in **XCENTRIC** is also necessary.

A list of all the information you will need in the course of basic configuration of **XCENTRIC** with the Configuration Wizard is given below. We recommend that you collect the necessary data in a clearly arranged form so that this is readily available during installation work.

The following data are required:

- IP address
  If you have an existing network, ask your system administrator for the IP address and netmask of your **XCENTRIC**. If you are configuring a new network, you can use the example values (192.168.1.254 for the IP address and 255.255.255.0 for the netmask).

- Detailed description of modules
  You need information about which communication module (XCM-5S0 or XCM-S04AB) is installed in each slot of **XCENTRIC**. For the XCM-5S0 module, you must also know which units are configured as external and which as internal (see chapter 6.7.1, page 83). For the external units on XCM-5S0 and the external unit 0 on XCM-S04AB, you must indicate if the connections are to a point-to-multipoint or point-to-point connection.

- Information about your ISDN connections
  For a point-to-multipoint connection, you need the individual MSNs assigned to you. For point-to-point connections, you need the main number and the extension numbers range assigned to you.

- External line access
  You must decide if you want to configure automatic external line access or external line access by dialing an exchange number as prefix.

- Users
  You need a list of all users in your network that are to use CAPI or TAPI services. A user name, a password and permission to use the CAPI and/or TAPI must be created for each user. See chapter 12.1, page 328.

- Extension numbers
  The Configuration Wizard configures one or no terminal (telephone) for each ab unit (XCM-S04AB) and one, two or no terminals (telephones) for each internal S0 unit (XCM-5S0) configured in accordance with the inputs. You can use a standard configuration from the Configuration Wizard for the

extension numbers.
If you want to configure your own extension numbers, you need a detailed list showing the terminal and subsystem to which each extension number is to be assigned. In this case, the users must be explicitly assigned to the terminals and CAPI in the Configuration Wizard.

Internet access

For access to the Internet via your Internet Service Provider (ISP), e.g. T-Online, you will need access information that should be provided by your ISP (different ISPs may use different terminology).

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

Some ISPs, e.g. T-Online, need additional information, such as the T-Online number and joint user account.

Corporate network connection (LAN-LAN)

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

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

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

Checking and installing TCP/IP protocol

The TCP/IP protocol is the "language" PCs use to communicate over the network and to connect to the Internet. Make sure the TCP/IP protocol is installed before you start the configuration. To check if the TCP/IP protocol is already installed or to install it now, proceed as follows:

- Click **Settings** ➧ **Control Panel** in the Start menu. Double click **Network**.
- Windows 95/98: Look for **TCP/IP** in the list of network components.
- For Windows NT: Select the **Protocols** tab. Search in the network protocols list for **TCP/IP protocol**.
- If you can't find the entry, install the TCP/IP protocol as explained below. Otherwise, close the dialog box and start configuration.

To install the TCP/IP protocol:

- Windows 95/98: Click **Add** in the **Network** dialog box. Select **Protocol** in the list of network components. Click **Add**. Select **Microsoft** as manufacturer and **TCP/IP** as network protocol. Click **OK**. In an existing network, you might have to configure additional settings here. Ask your system administrator. If you are setting up a new network, click **OK**. Your PC is now configured as a DHCP client.
- For 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**. Click **Yes** to set up a new network (PC as DHCP client). In an existing network, ask your system administrator.
- Follow the instructions on the screen and finally restart your PC. Repeat the installation on all PCs with which you need to access the Internet or corporate network.

9.1.2 XCENTRIC Configuration

Configuration of the basic settings of **XCENTRIC** is quick and easy with the Configuration Wizard. Please note: If you have already created a configuration with the Configuration Wizard, the Wizard can use the preset values. At the end, the configuration is transferred to **XCENTRIC** and also saved on the PC.

You can carry out the configuration in either Quick Mode or Expert Mode. If you are unfamiliar with networking technologies, choose Quick Mode.

You can select from the following configuration items: basic configuration, Internet access and corporate network connection (LAN-LAN connection). The basic configuration is essential. It integrates **XCENTRIC** in your local network.

- Select the desired items and follow the instructions on the screen.
- If you have set up a new network and installed the TCP/IP protocol on the PC as described above, configure your router as a DHCP server.

In this case, the PC must be assigned an IP address over DHCP at the end of configuration. This happens automatically under Windows NT. Under Windows 95 or 98, the Configuration Wizard starts the program WINIPCFG:

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

At the end of configuration with the Configuration Wizard, the CAPI/TAPI configuration on your PC is started automatically. You will find a description of configuration of Remote CAPI and TAPI in chapter 12.1.2, page 329.

9.1.3 Status of XCENTRIC Configuration

After you have run through the Configuration Wizard, you have created a basic configuration for **XCENTRIC**. This configuration is based on the settings you selected. Both the router part and PABX part have been configured. Details on configuring the PABX part with the Configuration Wizard can be found in chapter 11.2, page 211.

Depending on whether you have configured an Internet access or a corporate network connection with the Configuration Wizard, you have created one or two WAN partners with the relevant selected settings.

Carry out any necessary changes to the configuration with the Setup Tool. You will find descriptions of configuration with the Setup Tool in chapter 10, page 149 onwards.

9.2 Configuration Manager

The Configuration Manager contains a Windows-based SNMP manager and also offers you a facility for conveniently viewing and setting up the configuration of the extension numbers (PABX configuration). The Configuration Manager cannot be used for all parts of the PABX configuration.

The parts of the PABX that cannot be configured with the Configuration Manager can be configured with the Setup Tool. See also chapter 11, page 207.

We recommend you use the Configuration Wizard for initial basic configuration of the PABX. See also chapter 9, page 141.

The Configuration Wizard and Configuration Manager are parts of **BinTec**'s BRICKware for Windows, which you will find on your ISDN Companion CD. The latest version of BRICKware for Windows can be downloaded at any time from **BinTec**'s web server at www.bintec.net.

10 Basic Configuration of Router with Setup Tool

The basic configuration of the router part of **XCENTRIC** with the ➤➤ **Setup Tool** covers the same settings as configuration with the Configuration Wizard in chapter 9.1, page 142. However, the Setup Tool is independent of the operating system and also enables you to make additional settings.

The Configuration Wizard also creates the configuration for the PABX part of **XCENTRIC,** in its basic configuration. A description of this using the Setup Tool can be found in chapter 11, page 207. The Configuration Wizard for **XCENTRIC** can also be used to configure the DNS Proxy function for the router part if no DNS server is available in the local LAN. A description of the DNS Proxy function can be found in chapter 14.3.2, page 380.

This basic router configuration includes all the steps necessary on **XCENTRIC** for the operation of the router part. The configuration of the external ISDN interfaces that connect **XCENTRIC** to the ISDN is part of the PABX configuration (see chapter 11, page 207).

Basic router configuration

The basic router configuration of **XCENTRIC** includes:

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

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

Existing configuration extension

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 setup **XCENTRIC** 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 14, page 347.

How to configure security mechanisms according to SAFERNET is explained in chapter 15, page 415.

10.1 Basic Router Settings

The configuration of the basic settings for the router part concerns only your **XCENTRIC** and your local network. figure 10-1, page 151 contains examples of names, ➤➤ **IP addresses**, extensions, etc. If you are setting up a new Local Area Network (LAN) together with **XCENTRIC** 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. You can, of course, use any other relevant values you may have.

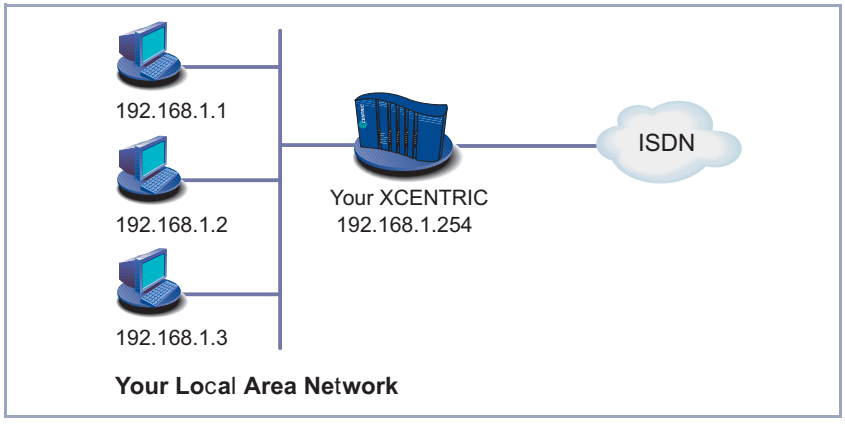


Figure 10-1: Basic router settings

The following steps are necessary:

- Entering your license
- Entering system data (e.g. passwords)
- Configuring the LAN Interface
- Configuring **XCENTRIC** as a DHCP ➤➤ **server** (optional)
- Setting ➤➤ **filters** (optional, explained in detail in chapter 15.2, page 435)

Off we go!

10.1.1 Entering a License

License card

After you have logged in to your **XCENTRIC** with the user name `admin` and called up the Setup Tool with `setup`, as described in chapter 8.1.4, page 127, enter the license information. This information is printed on the license card supplied. Entering this information activates the functions of **XCENTRIC**.

➤ Go to ***LICENSES***.

You see the following menu:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[LICENSE]: Licenses                                              MyXcentric


Available Licenses:

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

Serialnumber         Mask         Key          State
12345                55           ABCDEFG      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 to **XCENTRIC**, as well as their current state (*builtin* - always available, *valid* - activated, *not_valid* - not activated).

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

If you have not yet entered your license data, the subsystem list will be almost empty. Only **IP**, i.e. ➤➤ **IP** routing, and ➤➤ **TAPI** are available (*builtin*).

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

Subsystems	Meaning
IP	IP routing
STAC	➤➤ **STAC** ➤➤ **data compression**
CAPI	➤➤ **Remote CAPI** interface, permits communications applications on your PC, e.g. sending and receiving faxes.
BRIDGE	Bridging
IPX	➤➤ **IPX** routing
TAPI	Remote ➤➤ **TAPI** interface permits telephony applications (CTI) on your PC.

Table 10-1: 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. Your license has been entered and its current state *ok* is displayed.

If *not ok* is shown as the state, you have probably made a typing error.

- ➤ Try again.

10.1.2 Entering System Data

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

➤ Go to ***SYSTEM***.

You see the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[SYSTEM]: Change System Parameters                          MyXcentric

System Name                                 MyXcentric
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>
Password Settings>

            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 **XCENTRIC**, is also used as PPP host name. Appears as input prompt when logging in to **XCENTRIC**. If no system name is set, a warning appears on logging in with the user name `admin`.
Local PPP ID	This entry is necessary for identification of **XCENTRIC**, if ➤➤ **PPP authentication** (e.g. ➤➤ **PAP** or ➤➤ **CHAP**) is carried out that is not specific to a partner (see chapter 14.1.2, page 350).
Location	Indicates where **XCENTRIC** is located (optional).
Contact	States the contact person responsible (optional). If the person is to be reached from **XCENTRIC**'s HTTP status page, a valid e-mail address must be entered here.

Table 10-2: ***SYSTEM***

Passwords

Enter the passwords for **XCENTRIC** in the submenu ***SYSTEM*** ➧ ***PASSWORD SETTINGS***:

Field	Meaning
admin Login Password	Password for user name admin.
read Login Password	Password for user name read.
write Login Password	Password for user name write.
HTTP Server Password	Password for the HTTP status page of **XCENTRIC**.

Table 10-3: ***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 135.

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

The permission rights of the possible user names and passwords can be found in chapter 8.1.4, page 127.

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

➤ Enter **System Name** of **XCENTRIC**, e.g. ***MyXcentric***.

➤ 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.

10.1.3 Configuring the LAN Interface

➤➤ IP address,
➤➤ netmask,
➤➤ encapsulation

The next step is to configure **XCENTRIC**'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 as part of the LAN by other hosts.

You may have already assigned your **XCENTRIC** 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***.

You see the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[LAN]: Configure Ethernet Interface                          MyXcentric

IP Configuration
Local IP Number          192.168.1.254
Local Netmask            255.255.255.0
Encapsulation            Ethernet II

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

If you wish to use the IPX ➤➤ **protocol**, you will find an explanation of how to configure the LAN interface for IPX in chapter 14.5, page 405.

Information on bridging can be found in chapter 14.6, page 412.

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

Field	Meaning
Local IP Number	IP address of **XCENTRIC** in the LAN.
Local Netmask	Netmask of the network where **XCENTRIC** is located.
Encapsulation	Defines the kind of header added to the IP packets that run over this LAN interface. Possible values: ■ *Ethernet II* (conforms to IEEE 802.3) ■ *Ethernet SNAP* You can generally retain the preset value *Ethernet II*. The LAN interface is called en1 for *Ethernet II* and en1-snap for *Ethernet SNAP*.

Table 10-4: ***CM-100BT, FAST ETHERNET***

To do

Proceed as follows to configure **XCENTRIC**'s LAN interface:

➤ Enter **Local IP Number** of **XCENTRIC**, e.g. ***192.168.1.254***.

➤ Enter **Local Netmask**, e.g. ***255.255.255.0***.

➤ Select **Encapsulation**, e.g. ***Ethernet II***.

➤ Press **SAVE**.

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

10.1.4 Configuring XCENTRIC as DHCP Server

IP addresses in the LAN

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

XCENTRIC 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*** ➧ ***DHCP SERVER*** ➧ **ADD**.

You see the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[IP][DHCP][ADD]: Add Range of IP Addresses                  MyXcentric


    Interface                              en1
    IP Address                             192.168.1.1
    Number of Consecutive Addresses        8
    Lease Time (Minutes)                   120
    MAC Address

    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**.
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 *not specified*. A detailed description of this function is given in the Software Reference.

Table 10-5: ***IP*** ➧ ***DHCP SERVER*** ➧ **ADD**

To do Make the following entries to configure **XCENTRIC** 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.

➤ Select **NetBT Node Type**, e.g. *not specified*.

➤ Press **SAVE**.

You have returned to ***IP*** ➧ ***DHCP SERVER***, 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.

10.1.5 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 **XCENTRIC** setting up connections, e.g. to the Internet Service Provider (➤➤ **ISP**), in order to forward WINS requests from PCs in your network. That is, **XCENTRIC** 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 15.2, page 435.

To prevent these unnecessary connections, proceed as follows:

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

➤ Use the serial interface or isdnlogin on **XCENTRIC** for filter configuration.

➤ If you still decide to access telnet on **XCENTRIC**, select ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES*** ➧ ***EDIT*** **First Rule**: *none*.

➤ Go to ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER*** ➧ **ADD**.

You see the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[IP][ACCESS][FILTER][ADD]: Configure IP Access Filter       MyXcentric

    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**.

You see the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[IP][ACCESS][RULE][ADD]: Configure IP Access Rules          MyXcentric


    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.

The settings are listed:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[IP][ACCESS][RULE]: Configure IP Access Rules                MyXcentric

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***.

You see the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[IP][ACCESS][INTERFACES]: Configure First Rule               MyXcentric

    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 **XCENTRIC** (*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 **XCENTRIC** is switched off (chapter 10.3, page 205).

10.2 XCENTRIC and the WAN

If you have carried out the configuration steps in chapter 10.1, page 151, **XCENTRIC** 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 **XCENTRIC** to make connections to networks outside your LAN, you must configure the desired connection partners as WAN partners on your **XCENTRIC**. This applies to outgoing connections (**XCENTRIC** dials its WAN partner), as well as to incoming connections (a WAN partner dials the number of your **XCENTRIC**). 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 set up a WAN partner on your **XCENTRIC** is explained in general terms in chapter 10.2.1, page 167.

- 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 10.2.2, page 191. Here you will find a quick procedure if you want to access the Internet with **XCENTRIC** via one of the following providers:
  – T-Online
  – Compuserve

- Example of configuring a WAN partner for a corporate network connection:
  You will find an example of how to establish a corporate network connection with your **XCENTRIC** in chapter 10.2.3, page 197. This quick procedure should be sufficient in most cases.

A basic scenario is illustrated in figure 10-2, page 167, which gives an idea of what connections to the WAN partners, ISP and head office could look like.

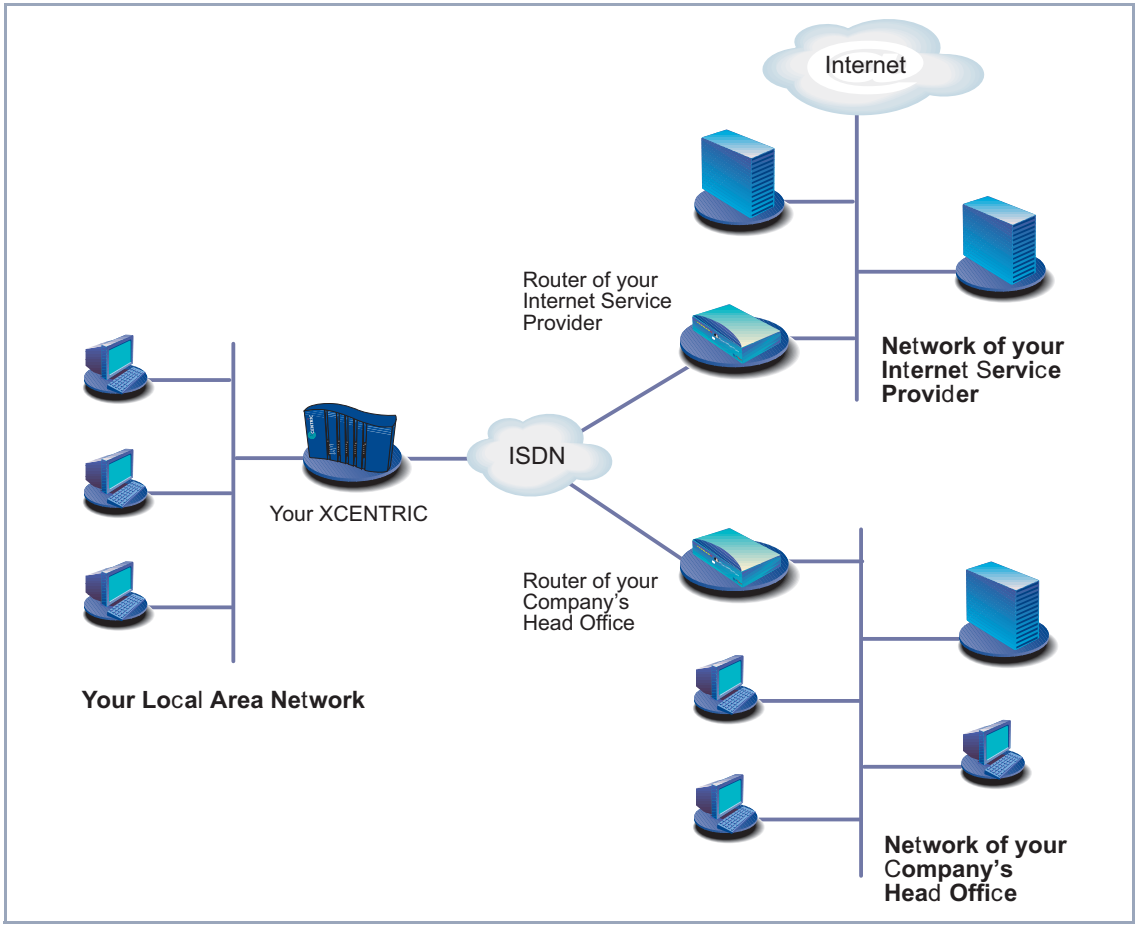


Figure 10-2: Basic scenario

10.2.1 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

WAN partner configuration

Here you are going to establish 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 9.1.1, page 142). The terms used may vary slightly from provider to provider.

To enter a WAN partner, proceed as follows:

➤ Go to ***WAN PARTNER***.

You see the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[WAN]: WAN Partners                                        MyXcentric

Current WAN Partner Configuration

    Partnername              Protocol        State
    BigBoss                  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**. **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 14.2.1, page 353).
- *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:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[WAN][ADD]: Configure WAN Partner                            MyXcentric

    Partner Name                 BigBoss

    Encapsulation                PPP
    Compression                  none
    Encryption                   none
    Calling Line Identification  no

    WAN Numbers >
    PPP >
    Advanced settings >

    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	➤➤ **Encapsulation**. Defines how the ➤➤ **data packets** are encapsulated for transfer to the WAN partner. Possible values: ■ *PPP* ■ *Multi-Protocol LAPB Framing* ■ *Multi-Protocol HDLC Framing* ■ *Async PPP over X.75* ■ *Async PPP over X.75/T.70/BTX* ■ *X.25_PPP:* not available on **XCENTRIC** ■ *X.25:* not available on **XCENTRIC** ■ *HDLC Framing (IP only)* ■ *LAPB Framing (IP only)* ■ *X31 B-Channel:* not available on **XCENTRIC** ■ *X.25 No Signalling:* not available on **XCENTRIC** ■ *X.25 PAD:* not available on **XCENTRIC** ■ *X.25 No Configuration:* not available on **XCENTRIC** ■ *Frame Relay:* not available on **XCENTRIC** ■ *X.25 No Configuration, No Signalling:* not available on **XCENTRIC**

Field	Meaning
Compression	Defines the type of compression that should be used for data traffic to the WAN partner. Possible values: ■ *STAC:* only if **Encapsulation** = *PPP* ■ *MS-STAC:* only if **Encapsulation** = *PPP* ■ *MPPC:* not available on **XCENTRIC** ■ *V.42bis:* only if **Encapsulation** = *Multi-Protocol LAPB Framing* or *LAPB Framing (IP only)* ■ *none*
Encryption	Defines the type of encryption that should be used for data traffic to the WAN partner. Only possible if STAC compression is not activated for the connection. Possible values: ■ *MPPE 40:* only if **Encapsulation** = *PPP* ■ *MPPE 128:* only if **Encapsulation** = *PPP* and **Authentication** = *MS-CHAP* ■ *none*
Calling Line Identification	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.

Table 10-6: ***WAN PARTNER*** ➧ **ADD**

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

Protocols		Encapsulation	Compression	
IP	IPX		STAC, MS-STAC	V.42bis
X	X	*PPP*	X	
X	X	*Async PPP over X.75*	X	
X	X	*Async PPP over X.75/T.70/BTX*	X	
X	X	*Multi-Protocol LAPB Framing*		X
X	X	*Multi-Protocol HDLC Framing*		
X		*HDLC Framing (IP only)*		
X		*LAPB Framing (IP only)*		X

Table 10-7: 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 ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS***.

Entering extensions

You see the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[WAN][ADD][WAN Numbers]: WAN Numbers (BigBoss)              MyXcentric


    WAN Numbers for this partner:

        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:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[WAN][ADD][WAN NUMBERS][ADD]:Add or Change WAN Numbers(BigB MyXcentric


    Number                   0911987654321
    Direction                outgoing

    Advanced settings >



            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 10-8: ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS*** ➧ **ADD**

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

Possible Values	Meaning
outgoing	For outgoing calls, where you dial your WAN partner.
both (CLID)	For incoming and outgoing calls.
incoming (CLID)	For incoming calls, where your WAN partner dials in to your **XCENTRIC**.

Table 10-9: **Direction**

If the prefix "0" must be dialed for external line access on **XCENTRIC**'s PABX, you must include this "0" when entering the extension.

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	XCENTRIC accepts incoming calls, e.g. with:	Outgoing calls, i.e. XCENTRIC 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 10-10: 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 **XCENTRIC** 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 **XCENTRIC** matches the caller's data.

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

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

You see the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[WAN][ADD][PPP]: PPP Settings (BigBoss)                      MyXcentric


    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	**XCENTRIC**'s ID
PPP Password	Password
Keepalives	Activates keepalive packets.
Link Quality Monitoring	PPP Link Quality Monitoring acc. to RFC 1989

Table 10-11: ***WAN PARTNER*** ➧ **ADD** ➧ ***PPP***

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

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

Table 10-12: **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 135.

- 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 **XCENTRIC** does not know which authentication protocol was set for this WAN partner. To enable the call to still be accepted, **XCENTRIC** falls back on general settings in the PPP, which you can change as necessary (chapter 14.1.2, page 350).

Defining short hold

Now set short hold so that **XCENTRIC** 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 **XCENTRIC** 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. Ask your telephone company.

When using dynamic Short Hold, you must also set static Short Hold so that you do not get a permanent ➤➤ **switched connection** if AOCD fails.

You should make sure static Short Hold comes into operation later than dynamic Short Hold. If not, **XCENTRIC** 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.

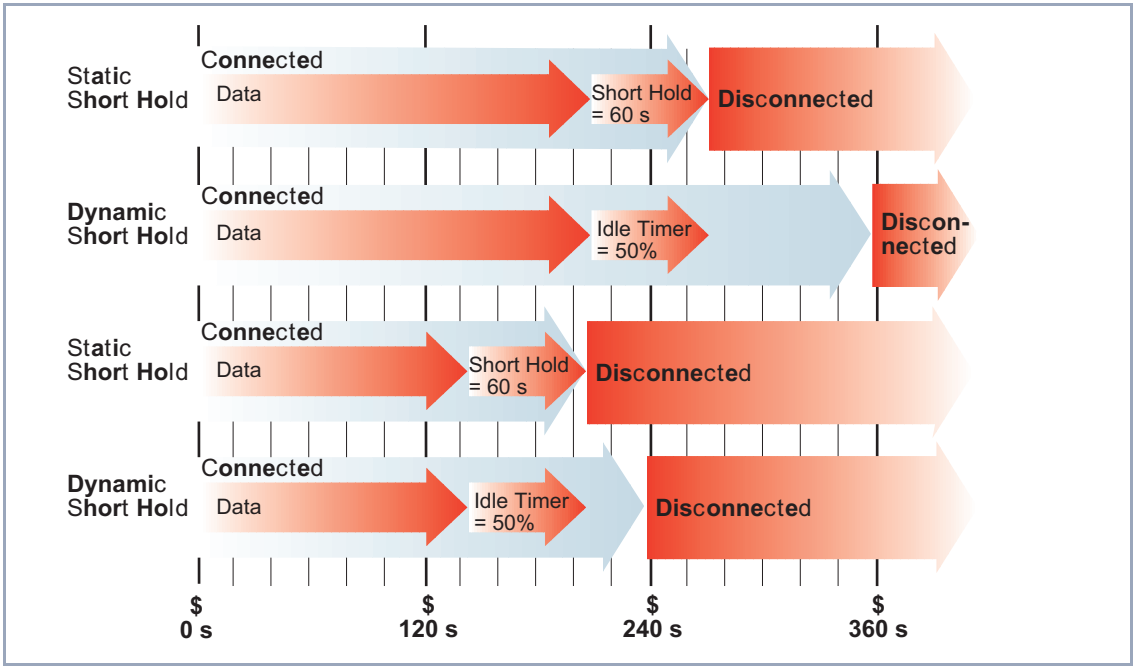


Figure 10-3: Dynamic and static short hold

Proceed as follows:

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

You see the following menu:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[WAN][ADD][ADVANCED]: Advanced Settings (BigBoss)              MyXcentric

Callback                                 no
Static Short Hold (sec)                  20
Idle for Dynamic Short Hold (%)          0
Delay after Connection Failure (sec)     300

Extended Interface Settings (optional) >

Channel Bundling                         no

Layer 1 Protocol                         ISDN 64 kbps


                  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: *60*, only effective if charging pulses are transmitted during the connection (AOCD), *20* otherwise.
Idle for Dynamic Short Hold (%)	Idle time in % for dynamic Short Hold. Only effective if charging pulses are transmitted during the connection (AOCD).

Table 10-13: ***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 transfer has been completed.

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***.

You see the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[WAN][ADD][IP]: IP Configuration (BigBoss)                  MyXcentric


    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 **XCENTRIC** sets up a transit network to the WAN partner.
Local IP Address	IP address of **XCENTRIC**. 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 14.2.5, page 362).
Local ISDN IP Address	ISDN IP address of **XCENTRIC** 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	WAN partner's LAN netmask. If you make no entry, **XCENTRIC** enters a default netmask for the net class used under **Partner's LAN IP Address**.

Table 10-14: ***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 **XCENTRIC** 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***:* **XCENTRIC**'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 **XCENTRIC**'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 14.2.5, page 362.

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

Routing entry creation

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

You see the following menu window:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[IP][ROUTING]: IP Routing                                      MyXcentric

The flags are:  U (Up), D (Dormant), B (Blocked),
                G (Gateway Route), I (Interface Route)
                S (Subnet Route), H (Host 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             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). The protocol with which **XCENTRIC** 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.

Another menu window opens:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[IP][ROUTING][ADD]: IP Routing                                 MyXcentric


    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: ■ *Host route:* Route to a single host ■ *Network route:* Route to a network ■ *Default route:* 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** = *Network route*. If no entry is made, the router uses a default netmask).
Partner / Interface	WAN partner (only possible for **Network** = *WAN without transit network*).
Gateway IP Address	IP address of the host to which **XCENTRIC** should forward the IP packets.
Metric	The lower the value, the higher the priority of the route (range of values 1...14).

Table 10-15: ***IP*** ➧ ***ROUTING*** ➧ **ADD**

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

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

Table 10-16: **Network**

You can only configure one default route on your **XCENTRIC**. 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 **XCENTRIC**.
If you configure both Internet access and a corporate network connection, enter a default route to the ISP and a network route to the head office.

Default route

To define a default route, proceed as follows:

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

➤ 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.

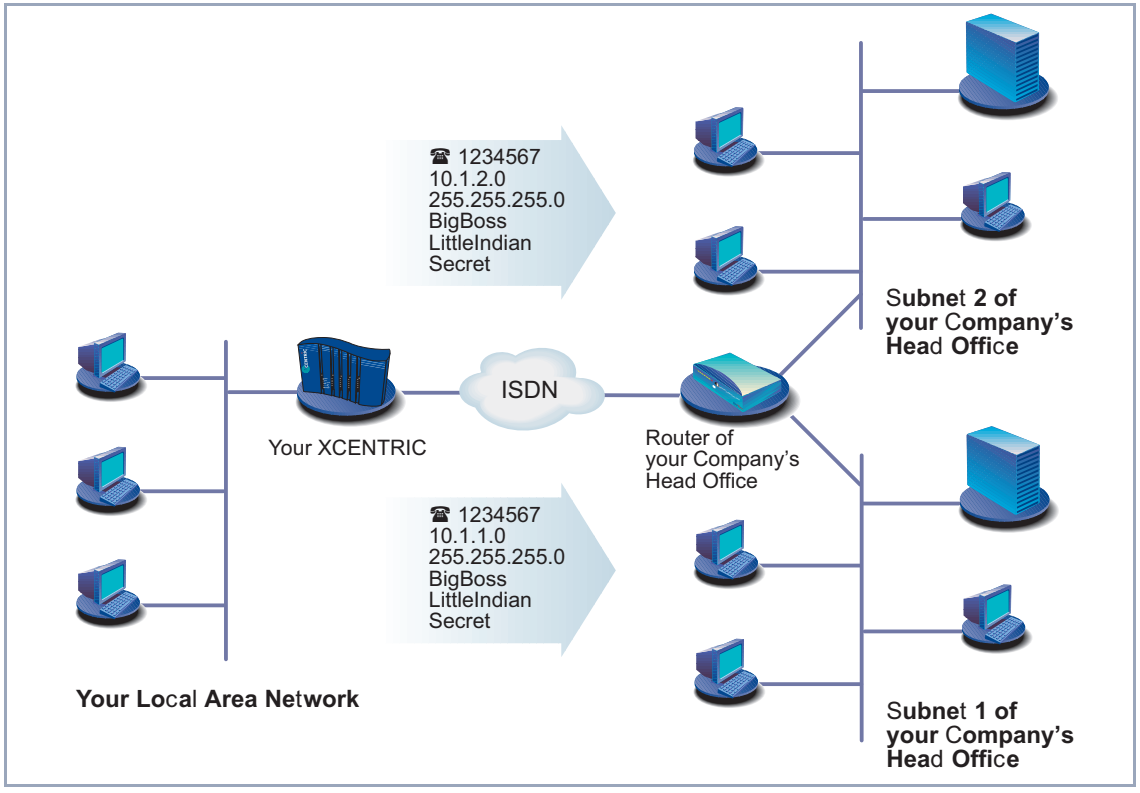


Figure 10-4: Corporate network with several connected LANs

Network route

To establish a network route, e.g. for a corporate network connection (without a default route), proceed as follows:

- 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 15.2.7, page 440.

Proceed as follows to activate NAT:

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

You see the following menu:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[IP][NAT]: NAT Configuration                                    MyXcentric

Select IP Interface to be configured for NAT

GoInternet
BigBoss
en1
en1-snap

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:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[IP][NAT][CONFIG]: NAT Configuration (GoInternet)               MyXcentric

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.

10.2.2 Internet Access with XCENTRIC

Examples

A few examples are given here following the general procedure described in chapter 10.2.1, page 167, 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 9.1.1, page 142). 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:

WAN partner configuration

➤ 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 **Local PPP ID** (= user account + T-Online number + joint user account), e.g. *123456789012081512345678#0001*.

How to enter the passwords is described in "Changing the password", page 135.

- Enter **PPP Password** (=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. *60*.
- Enter **Idle for Dynamic Short Hold (%)**, e.g. *0*.
- Enter **Delay after Connection Failure (sec)**, e.g. *300*.
- 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**.

Routing entry creation

- 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*.

WAN partner configuration

- 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)**, e.g. minimum *120*.
- Enter **Idle for Dynamic Short Hold (%)**, e.g. *0*.
- Enter **Delay after Connection Failure (sec)**, e.g. *300*.
- Select **Channel Bundling**: *no*.
- Select **Layer 1 Protocol**: *ISDN 64 kbps*.

Authentication definition

- Select **Provider Configuration** and press **Return**.
- Select **Provider**: *Compuserve Network*.
- Enter **Host**: *CIS*.
- Enter **User ID** (= your user name).

How to enter the passwords is described in "Changing the password", page 135.

- 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**.

Routing entry creation

- 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.

10.2.3 Connecting XCENTRIC to a Corporate Network

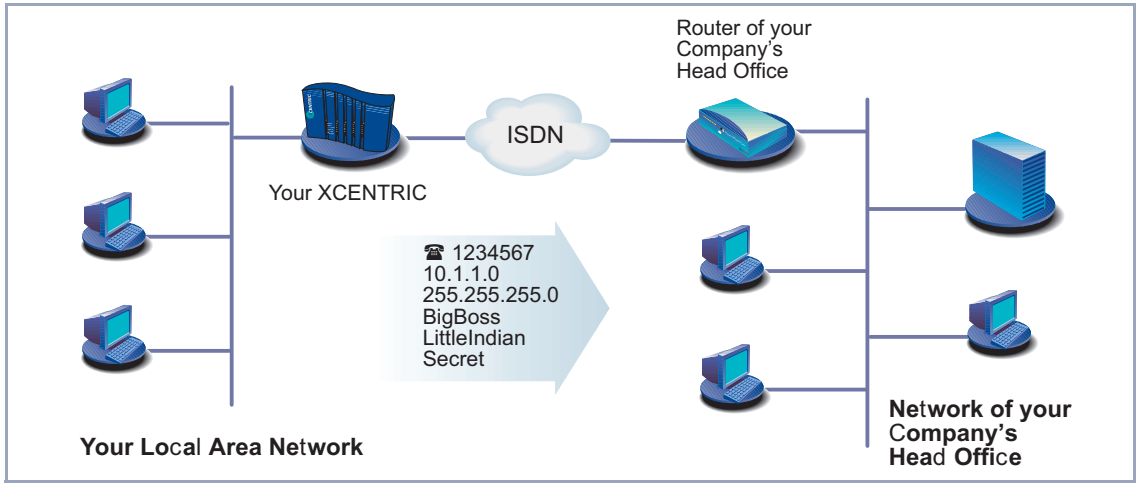


Figure 10-5: **XCENTRIC** and your head office

This chapter explains in quick and easy steps how to configure your **XCENTRIC** for a corporate network connection (LAN-LAN connection). Keep at hand the data you have received from the system administrator of your head office (see chapter 9.1.1, page 142). If you are not sure about some points, refer to chapter 10.2.1, page 167.

Proceed as follows:

WAN partner configuration

- 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*.

How to enter the passwords is described in "Changing the password", page 135.

- 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*.
- 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 **Local IP Address**, if applicable.
- 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.

Routing entry creation

If you have not configured any Internet access, then you can configure a default route for access to your head office (see chapter 10.2.1, page 167):

- 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 10.2.1, page 167 and figure 10-4, page 188.

- 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**.

10.2.4 Configuring the LAN Interface for Using ADSL (PPP-over-Ethernet)

ADSL To be able to use ADSL (Asymmetric Digital Subscriber Line) with **XCENTRIC**, you must configure a PPP-over-Ethernet interface over the LAN interface. This is done by connecting **XCENTRIC** via a hub to T-DSL, which is the ADSL connection of Deutsche Telekom AG.

T-DSL The T-DSL package is currently offered by Deutsche Telekom AG as high-speed access to the Internet. It consists of an ISDN connection and a data line with a bandwidth of up to 768 kbps from the Internet Service Provider to the customer (downstream) and 128 kbps in the upstream direction.

Restrictions and security risks

The following restrictions and security risks exist as the **XCENTRIC** connection to T-DSL is only over an Ethernet interface:

- If PPP-over-Ethernet is operated with only one Ethernet interface, there is a risk of unauthorized accesses from the Internet to the local **XCENTRIC** LAN. Such unauthorized accesses can originate from the first node of the Internet.
- Users of the local network can configure a PPP-over-Ethernet client on their PC and use the Internet unnoticed by **XCENTRIC**.
- Broadcasts in the local LAN are always forwarded by the ADSL modem (NTBBA) to the PTT exchange and are not rejected until the exchange. This means that the maximum bandwidth of 128 kbps upstream to the PTT may not be fully available.

The T-DSL connection (without **XCENTRIC**) looks like this:

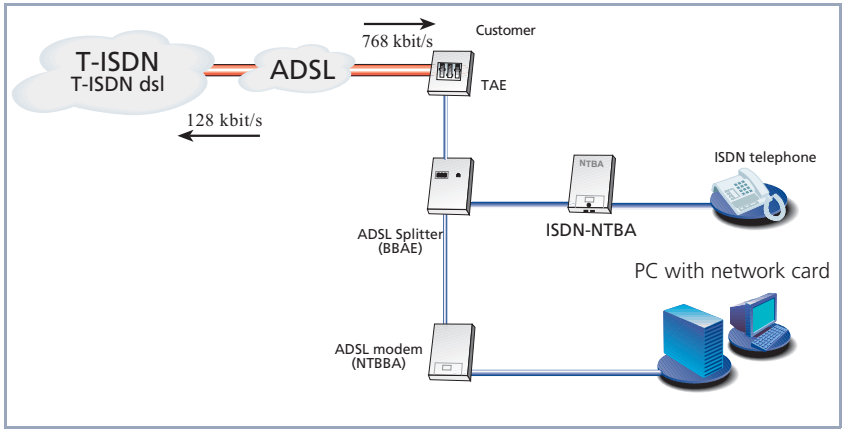


Figure 10-6: T-DSL connection (without **XCENTRIC**)

The following scenario (see figure 10-7, page 202) is used to describe the necessary configuration steps: The LAN interface of **XCENTRIC** is connected to your hub as described in chapter 6.3, page 66 and chapter 6.9.3, page 107. The ADSL modem (NTBBA) of Deutsche Telekom AG is also connected to the same hub.

If you use the internal hub modules (XCM-HUB) for **XCENTRIC**, we recommend connecting the ADSL modem of Deutsche Telekom AG to Port 1 or 2 or to Port 9 or 10 (see chapter 6.9, page 102).

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

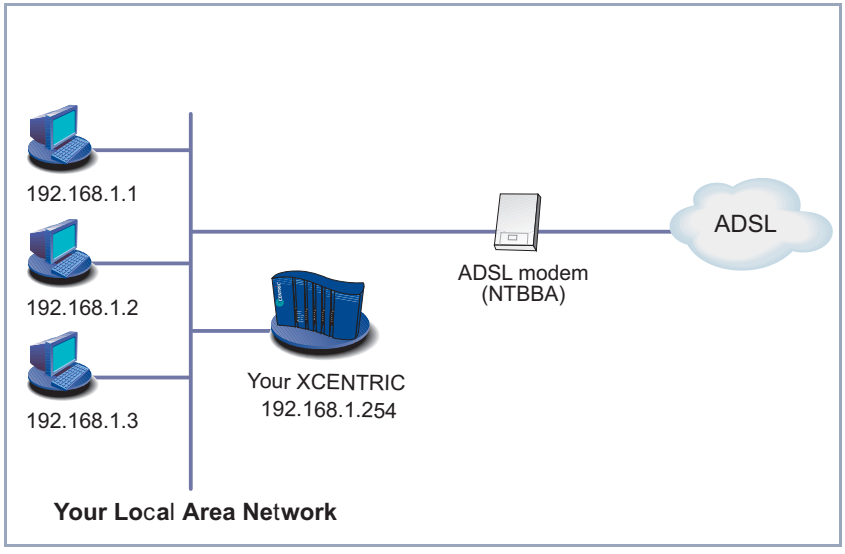


Figure 10-7: Example scenario (with **XCENTRIC**)

The following settings are necessary (the Setup Tool menus concerned are described elsewhere):

- Go to ***PPP*** (see chapter 14.1.2, page 350).
- Select **PPPoE Ethernet Interface**: *en1*.
- Press **SAVE**.
- Go to ***WAN PARTNER*** ➧ **ADD** (see table 10-6, page 171).
- Enter your **Partner Name**: e.g. *t-online.*
- Select **Encapsulation**: *PPP*

- Go to ***WAN PARTNER*** ➧ **ADD** ➧ ***PPP*** (see table 10-11, page 177).
- Enter **Local PPP ID** (= your user name): z. B. *000460004256091169386#0001@t-online.de.*

The T-Online user name comprises the following elements:

<user account><T-Online number>#<co-user number>@t-online.de

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.

- Enter **PPP Password** (= your T-Online password).
- Select **Keepalives**: *on.*
- Confirm with **OK**.
- Go to ***WAN PARTNER*** ➧ **ADD** ➧ ***ADVANCED SETTINGS*** (see chapter 14.2.4, page 359).
- Select **Layer 1 Protocol**: *PPP over Ethernet (PPPoE).*
- Confirm with **OK**.
- Go to ***WAN PARTNER*** ➧ **ADD** ➧ ***IP*** (see table 10-14, page 183).
- Select **IP Transit Network**: *dynamic client.*
- Press **SAVE**.
- Go to ***IP*** ➧ ***ROUTING*** ➧ **ADD** (see "Routing entry creation", page 184).
- Select **Route Type**: *Default route.*
- Select **Network**: *WAN without transit network.*
- Select **Partner / Interface**: e.g. *t-online.*
- Enter **Metric**: e.g. *1.*
- Press **SAVE**.
- Go to ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** (see "Activating Network Address Translation (NAT)", page 189).
- Select the PPPoE interface, e.g. **t-online**, and confirm with **Return**.

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

10.3 Saving the Configuration File

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

For handling configuration files, you should also refer to Chapter chapter 16.1, page 466.

If you use a flash card for **XCENTRIC**, you should also refer to chapter 16.2, page 474 for saving configurations.

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

Another menu window opens:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[EXIT]: Exit Setup                                              MyXcentric


            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 **XCENTRIC** appears with the login prompt. All the changes you have made with the Setup Tool are saved. The next time you start your **XCENTRIC**, 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 **XCENTRIC** appears with the login prompt. All settings or changes you have made with the Setup Tool will be lost when you turn off your **XCENTRIC**.

11 Configuration of PABX

You have already created a basic configuration for **XCENTRIC** with the Configuration Wizard as described in chapter 9, page 141.

You have already defined all the necessary settings for the PABX part with the Configuration Wizard. The functions for profiles, dial permissions, configuration of BinTec CS300 system telephones and LCR (Least Cost Routing) are not covered by the Configuration Wizard.

This chapter deals with the configuration of the PABX part with the Setup Tool. Here you will find descriptions on how to optimize and extend the configuration created with the Configuration Wizard.

If you wish to create the PABX configuration with the Setup Tool and not with the Configuration Wizard, you will also find a detailed description here of all PABX menus.

The procedures are described as if the configuration were created completely with the Setup Tool.

Have your network plan and extensions available before starting the configuration, so that you can read off the necessary configuration parameters (e.g. extensions and users).

Before you start configuration of the extension numbers, you should also think about the possible profiles and the related settings for the dial permissions. It is advisable to define the settings for profiles and dial permissions before you configure the extension numbers, so that you can assign them accordingly during the configuration of extensions and terminals. If you want to use profiles, please see chapter 11.11, page 289 and chapter 11.12, page 297.

The PABX configuration covers the configuration of the following settings and functions:

- Basic settings for the PABX part of **XCENTRIC** (door intercom, music on hold, etc.) in chapter 11.3, page 212.
- Configuration of the external connections of the communication modules in chapter 11.4, page 226.

- Configuration of the extensions (including router subsystems and CAPI) in chapter 11.5, page 239.
- Trunk prefixes in chapter 11.6, page 267.
- User configuration in chapter 11.7, page 272.
- Groups in chapter 11.8, page 276.
- Terminal configuration in chapter 11.9, page 281.
- Call forwarding in chapter 11.10, page 285.
- Profiles in chapter 11.11, page 289.
- Dial permissions in chapter 11.12, page 297.
- LCR configuration (Least Cost Routing) in chapter 11.13, page 311.
- Installation and configuration of BinTec CS300 system telephones in chapter 11.14, page 320.

If you leave the Setup Tool after a configuration step, you should always save the configuration you have created, as described in chapter 10.3, page 205.

Please also note the information on the ex works state of **XCENTRIC**.

The configuration examples for the Setup Tool refer to the following diagram, which shows a selection of connections to **XCENTRIC**:

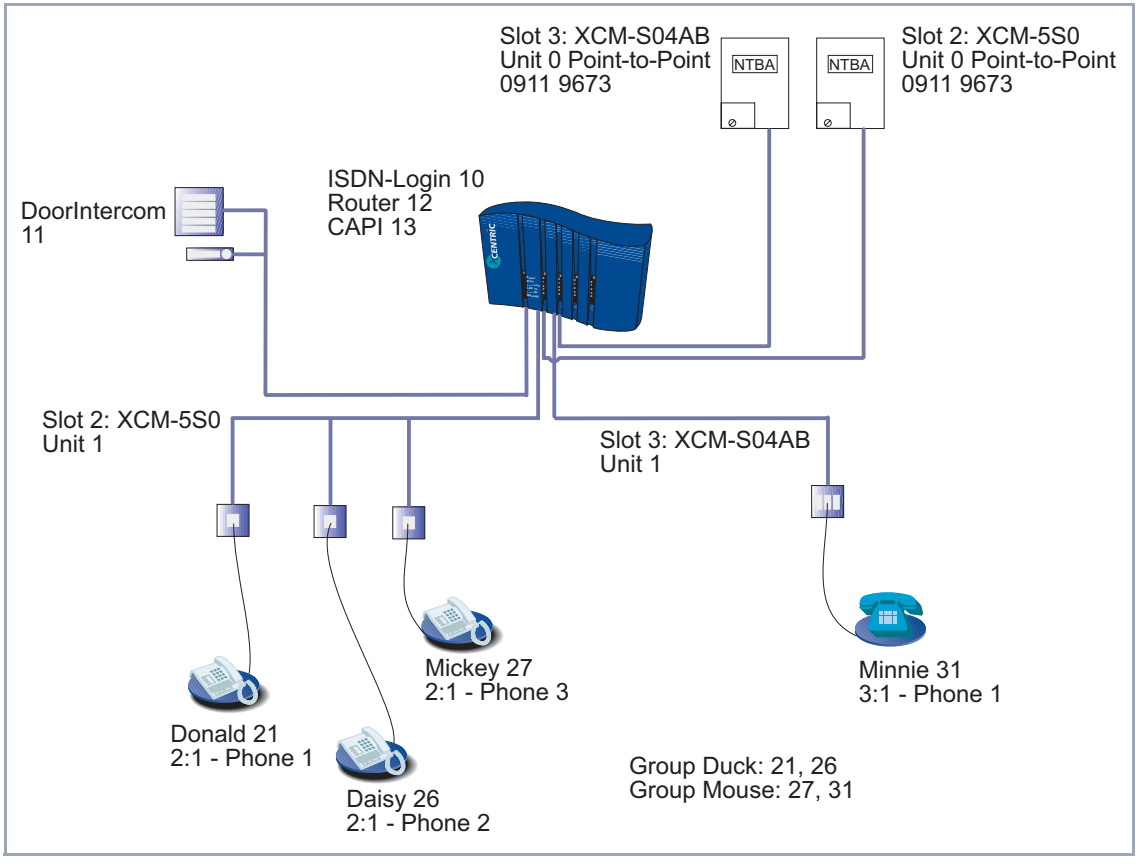


Figure 11-1: Example selection of connections to **XCENTRIC**

11.1 Ex Works State

With the PABX part of **XCENTRIC** in the ex works state (state before configuration with the Configuration Wizard), you can make external telephone calls immediately after connecting the terminals and without dialing a prefix number. All telephones connected to **XCENTRIC** can also be reached from outside (all telephones ring at the same time if an external call is received on the PABX number).

For this purpose, an entry with no extension is made for each unit of a module in the ex works state.

You should also read the instructions on configuration of the dialing procedure in chapter 11.3, page 212.

If **XCENTRIC** itself is connected to another PABX, which needs the extension of the calling party for outgoing calls, external telephone calls may not be possible in the ex works state.

The router subsystems ISDN Login and Router are similarly already preconfigured with no extension. The physical terminal for the door intercom is also already configured, but with no extension, so that only the telephone called by the door intercom can operate the door opener.

The entry for the extension that is called by the door intercom when the door bell button is pushed is "#" in the ex works state. This means all telephones ring as soon as someone rings the door bell.

11.2 After Configuration with the Configuration Wizard

After creating the basic configuration with the Configuration Wizard and the basic settings for the router part, a basic configuration was also created for the PABX, which covers the following:

- Configuration of the external point-to-point and/or point-to-multipoint connections.
- An extension has already been assigned for each of the router subsystems Router and ISDN Login. If one of your external ISDN connections is a point-to-multipoint connection, one MSN of this point-to-multipoint connection was used for the router or ISDN Login in the default assignment by the Configuration Wizard.
- An extension entry was also configured in the default assignment for the CAPI subsystem for each user configured by you with CAPI permission.
- No or one physical terminal (telephone) was configured on each unit for an internal ab connection. The extensions were assigned according to the extension numbers range entered by you (direct dialing range).
- No, one or two physical terminal(s) was (were) configured on each unit for an internal ISDN connection. The extensions were assigned according to the extension numbers range entered by you (direct dialing range).
- An extension from your extension numbers range (direct dialing range) was assigned as default for the door intercom. You should also refer to the description of the door intercom configuration in chapter 11.5.3, page 252.
- The extension called when someone rings the door bell was configured.
- It was decided if external line access is configured for external calls or if you must dial a prefix number for internal calls. The default exchange number for external calls is 0, but this could also be changed.

You can view and extend the PABX configuration via the Setup Tool or Configuration Manager.

11.3 Basic PABX Settings

First you configure the basic PABX settings:

➤ Go to ***PABX*** ➧ ***STATIC SETTINGS.***

You see the following menu:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[PABX][STATIC] PABX Static Settings                              MyXcentric

        System Profiles:
            Local Prefix                         #
            Auto Dialout                         on
            Number                               0
            Dial Permission                      full
            Availability                         full
        Country                                  Germany

        Music on Hold                            external
        Door Intercom Call Extension             #
        Door Intercom External Open              deny

        CTI Settings >
        Accounting Template >

            SAVE                              CANCEL

Use <Space> to select
```

The menu contains the following fields:

Note that a higher permission level always contains all the lower permission levels, which are described in the following table for the **Dial Permission** field. The permission *national special*, for example, therefore also contains the permission levels *national*, *local* and *internal*.

The meanings stated here for the individual permissions are suggestions, which conform with the default lists generated automatically by **XCENTRIC** (see chapter 11.12, page 297). The actual meaning of the individual permissions (*local*, *national*, *national special* and *full*) depend on your specific user configuration. See also chapter 11.12, page 297.

Field	Meaning
System Profiles	The **System Profiles** item contains 5 fields (**Local Prefix** to **Availability**), which form the values of the system profile for all terminals. The system profile contains the default values for all terminals (physical terminals and sub-systems).
Local Prefix	Here you see the local prefix of the system profile for internal calls if **Auto Dialout** is enabled in the system profile and a dialing prefix is entered. The local prefix shown here must be used by all terminals for which **Auto Dialout** is activated. This field cannot be edited.

Field	Meaning
Auto Dialout	Here you can select whether automatic external line access is to be enabled for the system profile. Possible values: ■ *on* (default setting) ■ *off* If you select *on*, a trunk prefix to be used for automatic external line access must be entered under **Number**. This means that the local prefix (#) must be dialed for setting up an internal connection and external connections are dialed without a trunk prefix (automatic external line access). If you set **Auto Dialout** to *off*, no prefix is dialed for internal calls. A trunk prefix must be dialed for setting up an external connection. To assign certain trunks (external S_0 connections) their own prefixes, you must set the desired prefix in the relevant menu for the external S_0 connection or in the ***PREFIXES*** menu. See chapter 11.4, page 226.
Number	Here you enter the dialing prefix for the system profile for automatic external line access if **Auto Dialout** is set to *on*.

Field	Meaning
Dial Permission	Here you assign the system profile the permission to create connections from the terminals (physical terminals and subsystems) connected to **XCENTRIC**. The descriptions of the individual values are suggestions in line with the default configuration for dial permissions. See the note before this table. Possible values: ■ *internal* Allows only internal calls to be set up. ■ *local* Allows the setting up of internal calls and external calls restricted to the local network. Dialing free special numbers is also allowed. ■ *national* Allows the setting up of internal calls and external calls restricted to the national network. Dialing free special numbers is also allowed. Calls to mobile phone networks or added-value services are not allowed.
Dial Permissions	■ *national special* Allows the setting up of internal calls and external calls restricted to the national network. Free special numbers and connections to mobile phone networks and national added-value services are also allowed. ■ *full* (default value) Allows internal calls and all types of external calls to be set up.

Field	Meaning
Availability	Here you can set the availability of terminals (physical terminals and subsystems) for the system profile. Possible values: ■ *full* (default value) Terminals can be reached internally and externally. ■ *internal* Terminals can only be reached internally. ■ *external* Terminals can only be reached externally.
Country	Here you can set the country for **XCENTRIC**. This activates special settings for the selected country. Possible values: ■ *Germany* (default setting) This default setting optimizes **XCENTRIC** for use in Germany. ■ *UK* This setting adapts the internal dial tone for telephones connected to **XCENTRIC** to the British standard. ■ *France* This setting activates adaptations to the French ISDN standard (VN6/VN7) for call forwarding and for processing charging information.

Field	Meaning
Music on Hold	Is used for configuration of the music-on-hold interface. Possible values: ■ *external* Music for music-on-hold feature is supplied from external audio equipment. The connection for external audio equipment is located on **XCENTRIC**'s basic unit. See also chapter 6.3, page 66. ■ *internal* An internal announcement is played back for waiting subscribers.
Door Intercom Call Extension	Extension that is called when someone rings the door bell. Both an internal and external extension can be entered here. The internal extension can, if necessary, also be a group extension.

Field	Meaning
Door Intercom External Open	This value determines whether the door opener can be operated by only one extension in the PABX of **XCENTRIC** (*deny*), or by a call from an external caller to the **Door Intercom Call Extension** (*allow*). Possible values: ■ *deny* (default value) ■ *allow* The default setting *deny* prevents the door being opened by a call set up externally. The door can only be opened by an external call if this setting is *allow*. We also recommend that the door intercom extension is assigned a profile so that it can only be reached internally, in order to prevent the door being opened by internal call forwarding of an external call. See also chapter 11.11, page 289.
CTI Settings	You pass to a submenu in which you can make the settings for CAPI and TAPI. See "Submenu CTI Settings", page 220.
Accounting Template	You pass to a submenu in which you can define an accounting string. See "Submenu Accounting Template", page 222.

Table 11-1: ***PABX*** ➧ ***STATIC SETTINGS***

To do Proceed as follows:

As the ex works state (before basic configuration with the Configuration Wizard) is configured so that all telephones can be reached from outside and external calls can be dialed by all telephones at any time without a prefix, the default entry in **System Profiles** for **Auto Dialout** is *on* and for **Number** *0*.

If you set **Auto Dialout** in the **System Profiles** to *off* and have not previously assigned extensions to the terminals, all the telephones connected ring as soon as the receiver is lifted at one terminal.

Note that the settings selected for the system profile apply to all terminals for which no separate user-defined profile has been selected for the extensions (***DIAL PLAN*** menu) or the terminal settings (***TERMINALS*** menu). The values of the system profile therefore also apply to the subsystems of **XCENTRIC**, such as ISDN Login, Router and CAPI, if these have not been assigned their own profile.

If, for example, **Dial Permission** in the system profile is set to *internal* and the router subsystem uses the system profile, the router cannot set up any PPP connections to the outside.

- Select the right values for the system profile (**Local Prefix** to **Availability** fields) or leave the default values, as applicable.
- Define the setting for **Music on Hold**.
- Assign the extension that is to be called by the door intercom (**Door Intercom Call Extension**). You should not set this entry until the relevant extension has been assigned to a terminal or a call group.

Caution!

If you set the **Door Intercom External Open** field to *allow*, an unauthorized person who has obtained the extension of your door intercom can gain access by operating the door opener from a mobile telephone. This can represent a security risk for your firm.

➤ Set this field to *allow* only if absolutely necessary.

To prevent the door opener being operated by internal call forwarding of an external call, we recommend that in addition to the setting *deny* for the **Door Intercom External Open** field, the extension is also assigned a profile with internal availability only. See also chapter 11.11, page 289.

➤ Assign the door intercom extension a profile with **Availability** set to *internal*.

➤ Set the value for **Door Intercom External Open**.

➤ Make any necessary settings in the submenus **CTI Settings** and **Accounting Template**. See "Submenu CTI Settings", page 220 and "Submenu Accounting Template", page 222.

➤ Leave the menu with **SAVE**.

You have returned to the ***PABX*** submenu.

Submenu *CTI SETTINGS*

The submenu ***PABX*** ➧ ***STATIC SETTINGS*** ➧ ***CTI SETTINGS*** contains the settings for CAPI and TAPI:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][STATIC]: PABX CTI Settings                          MyXcentric

    CTI Settings:

    Remote TAPI Server Port          2663
    TAPIadmin Password
    Remote CAPI Server Port          2662
    CAPIadmin Password


                SAVE                          CANCEL

Enter integer range 0.0.65535
```

The menu contains the following fields:

Field	Meaning
Remote TAPI Server Port	Indicates the port for the remote TAPI. The default setting is *2663*.
TAPIadmin Password	Here you can enter the password for the pre-configured **TAPIadmin** user. The **TAPIadmin** user is used in connection with TAPI server applications. The default setting of this field is empty, i.e. no password is configured. To disable the **TAPIadmin** user, you must leave the **TAPIadmin Password** field empty. We recommend disabling the **TAPIadmin** user if you do not use it in your configuration.
Remote CAPI Server Port	Indicates the port for the remote CAPI. The default setting is *2662*. This value can also be set under ***IP*** ➧ ***STATIC SETTINGS***.
CAPIadmin Password	Here you can enter the password for the pre-configured **CAPIadmin** user. The **CAPIadmin** user is used for CAPI server applications. The default setting of this field is empty, i.e. no password is configured. To disable the **CAPIadmin** user, you must leave the **CAPIadmin Password** field empty. We recommend disabling the **CAPIadmin** user if you do not use it in your configuration.

Table 11-2: ***PABX*** ➧ ***STATIC SETTINGS*** ➧ ***CTI SETTINGS***

To do Proceed as follows to edit the entries:

➤ Enter a **Remote TAPI Server Port**. You should normally leave the TAPI port on 2663.

To disable the **TAPIadmin** user, you must leave the **TAPIadmin Password** field empty (default setting). We recommend disabling the **TAPIadmin** user if you do not use it in your configuration.

How to change the passwords is described in "Changing the password", page 135.

- Configure the **TAPIadmin Password** for the **TAPIadmin** user or leave the field empty to disable the **TAPIadmin** user.
- Enter a **Remote CAPI Server Port**. You should normally leave the CAPI port on 2662.

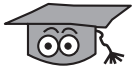
To disable the **CAPIadmin** user, you must leave the **CAPIadmin Password** field empty (default setting). We recommend disabling the **CAPIadmin** user if you do not use it in your configuration.

- Configure the **CAPIadmin Password** for the **CAPIadmin** user or leave the field empty to disable the **CAPIadmin** user.
- Leave the menu with **SAVE**.

  You have returned to ***PABX*** ➧ ***STATIC SETTINGS***.

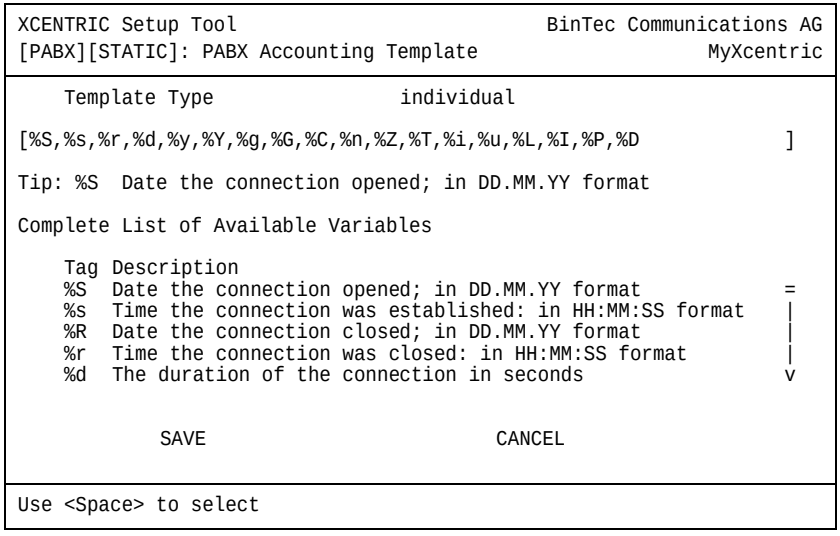
Submenu *ACCOUNTING TEMPLATE*

This menu enables you to compile your accounting string individually or to select a special accounting string for the PABX (under preparation for Windows application **BinTec PABX Accounting**) in addition to the default accounting string.



The accounting string is saved in the variable **isdnAccountingTemplate** in the MIB.

You will find the submenu under ***PABX*** ➧ ***STATIC SETTINGS*** ➧ ***ACCOUNTING TEMPLATE***:


XCENTRIC Setup Tool
BinTec Communications AG
[PABX][STATIC]: PABX Accounting Template
MyXcentric
Template Type
individual
[%S,%s,%r,%d,%y,%Y,%g,%G,%C,%n,%Z,%T,%i,%u,%L,%I,%P,%D
Tip: %S Date the connection opened; in DD.MM.YY format
Complete List of Available Variables
Tag Description
%S Date the connection opened; in DD.MM.YY format
%s Time the connection was established: in HH:MM:SS format
%R Date the connection closed; in DD.MM.YY format
%r Time the connection was closed: in HH:MM:SS format
%d The duration of the connection in seconds
SAVE
CANCEL
Use <Space> to select

The menu contains the following fields:

Field	Meaning
Template Type	Here you can set the various types of template. Possible values: ■ *default* ■ *pabx* (default value) ■ *individual* *default* defines a default accounting string. *pabx* defines a PABX accounting string, which you must select for the Windows application **BinTec PABX Accounting**. *individual* enables you to compile your own accounting string. See also the following descriptions of the menu elements. If you use an *individual* string, note that a set *individual* string is lost when a default accounting string (*pabx* or *default*) is saved.
Accounting String (second line in the configuration window)	Here you see the elements of the accounting string. The string cannot be changed if the **Template Type** is set to the values *default* and *pabx*. If the **Template Type** field is set to *individual*, you can enter your own accounting string here. Refer to the list of possible variables (**Complete List of Available Variables**). If a string variable is tagged, the corresponding information appears below in the **Tip** line.
Complete List of Available Variables	A list of the possible variables for the *individual* setting (in the **Template Type** field) is given here to simplify entering the variable.

Table 11-3: ***PABX*** ➧ ***STATIC SETTINGS*** ➧ ***ACCOUNTING TEMPLATE***

To do Proceed as follows to edit the accounting string:

- Select the desired accounting string under **Template Type**.
- If you have selected *individual* for **Template Type**, you must enter the desired string under **Accounting String**.
- Leave the menu with **SAVE**.

  You have returned to ***PABX*** ➧ ***STATIC SETTINGS***.

11.4 Configuration of External S_0 Connections

Now you must configure the external S_0 connection or the external S_0 connections.

One external S_0 connection is located on the ab module (XCM-S04AB). Other external S_0 connections that can be configured by setting jumpers are located on the 5-S_0 module (see chapter 6.7.1, page 83).

The following description describes the configuration of an external S_0 connection for point-to-point and point-to-multipoint connections.

You will find the external S_0 connections of the communication modules

- for XCM-S04AB
  in ***SLOT X: XCM-S04AB, 1xISDN 4xAB*** ➧ ***UNIT 0: ISDN EXTERNAL S0***

or

- for XCM-5S0
  in ***SLOT X: XCM-5S0, 5S0*** ➧ ***UNIT X: ISDN EXTERNAL S0***.

You will find information about configuring leased lines and cascading **XCENTRIC**s in chapter 11.4.1, page 237 and chapter 11.4.2, page 238.

Example of Setup Tool menu for configuration of an external S_0 connection:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[SLOT2 UNIT0 ISDN BRI]: Configure ISDN Basic Rate Interface MyXcentric


Type of Interface:                ISDN External S0
ISDN Switch Type                  autodetect on bootup
Result of Autoconfiguration:      Euro ISDN point-to-point

Country Code                      49
Area Code                         911
Subscriber Number                 9673

Prefixes:        Prefix
                 0

Configure Prefixes>
Advanced Settings>

                 SAVE                            CANCEL

Use <Space> to select
```

This menu has the following fields:

Field	Meaning
Type of Interface	Here you can set the type of interface. Possible values: ■ *ISDN External S0* (default setting) ■ *ISDN Tie S0 (Layer1:TE)* The setting *ISDN Tie S0 (Layer1:TE)* is for cascading **XCENTRIC**s (see chapter 11.4.2, page 238) and is only used in this specific case. The default value *ISDN External S0* should always be left here when configuring an external S_0 connection.
ISDN Switch Type	The configuration of the ISDN protocol. Possible values: ■ *autodetect on bootup* (default setting) ■ *Euro ISDN point-to-point* ■ *Euro ISDN point-to-multipoint* ■ *leased line B1 channel (64S)* ■ *leased line B1+B2 channel (64S2)* ■ *leased line D+B1+B2 channel (TS02)* ■ *leased line B1+B2 different endpoints* (digital 64S with dual connection) The last four values are used for leased lines. Leased lines are explained in more detail in chapter 11.4.1, page 237.

Field	Meaning
Result of Autoconfiguration	Result of autoconfiguration, if autoconfiguration was activated (**ISDN Switch Type** is *autodetect on bootup)*. Possible values: ■ *Euro ISDN point-to-point* ■ *Euro ISDN point-to-multipoint* The automatic D-channel detection runs until a setting is found or until the ISDN protocol is typed in manually under **ISDN Switch Type**.
Signaling TEI Value	For permanently set point-to-point connections (*Euro ISDN point to point* in the **ISDN Switch Type**) field, the **Signaling TEI Value** field is displayed. The default TEI (Terminal Endpoint Identifier) value is *0* and this should be retained. If a different TEI is required in exceptional cases, it can be configured here.
Country Code **Area Code** **Subscriber Number**	You only need to enter these settings for a point-to-point connection: country code and area code, each without the initial 0 and the PABX number without the extension, as you received it from your telephone company.
Prefixes	Here you can see the trunk prefixes assigned to the external S_0 connection under the **Prefix** field.
Configure Prefixes	Clicking **Configure Prefixes** opens a submenu in which you can assign prefixes to the external S_0 connection or delete assigned prefixes. You can also configure new prefixes or delete prefixes. The submenus are described below in "Configure Prefixes Submenu", page 231.

Field	Meaning
Advanced Settings	This submenu can be used for making additional settings for X.31 (X.25 in the D-channel), which are only necessary if you want to use the X.31 TEI for CAPI applications. The menu is described below in "Advanced Settings", page 235.

Table 11-4: Menu for configuration of an external S_0 connection

To do Proceed as follows:

- For an external S0 connection, leave **Type of Interface** set to the default value *ISDN External S0*.
- If you have set autoconfiguration, check **Result of Autoconfiguration** to see if the ISDN protocol has been detected correctly.
- If the protocol has not been detected correctly, or you wish to set it manually, set the protocol of the external S_0 connection under **ISDN Switch Type**.
- In the case of a point-to-point connection, enter **Country Code**, **Area Code** and **Subscriber Number**.
- The prefixes currently assigned to the S_0 connection can be seen under **Trunk Prefixes**. If applicable, configure the necessary dialing prefixes in the submenu under **Configure Prefixes >**.
  The procedure for configuration of prefixes is described in the "Configure Prefixes Submenu", page 231.
- Leave the menu with **SAVE**.
  You have returned to the submenu of your module.
- Configure all external S_0 connections in this way.

Configure Prefixes Submenu

Prefixes can also be configured in the ***PREFIXES*** menu in the ***PABX*** menu. See chapter 11.6, page 267.

Open the ***CONFIGURE PREFIXES*** menu by selecting the **Configure Prefixes** button in the menu for the external S_0 connection:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[SLOT2 UNIT0 ISDN BRI][TRUNK]: Configure Prefixes              MyXcentric

            Prefix       Usage        Config       Status
          X 0            TRUNK        external     valid

        SAVE          ADD           DELETE           CANCEL

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag for 'X' (item
selected) or 'D' (item marked for deletion and unselected on save),
<Return> to edit
```

This menu shows a list of all the configured prefixes. The menu indicates the use of the prefix (only *TRUNK* for external S_0 connections), the configuration (only *external* for external S_0 connections) and the status. These data are especially relevant for cascading **XCENTRIC**s (see chapter 11.4.2, page 238) and should always be set to the default values for a standard configuration of an external S_0 connection.

Prefixes assigned to the external S_0 connection are marked with an **X**.

This menu offers you the option of assigning an existing prefix to the external S_0 connection or deleting a prefix assigned to the external S_0 connection. You can configure a new prefix or delete a prefix.

Assigning and deleting a prefix

Proceed as follows to assign the external S_0 connection a prefix from the list of configured prefixes:

To connect several S_0 connections to form a trunk group, you must assign the same **Prefix** at this point to the various external S_0 connections.

- Use the **Cursor** key to go to the prefix to be assigned and mark it in the list with the **Space** bar.
  An **X** appears in front of the list entry.
- Press **SAVE**.
  You have returned to the previous menu and can see the assigned prefixes under **Prefix**.

To delete a prefix from the assignment to the external S_0 connection, proceed as follows:

- Use the **Cursor** key to go to the prefix marked with an **X** that you want to delete from the assignment and press the **Space** bar twice.
  Neither **X** nor **D** precede the list entry.
- Press **SAVE**.
  You have returned to the previous menu and can see that the prefix you have just deleted is no longer listed under **Prefix**.

Configuring a new prefix and deleting a prefix

Proceed as follows to configure a new prefix:

- Press the **ADD** button.

You change to the following menu:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[SLOT2 UNIT0 ISDN BRI][CONFIGURE PREFIXES]: Add Prefix      MyXcentric

            Prefix          01
            Usage           TRUNK
            Status          valid




        SAVE                      CANCEL

Enter string, max length = 15 chars
```

The menu contains the following fields:

Field	Meaning
Prefix	The prefix. The value of a trunk prefix can contain up to eight numbers, with up to two-digit numbers being used as a rule.
Usage	The use of a prefix. Possible values: ■ *TRUNK* (default value) ■ *TIE* The value *TIE* is used only for cascading **XCENTRIC**s. See chapter 11.4.2, page 238.
State	The status of the prefix. Possible values: ■ *valid* (default value) ■ *invalid* The *invalid* setting offers you the possibility of deactivating a prefix without having to delete it.

Table 11-5: ***SLOTX: XCM-5S0, 5S0*** ➧ ***UNITX: ISDN EXTERNAL S0*** ➧ ***CONFIGURE PREFIXES*** ➧ ***ADD***

➤ Enter the **Prefix**.

➤ Press ***SAVE***.
You have returned to the previous menu and the prefix just configured is already shown in the list.
Now you can assign the prefix to the external S_0 connection, as described in "Assigning and deleting a prefix", page 232.

To delete a prefix, proceed as follows:

Here you can delete prefixes assigned to an S_0 connection. Before you delete a prefix, you should make sure which S_0 connections the prefix is assigned to and whether it is advisable to delete the prefix.

Check the **Config** column in the list of the ***CONFIGURE PREFIXES*** menu to see if a prefix is unused (*<unused>*).

- Use the **Cursor** key to go to the prefix to be deleted in the list in the ***CONFIGURE PREFIXES*** menu.
- Press **Space** until a **D** appears in front of the list entry.
- Press **DELETE**.
  The prefix is deleted.

Advanced Settings

A brief description of the submenu ***ADVANCED SETTINGS*** is given below. You only need to make settings here if you want to use the X.31 TEI value for CAPI applications.

```
XCENTRIC Setup Tool                              BinTec Communications AG
[SLOT2 UNIT0 ISDN BRI][ADVANCED]: Advanced Settings of BRI  MyXcentric




X.31 TEI Value           specify
Specify TEI Value        64
X.31 TEI Service         CAPI Default


             SAVE                            CANCEL

Use <Space> to select
```

The submenu contains the following fields:

Field	Meaning
X.31 TEI Value	X.31 TEI is detected automatically in ISDN autoconfiguration and this value set to *specify*. If autoconfiguration has not detected TEI, you can set *specify* 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: ■ *Capi* ■ *Capi Default* ■ *Packet Switch* *Capi* and *Capi Default* are for using X.31 TEI for CAPI applications. For *CAPI*, the TEI value set in the CAPI application is used. For *CAPI Default*, the value of the CAPI application is ignored and the default value set here is always used. Set to *Packet Switch* if you want to use X.31 TEI for the X.25 router (X.25 license necessary!).

Table 11-6: ***ADVANCED SETTINGS*** of menu for external S_0 connection

11.4.1 Leased Lines

If you use **XCENTRIC** on a leased line, i.e. one of the values for leased lines is set under **ISDN Switch Type**, you will find the following fields in the menu:

Field	Meaning
D-channel	In most cases, you can keep the default value set here (*leased dte*). If you have requested a special service from your service provider, it may be necessary to set the local side of the leased line at this point (DTE or DCE). You must then ensure that the far end has set the opposite value. You must also set the same values under **D-channel**, **B-channel 1** and **B-channel 2**, if you have selected several D/B channels under **ISDN Switch Type** and the values can be changed. Possible values: ■ *leased dte* ■ *leased dce*
B-channel 1 **B-channel 2**	In most cases, you can keep the default value set here. The setting should be changed only in special cases. See **D-channel**.

Table 11-7: Menu for configuration of an external S_0 connection for leased lines

Proceed as follows to configure the WAN partner for a leased line:

A WAN partner interface for the leased line is configured automatically in the ***WAN PARTNER*** menu.

➤ Edit the previously configured entry for the leased line in the ***WAN PARTNER*** menu and enter the necessary parameters.
See chapter 10.2.1, page 167.

11.4.2 Cascading XCENTRICs

It is possible to connect other **XCENTRIC**s to a central **XCENTRIC** via the XCM-5S0 or XCM-S04AB communication modules for cascading purposes. This connection of two or more **XCENTRIC**s needs special configuration of the ISDN interfaces, which is described separately.

For a detailed description of cascading several **XCENTRIC**s, please refer to the Download section of **XCENTRIC** at www.bintec.net.

11.5 Extension Numbers (Dial Plan)

The ***DIAL PLAN*** menu is used to configure the extensions for the individual terminals, router subsystems, CAPI and group extensions. In this menu, you can configure all extensions and configure new terminals or select existing terminals. You can also configure users, groups and call forwarding.

In the ex works state before configuration with the Configuration Wizard, a physical terminal with no extension is entered for each internally configured unit of a module; this must be edited and an extension assigned or modified. Another possibility is to delete the default entry and then configure the desired extensions.

Any entries not required must be deleted, as otherwise such entries with no extension would be called by all incoming calls. Entries with no extension also mean that no more suffixes can be dialed for a call at a point-to-point connection. This means the terminal called cannot be reached.

Note that extensions on point-to-point connections of **XCENTRIC** are detected from left to right and that extensions on point-to-multipoint connections are compared from right to left.

For point-to-point connections, for example, this means if you have configured terminals with the extensions *27* and *29*, the *2* must not be configured as an extension, as the entry for extension *2* would "intercept" the calls for *27* and *29*.

For point-to-multipoint connections, for example, at least *567* and *667* must be configured as extensions for the MSNs 1234567 and 2345667, as *67* would not be unique. In addition, 7 must not be configured as an extension in this case, as this would in turn accept all calls for the stated MSNs.

If you have a combination of point-to-point and point-to-multipoint connections on your **XCENTRIC**, you must observe both the above rules.

Window for Dial Plan menu:

```
XCENTRIC Setup Tool                                BinTec Communications AG
[PABX][DIAL PLAN] Configure Dial Plan                              MyXcentric

Extension   User     Terminal Name    Destination      Primary Group
10          <none>   ISDN Login       isdnlogin        <none>
11          <none>   DoorIntercom     phys 1:1         <none>
12          <none>   Router           ppp              <none>
13          default  CAPI             application      <none>
21          Donald   2:1 - Phone 1    phys 2:1         Duck
26          Daisy    2:1 - Phone 2    phys 2:1         Duck
31          Minnie   3:1 - Phone 1    phys 3:1         <none>

        ADD              DELETE              EXIT

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

This menu displays a list of the extensions already configured. **Extension** shows the extension configured. **User** lists the user. **Destination** shows the type of terminal. The relevant module and unit for the physical terminals are also shown here in the form "Slot:Unit". **Terminal Name** shows the name of the terminal. **Primary Group** shows you the group to which the extension is assigned. If the name of the group is followed by *+*, this indicates that the extension is assigned to more than one group.

Access is possible over the Remote TAPI to every physical terminal (telephone) for which an extension and user are configured.

The information about incoming calls on these terminals is passed automatically to the Remote CAPI of the corresponding user at the same time. This function enables you to configure answering machine software on the PC in the network, which is based on the Remote CAPI and in which the user and extension are set according to the terminal configuration of **XCENTRIC**.

However, if a user is to use CAPI services such as fax, an extension entry for the CAPI subsystem must be made for this user. See chapter 11.5.5, page 259.

Due to the automatic connection of incoming calls through to the CAPI as described above, we recommend that a user (**User**) is also always configured for a physical terminal (and for CAPI entries in the ***DIAL PLAN***). Otherwise it is possible that a CAPI application in your LAN that is not configured for a certain extension intercepts calls to such extensions that have no user configured.

Configuring the individual physical terminals, router subsystems, CAPI and group extensions is described in the following chapters.

Each extension within a service type may only be assigned to one terminal or subsystem. A terminal or subsystem can, however, be reachable over different extensions.

Due to the separation into voice and data service types, an extension with the voice service type can theoretically be assigned to a physical terminal and the same extension with the data service type to a router subsystem.

➤ To configure an extension for a physical terminal, router subsystem, CAPI or group, press the **ADD** button.

11.5.1 Extension Assignment for an ISDN Terminal

Configuring the extension for an ISDN terminal (ISDN telephone) is described below:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][DIAL PLAN][ADD]: Configure Dial Plan                MyXcentric


    Extension                    27
    Type                         voice
    Destination                  physical
    Physical Port                Slot 2 Unit 1
    Presentation Number


    Terminal Name                2:1 Phone 3 (new)
    Profile                      <none>

    Select User                  Mickey
    New User
    Select Group                 <none>
    New Group

    Advanced settings >

            SAVE                          CANCEL

Enter string, max length = 15 chars
```

When assigning extensions for ISDN terminals, note that up to eight terminals (see hardware limitations) can be configured for each unit on the 5 x S_0 module.

The extensions must also be configured directly at the respective ISDN terminals.

The menu contains the following fields:

Field	Meaning
Extension	Here you enter the extension under which the terminal is to be reached.
Type	The service type of the extension. *voice* in this case.
Destination	The type of terminal. Always *physical* here.
Physical Port	Here you enter the slot and unit of the respective module to which the terminal is connected.
Presentation Number	In this field you can enter an extension that is presented to the called party as the calling party number. For a point-to-multipoint connection, this must be a valid number for the respective connection. For a point-to-point connection, the **Presentation Number** given here is attached to the PABX number of the point-to-point connection. The **Presentation Number** should only be entered if it differs from the **Extension**.
Terminal Name	Here you select a terminal that is already configured or select a new default terminal in the list, which is automatically configured as a new terminal.
Profiles	Here you can assign the extension a profile from the list of profiles configured in the ***PROFILES*** menu. Before assigning profiles make sure you read chapter 11.11, page 289.
Select User	Here you select a user from the list of users already configured.

Field	Meaning
New User	You pass via this field to a submenu, in which you can configure a new user.
Select Group	Here you select the call group to which you wish to assign the extension from the list of groups already configured.
New Group	You pass via this field to a submenu, in which you can configure a new group.
Advanced Settings	You pass to a submenu in which you can configure call forwarding for the extension as in the ***CALL FORWARDING*** menu. For the meaning of the fields see chapter 11.10, page 285.

Table 11-8: ***PABX*** ➧ ***DIAL PLAN*** ➧ ***ADD*** for assignment of extensions to an ISDN terminal

The Setup Tool also contains a ***DIAL PLAN*** for the internally configured units under the 5 x S_0 module, but this plan only contains the ISDN terminals that are connected to the respective unit.

Configuration is therefore possible at two different places in the Setup Tool.

To do To assign the extension for an ISDN telephone, proceed as follows:

- ➤ Enter the extension via which the terminal is to be reached under **Extension**.
- ➤ Select *voice* as **Type** for an ISDN telephone.

For example, if you have connected an ISDN card as ISDN terminal to an internal S_0 connection, you must select *all* or *data* as **Type** during the configuration.

- ➤ Select the type of terminal under **Destination**. For an ISDN telephone, select *physical*.
- ➤ Select the slot and unit of the corresponding module to which the terminal is connected under **Physical Port**.

- If necessary, you can enter an extension in the **Presentation Number** field, which is then presented to the called party as the calling party number.
- Under **Terminal Name**, either select a terminal already configured from the list or select a new default terminal, which is then configured automatically.

If you have selected a new default terminal here, you can edit the parameters of this terminal in the ***PABX*** ➧ ***TERMINALS*** menu (see chapter 11.9, page 281), e.g. to change the name of the terminal.

- If applicable, select a profile under **Profiles**. Before assigning profiles make sure you read chapter 11.11, page 289.
- In **Select User**, select the user from the list of users already configured or go to the **New User** field and press **Return** to configure a new user. A description of this menu is given below.
- In **Select Group**, select a group from the list of groups already configured or go to the **New Group** field and press **Return** to configure a new group. A description of this menu is given below.
- Leave the menu with **SAVE**.

  You have now returned to the ***DIAL PLAN*** menu.
- Assign all the necessary extensions for ISDN terminals as described above.

All extensions configured for a physical terminal (telephone) and a certain user are also passed internally to the CAPI of this user.

This functionality makes it possible to configure answering machine software for such an extension on the basis of BinTec's Remote CAPI, in which the user and extension are set according to the terminal configuration of **XCENTRIC**. The answering machine function must be configured with a time delay.

BinTec's Voice Mail Server provides the answering machine function via call forwarding. See the User's Guide for the Voice Mail Server at www.bintec.net.

If a user is to use CAPI services such as fax, an extension entry must be made for this user for the CAPI subsystem, as otherwise no outgoing connections can be made from the CAPI. See chapter 11.5.5, page 259.

New user configuration

To configure a new user in the ***DIAL PLAN*** menu, tag the **New User** field and press **Return**. You change to the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][DIAL PLAN][ADD][NEW USER]: Configure Dial Plan       MyXcentric


    Name                    Mickey
    PIN                     ****
    Password                *****

    TAPI Monitoring         enabled
    TAPI Controlling        enabled
    CAPI                    enabled

    Assigned Extensions     0


            SAVE                        CANCEL

Enter string, max length = 15 chars
```

The menu contains the following fields:

Field	Meaning
Name	The name of the user.
PIN	This field can be entered, but is not currently used by the system.
Password	The user's password for using CAPI and TAPI applications.
TAPI Monitoring	Permission for the user to view the status of his terminals via a TAPI application. The default setting is on.
TAPI Controlling	Permission for the user to check the calls of his terminals via a TAPI application. The default setting is on.
CAPI	User's access right for the CAPI interface. The default setting is on.

Table 11-9: ***PABX*** ➧ ***DIAL PLAN*** ➧ ***ADD*** ➧ ***NEW USER***

To do Proceed as follows:

- Enter the user name.

How to enter the passwords is described in "Changing the password", page 135.

- Enter a CAPI/TAPI password for the user.
- Select the desired setting for this user for **TAPI Monitoring**, **TAPI Controlling** and **CAPI**.
- Leave the menu with **SAVE**.

  You have returned to the menu for assigning the extension, a submenu of ***DIAL PLAN***.

New group configuration To configure a new group, tag the **New Group** field and press **Return**. You change to the following menu:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[PABX][DIAL PLAN][ADD][NEW GROUP]: Configure Dial Plan      MyXcentric

            Group Name           Mouse




                 SAVE                        CANCEL

Enter string, max. length = 15 char
```

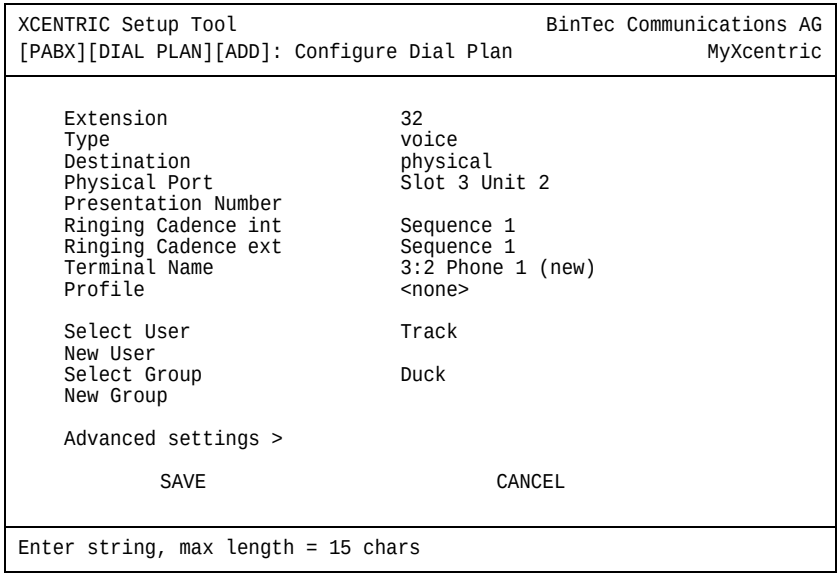
To do Proceed as follows:

- Enter the group name.
- Leave the menu with **SAVE**.

  You have returned to the menu for assigning the extension, a submenu of ***DIAL PLAN***.

11.5.2 Extension Assignment for an ab Terminal

Configuring the extension for an ab terminal (analog telephone or analog fax) is described below:



The menu contains the following fields:

Field	Meaning
Extension	Here you enter the extension under which the terminal is to be reached.
Type	The service type of the extension. *voice* in this case.
Destination	The type of terminal. Always *physical* here.
Physical Port	Here you enter the slot and unit of the respective module to which the terminal is connected.
Presentation Number	In this field you can enter an extension that is presented to the called party as the calling party number. For a point-to-multipoint connection, this must be a valid number for the respective connection. For a point-to-point connection, the **Presentation Number** given here is attached to the PABX number of the point-to-point connection. The **Presentation Number** should only be entered if it differs from the **Extension**.
Ringing Cadence int	Here you can select different ringing tones for analog terminals for internal calls.
Ringing Cadence ext	Here you can select different ringing tones for analog terminals for external calls.
Terminal Name	Here you select a terminal that is already configured or select a new default terminal in the list, which is automatically configured as a new terminal.

Field	Meaning
Profiles	Here you can assign the extension a profile from the list of profiles configured in the ***PROFILES*** menu. Before assigning profiles make sure you read chapter 11.11, page 289.
Select User	Here you select a user from the list of users already configured.
New User	You pass via this field to a submenu, in which you can configure a new user.
Select Group	Here you select the call group to which you wish to assign the extension from the list of groups already configured.
New Group	You pass via this field to a submenu, in which you can configure a new group.
Advanced Settings	You pass to a submenu in which you can configure call forwarding for the extension as in the ***CALL FORWARDING*** menu. For the meaning of the fields see chapter 11.10, page 285.

Table 11-10: ***PABX*** ➧ ***DIAL PLAN*** ➧ ***ADD*** for assignment of extensions to an ab terminal

The Setup Tool also contains a ***DIAL PLAN*** under the ab module for the internal ab units, but this plan only contains the ab terminal that is connected to the respective unit.

Configuration is therefore possible at two different places in the Setup Tool.

To do To assign the extension for an analog terminal, proceed as follows:

- ➤ Enter the extension via which the terminal is to be reached under **Extension**.
- ➤ Select *voice* as **Type** for an ab telephone.
- ➤ Select the type of terminal under **Destination**. For an ab telephone, select *physical*.

- Select the slot and unit of the corresponding module to which the terminal is connected under **Physical Port**.
- If necessary, you can enter an extension in the **Presentation Number** field, which is then presented to the called party as the calling party number.
- If necessary, select **Ringing Cadence int** and **Ringing Cadence ext**.
- Under **Terminal Name**, either select a terminal already configured from the list or select a new default terminal, which is then configured automatically.

If you have selected a new default terminal here, you can edit the parameters of this terminal in the ***PABX*** ➧ ***TERMINALS*** menu (see chapter 11.9, page 281), e.g. to change the name of the terminal.

- If applicable, select a profile under **Profiles**. Before assigning profiles make sure you read chapter 11.11, page 289.
- In **Select User**, select the user from the list of users already configured or go to the **New User** field and press **Return** to configure a new user. A description of this menu can be found in chapter 11.5.1, page 241.
- In **Select Group**, select a group from the list of groups already configured or go to the **New Group** field and press **Return** to configure a new group. A description of this menu can be found in chapter 11.9, page 281.
- Leave the menu with **SAVE**.

  You have now returned to the ***DIAL PLAN*** menu.
- Assign all the necessary extensions for ab terminals as described above.

All extensions configured for a physical terminal (telephone) and a certain user are also passed internally to the CAPI of this user.

This functionality makes it possible to configure answering machine software for such an extension on the basis of BinTec's Remote CAPI, in which the user and extension are set according to the terminal configuration of **XCENTRIC**. The answering machine function must be configured with a time delay.

BinTec's Voice Mail Server provides the answering machine function via call forwarding. See the User's Guide for the Voice Mail Server at www.bintec.net.

If a user is to use CAPI services such as fax, an extension entry must be made for this user for the CAPI subsystem, as otherwise no outgoing connections can be made from the CAPI. See chapter 11.5.5, page 259.

11.5.3 Extension Assignment for the Door Intercom

The assignment of extensions for the door intercom is described separately here, as this concerns a special case of a physical terminal.

Menu for door intercom configuration:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][DIAL PLAN][ADD]: Configure Dial Plan                  MyXcentric

    Extension                   11
    Type                        voice
    Destination                 physical
    Physical Port               Slot 1 Unit 1



    Terminal Name               DoorIntercom (new)
    Profile                     internal only

    Advanced settings >

            SAVE                          CANCEL

Enter string, max length = 15 chars
```

The menu contains the following fields:

Field	Meaning
Extension	Here you enter the extension under which the door intercom is to be reached. As the door intercom is only to be reachable internally, an extension outside the extension numbers range assigned by the telephone company can also be assigned to the door intercom. The Configuration Wizard assigns an extension from the stated extension numbers range as default.
Type	The service type of the extension. Always *voice* in this case.
Destination	The type of terminal. *physical* here.
Physical Port	Indicates the slot and unit of the respective module. The door intercom is defined for Slot 1 Unit 1.
Terminal Name	Here you select *DoorIntercom* from the list. If the door intercom was not previously configured as a physical terminal, *(new)* appears after *DoorIntercom* and the *DoorIntercom* terminal is configured automatically.
Profiles	Here you can assign the extension a profile from the list of profiles configured in the ***PROFILES*** menu. It is recommended that the door intercom extension is assigned a profile with internal availability only. See note after the table. Before assigning profiles make sure you read chapter 11.11, page 289.
Advanced Settings	You pass to a submenu for configuring call forwarding, which is not practical in conjunction with the door intercom. This configuration option should not be used here.

Table 11-11: ***PABX*** ➧ ***DIAL PLAN*** ➧ ***ADD*** for assignment of extensions to the door intercom

To assign the extension for the door intercom, proceed as follows:

- Under **Extension**, enter the extension via which the door intercom is to be reached.

Caution!

The **Door Intercom External Open** field, in which you can define whether the door opener of the door intercom is also reachable from outside, can be found in the ***PABX*** ➧ ***STATIC SETTINGS*** menu (see chapter 11.3, page 212).

If you set the **Door Intercom External Open** field to *allow*, an unauthorized person who has obtained the extension of your door intercom can gain access by operating the door opener from a mobile telephone. This can represent a security risk for your firm.

- Set this field to *allow* only if absolutely necessary.

To prevent the door opener being operated by internal call forwarding of an external call, we recommend that in addition to the setting *deny* for the **Door Intercom External Open** field, the extension is also assigned a profile with internal availability only. See also chapter 11.11, page 289.

- Assign the door intercom extension a profile with **Availability** set to *internal*.

- Select *voice* as **Type** for the door intercom.
- Select the type of terminal under **Destination**. For the door intercom, select *physical*.
- Select the slot and unit of the corresponding module to which the terminal is connected under **Physical Port**. The door intercom is located in Slot 1 Unit 1.
- Under **Terminal Name**, select *DoorIntercom* from the list for the door intercom. If *DoorIntercom* was not already configured as terminal, *(new)* appears after the value and *DoorIntercom* is configured as new terminal.
- Select a profile under **Profiles** that has internal availability only. See note above. Before assigning profiles make sure you also read chapter 11.11, page 289.
- Leave the menu with **SAVE**.

  You have now returned to the ***DIAL PLAN*** menu.

11.5.4 Extension Assignment for ISDN Login and Router (Router Subsystems)

The router subsystem of **XCENTRIC** supports:

- PPP (Routing):
  The router subsystem ➤➤ **PPP** is the general routing service of **XCENTRIC**. 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. This subsystem also enables outgoing data calls to be set up to WAN partners outside your local network.

- ISDN Login:
  The ➤➤ **ISDN Login** router subsystem allows incoming data calls access to the ➤➤ **SNMP shell** of your **XCENTRIC**. This is how **XCENTRIC** is remotely configured and administrated.

When a call is received, **XCENTRIC** first checks the Called Party Number (CPN) and the type of call (data or voice call). The call is then forwarded to the corresponding subsystem.

Configuring the extension for ISDN Login and the router (PPP) is described below.

Access to **XCENTRIC** via ISDN Login is denied by not configuring an extension for ISDN Login.

Note that if no extension is configured for ISDN Login, outgoing ISDN Login is also not possible from **XCENTRIC**.

The following menu is used for configuring the extension for the router (PPP):

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][DIAL PLAN][ADD]: Configure Dial Plan                MyXcentric

    Extension                   12
    Type                        data
    Destination                 ppp


    Terminal Name               Router (new)
    Profile                     <none>
    Layer 1 Protocol            auto
    Interface                   auto



    Advanced settings >

            SAVE                          CANCEL

Enter string, max length = 15 chars
```

The following menu is used for configuring the extension for ISDN Login:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][DIAL PLAN][ADD]: Configure Dial Plan                MyXcentric

    Extension                   10
    Type                        data
    Destination                 isdnlogin


    Terminal Name               ISDN Login (new)
    Profile                     <none>



    Advanced settings >

            SAVE                          CANCEL

Enter string, max length = 15 chars
```

The menu contains the following fields:

Field	Meaning
Extension	Here you enter the extension under which the Router or ISDN Login is to be reached.
Type	The service type of the extension. You normally set this to *data*. If you want modems to be able to dial in as well, you must select *all* here.
Destination	The type of terminal. *ppp* for *Router* or *isdnlogin* for *ISDN Login*.
Terminal Name	In this list you select *Router* or *ISDN Login*, which are automatically configured as a new router subsystems.
Profiles	Here you can assign the extension a profile from the list of profiles configured in the ***PROFILES*** menu. Before assigning profiles make sure you read chapter 11.11, page 289.
Advanced Settings	You pass to a submenu for configuring call forwarding, which is not practical in conjunction with *Router* and *ISDN Login*. This configuration option should not be used here.

Table 11-12: ***PABX*** ➧ ***DIAL PLAN*** ➧ ***ADD*** for assignment of extensions for a router subsystem

The additional **Layer 1 Protocol** and **Interface** fields that appear at the bottom of the menu when configuring the *Router* (*ppp*) are described below:

Layer 1 Protocol contains the following selection options for incoming calls only:

Possible Values	Meaning
auto	*auto* is the default value for this field, which can be used for all types of connection in this table (except for specific modem profiles 2 to 8). Select this setting in case of doubt.
sync 64 kbps	For 64-kbps ISDN data connections.
sync 56 kbps	For 56-kbps ISDN data connections.
Modem	For analog modem or fax connections. Uses modem profile 1 in **XCENTRIC**. This value is only available in **XCENTRIC** if the fax modem module (XFM-Fax) is installed in **XCENTRIC**.
V.110 (1200 ... 38400)	For connections to V.110 at bit rates of 1200 bps, 2400 bps,..., 38400 bps.
Modem profile 1 ... 8	Selects modem profile 1 to 8, as configured in the ***MODEM*** menu in **XCENTRIC**. See chapter 14.4, page 404. These values are only available in **XCENTRIC** if the fax modem module (XFM-Fax) is installed in **XCENTRIC**.

Table 11-13: **Layer 1 Protocol**

The **Interface** field is not used. You should leave the default value *auto* here.

To do Proceed as follows:

- Enter the extension under which the ISDN Login or router is to be reached in the **Extension** field.
- Select *data* or *all* as **Type** for the router subsystems.

- Select *ppp* for the *Router* under **Destination**. Select *isdnlogin* for the *ISDN Login*.
- Select *Router* or *ISDN Login* from the list under **Terminal Name**.
- If applicable, select a profile under **Profiles**. Before assigning profiles make sure you read chapter 11.11, page 289.
- Select **Layer 1 Protocol** for *Router*, if applicable.
- Leave the menu with **SAVE**.

  You have now returned to the ***DIAL PLAN*** menu.
- Assign the necessary extension to the router and ISDN Login as described above.

11.5.5 Extension Assignment for CAPI

This chapter describes the configuration of an extension for the CAPI subsystem.

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

Press **ADD** in the ***DIAL PLAN*** menu to access the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][DIAL PLAN][ADD]: Configure Dial Plan                MyXcentric

    Extension                   13
    Type                        all
    Destination                 application


    Terminal Name               CAPI (new)
    Profile                     <none>

    EAZ
    Select User                 default
    New User

    Advanced settings >

            SAVE                          CANCEL

Enter string, max length = 15 chars
```

All extensions configured for a physical terminal (telephone) and a certain user are also passed internally to the CAPI of this user.

This functionality makes it possible to configure an answering machine software application for such an extension on the basis of BinTec's Remote CAPI, in which the user and extension are set according to the terminal configuration of **XCENTRIC**. The answering machine function must be configured with a time delay. A separate extension entry for the CAPI subsystem is not necessary for this application.

BinTec's Voice Mail Server provides the answering machine function via call forwarding. See the User's Guide for the Voice Mail Server at www.bintec.net.

If a user is to use CAPI services such as fax, an extension entry must be made for this user for the CAPI subsystem, as otherwise no outgoing connections can be made from the CAPI.

Example application:

Your workplace is equipped with a telephone and a PC with software answering machine application and fax software application. The extensions *39* and *41* from the extension numbers range are available for this workplace.

You now configure *39* as extension for the physical terminal (the telephone) of the user at this workplace. You configure BinTec's Remote CAPI on the PC for the workplace user.

You now configure the software answering machine application on the PC of this workplace so that it responds to the extension *39* after a time delay. The answering machine on the PC then accepts an incoming call if the telephone receiver is not lifted after a set interval of time.

For the software fax application, you must configure a CAPI extension entry for extension *41* and the same workplace user. Now configure the software fax application on the PC so that it responds to extension *41*.

The menu contains the following fields:

Field	Meaning
Extension	Here you enter the extension under which the CAPI is to be reached.
Type	The service type of the extension. For the CAPI, select *all*.
Destination	For the CAPI, select *application*.
Terminal Name	In this list you select *CAPI* , which is automatically configured as new subsystem.
Profile	Here you can assign the extension a profile from the list of profiles configured in the ***PROFILES*** menu. Before assigning profiles make sure you read chapter 11.11, page 289.
Select User	Here you select a user from the list of users already configured.
New User	You pass via this field to a submenu, in which you can configure a new group. A description of this menu can be found in „New user configuration“ in chapter 11.5.1, page 241.
Advanced Settings	You pass to a submenu in which you can configure call forwarding for the extension as in the ***CALL FORWARDING*** menu. For the meaning of the fields see chapter 11.10, page 285.

Table 11-14: ***PABX*** ➧ ***DIAL PLAN*** ➧ ***ADD*** for assignment of extensions to the CAPI

The additional item **EAZ**, which appears in the menu under **Terminal Name** when configuring the extension number in the CAPI configuration, is described below:

Value	Meaning
Number: 0 ... 9	Permits connections to the Remote CAPI application of CAPI 1.1. Only necessary for CAPI 1.1 applications. Converts incoming MSNs to single-digit EAZs.

Table 11-15: **EAZ** field

If you work on your PCs with communication applications based on CAPI 1.1, (current version: Remote CAPI 2.0), **XCENTRIC** must convert the MSNs of the incoming call to single-digit EAZs (CAPI 1.1 can only recognize single-digit numbers).

So make sure with CAPI 1.1 that every number is "mapped" to its own EAZ.

In CAPI 2.0, the MSN is evaluated directly, so "conversion" to EAZ is not necessary.

Proceed as follows:

- Under **Extension**, enter the extension via which the *CAPI* is to be reached.
- Select *all* as **Type** for the *CAPI*.
- Select *application* for the *CAPI* under **Destination**.
- Select *CAPI* from the list under **Terminal Name**.
- If applicable, select a profile under **Profiles**. Before assigning profiles make sure you read chapter 11.11, page 289.
- Enter **EAZ**, if applicable.
- In **Select User**, select the user from the list of users already configured or go to the **New User** field and press **Return** to configure a new user. A description of this menu can be found in „New user configuration“ in chapter 11.5.1, page 241.
- Leave the menu with **SAVE**.

  You have now returned to the ***DIAL PLAN*** menu.

In special cases, you may wish to assign the CAPI subsystem a wide range of extension numbers. For example, if you wish to configure extensions 40 to 59 for the **Destination** *application* (CAPI), you have the option with point-to-point connections of only configuring extension 4 and 5, as this covers the above extension numbers range.

For point-to-point connections, the numbers are compared from left to right, so that extensions 40 to 49 from the entry with extension 4 are passed to the application and extensions 50 to 59 from the entry with extension 5.

The extensions to which the respective CAPI application is to respond must be configured directly in the application.

11.5.6 Extension Assignment for a Call Group

The assignment of the extension for a call group is described here.

Menu for assignment of extension:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][DIAL PLAN][ADD]: Configure Dial Plan                MyXcentric

    Extension                   35
    Type                        voice
    Destination                 group

    Profile                     <none>

    Select Group                Duck
    New Group

    Advanced settings >

            SAVE                          CANCEL

Enter string, max length = 15 chars
```

The menu contains the following fields:

Field	Meaning
Extension	Here you enter the extension under which the call group is to be reached.
Type	The service type of the extension. Here you select *voice* as **Service Type** for a call group.
Destination	The type of terminal. In this case, *group* for a call group.
Profile	Here you can assign the extension a profile from the list of profiles configured in the ***PROFILES*** menu. Before assigning profiles make sure you read chapter 11.11, page 289.
Select Group	Here you select the group in the list for which the extension is to be configured.
New Group	Tag the **New Group** field and press **Return** to pass to a submenu in which you can configure a new group. A description of this menu can be found in „New group configuration“ in chapter 11.5.1, page 241.
Advanced Settings	You pass to a submenu in which you can configure call forwarding for the extension as in the ***CALL FORWARDING*** menu. For the meaning of the fields see chapter 11.10, page 285.

Table 11-16: ***PABX*** ➧ ***DIAL PLAN*** ➧ ***ADD*** for assignment of extensions to a call group

Proceed as follows:

- Under **Extension**, enter the extension via which the call group is to be reached.
- Select *voice* as **Type**.
- Select *group* for the call group under **Destination**.

- If applicable, select a profile under **Profiles**. Before assigning profiles make sure you read chapter 11.11, page 289.
- In **Select Group**, select the group to which you wish to assign the extension from the list of groups already configured or go to the **New Group** field and press **Return** to configure a new group. A description of this menu can be found in „New group configuration“ in chapter 11.5.1, page 241.
- Leave the menu with **SAVE**.

  You have now returned to the ***DIAL PLAN*** menu.
- Repeat this procedure to configure all extensions for call groups.

11.6 Prefixes and External Line Access

In addition to configuring prefixes under the respective external S_0 interfaces in the Setup Tool (see chapter 11.4, page 226), you can also configure them in the ***PREFIXES*** menu of the ***PABX*** menu.

Here you can configure and delete prefixes and also assign prefixes to an external S_0 connection (trunk) or delete them from the assignment to an external S_0 connection.

➤ Go to ***PABX*** ➧ ***PREFIXES***.

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][PREFIXES]: Configure Prefixes                        MyXcentric

        Prefix          Usage       Config      Status
        0               TRUNK       external    valid




            SAVE        ADD         DELETE      CANCEL

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

This menu shows a list of all the configured prefixes. The menu indicates the use of the prefix (only *TRUNK* for external S_0 connections), the configuration (only *external* for external S_0 connections) and the status. These data are especially relevant for cascading **XCENTRIC**s (see chapter 11.4.2, page 238) and should always be set to the default values for a standard configuration of an external S_0 connection.

Configuring a new prefix

To configure a new prefix and then assign it to an S_0 interface, first configure a new prefix as described below and then edit it to assign it to an external S_0 interface, as described in "Assigning prefixes to an external S0 interface", page 270.

Proceed as follows to configure a new prefix:

➤ Press the **ADD** button.

You change to the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][CONFIGURE PREFIXES]: Add Prefix                      MyXcentric

            Prefix          01
            Usage           TRUNK
            Status          valid




        SAVE                    CANCEL

Enter string, max length = 15 chars
```

The menu contains the following fields:

Field	Meaning
Prefix	The prefix. The value of a trunk prefix can contain up to eight numbers, with up to two-digit numbers being used as a rule.
Usage	The use of a prefix. Possible values: ■ *TRUNK* (default value) ■ *TIE* The value *TIE* is used only for cascading **XCENTRIC**s. See chapter 11.4.2, page 238.
State	The status of the prefix. Possible values: ■ *valid* (default value) ■ *invalid* The *invalid* setting offers you the possibility of deactivating a prefix without having to delete it.

Table 11-17: ***PABX*** ➧ ***PREFIXES*** ➧ ***ADD***

➤ Enter the **Prefix**.

➤ Press ***SAVE***.
You have returned to the previous menu and the prefix just configured is already shown in the list.

Deleting a prefix

To delete a prefix, proceed as follows:

Here you can delete prefixes assigned to an S_0 connection. Before you delete a prefix, you should make sure which S_0 connections the prefix is assigned to and whether it is advisable to delete the prefix.

Check the **Config** column in the list of the ***PABX*** ➧ ***PREFIXES*** menu to see if a prefix is unused (*<unused>*).

- Use the **Cursor** key to go to the prefix to be deleted in the list in the ***CONFIGURE PREFIXES*** menu.
- Press the **Space** bar once.
  A **D** appears in front of the list entry.
- Press **DELETE**.
  The prefix is deleted.

Assigning prefixes to an external S_0 interface

To assign a prefix from the prefix list to an external S_0 connection, you must edit the prefix.

- Use the **Cursor** key to go to the prefix to be edited and press **Return**.
  You change to the ***EDIT PREFIX*** menu and can see a list of the external S_0 connections (trunks) already assigned to the prefix in the bottom half of the Setup Tool.

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][CONFIGURE PREFIXES]: Edit Prefix                    MyXcentric

            Prefix          01
            Usage           TRUNK
            Status          valid

Trunks:

    Slot    Unit    Type        Layer 2
    2       0       external    point-to-point
    3       0       external    point-to-point


Configure Trunks >

        SAVE                    CANCEL

Enter string, max length = 15 chars
```

The external S_0 connections are designated in the trunk list by slot and unit, the type of connection (external = external S_0 connection, internal = cascading of **XCENTRIC**s – see chapter 11.4.2, page 238) and the type of layer 2 connection.

- Now select **Configure Trunks** to assign a trunk to the prefix or delete a trunk from the assignment to a prefix.

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][CONFIGURE PREFIXES][TRUNK PREFIXES] Configure Trunks MyXcentric

        Slot    Unit    Type         Layer 2
      X 2       0       external     point-to-point
      X 3       0       external     point-to-point




             SAVE                     CANCEL


Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag ADD
```

External S_0 connections to which the prefix is already assigned are marked with an **X**.

To assign a prefix to an external S_0 connection (trunk), proceed as follows:

- Use the **Cursor** key to go to the trunk to be assigned and tag it by pressing the **Space** bar once.
  An **X** appears in front of the list entry.
- Press the **SAVE** button.
  You have returned to the previous menu and can already see the external S_0 connection just selected in the list of assigned external S_0 connections.

To delete a prefix from the assignment to an external S_0 connection (trunk), proceed as follows:

- Use the **Cursor** key to go to the trunk marked with an **X** that you want to delete from the assignment and press the **Space** bar once.
  The **X** in front of the list entry disappears.
- Press the **SAVE** button.
  You have returned to the previous menu and can see that the external S_0 connection you have just deleted from the assignment is no longer shown in the list of assigned external S_0 connections.

11.7 List of Users

A list of users is contained in the ***USERS*** menu, where you can configure and delete users.

➤ Go to ***PABX*** ➧ ***USERS.***

You see the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][USER]: Configure PABX Users                          MyXcentric

    Name                    Extensions
    default                 yes
    Donald                  yes
    Daisy                   yes
    Mickey                  yes
    Track                   yes




        ADD             DELETE          EXIT
```

If users are already entered, you will see a list of users here. **Extensions** shows *yes* if at least one extension is configured for the user or *no* if no extension is configured for the user. The user *default* is included as standard in the ex works state of **XCENTRIC**.

The **TAPIadmin** and **CAPIadmin** users are also preconfigured in **XCENTRIC**, but do not appear in the list of users. These users have access to all TAPI or CAPI lines configured in **XCENTRIC** and can therefore be used for connecting TAPI servers (e.g. BinTec CTI server) or CAPI servers to **XCENTRIC** . You will find important information about the configuration and use of the **TAPIadmin** and **CAPIadmin** users in chapter 13.2.3, page 339. An example application for the **TAPIadmin** user is given in chapter 13.2, page 338.

➤ To edit an existing user, select the user and press **Return**.

➤ To delete a user, tag it with the **Space** bar and press the **DELETE** button.

➤ To configure a new user, select **ADD**.

You are now in the menu ***PABX*** ➧ ***USERS*** ➧ ***ADD***:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][USER][ADD]: Configure PABX Users                      MyXcentric


    Name                    Trick
    PIN                     ****
    Password                *****

    TAPI Monitoring         enabled
    TAPI Controlling        enabled
    CAPI                    enabled

    Assigned Extensions     0


                SAVE                    CANCEL
```

The menu contains the following fields:

Field	Meaning
Name	The name of the user.
PIN	This field can be entered, but is not currently used by the system.
Password	The user's password for using CAPI and TAPI applications.
TAPI Monitoring	Permission for the user to view the status of his terminals via a TAPI application. The default setting is on.
TAPI Controlling	Permission for the user to check the calls of his terminals via a TAPI application. The default setting is on.
CAPI	User's access right for the CAPI interface. The default setting is on.
Assigned Extensions	Here you can see the number of extensions assigned to the user. If this value is greater than 0, another submenu appears below the field (**View Assigned Extensions**), which contains a list of the assigned extensions and terminals.

Table 11-18: ***PABX*** ➧ ***USERS*** ➧ ***ADD***

To do To create a new user entry, proceed as follows:

➤ Enter the user name.

How to enter the passwords is described in "Changing the password", page 135.

➤ Enter a CAPI/TAPI password for the user.

- Select the desired setting for this user for **TAPI Monitoring**, **TAPI Controlling** and **CAPI**.
- Leave the menu with **SAVE**.

  You return to the menu with the list of users and can see the user you have just configured in this list.
- You can configure all the users in your network in this way.

11.8 Call Groups and Call Pickup Groups

You can configure call groups and call pickup groups in the ***GROUPS*** menu.

Configuring groups provides the following features:

- Call groups (call pickup groups)
  The "call pickup" feature of the telephone can be used for extensions that are combined in one call group. See chapter 3.1, page 37 and chapter 4.5, page 47.
- Group call
  If the group extension is called, the telephones ring at all the extensions combined in this group.

The assignment to call groups and call pickup groups is based on the extension and not the user.

The assignment to groups via the extension gives you the following facility, for example:

If two extensions are assigned to one telephone, only one of the extensions is included in the group. By configuring different ringing tones for the two extensions, it is possible to determine from the ringing tones if the call is intended for the group or if someone is trying to reach the user directly. It is also only possible within a call-pickup group to pick up calls to the extensions included in the group. Calls to the other extensions cannot be picked up by the group.

➤ Go to ***PABX*** ➧ ***GROUPS***:

The following menu opens:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[PABX][GROUP]: Configure Groups                                  MyXcentric

                          Group Name
                          Duck




    ADD              DELETE               Exit
```

Here you see a list of the groups already configured.

- To add an entry, press the **ADD** button.
- To edit an existing entry, select the entry and press **Return**.
- To delete an entry, tag it with the **Space** bar and press the **DELETE** button.

When you add (or edit) an entry, pressing the **ADD** button (or editing the entry) opens the ***PABX*** ➧ ***GROUPS*** ➧ ***ADD*** (***EDIT***) menu:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[PABX][GROUP][ADD]: Configure PABX Groups                        MyXcentric

    Group Name                    Duck


    Configure Members >
    View Group Extensions >

            SAVE                  CANCEL

Enter string, max length = 15 chars
```

The menu contains the following fields:

Field	Meaning
Group Name	The name of the group.
Configure Members	You pass to a submenu, in which all the extensions configured are displayed with the respective users. Here you can select the extensions and users to be assigned to the group.
View Group Extensions	You pass to a submenu, in which all the group extensions assigned to the group are displayed. Group extensions are the extensions under which the whole group can be reached.

Table 11-19: ***PABX*** ➧ ***GROUPS*** ➧ ***ADD***

Group extensions are configured in ***DIAL PLAN***, where they can also be assigned to groups. You can also configure a new group in ***DIAL PLAN***. See chapter 11.5.6, page 264.

Group extensions can also be deleted with the ***DIAL PLAN***.

Configuring a group and adding extensions

Proceed as follows to configure a new group and assign user extensions to the group:

- Enter a group name under **Group Name**.
- Go to **Configure Members >** to the submenu in which you add extensions to the group as described in "Adding and deleting extensions", page 279.
- Press **SAVE** to confirm your entries.

  You return to the menu with the list of groups and can see the group you have just configured in this list.

Adding extensions and users to a group is carried out in the menu ***PABX*** ➧ ***GROUPS*** ➧ ***ADD*** ➧ ***CONFIGURE MEMBERS*** :

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][GROUP][ADD][MEMBERS]: Configure Members                MyXcentric

                     Group Name   Duck

    Extension        User         Terminal Name    Destination
    13               default      CAPI             application
 X  21               Donald       2:1 - Phone 1    physical
 X  26               Daisy        2:1 - Phone 2    physical
    27               Mickey       2:1 - Phone 3    physical
    31               Minnie       3:1 - Phone 1    physical
 X  32               Track        3:2 - Phone 1    physical


            SAVE                        EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag ADD
```

This menu displays a list of all the extensions and the respective users configured for **Destination** *physical* and *application* (except the door intercom extension).

Adding and deleting extensions

Proceed as follows to select an extension:

- Place the cursor on the entry you wish to assign to the group.
- Press the **Space** bar.
  An **X** appears in front of the entry.
- Repeat the operation for all extensions you wish to assign to the group.

  After you have left the menu by pressing **SAVE**, all the extensions marked by **X** are assigned to the group.

To delete an extension from the group to which it is assigned, proceed as follows:

- Place the cursor on the entry marked by **X** that you wish to delete from the group.
- Press the **Space** bar.
  The **X** in front of the entry disappears.

➤ Repeat the operation for all extensions you wish to delete from the group.

When you leave the menu by pressing **SAVE**, the extension is no longer assigned to the group.

Extensions can naturally be deleted/added from/to a group in a configuration step.

11.9 Terminals

The ***TERMINALS*** menu of the PABX group is used to delete terminals or to configure them – without assigning an extension at the same time. Here you can also make settings for the type of terminal, configure the BinTec CS300 system telephones and assign profiles to the terminals.

➤ Go to ***PABX*** ➧ ***TERMINALS***:

The following menu opens:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[PABX][TERMINAL]: Configure PABX Terminals                      MyXcentric

    Terminal Name    Terminal Type    Destination      Extensions
    2:1 - Phone 1    headset          phys 2:1         yes
    2:1 - Phone 2    phone            phys 2:1         yes
    2:1 - Phone 3    system phone     phys 2:1         yes
    3:1 - Phone 1    phone            phys 3:1         yes
    CAPI             internal         application      yes
    DoorIntercom     internal         phys 1:1         yes
    ISDN Login       internal         isdnlogin        yes
    Router           internal         ppp              yes


    ADD                  DELETE              EXIT

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

This menu displays all the configured physical terminals and subsystems.

➤ To delete a terminal or subsystem, tag it with the **Space** bar and press the **DELETE** button. Terminals can only be deleted if they are not assigned any extensions, i.e. *no* is shown in the **Extensions** column.

➤ To configure a new terminal, select **ADD**.

You are now in the ***PABX*** ➧ ***TERMINALS*** ➧ ***ADD*** menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][TERMINAL][ADD]: Configure PABX Terminals              MyXcentric


    Destination          physical
    Module               Slot 3 Unit 3
    Terminal Type        phone
    Profile              <none>

    Terminal Name        3:3 - Phone 1


    Primary Extension    <none>

    Assigned Extensions  0


    SAVE                 CANCEL

Enter integer range 0..214748364
```

This menu contains the following fields:

Field	Meaning
Destination	The type of terminal.
Modules	The slot and unit to which the terminal is connected. Appears only if **Destination** is *physical*.
Terminal Type	Here you can select between various settings for physical terminals. Possible values: ■ *phone* (default value) ■ *system phone* ■ *modem* ■ *answering machine* ■ *fax* ■ *headset* (for CTI applications only, see chapter 13.1.1, page 336) The **Terminal Type** field appears only if **Destination** is *physical*. If you have selected *system phone* for a system telephone as **Terminal Type**, the **Systel Serial No.** field also appears, in which you must select the serial number of the system telephone. Refer to chapter 11.14, page 320. The last four values listed above are only meaningful as settings for analog terminals.
Profile	Here you can assign the terminal a profile from the list of profiles configured in the ***PROFILES*** menu. Before assigning profiles make sure you read chapter 11.11, page 289.
Terminal Name	Terminal Name.

Field	Meaning
Primary Extension	This field appears only for analog terminals. Here you can enter which extension is to be used for outgoing calls if an analog telephone is assigned more than one extension.
Assigned Extensions	The number of extensions assigned to the terminal. If the terminal has at least one assigned extension, the additional **View Assigned Extensions** field appears.
View Assigned Extensions	Selecting this menu item opens a submenu in which you can view a list of extensions assigned to the terminal and the associated users.

Table 11-20: ***PABX*** ➧ ***TERMINALS*** ➧ ***ADD***

To do To configure a new terminal, proceed as follows:

- Enter a **Destination**. For physical terminals (phone, fax), select *physical*.
- If you have set *physical* under **Destination**, select the corresponding slot and unit under **Module**.
- For physical terminals (telephones), you can also select the type of terminal under **Terminal Type**. For configuration of BinTec CS300 system telephones see chapter 11.14, page 320.
- If applicable, select a profile from the list of configured profiles under **Profile**.
- Enter a terminal name for **Terminal Name**.
- For analog telephones where more than one extension is assigned, you can select the **Primary Extension**.
- Leave the menu with **SAVE**.

  You now return to the menu with the list of terminals and can already see the terminal you have just configured in the list.

11.10 Call Forwarding

In addition to configuring call forwarding via the telephone keypad (see chapter 3, page 35 and chapter 4, page 39) and in the ***DIAL PLAN*** menu (see chapter 11.5, page 239), you can also configure call forwarding for existing extensions in the ***CALL FORWARDING*** menu (submenu of ***PABX*** menu).

You can configure call forwarding on busy, call forwarding on no reply and immediate (unconditional) call forwarding. It is only practical to configure call forwarding for extensions of physical terminals, analog and ISDN telephones and CAPI.

Go to ***PABX*** ➧ ***CALL FORWARDING***:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][CALLFORW]: PABX Call Forwarding                       MyXcentric

Extension       User        Terminal Name       CF Mode
10              <none>      ISDN-Login          none
11              Donald      DoorIntercom        none
12              <none>      Router              none
13              default     CAPI                none
21              Donald      2:1 - Phone 1       none
26              Daisy       2:1 - Phone 2       busy
22              Mickey      2:1 - Phone 3       none
31              Minnie      3:1 - Phone 1       none

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

Here you can see a list of all extensions currently assigned for **XCENTRIC**. The list shows the extensions, associated users and terminal name and the type of call forwarding selected.

➤ To edit an entry, tag the relevant entry and press **Return**.

The following menu opens:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[PABX][CALLFORW][EDIT]: PABX Call Forwarding                   MyXcentric

    Extension               22
    User Name               Mickey
    Terminal Name           2:1 - Phone 3

    CF Mode                 busy_noreply

    Extension CF Busy       31
    Extension CF NoReply    31
    NoReply Timer           15


            SAVE                      CANCEL

Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
Extension	The extension for which call forwarding is to be configured. Cannot be edited.
User Name	The user assigned the physical terminal. Cannot be edited.
Terminal Name	The name of the terminal cannot be edited.
CF Mode	The type of call forwarding. Here you can select between five different options. ■ *none* (no call forwarding) ■ *uncond* (immediate call forwarding) ■ *busy* (call forwarding on busy) ■ *noreply* (call forwarding on no reply) ■ *busy_noreply* (call forwarding on busy and no reply)
Extension CF Busy	The extension to which a call is to be forwarded if the original extension is busy. This field appears only if **CF Mode** *busy* or *busy_noreply* has been selected.
Extension CF NoReply	The extension to which a call is to be forwarded if the call is not accepted. This field appears only if **CF Mode** *noreply* or *busy_noreply* has been selected.
Extension CF Uncond	The extension to which a call is to be forwarded if unconditional (immediate) call forwarding is selected. This field appears only if *uncond* has been selected for **CF Mode**.

Field	Meaning
NoReply Timer	A timer for forwarding a call. Defines when a call is to be forwarded if it is not accepted. The timer indicates the time in seconds. The preconfigured default value here is 15 s and the minimum value is 5 s. A practical range of values is between 8 s and 20 s. This field appears only if **CF Mode** *noreply* or *busy_noreply* has been selected.

Table 11-21: ***PABX*** ➧ ***CALL FORWARDING*** ➧ Editing an entry

To do Proceed as follows:

- Select the type of call forwarding you wish to configure for the edited extension under **CF Mode**.

When entering external extensions for configuring call forwarding, you must always enter the trunk prefix before the external extension.

The trunk prefix is either the number you dial before you make an external call or – with automatic external line access – the number you have configured as **Auto Dialout Number** for your telephone (see chapter 11.11, page 289).

- If applicable, enter the extension to which a call is to be forwarded under **Extension CF Busy**, **Extension CF NoReply** or **Extension CF Uncond**.
- If applicable, enter the time after which a call not accepted is to be forwarded under **NoReply Timer**.
- Leave the menu with **SAVE**.

  You return to the menu with the list of all extensions and can already see the settings made for the respective extension in the **CF Mode** column.
- Repeat the procedure described for all extensions for which call forwarding is to be configured.

11.11 Profiles

You can assign profiles to individual extensions or individual terminals (physical terminals and subsystems) in **XCENTRIC**.

A profile contains information about the **Auto Dialout Number** (trunk prefix for automatic external line access), the dial permissions of the respective terminal and the availability of the terminal.

The profiles are configured in the ***PROFILES*** menu and assigned to the terminals or extensions in the ***TERMINALS*** menu (see chapter 11.9, page 281) or the ***DIAL PLAN*** menu (see chapter 11.5, page 239).

XCENTRIC behaves as follows in terms of using the configured profiles:

1. The profile assigned to the extension is used.
2. If no profile is assigned to the extension, the profile assigned to the terminal is used.
3. If no profile is assigned to the terminal, the system profile (see chapter 11.3, page 212) is used.

The profile assigned to the extension therefore has the highest priority.

We recommend that the door intercom extension is assigned a profile that only permits internal availability (value for **Availability** is *internal*).

This prevents an external call operating the door opener via internal call forwarding. See chapter 11.3, page 212.

The ex works state includes three preconfigured example profiles that you can use if applicable.

Go to ***PABX*** ➧ ***PROFILES***:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][PROFILE]: Configure PABX Profiles                    MyXcentric

Name                    Auto Dialout No Dial Permission Availability
autodialout/full access 0                full            full
internal only           <none>           internal        internal
no dialout              <none>           internal        full

        ADD                 DELETE              EXIT

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

This menu shows a list of the profiles already configured. The figure above shows three profiles that are already preconfigured in the ex works state of **XCENTRIC**. These profiles are not assigned to any terminal in the ex works state.

Example profiles:

- *autodialout/full access*
  This profile contains automatic external line access with the trunk prefix *0*, full dialing access and external and internal availability.
- *internal only*
  This profile does not contain automatic external line access, i.e. no local prefix needs to be dialed for internal calls, only internal calls are allowed and the terminal is also only reachable internally.
- *no dialout*
  This profile does not contain automatic external line access, i.e. no local prefix needs to be dialed for internal calls, only internal calls are allowed and the terminal is reachable internally and externally.

The name of the profile, the Auto Dialout Number, the dial permissions and the availability are displayed. You will find a description of the meaning of these values in table 11-22, page 295.

You can delete and add profiles.

You can also delete profiles if they are assigned to extensions or terminals.

If a profile that was assigned to an extension or terminal is deleted, the next applicable profile applies according to priority (see note above).

Deleting a profile

To delete a profile, proceed as follows:

- Use the **Cursor** key to go to the profile to be deleted in the list in the ***PABX*** ➧ ***PROFILES*** menu.
- Press the **Space** bar.
  A **D** appears in front of the list entry.
- Press **DELETE**.
  The profile is deleted.

Configuring a new profile

Proceed as follows to configure a new profile:

- Press the **ADD** button in the ***PABX*** ➧ ***PROFILES*** menu.

You change to the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][ADD]: Configure PABX Profiles                          MyXcentric


    Profile              Profile 1

    Auto Dialout         on
    Number               0

    Dial Permissions     full

    Availability         full

        SAVE                        CANCEL

Enter string, max length = 31 chars
```

The menu contains the following fields:

For the individual permission levels, which are described in the following table for the **Dial Permission** field, note that a higher permission level always contains all the lower permission levels. The permission *national special* therefore also contains the permission levels *national*, *local* and *internal*.

The meanings stated here for the individual permissions are suggestions, which conform with the default lists generated automatically by **XCENTRIC** (see chapter 11.12, page 297). The actual meaning of the individual permissions (*local*, *national*, *national special* and *full*) naturally depend on your specific user configuration. See also chapter 11.12, page 297.

Field	Meaning
Profile	The name of the profile.
Auto Dialout	Here you can select whether automatic external line access is to be enabled for the profile. Possible values: ■ *on* (default setting) ■ *off* If you select *on*, a trunk prefix to be used for automatic external line access must be entered under **Number**. This means that the local prefix (#) must be dialed for setting up an internal connection and external connections are dialed without a trunk prefix (automatic external line access). If you set **Auto Dialout** to *off*, no prefix is dialed for internal calls. A trunk prefix must be dialed for setting up an external connection.
Number	Here you enter the dialing prefix for the system profile for automatic external line access if **Auto Dialout** is set to *on*. The **Number** field need not necessarily contain only the dialing prefix. You can, for example, enter the dialing prefix and the prefix of a call-by-call provider as **Number**.

Field	Meaning
Dial Permissions	Here you assign permission to create connections from the terminals (physical terminals and subsystems) connected to **XCENTRIC**. The descriptions of the individual values are suggestions in line with the default configuration for dial permissions. Refer to the note before this table. Possible values: ■ *internal* Allows only internal calls to be set up. ■ *local* Allows the setting up of internal calls and external calls restricted to the local network. Dialing free special numbers is also allowed. ■ *national* Allows the setting up of internal calls and external calls restricted to the national network. Dialing free special numbers is also allowed. Calls to mobile phone networks or added-value services are not allowed. ■ *national special* Allows the setting up of internal calls and external calls restricted to the national network. Free special numbers and connections to mobile phone networks and national added-value services are also allowed.
Dial Permissions	■ *full* (default value) Allows internal calls and all types of external calls to be set up.

Field	Meaning
Availability	Here you can set the availability of terminals (physical terminals and subsystems). Possible values: ■ *full* (default value) Terminals can be reached internally and externally. ■ *internal* Terminals can only be reached internally. ■ *external* Terminals can only be reached externally.

Table 11-22: ***PABX*** ➧ ***PROFILES*** ➧ ***ADD***

- Enter a name for the new profile under **Profile**.
- Select the value for **Auto Dialout**.
- If you have selected *on* for **Auto Dialout**, you must enter a dialing prefix for **Number**.
- Select **Dial Permission**.
- Select **Availability**.
- Leave the menu with **SAVE**.
  You have returned to the previous menu and the profile just configured is already shown in the list.
- Configure all the necessary profiles as described.

Profiles are assigned to terminals or extensions in the ***TERMINALS*** menu or in the ***DIAL PLAN*** menu. See chapter 11.9, page 281 and chapter 11.5, page 239.

If group extensions are assigned profiles in the ***DIAL PLAN*** menu, only the value for **Availability** is effective, as no outgoing calls can be initiated from a group extension.

11.12 Dial Permissions

The ***PABX*** ➧ ***DIAL PERMISSIONS*** menu is used for configuration of the dial permissions used for the various profiles. Dial permissions are used in the system profile (in the Setup Tool in the ***PABX*** ➧ ***STATIC SETTINGS*** menu) and in the profiles (***PABX*** ➧ ***PROFILES***) that can be assigned to a terminal or an extension (see also chapter 11.11, page 289).

Dial permissions can be modified for different countries using the ***PABX*** ➧ ***DIAL PERMISSIONS*** menu. Telephone provider prefixes can also be considered in the dial permissions and certain prefixes or numbers can be denied access throughout the system.

For Germany and France, default lists with relevant permissions can be created automatically, to which you only need to add your own local prefixes for *local* permission.

If the list of dial permissions in the ***DIAL PERMISSIONS*** menu is empty (see also chapter 11.12.1, page 298), then no configuration is available for the dial permissions. There are no limitations for dial permissions. Every profile that contains at least the *local* dial permission permits any external calls to be set up.

11.12.1 Configuration of Dial Permissions in the Setup Tool

You can see an illustration of the ***PABX*** ➧ ***DIAL PERMISSIONS*** menu in the Set-up Tool with the German default configuration in editing mode:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][Dial Permissions]: PABX Configuration                MyXcentric


    What to do              Edit Existing Table

    Number          Permission      Status      Description
    0               national        ok          national prefix    =
    00              full            ok          international pre-
fix|
    00800           local           ok          international free |
    0100??          provider        ok          alternative carrier|
    010[1-9]?       provider        ok          alternative carrier|
    0130            local           ok          old style national |
    01910           local           ok          T-Online account   v


        ADD                 DELETE                  EXIT


Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
What to do	This field contains the various options/modes available in this menu: ■ *Edit Existing Table* ■ *Reinitialize Table to Country Defaults* ■ *Clear Table* The options are explained in detail in table 11-24, page 301.
Reinit Table for Country	This field appears only if the *Reinitialize Table to Country Defaults* option is selected under **What to do**. You can then set this field to the country for which the default values are to be created. Possible values: ■ *Germany* ■ *France*

Field	Meaning
Number, **Permission**, **Status** and **Description**	If the *Edit Existing Table* option is set under **What to do**, you will see a list of the prefixes and permissions entered. ■ **Number** contains the initial digits of the extensions for which the permission applies. Note the use of the wildcards, which is described in table 11-27, page 308. ■ **Permission** contains the required permission. ■ **Status** describes if the entry is valid. ■ **Description** contains a description of the entry. You will find a supplementary description of the list entries in table 11-25, page 304.

Table 11-23: ***PABX*** ➧ ***DIAL PERMISSIONS***

Possible options/modes of the **What to do** field:

Possible Values	Meaning
Edit Existing Table	This option is for editing the entries in the list and creating new entries. You can add an entry by pressing the **ADD** button. See also table 11-25, page 304. Press the **DELETE** button to delete entries you have previously marked for deletion. You can edit an entry by tagging it and pressing **Return**.
Reinitialize Table to Country Defaults	With this option you can create a default list of prefixes for a certain country. Note that using this option deletes all the preceding entries, i.e. all the entries you have configured previously are lost. When you leave the **What to do** field, the **Reinit Table for Country** field appears, in which you can select the country for which the default list is to be created. See table 11-23, page 300. You can start this option – automatic generation of the list – by pressing the **Perform Operation** button. This list comprises suggested default values that can be optimized for the individual case. You must then edit the generated list to add your additional entries for *local* **Permission**. You can also add or edit other entries.
Clear Table	This option is for deleting the complete list of entries. You can start this option – deletion of the complete list – by pressing the **Perform Operation** button.

Table 11-24: **What to do**

Add an entry to the list of dial permissions with the **ADD** button or edit an entry to pass to the following menu:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][EDIT]: Configure Dial Permissions                    MyXcentric


Number                       0130
Permission                   local
Description                  old style national free numbers
Status                       ok

Hints:
    Number:  prefix of numbers to be dialed externally (i.e. w/o   =
             trunk prefix)                                          |
             sort of regular expressions allowed:                   |
             [ ... ]  denotes a set of digits, where ranges can be  |
                      given like 'a-b'; also the set can be inver-  |
                      ted by supplying '^' as first character in set|
                      examples:                                     |
                          [701]    =  0, 1, 7                       v

             SAVE                       CANCEL

Enter string, max length = 38 chars
```

This menu contains the following fields:

Field	Meaning
Number	The initial digits of the extensions for which the **Permission** is to apply. The number can be entered using wildcards, which are described in table 11-27, page 308.
Permission	**Permission** indicates the type of permission required for the prefix/digit string entered under **Number**. The following values are possible, which can be selected for a profile in the Setup Tool as **Dial Permission**: ■ *local* ■ *national* ■ *national special* ■ *full* The values ■ *provider* ■ *deny* can also be assigned. The values are described in detail in table 11-26, page 306.
Description	Here you can enter a brief description of the entry.

Field	Meaning
State	The value in this field indicates if the entry is valid. Three different values are possible: ■ *ok* ■ *format_error* ■ *exists_error* *ok* tags a valid entry. *format_error* indicates that a formal input error exists in the **Number** field. For example, invalid characters have been entered. *exists_error* indicates that a prefix or extension number is entered in the **Number** field that already exists as an entry or is covered by another entry using wildcards. Entries tagged with *format_error* or *exists_error* are not considered.
Hints	Offers you help for entering the values.

Table 11-25: ***PABX*** ➧ ***DIAL PERMISSIONS*** ➧ ***ADD/EDIT***

Possible values for the **Permission** field in the ***PABX*** ➧ ***DIAL PERMISSIONS*** ➧ ***ADD/EDIT*** menu:

For the individual permission levels, note that a higher permission level always contains all the lower permission levels. The permission *national special* therefore also contains the permission levels *national*, *local* and *internal*.

The meanings stated here for the individual permissions are suggestions, which conform with the default lists generated automatically by **XCENTRIC** (see table 11-24, page 301). The actual meaning of the individual permissions (*local*, *national*, *national special* and *full*) naturally depend on your specific user configuration.

Possible Values	Meaning
local	This permission allows the setting up of internal and external connections restricted to the local network. Dialing free special numbers is also allowed. Can be selected in the Setup Tool as **Dial Permission** for a profile.
national	This permission allows the setting up of internal and external connections restricted to the country. Dialing free special numbers is also allowed. Calls to mobile phone networks or added-value services are not allowed. Can be selected in the Setup Tool as **Dial Permission** for a profile.
national special	This permission allows the setting up of internal and external connections restricted to the country. Free special numbers and connections to mobile phone networks and national added-value services are also allowed. Can be selected in the Setup Tool as **Dial Permission** for a profile.
full	This permission allows the setting up of all kinds of internal and external connections. Can be selected in the Setup Tool as **Dial Permission** for a profile.
provider	*provider* is used for recognizing prefixes of alternative telephone providers for checking **Permissions**. For example, if *0100??* is configured as **Number** with *provider* as **Permission**, a number starting with "010012" is recognized as a telephone provider. Only the subsequent numbers are checked for permission. See the special form of the entry shown below.

Possible Values	Meaning
deny	The value *deny* is used to prevent dialing a prefix or an extension on a system-wide basis. For example, if *012345* is configured as **Number** with *deny* as **Permission**, this extension/prefix cannot be called from **XCENTRIC**.

Table 11-26: **Permission**

Special Form of Entry for *provider* Permission

In contrast to Germany, where the prefixes for alternative providers are placed in front of the default provider prefix, there are countries in which "0" at the start of the number for the default telephone provider must be replaced with the prefix of an alternative telephone provider (e.g. in France). A special form of entry with the value *provider* for **Permission** has been introduced for this.

The example below shows such a special form of entry:

A *local* dial permission exists for the digit string "0123", where "0" is the prefix of the default telephone provider. The entry with *provider* as **Permission** has the value *7:0* for the **Number** field, where *7* is the prefix of the alternative telephone provider, which **XCENTRIC** replaces with *0* for checking the permis-

sions. As a result, this example saves a second entry for *local* **Permission** for the digit string "7123".

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][EDIT]: Configure Dial Permissions                    MyXcentric


Number                       7:0
Permission                   provider
Description                  alternative provider
Status                       ok

Hints:
    Number:  prefix of numbers to be dialed externally (i.e. w/o   =
             trunk prefix)                                         |
             sort of regular expressions allowed:                  |
             [ ... ]  denotes a set of digits, where ranges can be |
                      given like 'a-b'; also the set can be inver- |
                      ted by supplying '^' as first character in set|
                      examples:                                    |
                          [701]    =  0, 1, 7                      v

             SAVE                       CANCEL


Enter string, max length = 38 chars
```

This makes it possible to configure all permission entries for only one telephone provider and to refer to the existing permission entries using the above-mentioned entries for alternative telephone providers. This avoids multiple input of permission entries for different telephone providers.

Wildcards for the Number Field

Wildcards that can be entered in the **Number** field:

Wildcard	Remarks	Example entry	matches …
?	Stands for any number.	0100??	010000 010001 010002 ... 010099
[...]	Describes a set of numbers, where …		
	■ the numbers can be consecutive.	0100[127]	01001 01002 01007
	■ Ranges can be indicated by "-".	0100[1-3]	01001 01002 01003
	■ the indicated set can be negated by "^". "^" may only be placed directly after the opening bracket, i.e. only the complete set can be negated.	0100[^3-9]	01000 01001 01002
	■ a combination of the above options can be used.	0100[^014-7]	01002 01003 01008 01009

Table 11-27: Wildcards for use in the **Number** field in the ***PABX*** ➧ ***DIAL PERMISSIONS*** ➧ ***ADD/EDIT*** menu.

Various Configuration Steps in *DIAL PERMISSIONS* Menu

The following points must be observed in connection with configuration in the ***DIAL PERMISSIONS*** menu:

- The permission level (**Permission**) assigned to the longest matching prefix/digit string (**Number**) is a prerequisite for setting up an external call.
  Example: The prerequisite for setting up a call with the number 0080012345 is **Permission** *local* (entry: **Number** is *00800* and **Permission** is *local* for free international numbers) and not **Permission** *full* (entry: **Number** is *00* and **Permission** is *full* for international numbers).
- The prefix/digit string entered for the **Number** field must be unique in the list of dial permissions.
  Example: If the list already contains an entry with *090[0-5]* for the **Number** field, a second entry must not be configured with *0904* in the **Number** field. Configuration errors are indicated by *exists_error* in the **Status** field for the last entry configured. See table 11-25, page 304.
- If you use the *Reinitialize Table to Country Defaults* option, at least the valid local entries (local prefix code) must be entered manually.

Configuring a default list

Proceed as follows to configure a default list of dial permissions automatically:

Note that automatic configuration of a default list of dial permissions deletes all the previous entries in the list.

➤ Go to ***PABX*** ➧ ***DIAL PERMISSIONS***.

➤ Select the *Reinitialize Table to Country Defaults* option in the **What to do** field.

➤ Select *France* or *Germany* in the **Reinit Table for Country** field, depending on which country you want to use the dial permissions for.

➤ Tag **Perform Operation** and press **Return** to start the option.

A default list of dial permissions is created for the relevant country. You can now adapt the list to suit your location and company.

Adding or editing an entry

Proceed as follows to change an entry in the list of dial permissions or add a new entry:

- Select an entry from the list in the ***PABX*** ➧ ***DIAL PERMISSIONS*** menu and press **Return** to edit an existing entry. Press the **ADD** button to add an entry.
- Enter a digit string for **Number** or modify the entry in the field.
- Select the **Permission**.
- Enter a description in the **Description** field or modify it.
  You only see the **Status** field if you have edited an existing entry. If a new entry is added, this field is not configured until the entry is saved.
- Leave the menu with **SAVE**.
- Check the list to see if the new/changed entry has the **Status** *ok*. If you receive an error message (see table 11-25, page 304), you must correct the entry, otherwise the entry remains ineffective.

  You have configured a new entry or adapted an existing entry.

Deleting the list

Proceed as follows to delete a list of dial permissions:

- Go to ***PABX*** ➧ ***DIAL PERMISSIONS***.
- Select the *Clear Table* option in the **What to do** field.
- Tag **Perform Operation** and press **Return** to start the option.

  All entries in the list of dial permissions have been deleted.

11.13 LCR (Least Cost Routing)

XCENTRIC is provided with an LCR function. Different telephone providers can be configured for different prefix areas and times of the day.

LCR is configured by loading an LCR configuration file, which you can create with the Windows application **BinTec LCR Manager**.

Below you will find an overview of the procedure for LCR configuration, followed by a description of the Setup Tool menu and finally detailed step-by-step instructions.

11.13.1 Overview

LCR is configured on **XCENTRIC** by the LCR configuration file, which you can create with the Windows application **BinTec LCR Manager**. You will find the **BinTec LCR Manager** application on your BinTec ISDN Companion CD or in the Download section of **XCENTRIC** at BinTec's web site.

After creating the LCR configuration file, transfer it via TFTP from your PC to **XCENTRIC**'s internal flash. The file is saved here under the name "boot_lcr". The configuration values for LCR are also loaded into **XCENTRIC**'s RAM.

You must now activate LCR.

You will find detailed step-by-step instructions for LCR configuration in chapter 11.13.3, page 317.

11.13.2 Menus for LCR

***LCR* menu**

You will find the ***LCR*** menu in the main menu of the Setup Tool. Select ***LCR*** to open this menu. The following illustration of the Setup Tool contains no real entries:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[LCR]: Least Cost Routing Settings                          MyXcentric

    Admin Status         enable
    Configuration >

Mon Nov 27  11:02:48  2000 (Workday) - Current Settings are:

Prefix                           Carrier              Access Code
0161                             Provider 3           01234
0170                             Provider 3           01234
0171                             Provider 3           01234
0172                             Provider 3           01234
0173                             Provider 3           01234
0176                             Provider 3           01234
0177                             Provider 4           05678

            SAVE                          EXIT

Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
Admin Status	Here you can activate (*enable*) or deactivate (*disable*) LCR for **XCENTRIC**.
Configuration	You pass via **Configuration** to a submenu in which you can transfer and load an LCR configuration file via TFTP. The menu is described below.
Prefix, Carrier, Access Code	This list shows the currently active LCR settings if LCR is activated in **Admin Status**. The line above shows the relevant date, day, time and day of the week (*Workday*, *Saturday*, *Sunday*). The list contains the **Prefix** (start of the number for which a certain telephone provider is to be dialed), the **Carrier** (name of the telephone provider) and the **Access Code** (prefix for the telephone provider).

Table 11-28: ***LCR***

LCR ➧ *CONFIGURATION* menu

Select the **Configuration** option in the ***LCR*** menu described above to open the menu for transferring and loading the LCR configuration:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[LCR][CONFIG]: LCR Configuration Handling                   MyXcentric


    Operation            Get: TFTP -> FLASH(boot_lcr)

    TFTP Server          192.168.1.1
    File Name            xc_lcr.csv

    Operation State      done


            START OPERATION              EXIT

Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
Operation	Operation you want to perform. See table 11-30, page 315.
TFTP Server	The IP address or host name (if the host name can be resolved) of the TFTP server from which you want to transfer an LCR configuration file.
File Name	Name of the LCR configuration file on the TFTP server; usually without path data. In exceptional cases, it may be necessary for certain Unix TFTP servers to enter the file name here with path data.
Operation State	Status of the last or currently executed operation.

Table 11-29: ***LCR*** ➧ ***CONFIGURATION***

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

Possible Values	Meaning
Get: TFTP -> FLASH(boot_lcr)	Transfer the LCR configuration file **File Name** from the TFTP host with the IP address **TFTP Server** to internal flash. In the flash, the LCR configuration file is given the name "boot_lcr". Any configuration file with the name "boot_lcr" that is already saved in the flash is overwritten. As the configuration file is transferred to the flash and not to the RAM, it is then necessary to execute *Load: FLASH(boot_lcr) -> MEMORY* to load the settings into the RAM of **XCENTRIC**.
Load: FLASH(boot_lcr) -> MEMORY	Loads the LCR configuration file "boot_lcr" from the internal flash to the RAM of **XCENTRIC**.
Update: Get + Load	This operation executes the two operations described above in succession. The LCR configuration file is transferred via TFTP into the internal flash of **XCENTRIC** and loaded into the RAM. Any configuration file with the name "boot_lcr" that is already saved in the flash is overwritten.

Table 11-30: **Operation**

The **Operation State** field can indicate the status of the operation *Get: TFTP -> FLASH(boot_lcr)* as follows:

Possible messages	Meaning
Running ...	The operation is being executed.
Done	The operation has been executed successfully.
Error	The operation could not be executed in full.

Table 11-31: **Operation State** for *Get: TFTP -> FLASH(boot_lcr)*

The **Operation State** field can indicate the status of the operation *Load: FLASH(boot_lcr) -> MEMORY* as follows:

Possible messages	Meaning
Running (<table>) ...	The operation is being executed. The *<table>* is being edited.
Done	The operation has been executed successfully.
Error (<table>)	The operation could not be fully executed. The operation was interrupted while loading the *<table>*.

Table 11-32: **Operation State** for *Load: FLASH(boot_lcr) -> MEMORY*

The **Operation State** field can indicate the status of the operation *Update: Get + Load* as follows:

Possible messages	Meaning
Running TFTP -> FLASH ... *Running FLASH -> MEMORY (<table>) ...*	The transfer from TFTP server into the internal flash of **XCENTRIC** or loading from the internal flash into RAM is being executed. The *<table>* is being edited in the second case.
Done	The operation has been executed successfully.
Error TFTP -> FLASH *Error FLASH -> MEMORY (<table>)*	The transfer from the TFTP server into the internal flash of **XCENTRIC** or loading from the internal flash into RAM could not be fully executed. The operation was interrupted in the second case while loading the *<table>*.

Table 11-33: **Operation State** for *Update: Get + Load*

The place marker *<table>* in table 11-32, page 316 and in table 11-33, page 316 represents the names of the LCR MIB tables *lcrtimezone*, *lcrroute* or *lcrcarrier*.

11.13.3 Step-by-Step Configuration Procedure for LCR

The individual steps for LCR configuration are described below. The description applies to both the initial configuration of LCR and to loading a new LCR configuration. This description uses the Windows application **BinTec LCR Manager** and the Setup Tool for the configuration of LCR.

The following three steps are necessary for configuring LCR on **XCENTRIC**:

1. Creating an LCR Configuration File.
2. Saving the LCR configuration file via TFTP to **XCENTRIC**'s internal flash EEPROM and loading the LCR configuration from the internal flash to **XCENTRIC**'s RAM.

The LCR configuration file can also be saved on the flash card of **XCENTRIC** and loaded from here into **XCENTRIC**'s RAM. See also chapter 16.2, page 474.

3. Activating LCR and saving the configuration.

Creating an LCR Configuration File

➤ Create the LCR configuration file using the Windows application **BinTec LCR Manager**. See also chapter 11.13.1, page 311.

Saving the LCR configuration file to the internal flash of XCENTRIC via TFTP and loading the LCR configuration into the RAM of XCENTRIC.

➤ Configure a TFTP server on a PC in your LAN and copy the LCR configuration file into the TFTP directory of the PC.
The DIME Tools of BinTec's BRICKware for Windows contain a TFTP server for a Windows PC. See the **BRICKware for Windows** documentation.

➤ Log in to **XCENTRIC** and start the Setup Tool. Select the ***LCR*** ➧ ***CONFIGURATION*** menu in the Setup Tool.

```
XCENTRIC Setup Tool                          BinTec Communications AG
[LCR][CONFIG]: LCR Configuration Handling                   MyXcentric


    Operation            Update: Get + Load

    TFTP Server          192.168.1.1
    File Name            xc_lcr.csv

    Operation State      done


            START OPERATION              EXIT

Use <Space> to select
```

➤ Make the necessary settings and carry out the operation *Update: Get + Load*. The LCR configuration is given the name "boot_lcr" in the internal flash of **XCENTRIC** so that the LCR tables from the configuration file are loaded automatically on system start. The LCR configuration is also loaded into **XCENTRIC**'s RAM.
Any configuration file with the name "boot_lcr" that is already saved in the flash is overwritten.
You will find detailed information about the ***LCR*** menu in chapter 11.13.2, page 312.

Activating LCR and Saving the Configuration

➤ To activate LCR on **XCENTRIC**, leave the ***LCR*** ➧ ***CONFIGURATION*** menu with **EXIT**. You have returned to the ***LCR*** menu.

The following illustration of the Setup Tool contains no real entries:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[LCR]: Least Cost Routing Settings                                MyXcentric

    Admin Status         enable
    Configuration >

Mon Nov 27  11:02:48  2000 (Workday) - Current Settings are:

Prefix                              Carrier              Access Code
0161                                Provider 3           01234
0170                                Provider 3           01234
0171                                Provider 3           01234
0172                                Provider 3           01234
0173                                Provider 3           01234
0176                                Provider 3           01234
0177                                Provider 4           05678

            SAVE                            EXIT

Use <Space> to select
```

- Select *enable* in the **Admin Status** field and leave the menu with **SAVE**.
- Leave the Setup Tool with **Save as boot configuration and exit**.

LCR is now active with the configuration loaded from the LCR configuration file. The current configuration has been saved, so that LCR also remains active after restarting **XCENTRIC**.

For a detailed description of LCR and the LCR configuration file, please refer to the Download section of **XCENTRIC** at www.bintec.net.

11.14 BinTec CS300 System Telephones

BinTec Communications AG offers BinTec CS300 system telephones specially designed for use with **XCENTRIC**. These system telephones offer you a number of convenient features. You will find a summary of which features of the BinTec CS300 system telephone are implemented for the respective software release level of **XCENTRIC** at http://www.bintec.de/XCENTRIC/de/loesungen/index.html.

The following chapters contain an overview of the configuration of system telephones and detailed step-by-step instructions that you must follow to carry out the installation and configuration of the BinTec CS300 system telephones.

11.14.1 Overview of Configuration Elements in the Setup Tool and MIB

Setup Tool

In the Setup Tool, *system phone* can be selected as type for the terminal configuration. If this is selected, the serial number of the respective system telephone must also be selected.

The ***PABX*** ➧ ***TERMINAL*** ➧ ***ADD/EDIT*** menu contains these settings:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[PABX][TERMINAL][EDIT]: Configure PABX Terminals            MyXcentric


    Destination              physical
    Module                   Slot 3 Unit 3
    Terminal Type            system phone
    Profile                  <none>
    Systel Serial No.        001234567

    Terminal Name            3:3 - Phone 1



    Assigned Extensions      1
    View Assigned Extensions >

    SAVE                                 CANCEL

Use <Space> to select
```

The value *system phone* is available for the **Terminal Type** field. If this value is selected, the **Systel Serial No.** field appears.

The **Systel Serial No.** field contains a list of serial numbers of system telephones currently assigned to this internal S_0 connection or which have unsuccessfully attempted to log in to this unit since the system start of **XCENTRIC**. Serial numbers already assigned to other terminals no longer appear here.

The internal serial number of the system telephone is required here, which is read from the system telephone software. This internal serial number is not the serial number printed on the package of the telephone or on the telephone itself.

The procedure for selecting the correct serial number is described in chapter 11.14.2, page 324.

MIB

The PABX group in the MIB contains the **systelTerminalTable** for the system telephones.

The **systelTerminalTable** contains the following variables:

```
xcentric:> systelTerminalTable

inx   SerialNo(*rw)      AutoMove(-rw)       SWVersion(ro)
      RelDate(ro)        Country(ro)         OEMString(ro)
      DBVersion(ro)      Slot(ro)            Unit(ro)
      Tei(ro)
```

Table 11-34: **systelTerminalTable**

The MIB **systelTerminalTable** mainly contains values that are read automatically from the system telephones connected and are needed for support purposes.

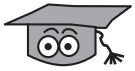
The following variables in the table are important for configuration of the system telephones:

Variable	Meaning
SerialNo	The internal serial number of the system telephone, which is read from the system telephone software. The internal serial number required here is not the serial number printed on the package of the telephone or on the telephone itself. This serial number is also used to reference the telephone in the relevant entry in the **pabxTerminalTable** in the variable **SystelSerialNo**. The assignment is made via the Setup Tool and the settings in the ***PABX*** ➧ ***TERMINAL*** ➧ ***ADD/EDIT*** menu, as described in "Setup Tool", page 320.
AutoMove	The **AutoMove** variable can contain the values ■ *enable* ■ *disable* (default value) If this value is set to *enable*, it is possible to move the relevant system telephone to another internal S_0 connection (to another unit or another slot) without affecting the functionality of the phone. The entry in the **systelTerminalTable** and the slot and unit in the **pabxTerminalTable** or in the ***TERMINAL*** menu of the Setup Tool are appropriately modified automatically on moving the **XCENTRIC** telephone.

Table 11-35: Individual variables in the **systelTerminalTable**

If you want to change the **AutoMove** variable for a certain system telephone, you must do this via the Configuration Manager or the SNMP shell.

A description of the SNMP shell is given in the Software Reference.



The following information may be useful for you if you are used to working with the SNMP shell and the MIB:

It is possible to read serial numbers of system telephones and their login status from the entries in the **systelTerminalTable**. The variables **SerialNo**, **Slot** and **Unit** contain information about the serial number of the system telephone and the slot and unit to which the telephone is logged in or has attempted to log in. The **Tei** variable, which contains the layer 2 TEI value if the system telephone has successfully logged in, can also be used to read the login status of the telephone. If this **Tei** variable contains the default value *127*, this means that the system telephone with the serial number corresponding to the entry was not logged in or incorrectly logged in. Incorrect means that the serial number in the ***TERMINALS*** menu or the **pabxTerminalTable** was not configured at all or incorrectly or that the system telephone was connected to another unit or slot without setting the **AutoMove** variable to *enable*. **XCENTRIC** cannot access the system telephone in both cases.

11.14.2 Step-by-Step Instructions for Installation of the BinTec CS300

Proceed as follows to log in a system telephone to **XCENTRIC**:

- Keep the **ESC** key of the BinTec CS300 pressed while plugging in to the internal S_0 connection; this gives you access to the BIOS of the system telephone.
- Now press the **Info** soft key on the telephone.
  The serial number of the telephone appears in the telephone display for 10 seconds.
- Note the serial number of the telephone (with preceding zeroes) and the slot and unit to which the telephone was connected.
- To leave the BIOS of the telephone, select the **Update** soft key and then the **Abort** soft key.

  The telephone is now connected and you can continue the configuration, for which you need the serial number you have just noted, in the Setup Tool of **XCENTRIC**.

- Go to ***PABX*** ➧ ***TERMINALS*** in the Setup Tool.
- Enter a new terminal for the system telephone here, or edit the entry if you have already configured an entry for the system telephone.
  You will find detailed information about the configuration of terminals with the Setup Tool in chapter 11.9, page 281.

To configure a new terminal for the system telephone, proceed as follows:

- Select a **Destination**. For the system telephone, select *physical*.
- Select the relevant slot and unit to which you have connected the system telephone under **Module**.
- Select *system phone* as type of terminal under **Terminal Type**.
- Under **Systel Serial No.** select the right serial number of the telephone. This is the serial number you made a note of when you connected the telephone.
- If applicable, select a profile from the list of configured profiles under **Profile**.
- Enter a terminal name for **Terminal Name**.
- Leave the menu with **SAVE**.

  You return to the menu with the list of terminals and can already see the entry you have just configured for the system telephone in the list.
- If the entry for the system telephone was already configured in the ***TERMINALS*** menu and you edit it to configure the system telephone, modify the individual fields of the menu as just described. Once you have made all the changes, leave the menu with **SAVE**.

11.14.3 LEDs on the BinTec CS300 System Telephone

Connections currently in progress are not indicated directly after programming the LEDs of the short-code and function keys of the system telephone or directly after connecting the system telephone. The LEDs only indicate connections that are set up after programming.

11.15 PABX MIB Tables

If you want to configure the PABX via the SNMP shell, you will find all the MIB tables that affect the PABX functionality in the **pabx** group.

Some of the PABX features cannot be configured with the Setup Tool at the moment, only in the MIB tables.

A description of the structure of the MIB tables can be found in the MIB Reference on BinTec's WWW server.

12 Configuring PCs in your LAN

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

- Remote TAPI/CAPI configuration
  Configuration of the CAPI/TAPI interface on the PCs enables you to use communication applications such as CTI (see chapter 13, page 335) and Unified Messaging.
- Settings for data connections
  You may have to make various settings on your PCs in the LAN to permit data transmission over **XCENTRIC**.

12.1 Remote CAPI/TAPI Interface Configuration

Enter **XCENTRIC** as CAPI/TAPI server in the Remote CAPI/TAPI configuration program.

The **XCENTRIC** CAPI/TAPI server provides the following facilities:

- Operating communications applications on every PC in the network (e.g. CTI, Unified Messaging).
- Simultaneous ISDN access over communications applications from several PCs.

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

All extensions configured for a physical terminal (telephone) and a certain user are also passed internally to the CAPI of this user.

This functionality makes it possible to configure answering machine software for such an extension on the basis of BinTec's Remote CAPI, in which the user and extension are set according to the terminal configuration of **XCENTRIC**. The answering machine function must be configured with a time delay.

BinTec's Voice Mail Server provides the answering machine function via call forwarding. See the User's Guide for the Voice Mail Server at www.bintec.net.

If a user is to use CAPI services such as fax, an extension entry must be made for this user for the CAPI subsystem, as otherwise no outgoing connections can be made from the CAPI. See chapter 11.5.5, page 259.

You have already installed BRICKware on the first PC and have opened the configuration window for Remote CAPI/TAPI configuration. You can shortly proceed with chapter 12.1.2, page 329. You must first install the CAPI and TAPI configuration program for all the other PCs in the network, as described in the next chapter.

12.1.1 Installing the CAPI and TAPI Configuration Program

To do

- Insert the BinTec ISDN Companion CD in the CD-ROM drive and wait for setup to start. If the Start window does not open automatically, click your CD-ROM drive in Windows Explorer and double-click **setup.exe**.
- Select **BRICKware** in the window and continue with the setup until you reach router selection.
- Select **XCENTRIC** and click **Next**.
- Select **Remote CAPI Client** and **TAPI Service Provider** in the component selection window.
- Click **Next**.

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

12.1.2 Configuring the Remote CAPI/TAPI

- Enter **XCENTRIC**'s IP address, e.g. ***192.168.1.254*** in the **Remote CAPI** tab.
- Enter the user name and password as configured on **XCENTRIC**. 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.
- Make the same settings in the **Remote TAPI** tab.

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

- **XCENTRIC**'s IP address is correct.
- You have entered a valid user name.
- The right port number is entered, 2662 for **Remote CAPI** and 2663 for **Remote TAPI**. The port numbers must agree with the port numbers configured on **XCENTRIC**.
- Your PC has been configured as a DHCP client and perhaps does not yet have an IP address.

➤ If no error message appears, click **OK**.

➤ Repeat the Remote CAPI/TAPI installation on all PCs in the network on which you want to use communications applications (e.g. Unified Messaging, CTI).

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

12.2 Configuring a PC

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

- If you have not configured **XCENTRIC** as a DCHP server with the Configuration Wizard (or the Setup Tool) and the PCs do not yet have any IP addresses, you will have to carry out the following (as per the next chapter):
  - 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 the next chapter. In this case, **XCENTRIC** 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 12.2.2, page 332.

12.2.1 Telling the PC the IP Address, Gateway and DNS

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

A TCP/IP protocol must be installed before the following configuration work can be carried out (see chapter 9.1.1, page 142).

Proceed as follows:

➤ Click the Windows Start button and then **Settings** ➧ **Control Panel**.

➤ Double click **Network**.

Windows 95/98

➤ Click **TCP/IP** ➧ **Properties**.

➤ Enter a unique IP address for your PC and the netmask in the **IP Address** tab, e.g. ***192.168.1.1*** and ***255.255.255.0.***

- Enter **XCENTRIC**'s IP address, e.g. ***192.168.1.254,*** in the **Gateway** tab. Click **Add**.
- If you do not have your own DNS server, enter **XCENTRIC**'s IP address in the **DNS Configuration** tab under **DNS Server Search Order**, e.g. ***192.168.1.254***.

Windows NT

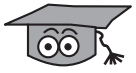
- Select the **Protocols** tab. Click **TCP/IP Protocol** ➧ **Properties**.
- Click **Specify IP Address** in the **IP Address** tab and set the IP address, netmask and default gateway, e.g. ***192.168.1.254***, ***255.255.255.0*** and ***192.168.1.1***. Enter the IP address of **XCENTRIC** as default gateway.
- Click **Add** in the **DNS** tab under **DNS Server Search Order** and enter **XCENTRIC**'s IP address, e.g. ***192.168.1.254***.

And finally,

- Confirm all entries and restart your PC.
- Repeat the installation for all the PCs in your network.

12.2.2 Finding PCs on your Partner's Network

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



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

We recommend using the DNS Proxy function of **XCENTRIC** for name resolution, which can replace the administration of HOSTS files. This is explained in chapter 14.3.2, page 380.

The settings for DNS Proxy can also be made in the Configuration Wizard.

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

Caution!

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

➤ To avoid unintentional charges, it is essential that you monitor your **XCENTRIC**. See also chapter 17, page 489 and the "Important Information on ISDN Charges" in the Download section of **XCENTRIC** on BinTec's website at www.bintec.net.

You can only use the following process if you have not configured extensive NetBIOS filtering in the Expert Mode of 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. You can find out more about configuring this access in Solutions & Products/ FAQ's at www.bintec.net in the section: BRICK/test access.

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

- Click the Windows Start button and then **Find** ➧**Files and Folders...**.
- Type in `lmhosts.*`.
- Click **Find now**.
- Open the file found with a text editor.
- Type in the IP address of the PC in the partner network, followed by a tab or space, followed by the name of the PC, e.g. `10.1.1.1 BossPC`. Save and close the file under the name lmhosts.
- Repeat the same procedure for each PC in the partner network that you want to reach over Windows.
- Click the Windows Start button and then **Find** ➧ **Computer...**.
- Type in the name of the PC, e.g. ***BossPC***, and click **Find now**.

  The name of the PC appears after a moment.

Creating a shortcut on the desktop

- To avoid having to look for the PC every time you restart, right-click the PC icon in the computer window and click **Create Shortcut**.

  You are then asked if you want the shortcut to be placed on the desktop.
- Click **Yes**.

  Now you can connect to the ***BossPC*** on your partner's network at any time.

Network drive mapping

Alternatively, you could establish a network drive connection:

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

13 BinTec CTI Phone (Server and Standalone Version)

The BinTec CTI phone (server and standalone version) from BinTec Communications AG is an OEM version of the OSITRON CTI software. The BinTec CTI phone in conjunction with BinTec's modern communications server **XCENTRIC** meets the requirements for a complete CTI solution. If applicable, the software key for the BinTec CTI phone is shown on your license card.

13.1 Introduction

The BinTec CTI phone is available in a server-based version and in a standalone version:

- BinTec CTI server
  The BinTec CTI server is a CTI solution based on central administration by a Windows NT server.
  The Windows NT server administrates the CTI users in the LAN via the central NT user administration. The CTI phone server, which is based on the NT server, provides facilities for administrating a central address book and a common short-code dialing list. A central journal facility is also available, even if the clients (CTI phone extensions) are switched off.
  Another advantage of the server-based CTI solution is central administration of the installation procedure and subsequent software updates.

- BinTec CTI phone standalone
  The BinTec CTI phone standalone is a network-based CTI solution without a central server. The individual PCs are connected to **XCENTRIC** over BinTec's Remote TAPI. The user administration is controlled by **XCENTRIC**'s PABX user concept.
  In contrast to the server solution, it is not possible to centrally administrate the address book, short-code dialing list and journal with this variant.
  The software installation takes place directly on each PC.

13.1.1 BinTec's Remote TAPI Concept

BinTec's unique Remote TAPI concept permits a CTI solution without the physical connection of telephones and PCs. Communication between telephony terminals and the individual PCs is over **XCENTRIC** in both cases described above.

BinTec CTI server

With the BinTec CTI server, **XCENTRIC** provides the NT server with control over all the telephone extensions via BinTec's Remote TAPI. The user **TAPIadmin** is available for this purpose in BinTec's PABX user concept (see chapter 13.2.3, page 339). The NT server (BinTec CTI server) communicates with the PCs over the Microsoft interface TAPI 2.1.

BinTec CTI phone standalone

With the BinTec CTI phone standalone solution, the PCs are connected to **XCENTRIC** over BinTec's Remote TAPI. The BinTec Remote TAPI Service Provider (TSP) is installed on the PCs for this purpose. This is available in a 16-bit version for Windows 95 and 98 and in a 32-bit version for Windows NT. BinTec's Remote TAPI Service Provider is network-capable and compatible with Microsoft TAPI 2.1.

Headset support

BinTec's Remote TAPI supports the use of headsets in conjunction with CTI applications. The *headset* setting (see chapter 11.9, page 281) is only suitable for headsets (in connection with CTI applications) that operate on the principle of a permanently lifted cradle switch.

13.1.2 User Documentation

BinTec's ISDN Companion CD contains the document "cti_eng.pdf" (English version) in the "docs/CTI/" directory. The document "cti_eng.pdf" contains the installation and operation of the BinTec CTI phone (server and standalone version).

Please follow the documentation for installation and operation of the BinTec CTI phone (server and standalone version).

It is possible that different designations are used for the following terms in the documentation:

- BinTec CTI server
  "OSITRON tel server" is also used.
  Describes the NT server-based installation of the CTI software.
- BinTec CTI phone (stand-alone)
  "OSITRON tel server" is also used.
  Describes the standalone installation of the BinTec CTI phone without NT server.
- BinTec CTI phone (extensions/client)
  "OSITRON tel client", "OSITRON tel workstation" or "OSITRON tel extension are also used.
  Describes the actual CTI application on the PC.

13.2 BinTec CTI Server

The BinTec CTI server is a CTI solution based on the use of a Windows NT server as BinTec CTI server in the LAN.

The following figure shows the setup of a CTI solution with the BinTec CTI server:

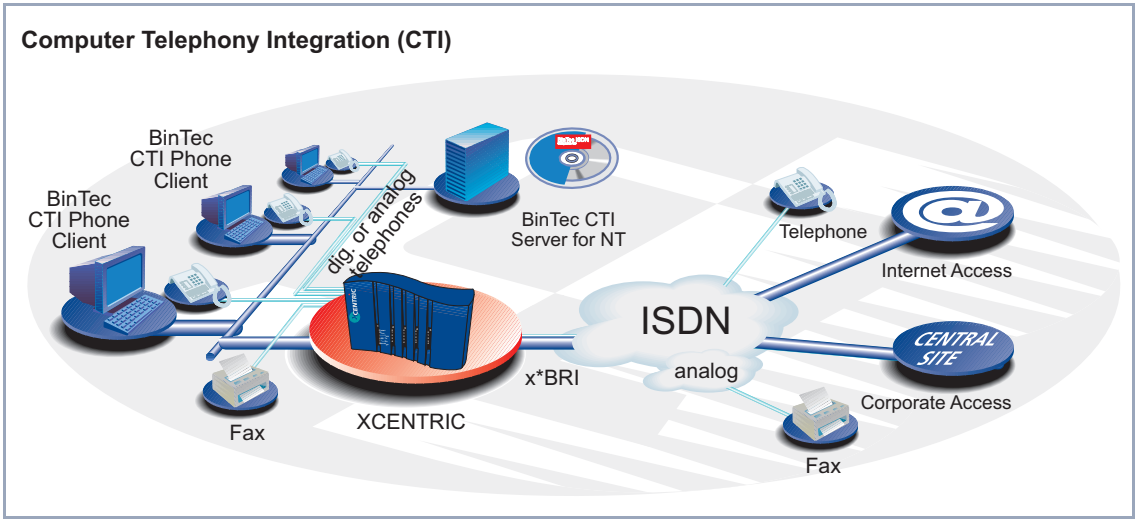


Figure 13-1: Possible scenario with BinTec CTI server

13.2.1 Requirements

The following system requirements must be fulfilled for installation of the BinTec CTI server:

- BinTec CTI server
  Windows NT server version 4.0, Service Pack 4 or later
- BinTec CTI phone extensions
  Windows 95/98 or
  Windows NT workstation/server 4.0

For further system requirements (e.g. memory), please see the user documentation for the BinTec CTI phone.

13.2.2 Functionality

XCENTRIC provides the BinTec CTI server based on the Windows NT server with all the TAPI and user information about the user **TAPIadmin** (see chapter 13.2.3, page 339). The CTI server is connected to the LAN over **XCENTRIC** using BinTec's network-capable Remote TAPI interface.

The BinTec CTI server administrates a central address book and a central short-code dialing list to which all CTI phone extensions have access. There is also a centrally administrated journal, which can be used by all extensions and can always be accessed, even if CTI phone extensions are switched off.

All data are installed and administrated on an enabled network drive or on a network path under an enable name, which keeps the administrative effort for this CTI solution relatively low.

An important functional requirement for the BinTec CTI server solution is that the BinTec CTI server and BinTec CTI phone extensions must be located in the same Windows NT domain.

13.2.3 TAPIadmin User

The **TAPIadmin** user has all rights to all lines on **XCENTRIC**. Lines in this context mean the access paths of the TAPI to the telephones.

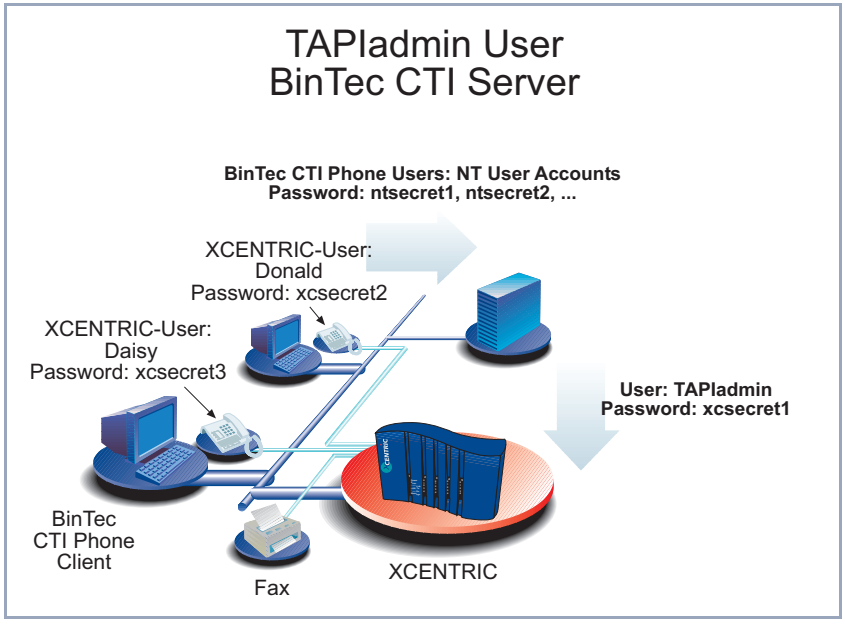


Figure 13-2: TAPIadmin user

When using BinTec's CTI server, it is possible to configure the **TAPIadmin** user on the NT server with the password set in **XCENTRIC** when configuring BinTec's Remote TAPI. This enables you to access and control all the lines of **XCENTRIC** from the NT server.

The **TAPIadmin** user is preconfigured on **XCENTRIC**. This user does not appear in the list of users in the Setup Tool.

Password configuration for the **TAPIadmin** user is made in **XCENTRIC**'s Setup Tool in the ***PABX*** ➧ ***STATIC SETTINGS*** menu: You will find a description of the configuration and important information on configuring the **TAPIadmin** user in chapter 11.3, page 212.

13.2.4 Installation

The installation of the BinTec CTI server must be carried out in the following order:

1. Complete configuration of **XCENTRIC**'s PABX (see **XCENTRIC** User's Guide), in which you must configure a secret password for the **TAPIadmin** user in the ***PABX*** ➧ ***STATIC SETTINGS*** menu (see chapter 11.3, page 212).
2. Installation of the BinTec Remote TAPI Service Provider (TSP) on the Windows NT server. The BinTec Remote TAPI Service Provider is part of BRICKware for Windows and is included on the BinTec ISDN Companion CD.
   After installation and configuration of the BinTec Remote TAPI Service Provider (TSP), check that all lines (terminal names) connected to **XCENTRIC** can be seen in the info field. The **TAPIadmin** user must be entered with the corresponding password in the TAPI configuration user field.
3. Installation of the BinTec CTI server on the Windows NT server. Insert BinTec's ISDN Companion CD and click "BinTec CTI Software" in CD-Setup or double click the "Setup.exe" file in the "\CTIServer\" directory.
   Further information can be found in the documentation for the BinTec CTI phone.
4. Installation of the BinTec CTI phone extensions on the PCs in the LAN. The installation is carried out via an enabled network drive or a network path under an enable name. The Remote TAPI Service Provider (TSP) for TAPI 2.1 is also installed automatically at the same time, if applicable.
   Further information can be found in the documentation for the BinTec CTI phone.

13.3 BinTec CTI Phone Standalone

The BinTec CTI phone standalone is the network-based CTI solution, which is suitable for use for LANs in which no NT server is available.

The interaction between the CTI software and telephones is over **XCENTRIC**. In this connection, **XCENTRIC** acts as a TAPI server for the clients.

The following figure shows the setup of a CTI solution with the BinTec CTI phone standalone:

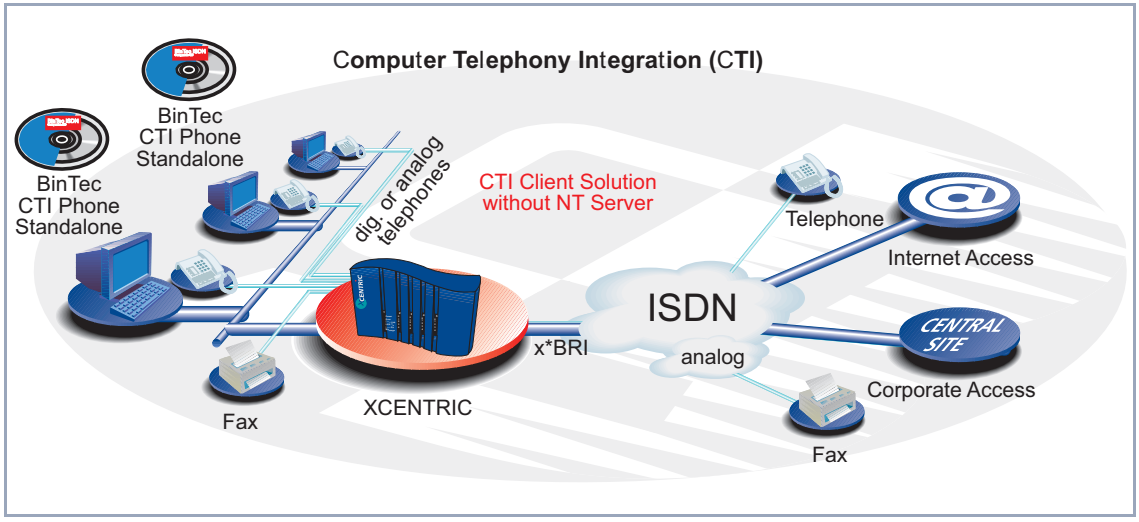


Figure 13-3: Possible scenario with BinTec CTI phone standalone.

The CTI phone standalone is installed on the PCs in the LAN that are connected to **XCENTRIC** over the BinTec Remote TAPI Service Provider (TSP). Data administration (address books, short-code lists and journal) is decentralized to the individual PCs. The user administration is implemented by **XCENTRIC**'s PABX user concept.

13.3.1 Requirements

The system requirements for LAN PCs on which the BinTec CTI phone standalone is to be installed are Windows 95/98 or Windows NT workstation/server 4.0 operating systems.

For further system requirements (e.g. memory), please see the user documentation for the BinTec CTI phone.

13.3.2 Functionality

In a LAN in which all PCs (over **XCENTRIC**'s hub component) and the telephones are connected to **XCENTRIC**, BinTec's Remote TAPI can be used for connecting the BinTec CTI phone standalone to telephones connected to **XCENTRIC**.

The BinTec CTI phone standalone is connected over the BinTec Remote TAPI Provider interface installed on the PC to the TAPI server on **XCENTRIC**, which in turn controls the corresponding telephony terminal.

The PABX user concept integrated in the PABX part of **XCENTRIC** is used to provide secure user administration to control access to the TAPI data.

13.3.3 Installation

The installation of the BinTec CTI phone standalone on the PCs in the LAN must be carried out in the following order:

1. Complete configuration of the PABX on **XCENTRIC** (see User's Guide for **XCENTRIC**), in which all telephony terminals to be controlled by each CTI phone standalone application must be assigned to the same user.
2. Installation of the BinTec Remote TAPI Service Provider (TSP) on the PC. The BinTec Remote TAPI Service Provider is part of BRICKware for Windows and is included on the BinTec ISDN Companion CD.
   After installation and configuration of the BinTec Remote TAPI Service Provider (TSP), check that the corresponding lines (terminal names) can be

seen in the info field. The first configured user must be entered in the user field of the TAPI configuration.

3. Installation of the BinTec CTI phone standalone on the PC. Insert BinTec's ISDN Companion CD and click "BinTec CTI Software" in CD-Setup or double click the "Setup.exe" file in the "\CTIServer\" directory.
   Further information can be found in the documentation for the BinTec CTI phone.

13.4 Restrictions and Troubleshooting for the BinTec CTI Phone (Server and Standalone Version)

Some features of the BinTec CTI phone software are not supported by **XCENTRIC**:

- Charging information.
- Call forwarding and configuring an answering machine.
- The "hold/brokering" and "three-party conference" features are not supported for ISDN telephones.

13.4.1 Calling Line Identification

Calling line identification with the BinTec CTI phone (chapter 10.2 of the BinTec CTI phone documentation) is currently only possible under a certain condition:

The extensions must not be entered in the directory in the internationally valid extension number format (described in chapter 9.2 of the BinTec CTI phone documentation), but must be entered as a string of digits without the international prefix code but with the local prefix code, e.g. "024194698100". The prefix "0" must also always be entered with the local prefix code. Even if you are in the same local area as the subscriber you enter in the directory, you must still enter the local prefix code for the extension.

13.4.2 Questions, Troubleshooting and Help

You will find the answers to further questions about the BinTec CTI phone in the "checklist.rtf" file. You can find this file after installation in the installation directory "program", e.g. under "C:\programs\BinTec\program\".

Information about support for the BinTec CTI phone can be found in the chapter "Support" in the documentation for the BinTec CTI phone (cti_eng.pdf).

14 Advanced Router Configuration

This chapter contains more configuration options for the router part of **XCENTRIC** 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 10, page 149.

The following configuration steps are described:

- General ➤➤ **WAN** Settings
- Settings Specific to WAN Partners
- Basic ➤➤ **IP** Settings
- Modem Profile
- ➤➤ **IPX** Settings
- Bridging
- Extra License Functions

Use the Credits Based Accounting System (see chapter 15.1.3, page 424). This enables you to set a limit for data connections to **XCENTRIC** to prevent unnecessary charges accumulating as a result of mistakes made during configuration.

14.1 General WAN Settings

General WAN functions:

- **XCENTRIC** as dynamic IP address ➤➤ **server**
- General ➤➤ **PPP** settings

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

14.1.1 Dynamic IP Address Server

IP address pools

XCENTRIC 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, **XCENTRIC** first checks whether a host route is entered in the routing table for this caller. If not, **XCENTRIC** 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*** ➧ ***DYNAMIC IP ADDRESSES (SERVER MODE)***
- ***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 14-1: ***IP*** ➧ ***DYNAMIC IP ADDRESSES (SERVER MODE)***

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

Table 14-2: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***

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

Table 14-3: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

To do Proceed as follows:

- Go to ***IP*** ➧ ***DYNAMIC IP ADDRESSES (SERVER MODE)*** ➧ **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**.

14.1.2 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 10.2.1, page 167). If a call is received, **XCENTRIC** 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, **XCENTRIC** receives no calling line number. The caller therefore cannot be identified by CLID, even if the caller is entered as a WAN partner. **XCENTRIC** 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, **XCENTRIC** 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, **XCENTRIC** accepts the incoming call.

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

Field	Meaning
Authentication Protocol	Defines the PPP authentication protocol offered to the caller first. Possible values: ■ *PAP:* PAP only ■ *CHAP:* CHAP only ■ *CHAP + PAP:* first CHAP, then PAP ■ *MS-CHAP:* MS-CHAP only ■ *CHAP + PAP + MS-CHAP:* first CHAP, if rejected then the protocol required by the caller ■ *none:* no PPP authentication
Radius Server Authentication	Settings for RADIUS server authentication. For further information about RADIUS, see the Software Reference.
PPP Link Quality Monitoring	Defines whether Link Quality Monitoring is executed for PPP connections. Possible values: ■ *no*, is not executed. ■ *yes*, the connection statistics are stored in the ➤➤ **MIB** table **biboPPPLQMTable**.
PPPoE Ethernet Interface	Defines the interface used by PPP-over-Ethernet for using an ADSL connection (see chapter 10.2.4, page 200).

Table 14-4: ***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 **Link Quality Monitoring**, e.g. *no*.

➤ Press **SAVE**.

14.2 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
- Channel Bundling
- Layer 1 Protocol
- IP Transit Network
- Transfer of DNS and WINS Server IP Addresses to WAN Partner
- ➤➤ **RIP**
- Compression: ➤➤ **VJHC**, ➤➤ **STAC**, MS-STAC
- ➤➤ **Proxy ARP**

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

14.2.1 Delay after Connection Failure

This function enables you to set the period of time **XCENTRIC** 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 **XCENTRIC** tries again after an attempt to establish a connection has failed.

Table 14-5: ***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**.

14.2.2 Channel Bundling

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

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

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

If you use the Bandwidth On Demand function (see chapter 14.2.3, page 356), the settings for Channel Bundling are replaced by the settings made for Bandwidth On Demand; the **Channel Bundling** field is grayed out in the Setup Tool.

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 complete connection.

Table 14-6: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***

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

Possible Values	Meaning
no	No channel bundling, only one B-channel is ever available for connections.
dynamic	Dynamic channel bundling.
static	Static channel bundling.

Table 14-7: *Channel Bundling*

To do Proceed as follows:

- Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***.
- Select **Channel Bundling**.
- Enter **Total Number of Channels**.
- Confirm with **OK**.
- Press **SAVE**.

14.2.3 Bandwidth on Demand (BoD)

This function permits dynamic bundling of leased lines with dialup lines to cope with large amounts of data. You have the following options:

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

If you use the Bandwidth On Demand function, the settings for **Channel Bundling** (see chapter 14.2.2, page 354) are replaced; the **Channel Bundling** field is grayed out in the Setup Tool.

Switching B-channels in and out

An additional B-channel is switched in 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 switching out 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 switched out. 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.

Authentication

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

Configuration is made in:

- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS*** ➧ ***EXTENDED INTERFACE SETTINGS (OPTIONAL)***
- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***WAN NUMBERS*** ➧ **ADD** (menu description in chapter 10.2.1, page 167)
- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***PPP*** (menu description in chapter 10.2.1, page 167)

Field	Meaning
Mode	Defines which mode is used for BOD. Possible values: see table 14-9, page 358.
Line Utilization Weighting	Defines how the line utilization is calculated. Possible values: ■ *equal:* All the measured values of throughput in **Line Utilization Sample (sec)** are weighted equally for the calculation (default value). ■ *proportional:* 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*).
Maximum Number of Dialup Channels	Maximum permitted number of channels that are opened for dialup connections.

Table 14-8: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS*** ➧ ***EXTENDED INTERFACE SETTINGS (OPTIONAL)***

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

Possible Values	Meaning
Bandwidth On Demand Disabled	Deactivates BOD, no additional channels are opened (default value).
Bandwidth On Demand Enabled	(For dialup connections only) Activates BOD, additional channels can be opened. The connection partner who initiated the connection opens the additional channels.
Backup	(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**.
Bandwidth On Demand Active	(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 switching in and out additional B-channels on demand.
Bandwidth On Demand Passive	(For leased lines only) Enables BOD and defines the passive partner. This page does not activate switching in and out additional channels.

Table 14-9: **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 **Maximum Number of Dialup Channels**.
- Press **SAVE**.
- 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**.

14.2.4 Layer 1 Protocol (ISDN B-Channel)

ISDN B-channel

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

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

Field	Meaning
Layer 1 Protocol	Defines which Layer 1 Protocol **XCENTRIC** 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 14-10: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***

For incoming calls that cannot be identified from the calling party number, **XCENTRIC** uses as Layer 1 Protocol the settings under **Layer 1 Protocol** in ***PABX*** ➧ ***DIAL PLAN*** for the **Destination** *ppp* (see chapter 11.5.4, page 255).

Layer 1 Protocol contains the following selection options:

Possible Values	Meaning
ISDN 64 kbps	For 64-kbps ISDN data connections. This is the default value.
ISDN 56 kbps	For 56-kbps ISDN data connections.
Modem	For modem connections. Modem profile 1 is used here as the default. This value is only available in **XCENTRIC** if the fax modem module (XFM-Fax) is installed in **XCENTRIC**.
DOVB	Data transmission Over Voice Bearer - useful in the USA, for example, where voice connections are sometimes cheaper than data connections.
V.110 (1200 ... 38400)	For connections to V.110 at bit rates of 1200 bps, 2400 bps,..., 38400 bps.
Modem Profile 1 ... 8	Selects a certain modem profile. See chapter 14.4, page 404. These values are only available in **XCENTRIC** if the fax modem module (XFM-Fax) is installed in **XCENTRIC**.
PPTP PNS	For VPN interface.
PPP over Ethernet (PPPoE)	For connections to ADSL (see chapter 10.2.4, page 200).

Table 14-11: *Layer 1 Protocol*

Most of the entries in *Layer 1 Protocol* correspond to the entries in **Layer 1 Protocol** in ***PABX*** ➧ ***DIAL PLAN*** for the **Destination** *ppp* (see chapter 11.5.4, page 255).

To do Proceed as follows:

➤ Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***.

- Select **Layer 1 Protocol**.
- Confirm with **OK**.
- Press **SAVE**.

14.2.5 IP Transit Network

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

- You enter the ➤➤ **IP address** and ➤➤ **netmask** of the partner or partner network. You must obviously have this information available.
- You use an additional ISDN IP address each for **XCENTRIC** 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.

This is shown in the diagram below:

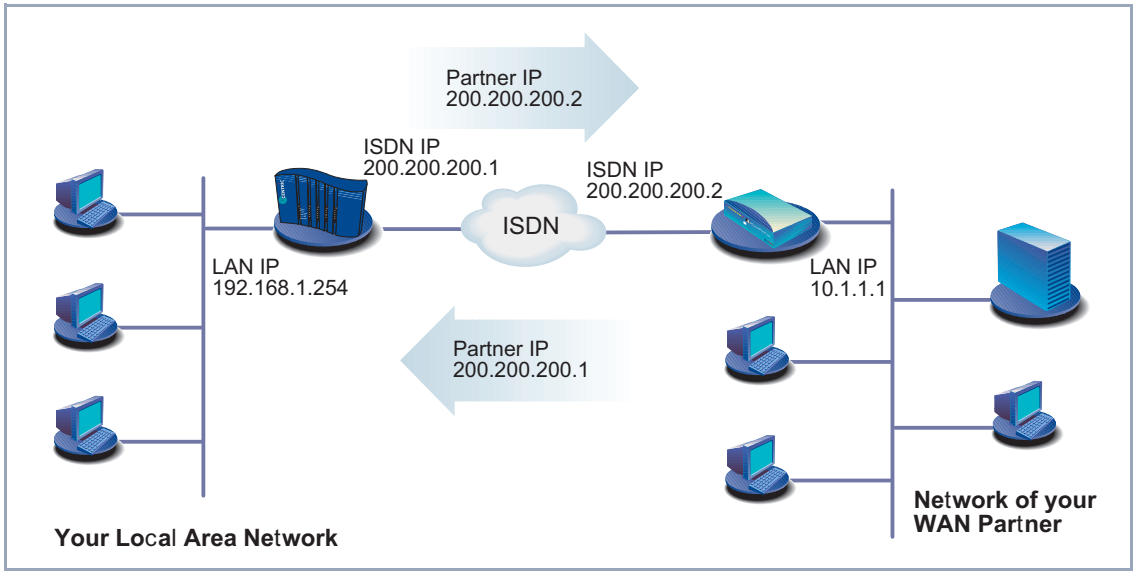


Figure 14-1: LAN-LAN link with transit network

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

Field	Meaning
IP Transit Network	Defines whether **XCENTRIC** sets up a transit network to the WAN partner.
Local IP Address	IP address of **XCENTRIC**. Appears only for the following value of **IP Transit Network**: *no*. 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.
Local ISDN IP Address	ISDN IP address of **XCENTRIC** 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	WAN partner's LAN netmask. If you make no entry, **XCENTRIC** enters a default netmask for the net class used under *Partner's LAN IP Address*.

Table 14-12: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***

IP Transit Network contains the following selection options:

Possible Values	Meaning
yes	A transit network is used.
dynamic client	**XCENTRIC** receives its IP address from the WAN partner for the duration of the connection.
dynamic server	**XCENTRIC** assigns the ➤➤ **Remote** WAN partner an IP address for the duration of the connection. In this case, **XCENTRIC** must be configured as a dynamic IP address server, i.e. it has an IP address pool available (see chapter 14.1.1, page 348).
no	No transit network. This setting is adequate for most WAN partners.

Table 14-13: *IP Transit Network*

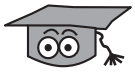
To do Proceed as follows:

- 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**.

14.2.6 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 a Domain Name Server, 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, **XCENTRIC** 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 **XCENTRIC** itself. How to configure the DNS Proxy function is described in chapter 14.3.2, page 380.

When you enter a WAN partner in **XCENTRIC**, you can define whether **XCENTRIC** 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 **XCENTRIC**'s first global Domain Name Server (DNS).
Secondary Domain Name Server	IP address of another global Domain Name Server.
Primary WINS	IP address of **XCENTRIC**'s first global WINS (Windows Internet Name Server) or NBNS (NetBIOS Name Server).
Secondary WINS	IP address of another global WINS or NBNS.

Table 14-14: ***IP*** ➧ ***STATIC SETTINGS***

Field	Meaning
Dynamic Name Server Negotiation	In the event of dynamic name server negotiation, defines whether **XCENTRIC** 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 14-15: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

The **Dynamic Name Server Negotiation** field contains the following selection options:

Possible Values	Meaning
off	**XCENTRIC** does not send or answer requests for WINS or DNS IP addresses.
yes	The response is linked to the mode for issuing/receiving an IP address (setting in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** under **IP Transit Network**): ■ **XCENTRIC** sends requests for name server addresses to the WAN partner if *dynamic client* is selected. ■ **XCENTRIC** answers requests for name server addresses from the WAN partner if *dynamic server* is selected. ■ **XCENTRIC** answers but does not send requests for name server addresses if *yes* or *no* is selected.
client (receive)	**XCENTRIC** sends requests for name server addresses to the WAN partner.
server (send)	**XCENTRIC** answers requests from the WAN partner for name server addresses.

Table 14-16: **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 (see chapter 14.3.2, page 380):

➤ 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 **XCENTRIC** to report the name server addresses entered to the WAN partner (Server Mode) or if other name server addresses other than those in the LAN are to be used for connections to the WAN partner (Client Mode, e.g. for dialing in to an Internet Service Provider):

- Go to ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***.
- Select **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.

14.2.7 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 10.2.1, page 167), 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. **XCENTRIC** 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. **XCENTRIC** can do both.

WAN partner

If you negotiate to receive and/or send RIP packets from/to your WAN partner, **XCENTRIC** 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 **XCENTRIC**'s routing functionality.

RIP packets do not set up or hold ISDN connections.

Configuration is made in:

- ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***
- ***CM-100BT, Fast 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 14-17: ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings*** or ***CM-100BT, Fast Ethernet*** ➧ ***Advanced Settings***

RIP Send and **RIP Receive** contain the following selection options:

Possible Values	Meaning
none	Not activated.
RIP V1	Enables sending and receiving of RIP packets in version 1.
RIP V2	Enables sending and receiving of RIP packets in version 2.
RIP V1 + V2	Enables sending and receiving of RIP packets in both version 1 and version 2.

Table 14-18: **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-100BT, Fast Ethernet*** ➧ ***Advanced Settings***.
- Select **RIP Send**.
- Select **RIP Receive**.
- Press **SAVE**.

14.2.8 Compression

Data compression You can increase the data throughput and so reduce the connection costs by using ➤➤ **data compression**. **XCENTRIC** supports several options, depend-

ing on the ➤➤ **encapsulation** selected, e.g. PPP (see chapter 10.2.1, page 167):

- ➤➤ **STAC**:
  The industry standard STAC data compression (Check Mode 3 in RFC 1974) implemented in **XCENTRIC** 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.
- ➤➤ **V.42bis**:
  Compression algorithm that requires a security layer. Only possible with *Encapsulation* = *Multi-Protocol LAPB Framing* or *LAPB Framing (only IP)*.
- 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, **XCENTRIC** 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 14-19: ***WAN Partner*** ➧ ***Edit***

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

Possible Values	Meaning
none	No compression.
STAC	Enables STAC data compression (if *Encapsulation* = *PPP*).
MS-STAC	Enables STAC data compression for dialing into a Windows Remote Access Server (if *Encapsulation* = *PPP*).
MPPC	Not available in **XCENTRIC**.
V.42bis	Enables data compression with V.42bis (if *Encapsulation* = *Multi-Protocol LAPB Framing* or *LAPB Framing (only IP)*).

Table 14-20: **Compression**

Field	Meaning
Van Jacobson Header Compression	Enables VJHC.

Table 14-21: ***WAN Partner*** ➧ ***Edit*** ➧ ***IP*** ➧ ***Advanced Settings***

STAC, MS-STAC, V.42bis

Proceed as follows to set STAC, MS-STAC or V.42bis:

- 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**.

14.2.9 Proxy ARP (Address Resolution Protocol)

ARP requests

The ➤➤ **Proxy ARP** function enables **XCENTRIC** 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 **XCENTRIC** and the desired host can be reached over a defined WAN connection, **XCENTRIC** answers the ARP request with its own hardware address. This is sufficient for establishing the connection: The ➤➤ **data packets** are sent to **XCENTRIC** and then forwarded to the desired host.

This is shown in the diagram below:

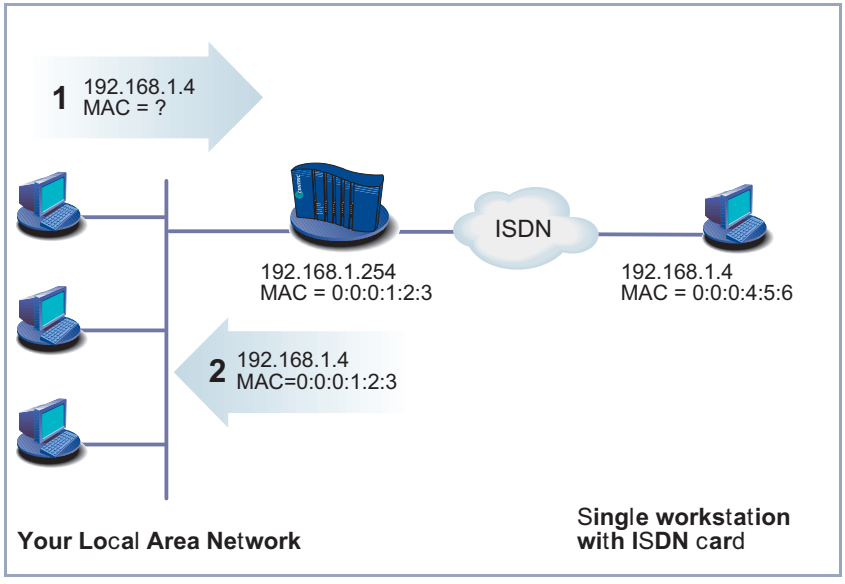


Figure 14-2: Proxy ARP

Configuration is made in:

- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***
- ***CM-100BT, FAST ETHERNET*** ➧ ***ADVANCED SETTINGS***

Field	Meaning
Proxy Arp	Enables **XCENTRIC** to answer ARP requests.

Table 14-22: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** or ***CM-100BT, FAST ETHERNET*** ➧ ***ADVANCED SETTINGS***

Proxy Arp in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** contains the following selection options:

Possible Values	Meaning
off	Disables Proxy ARP via the interface to the WAN partner.
on (up or dormant)	**XCENTRIC** answers an ARP request only if the status of the connection to the WAN partner is *up* (active) or *dormant* (idle). In the case of *dormant*, **XCENTRIC** only answers the ARP request; the connection is not set up until someone actually wants to use the route.
on (up only)	**XCENTRIC** 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 14-23: **Proxy Arp**

Proxy Arp in ***CM-100BT, FAST ETHERNET*** ➧ ***ADVANCED SETTINGS*** contains the following selection options:

Possible Values	Meaning
off	Disables Proxy ARP via the LAN interface.
on	Enables Proxy ARP via the LAN interface.

Table 14-24: **Proxy Arp**

To do Proceed as follows:

- Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.
- Select **Proxy Arp**.
- Press **SAVE**.
- Press **SAVE**.
- Go to ***CM-100BT, FAST ETHERNET*** ➧ ***ADVANCED SETTINGS***.
- Select **Proxy Arp**.
- Press **SAVE**.
- Press **SAVE**.

14.3 Basic IP Settings

Here you will find a number of basic settings you can define in **XCENTRIC**:

- Deriving system time
- Name resolution (➤➤ **DNS**) in **XCENTRIC**
- ➤➤ **port** numbers
- ➤➤ **BOOTP** Relay Agent

The necessary configuration steps are explained below.

14.3.1 System Time

System time

You need the system time to obtain correct timestamps for recording connection data (for accounting).

Configuration is made in ***IP*** ➧ ***STATIC SETTINGS***:

Field	Meaning
Time Protocol	Protocol used to derive the current time. Possible values: ■ *TIME/UDP* ■ *TIME/TCP* ■ *SNTP* ■ *ISDN* ■ *none*
Time Offset (sec)	Number of seconds added to or subtracted from the derived time. If you enter values between -24 and +24, **XCENTRIC** interprets the input as the number of hours and converts it to the corresponding number of seconds automatically after you press **SAVE**. Note: If you select *ISDN* as **Time Protocol**, you must set the **Time Offset** to *0*. If you change **Time Offset (sec)** (turn back the time), there should be no data flow.
Time Update Interval (sec)	Time interval in seconds, after which the system time is checked and updated if necessary. If you enter values between 1 and 24, **XCENTRIC** interprets the input as the number of hours and converts it to the corresponding number of seconds automatically after you press **SAVE**. For **Time Protocol** = *TIME/UDP*, *TIME/TCP* or *SNTP*: Current time is checked after every *Time Update Interval* in seconds. For **Time Protocol** = *ISDN:* Current time is checked for each first ISDN connection after expiry of the **Time Update Interval**.

Field	Meaning
Time server	IP address of the time ➤➤ **server** used by **XCENTRIC**. **Time Server** is not needed if you set *ISDN* as **Time Protocol**.

Table 14-25: ***IP*** ➧ ***STATIC SETTINGS***

The **Time Protocol** field contains the following selection options:

Possible Values	Meaning
TIME/UDP	System time (RFC 868) via ➤➤ **UDP**.
TIME/TCP	System time (RFC 868) via ➤➤ **TCP**.
TIME/SNTP	System time as per SNTP (Simple Network Time Protocol, RFC 1769) via UDP.
ISDN	System time from ISDN ➤➤ **D-channel** (free).
none	System time not derived.

Table 14-26: **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**.

  After the first ISDN connection has been ended, **XCENTRIC** derives the system time from the ISDN.

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**.

  XCENTRIC now derives the system time via a time server. **XCENTRIC** 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 **XCENTRIC**.

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.

14.3.2 Name Resolution in XCENTRIC 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 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:
  HOSTS files are located on the PCs in the LAN. You can use these files to create a table of host names with associated addresses. This means connections to DNS are no longer needed to resolve these names. As the HOSTS files must be updated on each PC, this method of name resolution is not very practicable.

In practice, the DNS of the Internet Service Provider is often used for name resolution.

Advantages of Name Resolution with XCENTRIC

XCENTRIC 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 **XCENTRIC**.

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 **XCENTRIC** as DNS on the relevant PCs. DNS requests are passed by the PC to **XCENTRIC** 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 **XCENTRIC** as DHCP server.

Forwarding entries enable **XCENTRIC** to decide which DNS is to be used for the resolution of certain names. If, for example, you have configured two WAN partners in **XCENTRIC**, 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 **XCENTRIC** 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 **XCENTRIC**. This means that once a name has been resolved and is required again, **XCENTRIC** can answer the request from the cache and a new request to an external name server is not necessary. These requests can therefore be answered more quickly, bandwidth is reduced on the WAN connections and the costs of unnecessary connections are saved.

If a DNS request cannot be answered by any of the DNS asked, this is saved in the cache as a negative dynamic entry. As failed DNS requests (requests that cannot be answered) are not usually saved by applications or IP stacks, these negative dynamic entries in the cache prevent frequent unsuccessful connection setups to external DNS.

The validity of the positive dynamic entries in the cache is given by the TTL (Time To Live), which is contained in the DNS record. Negative entries are assigned the value **Maximum TTL for Neg Cache Entries**. A dynamic entry is deleted from the cache when the TTL expires.

Static name entries

You use positive static entries to enter names with the associated IP addresses in **XCENTRIC**. If you save frequently needed IP addresses in this way, **XCENTRIC** 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 **XCENTRIC**. 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 14-31, page 392).

Filter function

By using negative static entries, you can limit name resolution in **XCENTRIC** 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 **XCENTRIC** 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 **XCENTRIC** or another name server (see chapter 18.1, page 500). To obtain help information for the command, enter `nslookup -?`.

Other Options

Global name server

In ***IP*** ➧ ***STATIC SETTINGS***, you can also enter the IP address of preferred global name servers that are to be asked if **XCENTRIC** cannot answer requests itself or with forwarding entries.

For local applications, the IP address of **XCENTRIC** or the loopback address (127.0.0.1) can be entered as global name server.

If necessary, **XCENTRIC** 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 **XCENTRIC** 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 **XCENTRIC** can be sent or the address of **XCENTRIC** itself. In the latter case, DNS requests from the DHCP clients are sent to **XCENTRIC**, which either answers these itself or passes them on if necessary (proxy function).

Exchanging DNS Addresses with WAN Partners

IPCP The same applies if the dynamic negotiation of name servers is activated for the IP configuration of a WAN partner and **XCENTRIC** 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 **XCENTRIC** itself can also be sent for name server negotiations via IPCP to the WAN partner, who is the IP address client.

If **XCENTRIC** 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 **XCENTRIC**. These can be entered as global name servers in **XCENTRIC** and are thus available for future name resolutions.

Strategy for Name Resolution in XCENTRIC

A DNS request is handled by **XCENTRIC** 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 **XCENTRIC** or the loopback address is entered for local applications, these are ignored here.
   – If a DNS can resolve the name, the information is forwarded and a dynamic entry created in the cache.
   – If none of the DNS asked can resolve the name or no static name servers are entered, see 4.
4. Is a WAN partner selected as default interface?
   In this case, the associated DNS are asked. If the connection to the WAN partner is not active, an attempt is made to set it up.
   – If a DNS can resolve the name, the information is forwarded and a dynamic entry created in the cache.
   – If none of the DNS asked can resolve the name or no default interface has been selected, see 5.
5. Is overwriting the global name server addresses admissible (**Overwrite Global Nameserver** = *yes*)?
   In this case, a connection is set up to the first WAN partner, which is configured so that addresses of DNS can be sent – provided this has not previously been attempted. If name server negotiation is successful, these are entered as global name servers and are therefore available for further requests.
6. Request is answered with server error.

If one of the DNS answers with "non-existent domain", this answer is forwarded to the source of the request immediately and included in the cache as negative entry.

Overview of Configuration with the Setup Tool

The configuration and monitoring of name resolution in **XCENTRIC** 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 **XCENTRIC**'s Domain Name.
Primary Domain Name Server	IP address of **XCENTRIC**'s first global Domain Name Server (DNS).
Secondary Domain Name Server	IP address of another global Domain Name Server.
Primary WINS	IP address of **XCENTRIC**'s first global WINS (Windows Internet Name Server) or NBNS (NetBIOS Name Server).
Secondary WINS	IP address of another global WINS or NBNS.

Table 14-27: *IP* ➧ *STATIC SETTINGS*

IP ➧ ***DNS*** contains the following fields:

Field	Meaning
Positive Cache	Enables positive dynamic entries in the cache. Possible values: ■ *enabled* (default value): Successfully resolved names and IP addresses are saved in the cache. ■ *flush*: All positive dynamic entries in the cache are deleted. ■ *disabled*: 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	Enables negative dynamic entries in the cache. Possible values: ■ *enabled* (default value): Names that could not be resolved are saved in the cache as negative entries. ■ *flush*: All negative dynamic entries in the cache are deleted. ■ *disabled*: 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	Defines whether the addresses of global name servers in **XCENTRIC** (in ***IP*** ➧ ***STATIC SETTINGS***) may be overwritten with name server addresses sent by WAN partners. Possible values: ■ *yes* (default value) ■ *no*

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	Defines which name server addresses are sent to the DHCP client if **XCENTRIC** is configured as DHCP server. Possible values: ■ *none*: No name server address is sent. ■ *self* (default value): The address of **XCENTRIC** is sent as name server address. ■ *global*: The addresses of the global name servers entered in **XCENTRIC** are sent.
IPCP Assignment	Defines which name server addresses are sent by **XCENTRIC** to a WAN partner for dynamic name server negotiation. Possible values: ■ *none*: No name server address is sent. ■ *self*: The address of **XCENTRIC** is sent as name server address. ■ *global* (default value): The addresses of the global name servers entered in **XCENTRIC** 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 14-28: ***IP*** ➧ ***DNS***

IP ➧ ***DNS*** ➧ ***STATIC HOSTS*** ➧ ***ADD*** contains the following fields:

Field	Meaning
Default Domain:	The Domain Name of **XCENTRIC** 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. *.bin-tec.de). 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: ■ *positive* (default value): A DNS request for **Name** is answered with a DNS record, which contains the associated **Address**. ■ *ignore*: A DNS request is ignored; no answer is given (not even a negative answer). ■ *negative*: A DNS request for **Name** is answered with a negative answer.
Address	(Only for **Response** = *positive*) IP address, which is assigned to **Name**.
TTL	Period of validity in s for the assignment of **Name** to **Address** (only relevant for **Response** = *positive*). This value is displayed in the TTL field (Time To Live) if **XCENTRIC** sends a corresponding DNS record. Default value: *86400* (= 24 h)

Table 14-29: ***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 **XCENTRIC** entered in ***IP*** ➧ ***STATIC SETTINGS*** is displayed.
Name	Host name that is to be resolved with this forwarding entry. May also contain wildcards (only at the start of **Name**, e.g. *.bintec.de). If an incomplete name is entered without a dot, this is completed with ".**Default Domain**" after confirming with **SAVE**.
Interface	Defines the WAN partner to which a connection is set up for the resolution of **Name**.
TTL	Period of validity in s for the assignment of **Name** to **Address**. Default value: *86400* (= 24 h) If the request from **XCENTRIC** 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 **XCENTRIC** 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 14-30: ***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	Defines the type of dynamic entry. Possible values: ■ *positive*: A DNS request for **Name** is answered with the associated IP address from the cache. ■ *negative*: A DNS request for **Name** is answered with a negative answer from the cache.
TTL	Indicates how many seconds the dynamic entry remains in the cache. The entry is deleted on expiry of **TTL**. 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. When a negative dynamic entry is saved in the cache, **Maximum TTL for Neg Cache Entries** is always assigned as this value.
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 14-31: ***IP*** ➧ ***DNS*** ➧ ***DYNAMIC CACHE***

IP ➧ ***DNS*** ➧ ***ADVANCED SETTINGS...*** contains the following fields:

Field	Meaning
Maximum Number of DNS Records	Defines the maximum number of static and dynamic entries. 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. If **Maximum Number of DNS Records** is reduced by the user, dynamic entries are also deleted, if necessary. 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!
Maximum TTL for Pos Cache Entries	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**.
Maximum TTL for Neg Cache Entries	Is assigned as **TTL** to a negative dynamic entry in the cache.

Table 14-32: ***IP*** ➧ ***DNS*** ➧ ***ADVANCED SETTINGS...***

IP ➧ ***DNS*** ➧ ***GLOBAL STATISTICS...*** contains the following fields (the menu is updated by pressing the **UPDATE** button):

Field	Meaning
Received DNS Packets	Displays the number of received DNS packets, 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 14-33: ***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 **XCENTRIC** 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 14-34: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

The **Dynamic Name Server Negotiation** field contains the following selection options:

Possible Values	Meaning
off	**XCENTRIC** does not send or answer requests for name server addresses.
yes	The response is linked to the mode for issuing/receiving an IP address (setting in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** under **IP Transit Network**): ■ **XCENTRIC** sends requests for name server addresses to the WAN partner if *dynamic client* is selected. ■ **XCENTRIC** answers requests for name server addresses from the WAN partner if *dynamic server* is selected. ■ **XCENTRIC** answers but does not send requests for name server addresses if *yes* or *no* is selected.
client (receive)	**XCENTRIC** sends requests for name server addresses to the WAN partner.
server (send)	**XCENTRIC** answers requests from the WAN partner for name server addresses.

Table 14-35: **Dynamic Name Server Negotiation**

Procedure for Configuration with the Setup Tool

To do Proceed as follows to configure name resolution with DNS Proxy in **XCENTRIC**:

Name resolution in XCENTRIC

If applicable, first enter the global name servers in **XCENTRIC**:

➤ 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**.

XCENTRIC <–––> WAN partner

Proceed as follows if you would like to configure a WAN partner so that the address of a name server is sent from **XCENTRIC** to the WAN partner or from the WAN partner to **XCENTRIC**, as applicable:

- Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.
- Select **Dynamic Name Server Negotiation**.
- Confirm with **OK**.
- Press **SAVE**.

Monitoring and statistics

How to obtain a list of dynamic entries in the cache:

If your network contains PCs using the Windows 2000 operating system, these frequently send DNS requests of the SRV type. As these requests are usually answered negatively, the DNS Proxy function of **XCENTRIC** prevents the setup of such unnecessary connections.

If the negative dynamic cache of the DNS Proxy function is enabled (in the **Negative Cache** field in the ***IP*** ➧ ***DNS*** menu), these unnecessary connection setups are avoided automatically by dynamic negative entries. The dynamic entries are deleted after the TTL time expires (default setting is one day; configurable in the ***IP*** ➧ ***DNS*** ➧ ***ADVANCED SETTINGS*** menu). After deletion of the dynamic negative entry, a connection is set up again with a DNS request of the Windows 2000 PC, from which a negative cache entry is again generated immediately if the request is answered negatively. This in turn prevents further connection setups during the TTL time. If you also wish to avoid this one connection setup after expiry of the TTL time, you can tag the relevant dynamic entry in the ***IP*** ➧ ***DNS*** ➧ ***DYNAMIC CACHE*** menu as static.

➤ 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.

14.3.3 Port Numbers

What is a ➤➤ port?

XCENTRIC 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 **XCENTRIC**. This addresses the relevant application. Ports are only used in the TCP and UDP protocols.

XCENTRIC forwards incoming ➤➤ **data packets** to the port with the number associated with the desired application. This addresses the relevant **XCENTRIC** 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 **XCENTRIC**'s HTTP status page (see chapter 15.1.4, page 428).

Table 14-36: ***IP*** ➧ ***STATIC SETTINGS***

You will find the **Remote TAPI Server Port** in the ***PABX*** ➧ ***STATIC SETTINGS:*** menu.

Field	Meaning
Remote TAPI Server Port	Port number for Remote TAPI connections: 2663 (defined by IANA, www.iana.com).

Table 14-37: ***PABX*** ➧ ***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**.

Change the **Remote TAPI Server Port** accordingly in the ***PABX*** ➧ ***STATIC SETTINGS*** menu.

14.3.4 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.

This is shown in the diagram below:

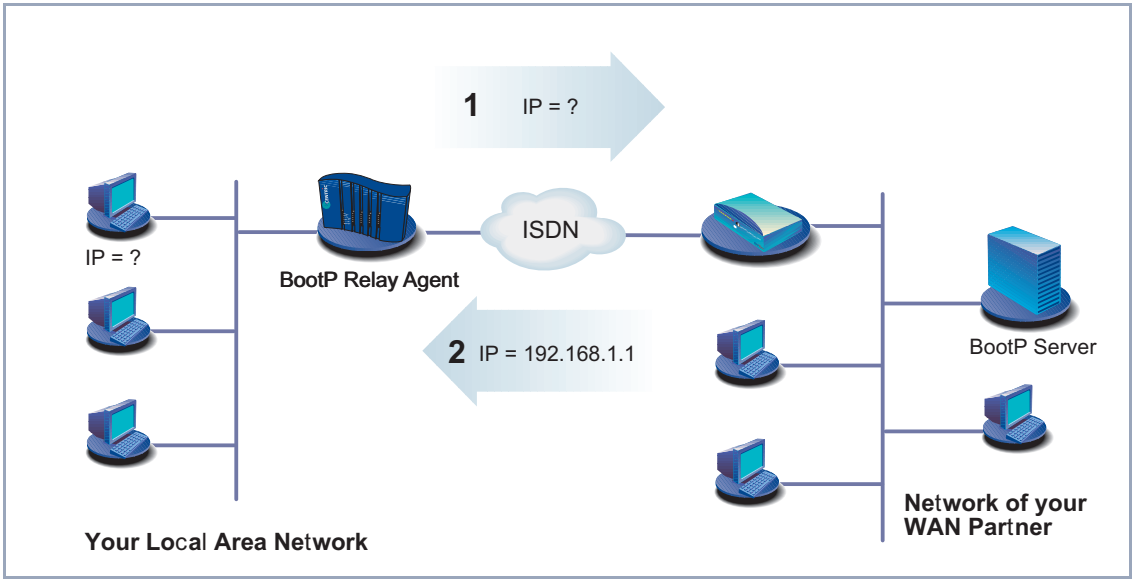


Figure 14-3: **XCENTRIC** as BOOTP Relay Agent

Configuration is made in ***IP*** ➧ ***STATIC SETTINGS***:

Field	Meaning
BOOTP Relay Server	IP address of the BOOTP server.

Table 14-38: ***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 10.2.1, page 167).

14.4 Modem Profile

The ***MODEM*** menu is only available if the fax modem module (XFM-Fax) is installed in **XCENTRIC**.

The ***MODEM*** submenu gives you the option of defining modem profiles. The default profile is Profile 1, which is used automatically for a modem connection to an analog far end station.

You should not normally make any changes in this menu, as the transmission speed is negotiated automatically and all the desired modem connections are set up.

You can, however, use the modem profiles to limit the transmission speed of the modem by entering the parameters used.

A modem status display can be found in the ***MONITORING*** ➧ ***MODEM*** menu.

14.5 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

14.5.1 General Settings

Here you will find the global parameters for IPX. These settings apply to all IPX connections of **XCENTRIC**.

The configuration is made in ***IPX***:

Field	Meaning
Local System Name	IPX system name of **XCENTRIC** using upper case letters, numbers and -: /.
Internal Network Number	**XCENTRIC**'s internal network number. This value must be unique among all the network numbers and normally comprises the last four bytes of **XCENTRIC**'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: ■ *yes*: low cost for IPX-WAN connections ■ *no*
Enable SPX Spoofing	Enables and disables spoofing of SPX session watchdog packets. Possible values: ■ *yes*: low cost for SPX sessions over WAN connections ■ *no*
NetBIOS Broadcast Replication	Defines how **XCENTRIC** handles ➤➤ **NetBIOS** packets.

Table 14-39: ***IPX***

NetBIOS Broadcast Replication contains the following selection options:

Possible Values	Meaning
yes	All NetBIOS hosts in the network can access each other, even if WAN connections must be set up frequently. Cost-intensive!
no *on LAN only*	NetBIOS hosts in the LAN can only access each other if they do not need WAN connections to be set up. Low cost.

Table 14-40: **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**.

14.5.2 Configuring the LAN Interface

The next step is to configure **XCENTRIC**'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 **XCENTRIC** does not have this information, **XCENTRIC** cannot actively participate in its own IPX LAN.

The configuration is made in ***CM-100BT, FAST ETHERNET***:

Field	Meaning
Local IPX NetNumber	The IPX network number of the LAN to which **XCENTRIC** is connected.
Encapsulation	Defines the type of header to be used for IPX packets in the LAN connected. Possible values: ■ *none* ■ *Ethernet II* ■ *Ethernet 802.2 LLC* ■ *Ethernet SNAP* ■ *Ethernet NOVELL 802.3*

Table 14-41: ***CM-100BT, FAST ETHERNET***

To do Proceed as follows:

- Go to ***CM-100BT, FAST ETHERNET***.
- Enter **Local IPX NetNumber**.
- Select **Encapsulation**.
- Press **SAVE**.

14.5.3 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: ■ *yes* ■ *no*
IPX NetNumber	IPX network number of the WAN connection. This is required by some IPX routers.
Send RIP/SAP Updates	Defines how often ➤➤ **RIP** (Routing Information Protocol) and SAP (Service Advertising Protocol) packets are sent by **XCENTRIC** 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 14-42: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IPX***

The **Send RIP/SAP Updates** field contains the following selection options, which are explained with the aid of a table:

Possible values	New connection opened?	Update the existing tables?	Periodic updating?	Remarks
off	never	no	no	All routes and services must be entered statically.
triggered + piggyback (on changes, only if link active)	only for changes	yes	yes	This is the default setting, which is sufficient in most cases.
triggered (on changes)	only for changes	yes	no	Less data traffic than *triggered + piggyback*, but also less reliable.
piggyback (only if link active)	never	yes	yes	At least 1 static route and 1 static service must be entered for the WAN partner.
passive triggered (on changes only if link active)	never	yes	no	At least 1 static route and 1 static service must be entered for the WAN partner.
timed update (always)	always	yes	yes	Can cause higher ISDN charges.

Table 14-43: **Send RIP/SAP Updates**

To do Proceed as follows:

- Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IPX***.
- Select **Enable IPX**.
- Enter **IPX NetNumber**.
- Select **Send RIP/SAP Updates**.
- Enter **Update Time**, if applicable.
- Enter **Age Multiplier**, if applicable.
- Confirm with **OK**.

➤ Press **SAVE**.

14.6 Bridging

XCENTRIC supports the bridging function. The description of the configuration of **XCENTRIC** as a bridge can be found in the Software Reference.

14.7 Extra License Functions

This chapter briefly describes the **XCENTRIC** features you can activate with extra licenses.

14.7.1 VPN (Virtual Private Network)

XCENTRIC can set up 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).

You can find detailed information and configuration instructions (with examples) in the Software Reference.

15 Security Mechanisms

SAFERNET

The **XCENTRIC** 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 over the router and PABX 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

15.1 Activity Monitoring

A major requirement for a high degree of security is the possibility of accurately monitoring all activities on and over the router. BinTec Communications AG provides a variety of facilities for this purpose.

15.1.1 Syslog Messages

All major events on **XCENTRIC**'s various subsystems (➤➤ **ISDN**, ➤➤ **PPP**, ➤➤ **CAPI**, ➤➤ **TAPI**, 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 **XCENTRIC** 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 **XCENTRIC**.

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-100BT, FAST ETHERNET ➧ ADVANCED SETTINGS*
- *WAN PARTNER ➧ EDIT ➧ IP ➧ ADVANCED SETTINGS*

Field	Meaning
Syslog Output on Serial Console	Displays syslog messages on the PC connected to **XCENTRIC**'s serial interface (you should avoid this setting if possible, as the connection is very slow). Possible values: ■ *yes* ■ *no*
Message Level for Syslog Table	Specifies the priority of the syslog messages to be recorded internally. Possible values: ■ *emerg*: emergency messages (highest priority) ■ *alert*: alert messages ■ *crit*: critical messages ■ *err*: error messages ■ *warning*: warning messages ■ *notice*: notice messages ■ *info*: info messages ■ *debug*: debug messages (lowest priority) Syslog messages are only recorded internally if they have a higher or identical priority to that indicated.
Maximum Number of Syslog Entries	Maximum number of syslog messages saved in **XCENTRIC**. (Possible values: *0* - *100*)

Table 15-1: ***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: ■ *all*: all messages. ■ *system*: syslog messages except ➤➤ **accounting** messages. ■ *accounting*: accounting messages.

Table 15-2: ***SYSTEM*** ➧ ***EXTERNAL SYSTEM LOGGING***

Field	Meaning
IP Accounting	For saving accounting messages for ➤➤ **TCP**, ➤➤ **UDP** and ICMP sessions. Possible values: *on*, *off*.

Table 15-3: ***CM-100BT, FAST ETHERNET*** ➧ ***ADVANCED SETTINGS***

Field	Meaning
IP Accounting	For saving accounting messages for ➤➤ **TCP**, ➤➤ **UDP** and ICMP sessions. Possible values: *on*, *off*.

Table 15-4: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***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 on LAN

Proceed as follows to activate IP accounting on the LAN. **XCENTRIC** then generates and records accounting messages for the LAN for TCP, UDP and ICMP sessions.

- Go to ***CM-100BT, FAST ETHERNET*** ➧ ***ADVANCED SETTINGS***.
- Activate **IP Accounting** with *on*.

IP accounting on WAN

Proceed as follows to activate extended IP accounting. **XCENTRIC** then generates and records accounting messages for the selected WAN partner from TCP, UDP and ICMP sessions:

- Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.
- Activate **IP Accounting** with *on*.

Displaying syslog messages

Proceed as follows to display syslog messages:

- Go to ***MONITORING AND DEBUGGING*** ➧ ***MESSAGES***.

  This displays the syslog messages saved internally in **XCENTRIC**:

```
XCENTRIC Setup Tool                          BinTec Communications AG
[MONITOR][MESSAGE]: Syslog Messages                          MyXcentric

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




Press <Ctrl-n>, <Ctrl-p> to scroll
```

Deleting syslog messages

➤ Select **RESET** to delete the syslog messages in **XCENTRIC**.

For interpretation of syslog messages: see the Software Reference.

15.1.2 Monitoring Functions in the Setup Tool

You can also use the Setup Tool to display other data in addition to syslog messages. The current status of certain subsystems is updated periodically and displayed. Display modules are available for the following functional areas:

- ISDN connections
- Credits Based Accounting System
- Interface statistics (comparative display of several interfaces)
- ➤➤ **TCP/IP** statistics
- Syslog messages (see chapter 15.1.1, page 416)

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.

```
XCENTRIC Setup Tool                              BinTec Communications AG
[MONITOR][ISDN CALLS]: ISDN Monitor - Calls                     MyXcentric

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

Proceed as follows to display the credits status:

- 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.

```
XCENTRIC Setup Tool                          BinTec Communications AG
[MONITOR][CREDITS][STAT]: Monitor isdnlogin Credits          MyXcentric


Total           Maximum             % reached
Time till end of measure interval (sec)
7794            86400           91

Number of Incoming Connections                                    020
Number of Outgoing Connections                                    020
0

Time of Incoming Connections                                        4
28800           0
Time of Outgoing Connections                                       13
28800           0

Charge                                                              0

EXIT
```

Interface statistics

Proceed as follows to display the current values and activities of **XCENTRIC**'s interfaces:

➤ Go to ***MONITORING AND DEBUGGING*** ➧ ***INTERFACES***.

The values for two interfaces are displayed side by side.

The following menu opens:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[MONITOR][INTERFACE]: Interface Monitoring                      MyXcentric

Interface Name                                   en1
PROVIDER
Operational Status                               up
dormant

                                                 total            per second
total            per second

Received Packets                                 5512             0     00
Received Octets                                  920664           0     00
Received Errors                                  0                      0

Transmit Packets                                 9                   0 00
Transmit Octets                                  1193             0     00
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.

The following menu opens:

```
XCENTRIC Setup Tool                              BinTec Communications AG
[MONITOR][IP]: IP Statistics                                    MyXcentric

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.

15.1.3 Credits Based Accounting System

ISDN charges

XCENTRIC's Credits Based Accounting System enables you to control the costs billed for ISDN charges for data connections. This means you can keep the effects of possible configuration errors within limits. For example, the system enables you to define the maximum number of connections allowed in a certain period of time. You can make settings for each subsystem (➤➤ **PPP**, ➤➤ **CAPI**, ➤➤ **ISDN Login,** ➤➤ **POTS**) to define the number of connections, the connection time and the charges billed. If the defined limit is exceeded, **XCENTRIC** 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!

The POTS subsystem for **XCENTRIC** includes all telephone terminals connected. With the size of **XCENTRIC**'s PABX, it makes little sense in practice to define limits for the Credits Based Accounting System for the POTS subsystem.

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 **XCENTRIC** off and then switch it on again (i.e. reboot).

The configuration is made in ***ISDN*** ➧ ***CREDITS***:

Field	Meaning
Surveillance	Defines whether the Credits Based Accounting System is to be activated for the respective subsystem. Possible values: *off*, *on*. With *on*, 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)*. If you activate this setting with *on*, 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 *on*, you can enter the desired value in the line below.
Maximum Charge	Maximum charges allowed (units) during the *Measure Time (sec)*. If you activate this setting with *on*, you can enter the desired value in the line below. The **Maximum Charge** is shown in units. If the charges are transferred in money terms, the **Maximum Charge** is shown in units of 1/1000th of the respective currency (e.g. "0.12 DM" would be 120 charging units). Possible values are between 0 and 2147483647.
Maximum Time for Incoming Connections (sec)	Maximum time in seconds allowed for incoming connections during the *Measure Time (sec)*. If you activate this setting with *on*, 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 *on*, 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. If you activate this setting with *on*, 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. If you activate this setting with *on*, you can enter the desired value in the line below.

Table 15-5: ***ISDN ➧ CREDITS***

To do Proceed as follows:

- Go to ***ISDN ➧ CREDITS***.
- Select **Subsystem** and confirm with **Return**.
- Select **Surveillance**: *on*, if you want to use the Credits Based Accounting System for the selected **Subsystem**.
- Enter **Measure Time (sec)**, e.g. *86400* (= 24 hours).
- Activate **Maximum Number of Incoming Connections**, if applicable, and enter the desired value.
- Activate **Maximum Number of Outgoing Connections**, if applicable, and enter the desired value.
- Activate **Maximum Charge**, if applicable, and enter the desired value.
- Activate **Maximum Time for Incoming Connections (sec)**, if applicable, and enter the desired value.
- Activate **Maximum Time for Outgoing Connections (sec)**, if applicable, and enter the desired value.
- Activate **Maximum Number of Current Incoming Connections**, if applicable, and enter the desired value.

- Activate **Maximum Number of Current Outgoing Connections**, if applicable, and enter the desired value.
- Press **SAVE**.

15.1.4 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 **XCENTRIC**. This enables all users of the **XCENTRIC** 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 **XCENTRIC**'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.

An extract of the HTTP status page is shown below:

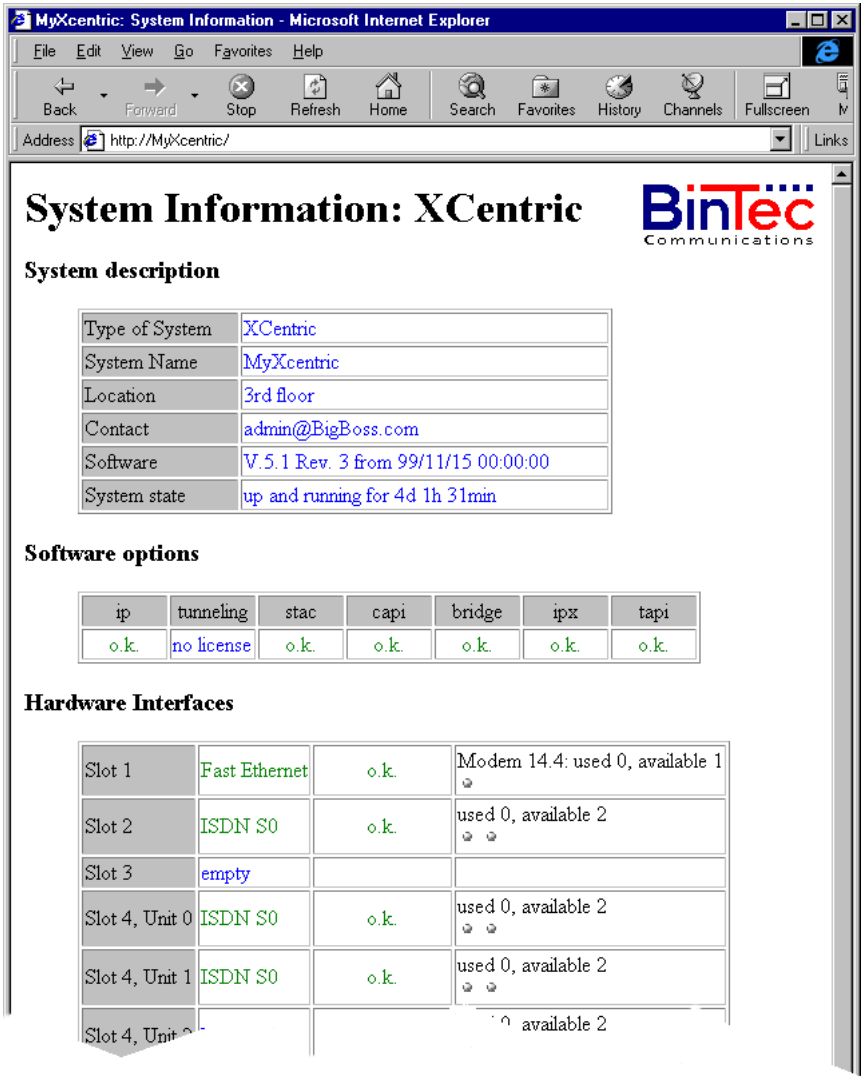


Figure 15-1: HTTP status page

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 **XCENTRIC**'s subsystems.
- Hardware interfaces
  This table displays the LAN and WAN interface of **XCENTRIC**. 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	o.k.	Normal operation.
	inactive	LAN cable is not connected.
WAN	o.k.	Normal operation.
	inactive	None of the B-channels used at present.
	unconfigured	ISDN cable is not connected or a wrong ➤➤ **D-channel** protocol is entered.

Table 15-6: 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**.
- http://www.bintec.de
  Use this link to access BinTec's WWW server with the latest information on products and the current system software and documentation for **XCENTRIC**.

- system tables
  Click system tables to display a list with all the **XCENTRIC** MIB tables. Clicking a table name lists the variables contained in the table.

If you don't want to display **XCENTRIC**'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**.

15.1.5 Java Status Monitor

The Java status monitor offers you another facility for displaying information about **XCENTRIC** using an Internet browser. You can call up the following information with the Java status monitor:

- Static information such as the system name of the BinTec router and the software version.
- Data flow over the individual interfaces.
- Connections to WAN partners.

If you have installed the Java status monitor together with BRICKware (see chapter 8.3, page 140), you can start it as follows:

➤ Select **Program** ➧ **BRICKware** ➧ **Java Status Monitor** in the Windows Start menu.

The Java status monitor opens with your standard browser.

Further information about the Java status monitor can be found in **BRICKware for Windows**.

15.1.6 Activity Monitor

What do you need it for?

The Activity Monitor enables Windows users to monitor the activities of **XCENTRIC**. 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 **XCENTRIC**'s interfaces is possible.

How does it work?

A Status Demon collects information on **XCENTRIC** 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 **XCENTRIC** interface and 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 approx. 4000 bytes is not exceeded. A Windows application on your PC receives the packets and displays the information received in various forms. This application is obtainable with BRICKware Release 5.1.1 and higher.

Activate the Activity Monitor as follows:

- Appropriately configure the **XCENTRIC**(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	IP address to which **XCENTRIC** sends the UDP packets. The default value *255.255.255.255* means that the broadcast address of the first LAN interface is used. Note: If you enter the IP address of a WAN partner that can be reached over an ISDN dial-up connection, you will get a large telephone bill due to frequent setting up of ISDN connections (a packet is usually sent every 5 seconds).
Client UDP Port	Port number for Activity Monitor (default value: *2107*, registered by IANA - Internet Assigned Numbers Authority).
Type	Type of information sent in the UDP packets to the Windows application. Possible values: ■ *off:* deactivates Activity Monitor (default value) ■ *physical:* only information about physical interfaces ■ *physical_virt:* information about physical and virtual interfaces
Update Interval (sec)	Update interval in seconds. Possible values: *0* to *60* (default value: *5*).

Table 15-7: ***SYSTEM*** ➧ ***EXTERNAL ACTIVITY MONITOR***

The breakdown of **XCENTRIC**'s interfaces into physical and virtual interfaces is described in detail in the Software Reference.

Note: A leased line always represents a physical interface, but a group of leased lines is displayed as both a physical and virtual interface!

To do Proceed as follows:

- Go to ***System*** ➧ ***External Activity Monitor***.
- Enter **Client IP Address**, **Client UDP Port**, **Type** and **Update Interval (sec)**.
- Press **SAVE**.

15.2 Access Security

There are several ways of restricting logging in and access to **XCENTRIC** to authorized users only.

15.2.1 Logging In

Password

Logging in to **XCENTRIC** can be done in several ways as described in chapter 8.1.4, page 127, 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 135.

- You must change the passwords as described in chapter 8.1.4, page 127.
- Also make sure that unauthorized persons do not have access to the **XCENTRIC** power supply, serial console and ➤➤ **Ethernet** connection.

Until you have changed the preset 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 **XCENTRIC** 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 18.1, page 500).

If you carry out a software update (see chapter 16.3, page 485), 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.

15.2.2 Checking the Calling Party Number

CLID

XCENTRIC 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). **XCENTRIC** 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 **XCENTRIC** 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**.

15.2.3 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 10.2.1, page 167 and chapter 14.1.2, page 350.

15.2.4 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. **XCENTRIC** 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 15-8: ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***

Callback offers the following selection options:

Possible Values	Meaning
no	**XCENTRIC** does not call back.
expected (awaiting callback)	**XCENTRIC** calls the WAN partner to initiate callback.
yes (PPP negotiation)	**XCENTRIC** 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.
yes (delayed, CLID only)	**XCENTRIC** calls back after approx. four seconds, if requested to by the WAN partner.
yes (PPP negotiation, callback optional)	Corresponds to the value *yes (PPP negotiation)*, but contains an abort option. The Microsoft client has the option of aborting callback and maintaining the initial connection to **XCENTRIC** 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 **XCENTRIC**.
yes	**XCENTRIC** calls back immediately, if requested to by the WAN partner.

Table 15-9: **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**.

15.2.5 Closed User Group

XCENTRIC 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**.

15.2.6 Access to Remote CAPI and Remote TAPI

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.

PABX user concept By using BinTecs's user concept, you can make sure that only users authenticated by user name and password can access **XCENTRIC**'s Remote CAPI and Remote CAPI interfaces.

Filters You can also prevent unauthorized access by defining filters (see chapter 15.2.8, page 445) and local filters (see chapter 15.2.9, page 456).

15.2.7 NAT (Network Address Translation)

➤➤ **NAT** is a simple-to-operate procedure that can be used for several purposes in the BinTec implementation:

- Hiding the internal host addresses of a LAN by remapping to one or more external addresses.
- Controlling external to internal access. In the external direction, the router forwards all ➤➤ **data packets** (forward NAT) and connections from external callers are only allowed if explicitly enabled.

A diagram of Forward NAT is shown below:

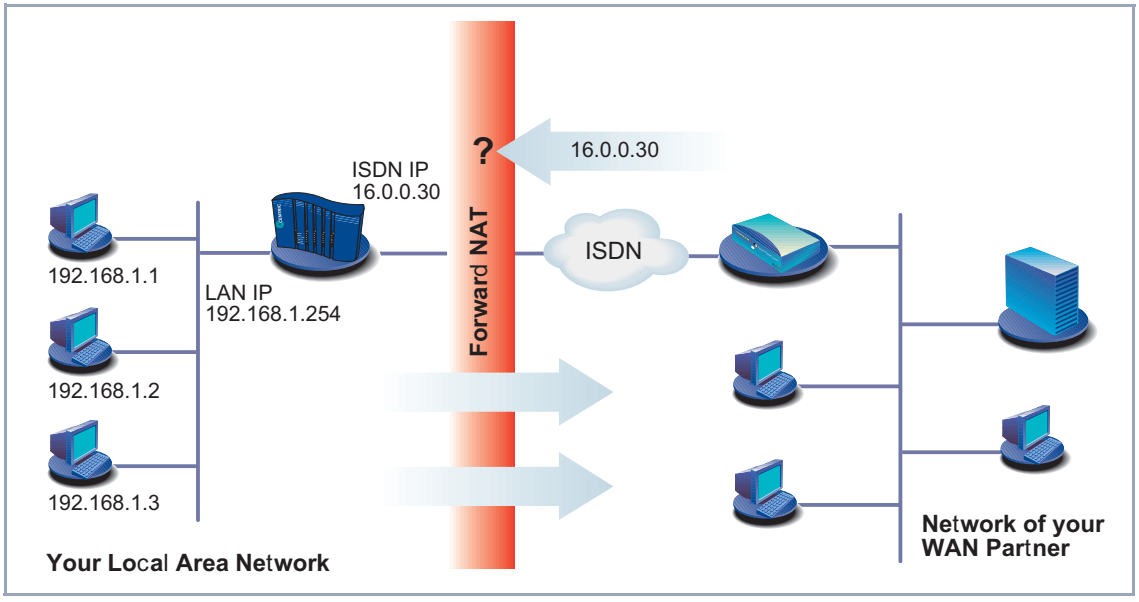


Figure 15-2: Forward NAT

- 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. **XCENTRIC**'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 **XCENTRIC** interface with ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ ***EDIT***:

Field	Meaning
Network Address Translation	Defines the type of NAT for the selected interface. Possible values: ■ *off:* Do not execute NAT. ■ *on:* Execute Forward NAT. ■ *reverse:* Execute Reverse NAT.

Table 15-10: ***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	Service allowed for connections to the host defined under **Destination**. Possible values: ■ *ftp* ■ *telnet* ■ *smtp* ■ *domain/udp* ■ *domain/tcp* ■ *http* ■ *nntp* ■ *user defined:* If you do not use any of the predefined services. Enter the required values under *Protocol* and *Port* to define a service.
Protocol	Only for **Service** = *user defined*. Defines the protocol allowed. Possible values: ■ *icmp* ■ *tcp* ■ *udp* ■ *gre* ■ *esp* ■ *ah* ■ *l2tp*

Field	Meaning
Port (-1 for any)	Only for **Service** = *user defined*. Defines the port allowed. Entering -1 allows any port for **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 15-11: ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Return** ➧ **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.

15.2.8 Filters (Access Lists)

IP filters (➤➤ **Access Lists**) in **XCENTRIC** 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 **XCENTRIC** for certain data.

Filters A filter describes a certain part of the IP data traffic based on the source and/or destination IP address, ➤➤ **netmask**, protocol and source and/or destination port. If you define a filter, you should therefore tell **XCENTRIC**: "Watch out for all incoming data packets that match the following: ...".

Rule You use a rule to tell **XCENTRIC** 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.
- Combinations 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 **XCENTRIC** interface.

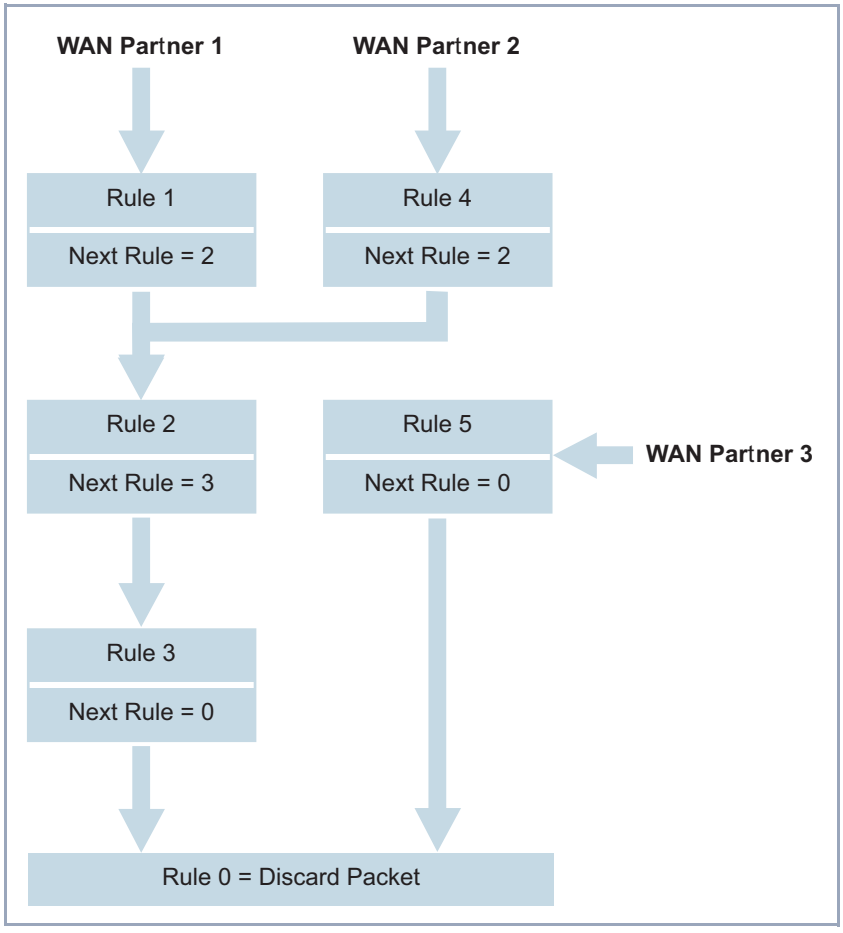


Figure 15-3: Rule chains for various interfaces

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. **XCENTRIC** automatically issues a number to newly defined filters.
Protocol	Defines a protocol. Possible values: *any*, *icmp*, *ggp*, *tcp*, *egp*, *pup*, *udp*, *hmp*, *xns_idp*, *rdp*, *rsvp*, *gre*, *esp*, *ah*, *igrp*, *ospf*, *l2tp*. *any* matches any protocol, *tcp* matches only TCP data packets, etc.
Connection State	If **Protocol** = *tcp*, you can define a filter based on the status of the TCP connection. Possible values: *established:* All TCP packets that would not open any new TCP connection on routing over **XCENTRIC** match the filter. *any:* All TCP packets match the filter.
Type	Only if **Protocol** = *icmp*. Possible values: *any*, *echo reply*, *destination unreachable*, *source quench*, *redirect*, *echo*, *time exceeded*, *param problem*, *timestamp*, *timestamp reply*, *address mask*, *address mask reply*. 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.
Specify Port	If **Source / Destination Port** = *specify* or *specify range:* Enter port numbers or range of port numbers.

Table 15-12: ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER***

The **Source Port** and **Destination Port** fields contain the following selection options:

Possible Values	Meaning
any	All ➤➤ **port** numbers match the filter.
specify	Permits the entry of a port number under **Specify Port**.
specify range	Permits the entry of a range of port numbers under **Specify Port**.
priv (0..1023)	Port numbers: 0 ... 1023.
server (5000..32767)	Port numbers: 5000 ... 32767.
clients 1 (1024.0.4999)	Port numbers: 1024 ... 4999.
clients 2 (32768..65535)	Port numbers: 32768 ... 65535.
unpriv (1024..65535)	Port numbers: 1024 ... 65535.

Table 15-13: *Source Port* and *Destination Port*

Port numbers

The port numbers are distributed as follows:

<table>
<tr><th>0 ... 1023</th><th>1024 ... 4999</th><th>5000 ... 32767</th><th>32768 ... 65535</th></tr>
<tr><td rowspan="2">Well-known ports, i.e. permanently assigned.

priv (0..1023)</td><td colspan="3">The ports are created dynamically by ➤➤ clients and ➤➤ servers and have no permanent meaning (with the exception of special agreements):
unpriv (1024..65535)</td></tr>
<tr><td>clients 1 (1024.0.4999)</td><td>server (5000..32767)</td><td>clients 2 (32768..65535)</td></tr>
</table>

Table 15-14: 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 15-15: 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 IP packets that use 21 as source port and xyz as destination port:

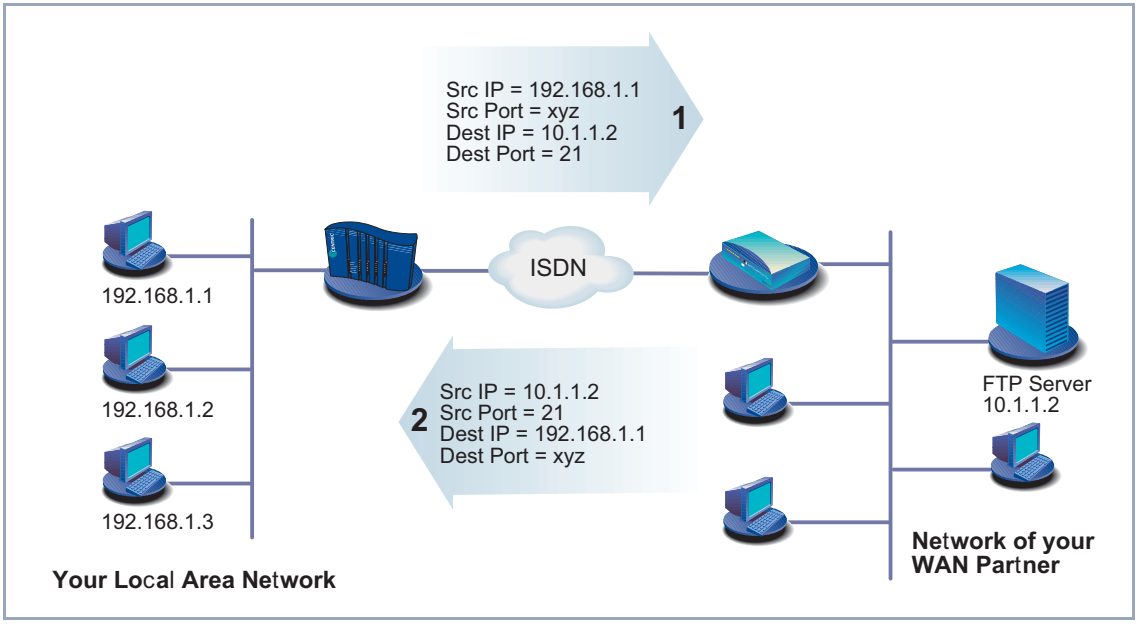


Figure 15-4: Example: FTP connection

You can define rules in ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES***:

Field	Meaning
Index	Cannot be changed. **XCENTRIC** 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 *none*.
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 15-16: ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES***

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

Possible Values	Meaning
allow M	Allow packet if it matches the filter.
allow !M	Allow packet if it does not match the filter.
deny M	Deny packet if it matches the filter.
deny !M	Deny packet if it does not match the filter.
ignore	Use next rule.

Table 15-17: *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 15-18: ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **REORG**

If you reorganize such a chain, **XCENTRIC** renumbers the remaining rules according to the selection in **Index of Rule that gets Index 1**:

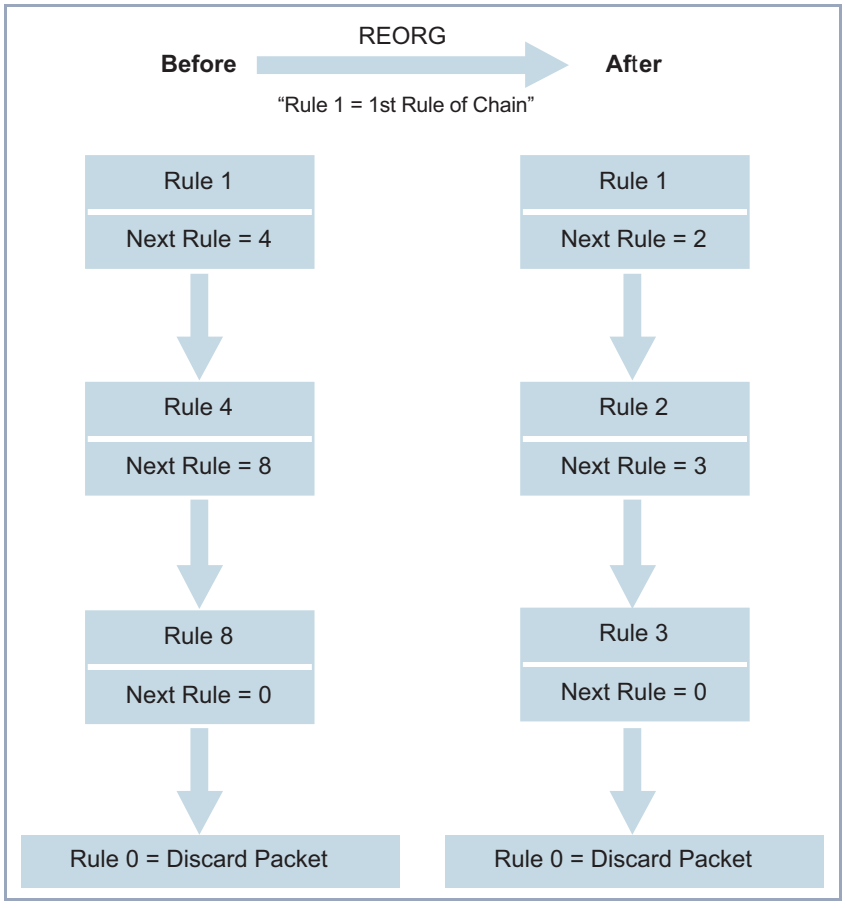


Figure 15-5: Example of chain reorganization

You can define which interface starts and with which rule in ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES***:

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	**XCENTRIC** interface
First Rule	Defines which rule is used first for data packets that reach **XCENTRIC** via the **interface**. If you enter *none*, you specify that no filters are used for the **Interface**.

Table 15-19: ***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 **XCENTRIC** 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 **XCENTRIC** from the LAN over telnet.
- If you access **XCENTRIC** 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 suitable filters 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**.
- 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 10.1.5, page 161.

15.2.9 Local Filters

Access to the local services in **XCENTRIC** (telnet, ➧➧ **CAPI**, trace, etc.) can be controlled via a separate MIB table. As long as this is empty, access to local services is possible via all interfaces, provided it is not prohibited by the use of NAT (see chapter 15.2.7, page 440) or global filters (see chapter 15.2.8, page 445).

Local filters therefore provide an additional tool that is different to handle than global filters and does not adversely affect performance in normal routing either.

Activate local filters by entries in the MIB tables **localTcpAllowTable** and **localUdpAllowTable**.

15.2.10 Back Route Verification

This term conceals a simple but very effective **XCENTRIC** 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**.

15.2.11 TAF Client

Personalized authentication The Token Authentication Firewall (TAF) function permits personal authentication of IP connection partners. BinTec's solution integrates the Security Dynamics token authentication mechanisms and allows data packets to pass through the router only after successful authentication of the associated source address.

You can enable this function on BinTec's corporate access routers and configure the router as TAF server. You can configure the **XCENTRIC** workgroup 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 is contained in **BRICKware for Windows**.

15.2.12 Extended IP Routing (XIPR)

In addition to the normal routing table, **XCENTRIC** can also make routing decisions based on an additional table called the Extended Routing Table. Apart from the destination address, **XCENTRIC**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 the Software Reference).

The configuration is made in the MIB table **ipExtRtTable**. A detailed description is given in the Software Reference.

15.3 Line Tapping Security

You can use an encryption mechanism to obtain data security for critical PPP connections, provided both connection partners support this mechanism.

15.3.1 Encryption

XCENTRIC supports encryption of PPP connections to WAN partners. Encryption is based on the ➤➤ **MPPE** (Microsoft Point to Point ➤➤ **Encryption**) procedure with code lengths of 40 bits or 128 bits.

The configuration is made in ***WAN PARTNER*** ➧ ***EDIT***:

Field	Meaning
Encryption	Defines the type of encryption. Possible values: ■ *MPPE 40:* code length 40 bits. ■ *MPPE 128:* code length 128 bits. ■ *none:* no encryption.

Table 15-20: ***WAN PARTNER*** ➧ ***EDIT***

To do Proceed as follows to set encryption:

➤ Go to ***WAN PARTNER***.

➤ Select a WAN partner and confirm with **Return** to encrypt the PPP connections to this partner.

➤ Select **Encryption**, e.g. *MPPE 40*.

➤ Press **SAVE**.

15.3.2 VPN (with extra license)

XCENTRIC 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.

15.4 Special Features

15.4.1 Startup Procedure

XCENTRIC 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.

15.4.2 Auto Logout

Connections to **XCENTRIC** 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 18.1, page 500).

15.4.3 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 **XCENTRIC** 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 15.2.10, page 456).

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.

15.5 Checklist

The following list indicates the most important critical security points that you should observe when configuring **XCENTRIC**:

- Have you changed all four passwords for system access (admin, read, write, http)? See chapter 10.1.2, page 154.
- Are the activities of your **XCENTRIC** sufficiently accurately logged on at least one external computer and do you check the syslog messages regularly? See chapter 15.1.1, page 416.
- Have you restricted access to the local services and resources to known computers or networks? In particular, you should only allow access via CAPI, 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 15.2.7, page 440.
- 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 15.2.8, page 445.
- Have you restricted remote maintenance access via ISDN Login? Have you made a suitable entry under ***PABX*** ➧ ***DIAL PLAN***? See chapter 11.5.4, page 255.

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 15.2.4, page 437.
- Do you use an encryption protocol for line tapping security on connections with critical security? See chapter 15.3.1, page 459.
- 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 14.2.7, page 369.
- Do you check what computers have access to the Remote CAPI and Remote TAPI interfaces, what applications are used on them and whether the connections used with these applications are desired? Do you use the 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?

16 Configuration Management and Flash Card

In this chapter you will find instructions on administration of your configuration files, handling the flash card and updating the **XCENTRIC** 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?
- Working with the flash card
- Updating software
  - How do I keep in touch with the latest developments?
  - How do I load new system software (software image/boot image)?

16.1 Administration of Configuration Files

Internal flash

XCENTRIC reads its configuration information from configuration files. These configuration files are usually (see flash card in chapter 16.2.3, page 475) in the internal flash EEPROM (electronically eraseable programmable read-only memory) of **XCENTRIC**. Several different configuration files can be stored in the internal flash memory. The data also remains stored in the internal flash when **XCENTRIC** is switched off.

Flash card

The basic unit of **XCENTRIC** is equipped with a flash card slot for SmartMedia flash cards. SmartMedia flash cards (such as obtainable from photo shops) can be used for saving configurations and different versions of **XCENTRIC**'s system software. Cards with 4 MB, 8 MB, 16 MB and 32 MB of memory (all 3.3 V only) are supported. The slot for the flash card on the basic unit of **XCENTRIC** is described in chapter 6.3, page 66. You will find a description of handling the flash card in chapter 16.2, page 474.

XCENTRIC can also access system software or a configuration stored on the flash card when it restarts.

Memory

The current configuration and all changes you set during the operation of **XCENTRIC** are stored in the memory (RAM). The contents of the RAM are lost when **XCENTRIC** is switched off. So if you modify your configuration and want to keep these changes for the next time you start **XCENTRIC**, you have to save the modified configuration to the internal flash before switching off: **Exit** ➧ **Save as boot configuration and exit** (see chapter 10.3, page 205). This file is then saved in the internal flash as a boot configuration file under the name "boot". When **XCENTRIC** is started, it is usually this configuration file (see flash card in chapter 16.2.3, page 475) with the name "boot" that is loaded into the memory and takes effect.

Operations

Imagine the internal flash memory as a directory of configuration files. The files in this directory can be copied, moved, erased and newly created. It is also possible to transfer configuration files between **XCENTRIC** and a remote host by TFTP.

Windows

In Windows, you can use the TFTP server of **DIME Tools** (see **BRICKware for Windows**). You can then, for example, save a configuration file from **XCENTRIC** on your local PC.

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:

You will find a detailed description of using the flash card in chapter 16.2, page 474.

➤ Go to the ***CONFIGURATION MANAGEMENT*** menu.

The following menu opens:

```
XCENTRIC Setup Tool                              BinTec Communications AG
                                                                MyXcentric

    Operation                    get  (TFTP --> FLASH)

    TFTP Server IP Address       192.168.1.1
    TFTP File Name               xcentric.cf

    Type of Flash                internal Flash Memory
    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). In exceptional cases, it may be necessary for certain Unix TFTP servers to enter the file name here with path data.
Type of Flash	Here you enter the type of flash (internal flash EEPROM of **XCENTRIC** or flash card). Possible values: ■ *internal Flash Memory* (default value) ■ *removable Flash Card* This field appears only for the operations *save*, *load*, *put* and *get* to enable the relevant flash to be selected if using a flash card.
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* = *move* or *copy*).
Type of Last Operation	Type of previous operation (since the last **XCENTRIC** start).
State of Last Operation	The state of the last operation executed.

Table 16-1: ***CONFIGURATION MANAGEMENT***

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

Possible Values	Meaning
save (MEMORY --> FLASH)	Save all current settings from memory to flash as configuration file **Name in Flash**. **Name in Flash** is overwritten or recreated.
load (FLASH --> MEMORY)	Loading the configuration file **Name in Flash** from flash to memory. The settings in **Name in Flash** take immediate effect.
move (FLASH --> FLASH)	Rename configuration file from **Name in Flash** to **New Name in Flash** in the internal flash EEPROM.
copy (FLASH --> FLASH)	Copy configuration file **Name in Flash** as **New Name in Flash** in the internal flash EEPROM.
delete (FLASH)	Delete configuration file **Name in Flash** in the internal flash EEPROM.
put (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.
get (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 or 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 (*load FLASH --> MEMORY)*, so that the settings can take effect on **XCENTRIC**.

Possible Values	Meaning
state (MEMORY --> TFTP)	Save all current settings in the memory as **TFTP File Name** on the TFTP host with the IP address **TFTP Server IP Address**. **TFTP File Name** is then overwritten or recreated.
reboot	Restart **XCENTRIC**. Settings in the memory are replaced with the settings in the "boot" configuration file from the flash EEPROM (or the flash card).

Table 16-2: *Operation*

The **State of last operation** field can display the following:

Possible Values	Meaning
todo	The operation has not yet been started.
running	The operation is being executed.
done	The operation has been executed successfully.
error	The operation could not be fully executed (see syslog message).

Table 16-3: *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, **XCENTRIC**'s boot file will be deleted and **XCENTRIC** cannot load a configuration on restarting. If necessary, rename the file to be transferred!

To run *put (Flash --> TFTP)*, *get (TFTP --> Flash)* and *state (MEMORY --> TFTP)*, you need a TFTP server on the host to or from which you want to transfer a configuration file.
If the TFTP host is a Windows PC, click **Program** ➧ **BRICKware** ➧ **DIME Tools** in the Windows Start menu to open **DIME Tools** and activate the TFTP server with **File** ➧ **TFTP Server** before you run the operation in question.

If you want to use your Windows PC as a TFTP host but are not sure what the IP address of the PC is, proceed as follows:

For Windows 95:

- 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 xcentric.cf, e.g. with the help of the Configuration Wizard. You have not transferred the file to **XCENTRIC** over the serial interface; xcentric.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 xcentric.cf from your PC to **XCENTRIC**, 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***.

TFTP host --> flash

- Select **Operation**: *get (TFTP --> FLASH)*.
- Type in **TFTP Server IP Address**, e.g. *192.168.1.1*.

- Type in **TFTP File Name**: *xcentric.cf.*
- Leave *internal Flash Memory* as **Type of Flash**.
- Type in **Name in Flash**, e.g. *boot*.
- Select **START OPERATION** and press **Return**.

  As long as the operation is being carried out, *OPERATING* appears in the help line of the Setup Tool; **State of last operation** displays *running.*

  When the operation has been successfully executed, *get (TFTP --> FLASH)* is displayed under **Type of last operation**; **State of last operation** assumes the value *done*.

  The configuration file xcentric.cf is saved, for example, in **XCENTRIC**'s flash under the name boot.

To make the settings of xcentric.cf take immediate effect in **XCENTRIC**, proceed as follows:

Flash --> memory

- Reselect **Operation**: *load (FLASH --> MEMORY)*.
- Leave *internal Flash Memory* as **Type of Flash**.
- Select **Name in Flash**, e.g. *boot*.
- Select **START OPERATION** and press **Return**.

  As long as the operation is being carried out, *OPERATING* appears in the help line of the Setup Tool; **State of last operation** displays *running.*

  When the operation has been successfully executed, *load (FLASH --> MEMORY)* is displayed under **Type of last operation**; **State of last operation** assumes the value *done*.

  The configuration file boot has been loaded to **XCENTRIC**'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.

16.2 Flash Card

SmartMedia flash cards (such as obtainable from photo shops) can be used for saving configurations and different versions of **XCENTRIC**'s system software. Cards with 4 MB, 8 MB, 16 MB and 32 MB of memory (all 3.3 V only) are supported. The slot for the flash card on the basic unit of **XCENTRIC** is described in chapter 6.3, page 66.

Configurations and versions of the system software are stored on the flash card in files, which are administrated using a DOS file system. The file names to be administrated must have the "8.3" format. Upper and lower case are ignored.

Configuration files are loaded and saved via the Setup Tool. Other functions for administrating the files on the flash card are executed via the command line application "fssh" in the SNMP shell.

At least BOOTmonitor version 5.2.1 is necessary to be able to boot the system software from the flash card. The current BOOTmonitor versions are obtainable from BinTec's web site at http://www.bintec.net.

16.2.1 Formatting the Flash Card

Before being used for the first time, the flash card must be formatted with the command `fssh format` in the SNMP shell. Refer to the description of the commands in chapter 16.2.5, page 481.

The file system described below and the default directories are created on the flash card with the command `format`.

16.2.2 File System and Directory Structures on the Flash Card

The flash card contains an FAT-12 file system. All files must be named according to the DOS name convention in "8.3" format and upper and lower case are ignored.

The main directory of the flash card is called "/card/". The working directory is "/card/xcentric/autoexec/". All system software files or configuration files are saved automatically in this subdirectory using the command `fssh` (see chapter 16.2.5, page 481) or the Configuration Management via the Setup Tool (see chapter 16.2.4, page 476). If directories other than the working directory are to be administrated with the command `fssh` or the Configuration Management commands, the full path name must always be given (also in the Setup Tool). The file name is sufficient for files in the working directory.

16.2.3 Behavior of XCENTRIC with Flash Card in Boot Operation and Saving the Configuration

System software

If at the time of restarting **XCENTRIC** the working directory of the flash card contains a system software file with the attribute `boot` (see chapter 16.2.5, page 481), **XCENTRIC** uses this system software for the restart. If the flash card contains no such file or loading the system software file from the flash card fails, **XCENTRIC** boots as usual from the internal flash.

A system message shows which system software **XCENTRIC** used for booting.

Booting the system software from the flash card:

```
Searching image on Flash Card
Booting image from Flash Card .............OK (1114112 bytes)
Checking image ... OK
```

Table 16-4: Example of a system message for booting the system software from the flash card

Booting the system software from the internal flash:

```
Booting Image from Flash ROM
```

Table 16-5: System message on booting the system software from the internal flash

Loading and saving the system configuration

If at the time of restarting **XCENTRIC** the working directory of the flash card contains a configuration file with the name "boot", this configuration is loaded during the restart and the configuration in the internal flash EEPROM is ignored. **XCENTRIC** behaves the same if an LCR file with the name "boot_lcr" is saved

on the flash card. If these files are not present on the flash card, **XCENTRIC** uses the configuration from the internal flash EEPROM as usual.

Syslog messages give you information about the configuration used for the restart. You can view syslog messages in **XCENTRIC**'s Setup Tool in the ***MONITORING AND DEBUGGING*** ➧ ***MESSAGES*** menu.

The following syslog messages are created on loading the system configuration and the LCR configuration from the flash card:

```
INFO/CONFIG: Flash Card configuration loaded
INFO/CONFIG: Flash Card LCR configuration loaded
```

If a flash card is inserted in **XCENTRIC** at the time of saving the configuration with the Setup Tool (***EXIT*** ➧ ***SAVE AS BOOT CONFIGURATION AND EXIT***) and this card contains a configuration file with the name "boot", the configuration is written to this "boot" file when the configuration is saved on the flash card. The existing content of the configuration file with the name "boot" on the flash card is lost.

If no flash card is inserted that contains a configuration file with the name "boot", the configuration is saved to the internal flash under the name "boot" using ***EXIT*** ➧ ***SAVE AS BOOT CONFIGURATION AND EXIT***.

16.2.4 Configuration Management for the Flash Card

Configuration Management with the Setup Tool (in the ***CONFIGURATION MANAGEMENT*** menu) has been extended for the flash card.

```
XCENTRIC Setup Tool                              BinTec Communications AG
                                                                MyXcentric

Operation                       get  (TFTP --> FLASH)

TFTP Server IP Address          192.168.1.1
TFTP File Name                  xcentric.cf

Flash Type                      removable Flash Card
Name in Flash                   xc1.cf

Type of last operation          get  (TFTP --> FLASH)
State of last operation         done

        START OPERATION                  EXIT

Use <Space> to select
```

For the meaning of the individual fields of the Setup Tool, see table 16-1, page 468, table 16-2, page 470 and table 16-3, page 470.

To copy a configuration file from the internal flash EEPROM to the flash card or vice versa, the desired configuration file must first be loaded into the RAM (*MEMORY*) of **XCENTRIC** using *load*. The configuration must then be saved again to the flash card or internal flash EEPROM using *save*.

If an error should occur while running *get (TFTP --> FLASH)* and the operation is aborted, the file to be overwritten in the flash is deleted. So if you transfer a "boot" file to the internal flash EEPROM of **XCENTRIC**, **XCENTRIC**'s boot file will be deleted. **XCENTRIC** can no longer load a configuration on booting. If necessary, rename the file to be transferred!

To run *put (Flash --> TFTP)*, *get (TFTP --> Flash)* and *state (MEMORY --> TFTP),* you need a TFTP server on the host which you want to transfer a configuration file to or from.
If the TFTP host is a Windows PC, click **Program** ➧ **BRICKware** ➧ **DIME Tools** in the Windows Start menu to open **DIME Tools** and activate the TFTP server with **File** ➧ **TFTP Server** before you run the operation in question.

If you want to use your Windows PC as a TFTP host but are not sure what the IP address of the PC is, proceed as follows:

For Windows 95:

- 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

Proceed as follows to run an operation in the ***CONFIGURATION MANAGEMENT*** menu:

- Select **Operation**.
- Activate a TFTP server if you have selected *put*, *get* or *state* as the **Operation**.
- Select or type in the necessary settings in the ***CONFIGURATION MANAGEMENT*** menu.
- Select **START OPERATION** and press **Return**.

  As long as the operation is being carried out, *OPERATING* appears in the help line of the Setup Tool and **State of last operation** displays *running*.

  When the operation has been successfully executed, it is shown under **Type of last operation**. **State of last operation** shows the value *done*.

If *error* is displayed under **State of last operation**, check your settings:

- Have you entered the right IP address under **TFTP Server IP Address**?
- If using older versions of BRICKware for Windows: Does the name of the configuration file consist of maximum eight characters and the extension of maximum three characters (when using DIME Tools)?
- Does the host support TFTP (did you start the TFTP server of DIME Tools before starting the operation)?
- Is the source file in the configured directory of the TFTP path of DIME Tools (when **Operation** = *get*)? To change the TFTP path, refer to **BRICKware for Windows**.

If no errors are found in the above points, proceed as follows to find the cause of the problem:

➤ Leave the Setup Tool.

➤ Type in the following in the SNMP shell: `debug config &`.

➤ Reopen the Setup Tool with `setup`.

➤ Carry out the desired operation in ***CONFIGURATION MANAGEMENT***.
If an error occurs, an error message is displayed to indicate the cause.

➤ Leave ***CONFIGURATION MANAGEMENT*** with **EXIT**.

Example

Your flash card contains the file "xc1.cf". You want to copy the file with the name "boot" from the flash card to the internal flash EEPROM of **XCENTRIC**. The file is then available as a new configuration file when **XCENTRIC** restarts. Copying a configuration file from the flash card into the internal flash EEPROM is only possible by loading it into the RAM of **XCENTRIC**.

Note that the operation described here will overwrite any existing file with the name "boot" that is present in the internal flash EEPROM of **XCENTRIC**. We recommend that you first rename or make a backup copy of the old "boot" file.

The flash card must be inserted in **XCENTRIC**.

➤ Go to ***CONFIGURATION MANAGEMENT***.

Loading from the Flash Card into XCENTRIC's RAM

- Select **Operation**: *load (FLASH --> MEMORY)*.
- Select **Flash Type**: *removable Flash Card*.
- Select **START OPERATION** and press **Return**.

  OPERATING appears in the help line of the Setup Tools as long as the operation is running. **State of last operation** shows *running*.

  When the operation has been successfully executed, *load (FLASH --> MEMORY)* is shown under **Type of last operation**. **State of last operation** shows the value *done*.

  The configuration file "xc1.cf" has been loaded to **XCENTRIC**'s memory and the settings are active immediately.

Finally, proceed as follows to save the now active configuration file to the flash EEPROM of **XCENTRIC**:

Saving a Configuration File from the RAM to the Internal Flash EEPROM of XCENTRIC

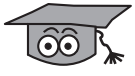
- Select **Operation**: *save (MEMORY --> FLASH)*.
- Select **Flash Type**: *internal Flash Memory*.
- Enter **Name in Flash**: *boot*.
- Select **START OPERATION** and press **Return**.

  OPERATING appears in the help line of the Setup Tools as long as the operation is running. **State of last operation** shows *running*.

  When the operation has been successfully executed, *save (MEMORY --> FLASH)* is shown under **Type of last operation**. **State of last operation** shows the value *done*.

  The configuration file "boot" has been saved to the flash EEPROM of **XCENTRIC**. Your settings remain active and will also be loaded again on a restart even if the flash card is not inserted.

- Leave ***CONFIGURATION MANAGEMENT*** with **EXIT**.



How to use the commands `cmd=load`, `cmd=save`, `cmd=put` and `cmd=get` in the SNMP shell is described in BinTec's **Software Reference**. You can use these commands to access the flash card by inserting the file name "`/card/`" before the parameter `path`. See chapter 16.2.2, page 474.

16.2.5 Command `fssh` in the SNMP Shell of XCENTRIC

The command `fssh` is available in the SNMP shell for operations with the flash card. `fssh` can be started in command line mode (`fssh <command> <parameter>`) or in interactive mode (`fssh -i`).

Please note:
Parameters shown in the command lines inside square brackets [ ] represent optional values. Terms inside angle brackets < > can have different values. Do not enter any brackets!

Command Line Mode

```
fssh <command> <parameter>
```

In this mode, you must always enter the command `fssh` first and then the relevant command for executing an operation.

Interactive Mode

```
fssh -i
```

`fssh -i` starts the interactive mode for flash card operations. If you are in interactive mode, `fssh >` appears as input prompt. You can now enter all commands directly – without "`fssh`". To leave the interactive mode enter the command `quit`.

The following commands are available for operations on the flash card:

format

```
format
```

The command `format` deletes all data on the flash card!

The command `format` is used to format a flash card. The flash card must be formatted before being used for the first time in order to create the file system and directory structure described in chapter 16.2.2, page 474.

dir

`dir [<directory name>]`

Shows the content of the flash card (file names and attributes set) in the working directory without parameters. Entering a directory shows the content of this directory.

del

`del <file name>`

Deletes the file `<file name>` from the flash card.

- `file name`: File name of the file to be deleted.

copy

`copy <file name> <new file name>`

Creates a copy of the file `<file name>` under the new name `<new file name>`.

- `file name`: File name of the original file.
- `new file name`: File name of the copy of the file.

move

`move <file name> <new file name>`

Renames the file `<file name>` to the file `<new file name>`.

- `file name`: File name of the file.
- `new file name`: New file name of the file.

update

`update <host> <remote file> [<local file>]`

Loads the system software file <remote file> from the PC <host> via TFTP with the file name <local file> into the working directory (see chapter 16.2.2, page 474) on the flash card. The attribute boot is set for the system software file. This makes the file bootable. See also "chattr", page 483.

- host: The IP address of the PC (TFTP server) on which the file is located.
- remote file: File name of the system software file.
- local file: File name of the system software file on the flash card.

If the parameter local file is not used, the system software file is automatically given the file name "XCnnn.XCM" on writing to the flash card, where "nnn" stands for the version number of the system software file. If the parameter local file is used, the system software file on the flash card is given this name. The file name is not assigned automatically as described above.

Information about patch or beta versions of system software is lost if the command update is used without the parameter local file.

Example: The system software file for version 5.1.4 is overwritten by the system software file version 5.1.4 Patch 4, because both files are given the same file name on writing to the flash card.

Use the parameter local file for such cases.

chattr

```
chattr <file name> <+boot | -boot>
```

Changes the boot attribute of a file. Only one system software file can be bootable on the flash card at any one time. If the boot attribute is set for a second file, this automatically resets the boot attribute of the first file.

- file name: File name of the file for which the boot attribute is to be set or removed.
- +boot: Sets the boot attribute of a file.
- -boot: Removes the boot attribute of a file.

For checking the attributes, see "dir", page 482.

tftpget

```
tftpget <host> <remote file> <file name>
```

Loads the file <remote file> from the PC (TFTP server) <host> and saves it under the indicated name <file name> on the flash card.

- host: The IP address of the PC (TFTP server) on which the file is located.
- remote file: File name of the file on the TFTP server.
- file name: File name of the file on the flash card.

The commands tftpget and tftpput are only to be used for transferring system software files. For the management of configuration files, the commands described in chapter 16.2.4, page 476 must be used.

A configuration file that is saved to the flash card by a TFTP server using the command tftpget cannot be read by the system software of **XCENTRIC**!

tftpput

```
tftpput <host> <remote file> <file name>
```

Saves the file <file name> under the name <remote file> via TFTP on the PC (TFTP server) <host>.

- host: The IP address of the PC (TFTP server) on which the file is to be saved.
- remote file: File name of the file on the TFTP server.
- file name: File name of the file on the flash card.

fsck

```
fsck
```

Checks the file system of the flash card, but makes no corrections.

16.3 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 **XCENTRIC**, this chapter tells you how to update your software.

www.bintec.de

If you want to update your software, load the new system software in **XCENTRIC** (software image/boot image). Every system software includes new features, better performance and any necessary bugfixes from the previous version. You can find the most up-to-date system software available from BinTec Communications AG on the World Wide Web at www.bintec.net. Here you can also find current product-specific documentation (release notes, manuals, quick install guides) and general product information (Software Reference, BRICKware for Windows).

If you want to update your software, make sure you read the corresponding release notes. The release notes describe the changes provided by the new system software (software image/boot image).

update

There are various ways to update software. This chapter will show you how to update with the help of the update command in the SNMP shell, which is described step for step. The alternatives to this method can be found in the Software Reference and in chapter 19.6, page 521.

Caution!

An update of the module logic, BOOTmonitor and/or firmware logic is also recommended in isolated cases. If this should be the case with a new release, this is clearly noted in the corresponding release notes. The procedure and recommendation can then be found in the "BOOTmonitor and Firmware Logic Update" release notes at www.bintec.net (Section: "Download").
The result of incorrect updating operations (e.g. power cut during the update) could be that **XCENTRIC** no longer boots!

➤ Update the module logic, BOOTmonitor or firmware logic only if BinTec Communications AG explicitly recommends such action!

To do Proceed as follows to update the system software:

Do not turn **XCENTRIC** off during the update!

Before starting the update, deactivate auto logout by entering `t 0` in the SNMP shell.

- Type in the URL `www.bintec.de` in your browser (e.g. Internet Explorer or Netscape Navigator).

  The BinTec home page opens.

- Click "Solutions & Products" and then "Download".

  Here you will find the latest software and documentation for BinTec products.

- Click **XCENTRIC**.

  Here you will find the latest software and documentation for **XCENTRIC**.

- Click the current system software (software image/boot image) with the right mouse button, e.g. Software Image Rel. 5.1 Rev.2.

- In the context menu, click **Save link as...**

- Type in the directory and name under which the new system software (software image/boot image) should be saved on your PC. The directory is normally C:\BRICK for Windows PCs and /tftpboot for Unix workstations. Use a clearly recognizable name, e.g. xc512.xc.

- 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 8.3, page 140). Activate the TFTP server.
  For a Unix computer: Follow the instructions in the Software Reference.

- Log in to **XCENTRIC**, if you have not already done so.

- Deactivate auto logout with `t 0`.

- In the SNMP shell, type in `update <IP address> <file name>`.
  The `<IP address>` is the IP address of the TFTP server, e.g. the IP address of your Windows PC on which the TFTP server of DIME Tools is run-

ning and on which you have saved the new system software (e.g. 192.168.1.1).

In exceptional cases, it may be necessary for certain Unix TFTP servers to enter the file name here with path data.

`<file name>` is the name of the system software you have saved on your PC (e.g. xc512.xc).

The file <file name> is first transferred to the memory of **XCENTRIC** 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 internal flash memory.

XCENTRIC requires a connected block of free working memory that is somewhat larger than the new system software (software image/boot image). If insufficient memory is available on **XCENTRIC**, **XCENTRIC** offers an incremental update, in which the image 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 software 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**.

XCENTRIC 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**.

XCENTRIC starts with the new system software. The existing configuration is transferred.

17 Trouble Shooting

Tips If you are having problems with **XCENTRIC**, the following tips should help you to overcome some of the more usual stumbling blocks:

- Log in to **XCENTRIC** 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 **XCENTRIC** (see chapter 15.1.1, page 416). 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

17.1 Aids to Troubleshooting

Here you can find methods to help narrow down the possible causes of your problem:

- Local SNMP Shell Commands
- External Aids

17.1.1 Local SNMP Shell Commands

These commands are entered directly in **XCENTRIC**'s SNMP shell:

debug

You can use the `debug` command for troubleshooting in one or more subsystems of **XCENTRIC**. A detailed explanation of the syntax and options can be found in chapter 18.1, page 500.

Examples:

- Enter `debug all` to display debugging information for all subsystems.
- Enter `debug config &` for tracking down configuration management problems (see chapter 16, page 465).

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 detail in chapter 18.1, page 500.

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 18.1, page 500.

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 **XCENTRIC**'s MAC address over the LAN to the host with the MAC address 0:a0:f9:d:5:a.

17.1.2 External Aids

You can analyze connections to **XCENTRIC** using the following utility programs on a Windows PC or Unix workstation.

DIME Tracer (Windows)

The DIME Tracer enables you to trace **XCENTRIC**'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 **XCENTRIC**'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 18.2, page 507.

17.2 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

17.2.1 System Errors

I have forgotten my password.

You must reset **XCENTRIC** to the unconfigured initial state (ex works state):

1. Connect your router over the serial interface to **XCENTRIC** as explained in chapter 8.1.1, page 123.
2. Switch **XCENTRIC** off and then switch it on again.

   You see various selftests and then "Press <sp> for BOOTmonitor or any other key to boot system".
3. Now press the Space bar.

   A BOOTmonitor menu is displayed.
4. Select (4) Delete Configuration and press **Return**. Note and confirm the following safety prompts.

   The password as well as the complete configuration of **XCENTRIC** are deleted.
5. Select (1) Boot System.

   XCENTRIC is restarted.
6. Reconfigure **XCENTRIC**.

I can't reach XCENTRIC in the LAN.

Try to establish a serial connection:

- Connect your PC to **XCENTRIC** 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? If so, make the required corrections.

If a serial connection does not work either:

- Check the settings of the terminal program (see chapter 8.1.1, page 123). 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".

17.2.2 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 15.1.3, page 424). This enables you to set a limit for connections to **XCENTRIC** to prevent unnecessary charges accumulating as a result of mistakes made during configuration.

In case of ISDN connections on **XCENTRIC** 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 **XCENTRIC**.
- 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 **XCENTRIC** 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 **XCENTRIC** is configured so that SNMP traps are sent to a host outside the LAN (destination ports 161, 162).
- Check if the second B-channel is frequently set up and cleared for connections with dynamic channel bundling due to fluctuating traffic.
- Use `debug all` or `trace` to check if a PC in the LAN is configured for the WINS server with an incorrect IP address (destination ports 137-139). If necessary, configure the PC properly or set the corresponding filters.
- Use `debug all` or `trace` to check if a PC in the LAN is configured for the resolution of NetBIOS names with the help of DNS (it is accessed from a client port to destination port 53). Do not try to resolve NetBIOS names with DNS!
- Use `debug all` or `trace` to check if an application on a PC in the LAN is trying to resolve names that the name server at the Internet provider does not know (it is accessed from a client port to destination port 53). Configure a local HOSTS file in the Windows directory that can carry out name resolution (see chapter 12.2.2, page 332).
- Use `debug all` or `trace` to check if NetBIOS over IP is configured on a PC in the LAN (it is accessed from source port 137 to destination port 53). An attempt is thus made to resolve NetBIOS names over DNS. Disable NetBIOS over IP or insert filters (configuration of the corresponding filters can be found in chapter 10.1.5, page 161 or use the simple NetBIOS filter of the Configuration Wizard).
- Check if you have configured Callback (see chapter 15.2.4, page 437) 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 **XCENTRIC** to determine if a connection is made (see chapter 7, page 111).
- 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.
- Check ***WAN PARTNER*** ➧ ***WAN NUMBERS*** to see if you have taken external line access into account on entering the extension of the WAN partner, if applicable. See chapter 10.2.1, page 167.
- Use `trace` to check what is being sent over the ISDN channels.
- Check if you have correctly entered your own extension for external S_0 connections. This also applies to outgoing calls.

Incoming calls cannot be made.

- Check the LEDs on the front of **XCENTRIC** (see chapter 7, page 111) 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 ***PABX*** ➧ ***EXTENSIONS*** to determine if you have made the necessary entries for incoming calls.

- Check if *Encapsulation* in ***WAN PARTNER*** ➧ ***EDIT*** is the same for both connection partners.
- Check if *Authentication* in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***PPP*** is the same for both connection partners.

17.2.3 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 **XCENTRIC**'s LAN.
- Check if a router between them filters out the SAP packets.
- Check with ISDN Login 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 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.

XCENTRIC 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 **XCENTRIC** 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.

18 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

18.1 SNMP Shell Commands

XCENTRIC 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 a ? displays a list of the most important commands available on **XCENTRIC**.

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 millisecondsn
- `-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 ... 4. Selects the physical interface for modules with five interfaces.
- `slot`: 1 ... 5. 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 504).
- `-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` = **XCENTRIC**'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] [-b <bits>] isdn-number
[isdn-service]| layer1-protocol]
```

Is used to open a remote login shell on **XCENTRIC** over ISDN.

- `-c <stknumber>`: selects the ISDN stack to use for this login.
- `-C`: tries to use compression (V.42bis).
- `-b <bits>`: use only <bits> bits for transmission (e.g. enter `-b 7` for 7-bit ASCII transmission).
- `isdn-number`: isdn number of the ISDN partner you want to log in to.

- `isdn-service`: the ISDN service you want to use (data, telephony, fax g3, fax g4, btx).
- `layer1-protocol`: Possible values: v110_1200, v110_2400, v110_4800, v110_9600, v110_19200, v110_38400, modem, dovb56k, telephony.

The option `-c` cannot be used on **XCENTRIC**.

You can obtain other options for the `isdnlogin` command with `isdnlogin -?`.

debug

```
debug [show]|[[-q] all|acct|system|<subs> [<subs> ...]]
```

Is used to selectively display debugging information originating from one of **XCENTRIC**'s subsystems.

- `show`: displays all possible subsystems that can be debugged.
- `-q`: no timestamp attached before each debugging message.
- `all`: displays debugging information for all subsystems.
- `acct`: displays debugging information for the accounting subsystem.
- `system`: displays debugging information for all subsystems except the accounting subsystem.
- `subs`: subsystem for which debugging information is to be displayed. Several entries are possible (separated by a space).

ifconfig

```
ifconfig <interface> [destination <destaddrs>] [<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 <destaddrs>`: destination IP address of a host. This adds a host route for this host in the routing table (**ipRouteDest**).
- `address`: **XCENTRIC**'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-IIc 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]`

XCENTRIC 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 **XCENTRIC** 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 **XCENTRIC** 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 `-?` usually provides syntax help.

The `update` command can be found in chapter 16.3, page 485.

Further SNMP commands can be found in the Software Reference.

18.2 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 **XCENTRIC** 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 ... 4. Selects the physical interface for modules with five interfaces.
- `slot`: 1 ... 5. 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 **XCENTRIC** are displayed. The IP address of **XCENTRIC** 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>)

19 Technical Data

General product features:

Feature	Description
Dimensions without cables	428 mm W x 305 mm H x 175 mm D
Installation	Wall mounting
Weight	approx. 5 kg
Transport weight (incl. documentation, cabling, packaging)	approx. 8 kg
Ambient requirements:	
Storage temperature	-20 °C to +85 °C
Operating temperature	0 to 40 °C
Relative humidity	20 to 90 % non-condensing in operation
	5 to 95 % non-condensing in storage
Room classification	Operate only in dry rooms
Installation	The equipment is only to be operated when mounted vertically on a wall.

Table 19-1: Technical data for complete product

19.1 Mains Unit

Connect the IEC AC socket of the mains unit to the power supply using the power cord supplied with the equipment.

	Electrical ratings
Mains voltage	230 to 240 V AC
Mains frequency	50/60 Hz
Max. current	600 mA

Table 19-2: Technical data for mains unit

19.2 Basic Unit

Features of basic unit:

Feature	Description
Processor	Motorola MC68EC020, 20 MHz
Memory	8 MB RAM 2 MB flash ROM
Interfaces	Serial interface Ethernet/LAN Interface Door intercom interface Music-on-hold interface
Slots	Altogether six slots available for use: Slot 2 to 5 for communication modules Slot 6 and 7 for hub modules

Table 19-3: Technical data for basic unit

19.2.1 Serial Interface

Pin assignment of serial interface of basic unit (8-pole mini DIN socket):

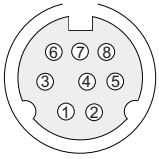


Figure 19-1: Serial interface of basic unit

Pins of mini DIN socket	Assignment
1	NC
2	NC
3	T
4	GND
5	R
6	NC
7	NC
8	NC

Table 19-4: Pin assignment of serial interface of basic unit

19.2.2 Ethernet/LAN Interface

Pin assignment of 10/100 Mbps Ethernet/LAN interface of basic unit (RJ45 socket):

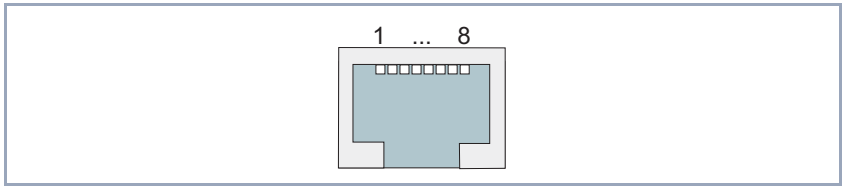


Figure 19-2: 10/100 Mbps Ethernet/LAN interface of basic unit

Pins of RJ45 socket	Assignment
1	T+
2	T-
3	R+
4	NC
5	NC
6	R-
7	NC
8	NC

Table 19-5: Pin assignment of 10/100 Mbps Ethernet/LAN interface of basic unit

19.2.3 Door Intercom Interface

Pin assignment and detailed description of connection of door intercom unit (XCM-TFE) in basic unit:

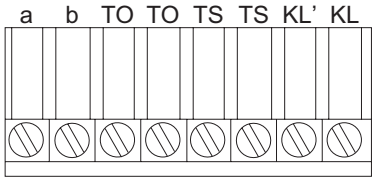


Figure 19-3: Pin assignment of 8-pole screw terminal connector of XCM-TFE

Connections of door intercom interface	Remarks
a/b	ab interface for connecting a speech circuit without DC component.
TO/TO	Floating connection for the door opener. Max. load of floating connection: max.: switching power: 30 W/ 62.5 VA max. switching voltage: 110 V DC/ 125 V AC max. switching current: 1 A All three values must be maintained at all times.
TS/TS	Floating connection for the door intercom supply voltage. Max. load of floating connection: max.: switching power: 30 W/ 62.5 VA max. switching voltage: 110 V DC/ 125 V AC max. switching current: 1 A All three values must be maintained at all times.
KL'/KL	Connection for a door bell button Max. input voltage: 8 to 20 V (AC/DC) If the bell circuit is operated with DC voltage, KL' is the positive terminal (+).

Table 19-6: Description of connections of door intercom interface

19.2.4 Flash Card Slot

The flash card slot is planned for a future extension and is not used at present.

19.2.5 Music-on-Hold Interface

The music-on-hold interface is a stereo jack, which must be connected by a 3.5 mm jack plug to the headphone output of external audio equipment.

19.3 XCM-5S0

The XCM-5S0 has five 4-pole screw terminal connectors, whose pin assignment for an external and internal connection is shown in the following figures.

The signals are indicated from the module's viewpoint, for example, "T" is an outgoing signal from the module.

Internal S_0 connection:

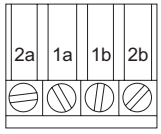


Figure 19-4: Pin assignment of internal S_0 connection on XCM-5S0

ISDN pin assignment	Signals
2a	R+
1a	T+
1b	T-
2b	R-

Table 19-7: Signals and ISDN pin assignment for an internal S_0 connection

External S_0 connection:

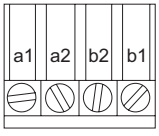


Figure 19-5: Pin assignment for external S_0 connection on XCM-5S0

ISDN pin assignment	Signals
a1	R+
a2	T+
b2	T-
b1	R-

Table 19-8: Signals and ISDN pin assignment for an external S_0 connection

19.4 XCM-S04AB

19.4.1 S_0 Interface

Pin assignment of external S_0 interface of XCM-S04AB module (RJ45 socket).

The signals are indicated from the module's viewpoint, for example, "T" is an outgoing signal from the module.

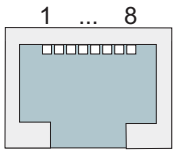


Figure 19-6: S_0 interface of XCM-S04AB

Pins of RJ45 socket	ISDN pin assignment	Signals
1		NC
2		NC
3	a2	T+
4	a1	R+
5	b1	R-
6	b2	T-
7		NC
8		NC

Table 19-9: Pin assignment of external S_0 interface of XCM-S04AB (RJ45 socket)

19.4.2 ab Interface

Pin assignment of 3-pole screw terminal connector for ab interface:

BT is a ringing capacitor that is used for British Telecom purposes only.

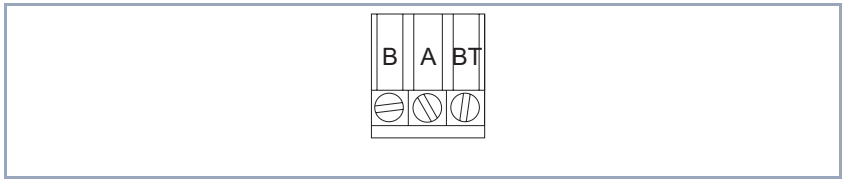


Figure 19-7: ab interface of XCM-S04AB

19.5 XCM-HUB

The XCM-HUB module has 8 ports as Ethernet/LAN interfaces. These ports are RJ45 sockets with the following pin assignment:

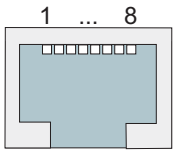


Figure 19-8: 10/100 Mbps Ethernet/LAN interface of XCM-HUB

Pins of RJ45 socket	Assignment
1	R+
2	R-
3	T+
4	NC
5	NC
6	T-
7	NC
8	NC

Table 19-10: Pin assignment of 10/100 Mbps Ethernet/LAN interface of XCM-HUB

19.6 BOOT Sequence

XCENTRIC passes through various functional states on starting (see also chapter 7.1, page 112):

- Start Mode
- BOOTmonitor Mode
- Normal Operation Mode

After several selftests have been performed successfully in Start Mode, **XCENTRIC** changes to the BOOTmonitor Mode. The BOOTmonitor prompt is displayed if you are connected to **XCENTRIC** via a terminal program.

BOOTmonitor

Press **Space** within four seconds of the display of the BOOTmonitor prompt if you want to use the BOOTmonitor functions. If you do not make an entry within 4 seconds, **XCENTRIC** changes back to Normal Mode.

Functions

The BOOTmonitor provides the following functions, which you select by entering the relevant digit (for more detailed information, refer to **Software Reference**):

- (1) Boot system:
  XCENTRIC loads the compressed boot file from the flash memory to the RAM memory. This happens automatically when started.
- (2) Software update via TFTP:
  XCENTRIC performs a software update via a TFTP server.
- (3) Software update via XMODEM:
  XCENTRIC performs a software update over a serial interface with XMODEM.
- (4) Delete configuration:
  XCENTRIC 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 **XCENTRIC**'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 **XCENTRIC**!

20 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 **XCENTRIC** 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 **XCENTRIC** die Hinweise für die Umgebungsbedingungen (vgl. Technische Daten).
- Beachten Sie bei der Installation externer ISDN-Basisanschlüsse die jeweils gültigen Rahmenbedingungen Ihres Landes. Gegebenenfalls ist ein Techniker erforderlich, der über die entsprechende Zulassung verfügt. Informieren Sie sich über die Besonderheiten nationaler Verordnungen und beachten Sie deren rechtliche Grundlagen bei der Installation.
- Elektrostatische Aufladungen können zu Geräteschäden führen. Tragen Sie daher eine antistatische Manschette um das Handgelenk oder berühren Sie eine geerdete Fläche, bevor Sie das geöffnete Gerät oder eines der Module berühren. Berühren Sie Platinen grundsätzlich nur an den Rändern und fassen Sie nicht auf Leitungen oder Bauteile.
- Installieren Sie die Module nur in die dafür vorgesehenen Slots. Bei falscher Montage kann es zur Beschädigung des Moduls oder des gesamten Geräts kommen.
- Speziell bei der Installation der Hub-Module ist darauf zu achten, daß Slot 6 immer bestückt ist und kein einzelnes Hub-Modul in Slot 7 stecken darf, da es sonst zur Beschädigung des Moduls oder des ganzen Geräts kommen kann.
- Verschließen Sie nichtbenutzte Moduleinschübe mit den Blindabdeckungen, damit keine Gegenstände ins Innere des Geräts gelangen können. Befinden sich während des Betriebs Fremdgegenstände im Gerät, besteht Stromschlag- und Kurzschlußgefahr.

- Ein 5-S_0-Modul, auf dem Brücken falsch gesteckt sind, kann bei Inbetriebnahme beschädigt werden. Die Module besitzen in Grenzen integrierte Schutzmaßnahmen, um solche Beschädigungen zu verhindern, Sie sollten beim Stecken von Brücken dennoch sorgfältig vorgehen. Achten Sie unbedingt darauf, daß entsprechend konfigurierte (intern oder extern) Units auch passend verbunden werden.
- Achten Sie bei der Verkabelung darauf, daß die Lüftungsschlitze des Geräts nicht verdeckt werden und die Lüftung nicht behindert wird. Durch Beeinträchtigung der Lüftung von **XCENTRIC** kann es zu Schäden am Gerät kommen. Durch mangelnde Lüftung entstandene Schäden führen zum Garantieverlust.
- Öffnen Sie weder das Netzteil noch das Basisgerät (inklusive TFE-Modul) und nehmen Sie keinerlei Manipulationen am Netzteil vor, da sonst Lebensgefahr durch einen Stromschlag besteht. Entfernen Sie keine Schrauben der Befestigung des Netzteils und des Basisgeräts.
- Wenn das Gerät aus kalter Umgebung in den Betriebsraum gebracht wird, kann Betauung sowohl am Geräteäußeren als auch im Geräteinneren auftreten. Warten Sie, bis Ihr Gerät temperaturangeglichen und absolut trokken ist, bevor Sie es in Betrieb nehmen. Beachten Sie die Umweltbedingungen in den Technischen Daten.
- Prüfen Sie, ob die örtliche Netzspannung mit den Nennspannungen des Netzteils übereinstimmt. Das Gerät darf unter folgenden Bedingungen betrieben werden:
  - 230 - 240 VAC
  - 50/60 Hz
- Stellen Sie sicher, daß die Schutzkontakt-Steckdose der Installation frei zugänglich ist. Zur vollständigen Netztrennung muß der Netzstecker gezogen werden.
- Beachten Sie beim Verkabeln die Reihenfolge, wie im Handbuch beschrieben. Verwenden Sie nur Kabel, die den Spezifikationen in diesem Handbuch genügen oder original mitgeliefert wurden. Falls Sie andere Kabel verwenden, übernimmt BinTec Communications AG für auftretende Schäden oder Beeinträchtigung der Funktionalität keine Haftung. Die Gerätegarantie erlischt in diesen Fällen.

- Beachten Sie beim Anschluß des Geräts die Hinweise im Handbuch. Achten Sie insbesondere beim Aufstecken der Klemmblöcke darauf, daß die Stifte nicht verbogen werden und die Schrauben des aufgesteckten Klemmblocks nach rechts zeigen, da sonst die Schnittstelle nicht funktionsfähig ist und beschädigt werden kann.
- Verlegen Sie Leitungen so, daß sie keine Gefahrenquelle (Stolpergefahr) bilden und nicht beschädigt werden.
- Schließen Sie Datenübertragungsleitungen während eines Gewitters weder an noch ziehen Sie sie ab oder berühren Sie diese.
- Schließen Sie an **XCENTRIC** nur Endgeräte an, die den allgemeinen Sicherheitsanforderungen für Kommunikationsgeräte ensprechen. Endgeräte mit einer Zulassung durch das CETECON (ehemals BZT) entsprechen diesen Anforderungen. ISDN-Endgeräte, die an **XCENTRIC** angeschlossen werden, müssen für das Euro-ISDN (DSS1) zugelassen sein, analoge Endgeräte müssen das DTMF-/Tonfrequenzwahlverfahren unterstützen und auf Tonfrequenzwahlverfahren eingestellt sein.

Bestimmungsgemäße Verwendung, Betrieb

- **XCENTRIC** ist für den Einsatz in einer Büroumgebung bestimmt. Als Multiprotokoll-Router baut **XCENTRIC** in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen.
- **XCENTRIC** entspricht den einschlägigen Sicherheitsbestimmungen für Einrichtungen der Informationstechnik für den Einsatz in einer Büroumgebung.
- **XCENTRIC** ist für die Montage an der Wand vorgesehen und darf nur hängend betrieben werden. Die Lüftung darf auf keinen Fall behindert werden.
- Der bestimmungsgemäße Betrieb gemäß IEC 950/EN 60950 des Systems ist nur bei komplett montiertem Blechgehäuse gewährleistet (Kühlung, Brandschutz, Funkentstörung).
- Die Umgebungstemperatur sollte 40°C nicht übersteigen. Vermeiden Sie direkte Sonneneinstrahlung.

- Achten Sie darauf, daß keine Gegenstände (z. B. Büroklammern) oder Flüssigkeiten ins Innere des Geräts gelangen (elektrischer Schlag, Kurzschluß). Achten Sie auf ausreichende Kühlung.
- Unterbrechen Sie in Notfällen (z. B. beschädigtes Gehäuse oder Bedienelement, Eindringen von Flüssigkeit oder Fremdkörpern) sofort die Stromversorgung und verständigen Sie den Service.

Reinigung und Reparatur

- Das Gerät darf nur durch geschultes Fachpersonal geöffnet werden. Vor Öffnen des Geräts unbedingt den Netzstecker ziehen. Durch unbefugtes Öffnen und unsachgemäße Reparaturen können erhebliche Gefahren für den Benutzer entstehen (z. B. Stromschlag). Lassen Sie Reparaturen am Gerät nur von einer BinTec-autorisierten Servicestelle durchführen. Wo sich die Servicestelle befindet, erfahren Sie von Ihrem Händler.
- 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 **XCENTRIC** vain alkuperäispakkauksessaan tai muussa sopivassa pakkauksessa, joka suojaa töytäisyiltä ja iskuilta.

Asennus ja käyttöönotto

- Tarkista ennen **XCENTRIC** -laitteen asennusta ja käyttöä, että ympäristöolosuhteista annettuja ohjeita (kts. lukua Tekniset tiedot) on noudatettu.
- Asentaessasi ulkoisia ISDN-perusliitäntöjä ota huomioon maassa voimassa olevat ehdot. Joudut mahdollisesti käyttämään apuna teknistä asiantuntijaa, jolla on lupa kyseisentyyppisiin asennustöihin. Ota selvää kansallisista määräyksistä ja noudata niitä asennuksessa.
- Sähköstaattiset varaukset voivat aiheuttaa laitevikoja. Pidä ranteen ympärillä antistaattista ranneketta tai kosketa maadoitettua pintaa, ennen kuin kosket avoimeen laitteeseen tai moduliin. Kosketa kortteja periaatteessa vain reunoista äläkä tartu johtoihin tai komponentteihin.
- Asenna modulit ainoastaan niille varattuihin aukkoihin. Mikäli asennus tapahtuu väärin, moduli tai koko laite voi vahingoittua.
- Erityisesti keskittimiä asennettaessa on huomattava, että aukossa 6 tulee olla aina kortti eikä aukkoon 7 saa asentaa yhtään keskitintä, sillä muuten moduli tai koko laite voi vahingoittua.
- Sulje käyttämättömät aukot suojuksilla, jottei laitteen sisään pääse vieraita kappaleita. Mikäli laitteessa on käytön aikana vieraita kappaleita, voi tapahtua sähköisku tai oikosulku.
- 5-S_0-moduli, jonka jumpperit on asennettu väärin, voi vahingoittua käyttöönotossa. Moduleissa on rajoihin integroituja suojatoimenpiteitä, joilla tällaiset vahingot estetään. Jumppereita asennettaessa suojatoimenpiteiden on toteuduttava tarkasti. Tarkista ehdottomasti, että oikein konfiguroidut sisäiset tai ulkoiset yksiköt myös liitetään oikein.
- Huomaa kaapeloitaessa, että laitteen tuuletusraot eivät peity ja tuuletus ei esty. **XCENTRIC**:n tuuletuksen estyessä laitteeseen voi syntyä vaurioita. Puutteellisesta tuuletuksesta aiheuneet vauriot johtavat takuun raukeamiseen.

- Älä avaa verkko-osaa äläkä peruslaitetta (ja TFE-modulia) äläkä tee mitään toimenpiteitä verkko-osalle, sillä sähköisku voi aiheuttaa hengenvaaran. Älä poista verkko-osasta ja peruslaitteesta kiinnitysruuveja.
- 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, vastaako paikallinen verkkojännite verkko-osan nimellisjännitettä. Laitetta saa käyttää seuraavissa olosuhteissa:
  – 230 - 240 VAC
  – 50/60 Hz
- Varmista, että suko-pistorasia on asennusta varten vapaasti tavoitettavissa. Verkkopistoke on vedettävä pistorasiasta laitteen irrottamiseksi täydellisesti verkosta.
- Huomaa kaapeloitaessa käsikirjassa kuvailtu järjestys. Käytä vain kaapelia, joka vastaa tämän käsikirjan spesifikaatioita tai joka toimitettiin alunperin laitteen mukana. Jos käytät toista kaapelia, BinTec Communications AG ei ota vastuuta vahingoista tai toiminnan huonontumisesta. Tällaisissa tapauksissa laitetakuu raukeaa.
- Noudata laitetta kytkiessäsi käsikirjan ohjeita. Erityisesti riviliittimiä asennettaessa on varottava, etteivät nastat väänny ja että paikalleen asennetun riviliittimen ruuvit osoittavat oikealla, sillä muuten liitäntä ei ole kunnossa ja voi vahingoittua.
- Vedä kaapelit sellaisiin paikkoihin, että ne eivät aiheuta vaaratilanteita (kompastumisia) eivätkä vahingoitu.
- Älä liitä, irrota tai kosketa tiedonsiirtokaapeleita ukonilman aikana.
- Kytke **XCENTRIC** -laitteeseen ainoastaan päätelaitteita, jotka vastaavat telelaitteiden yleisiä turvavaatimuksia. CETECONIN (entisen BZT:n) luvalla varustetut päätelaitteet vastaavat näitä ehtoja. ISDN-päätelaitteilla, jotka liitetään **XCENTRIC** -laitteisiin, on oltava Euro-ISDN-lupa (DSS1). Analogisten päätelaitteiden on tuettava DTMF:ää/äänitaajuusvalintaa ja niiden on oltava äänitaajusvalintaa varten säädettyjä.

Määräystenmukainen käyttö, käyttö

- **XCENTRIC** on tarkoitettu käytettäväksi toimistoympäristössä. **XCENTRIC** on moniprotokollareititin, jonka avulla voidaan luoda järjestelmäkonfiguraatiosta riippuen WAN-yhteyksiä. Jotta ei-toivotuilta maksuilta vältytään, laitetta tulee ehdottomasti valvoa.
- **XCENTRIC** vastaa toimistotiloissa käytettäville tietotekniikan laitteistoille asetettuja asiaankuuluvia turvallisuusmääräyksiä.
- **XCENTRIC** on tarkoitettu seinäasennukseen, ja sitä saa käyttää ainoastaan ripustettuna. Tuuletuksen tulee ehdottomasti tapahtua esteettömästi.
- Järjestelmän IEC 950/EN 60950 mukainen käyttö on taattu ainoastaan, mikäli peltikotelo on asennettu täydellisesti (jäähdytys,palosuoja, kipinäsuoja).
- Ympäristön lämpötila ei saisi nousta yli 40°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

- Laitteen avaaminen on sallittua ainoastaan koulutetulle ammattihenkilökunnalle. Vedä ehdottomasti verkkotöpseli irti ennen laitteen avaamista. Luvaton avaaminen ja epäasialliset korjaukset voivat aiheuttaa käyttäjälle huomattavaa vaaraa(esim. sähköisku). Teetä laitekorjaukset ainoastaan BinTec-valtuutetussa huoltopisteessä. Tietoja huoltopisteistä saa myyjältä.
- Älä missään tapauksessa puhdista 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 **XCENTRIC** 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 **XCENTRIC**, veuillez vous référer aux indications concernant les conditions d'environnement (cf. Caractéristiques techniques).
- Lors de l'installation d'appareils de base RNIS externes, respectez impérativement les conditions cadres en vigueur dans votre pays. Au besoin, faites appel à un technicien dûment agréé. Pour l'installation, veuillez vous informer des particularités des dispositions nationales et en respecter les bases juridiques.
- Des charges électrostatiques peuvent endommager l'appareil. Il est donc important que vous portiez un bracelet antistatique ou que vous touchiez une surface mise à la terre avant de toucher l'appareil ouvert ou l'un des modules. Il est impératif de ne saisir les platines que par les bords et de ne pas toucher aux conducteurs ni aux composants.
- N'installez les modules que dans les slots prévus à cet effet. Un montage incorrect risque d'entraîner des dommages du module ou de l'ensemble de l'appareil.
- Pour l'installation des modules nodaux en particulier, veillez à ce que le slot 6 soit toujours occupé et qu'aucun module nodal ne se trouve dans le slot 7, car ceci pourrait endommager le module ou l'ensemble de l'appareil.
- Refermez les tiroirs à modules non utilisés avec des caches borgnes, de manière à ce que rien ne puisse pénétrer à l'intérieur de l'appareil. Si des objets se trouvent à l'intérieur de l'appareil en fonctionnement, il y a risque d'électrocution et de court-circuit.
- Un module 5-S_0 peut être endommagé au moment de la mise en service, si des pontages y ont été mal placés. Ces modules sont équipés de dispositifs de protection intégrés offrant une protection dans certaines limites et

permettant d'éviter ce genre de dommages ; toutefois, il est vivement conseillé de procéder à la mise en place des pontages avec une extrême prudence. Veillez impérativement à ce que les unités correctement configurées (de façon interne ou externe) soient reliées de manière adéquate.

- Lors du câblage, veillez à ne pas recouvrir les fentes d'aération de l'appareil de manière à ne pas entraver la ventilaton. Le droit de garantie est annulé lorsque les dommages résultent d'une ventilation insuffisante.
- N'ouvrez ni le bloc d'alimentation, ni l'appareil de base (y compris le modu-le ouvre-porte) et n'effectuez aucune manipulation sur le bloc d'alimentati-on, sous risque de danger de mort par électrocution. Ne retirez aucune vis du dispositif de fixation du bloc d'alimentation et de l'appareil de base.
- 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 secteur locale correspond aux tensions nominales du bloc d'alimentation. L'appareil ne devra fonctionner que dans les conditions ci-après :
  - 230 - 240 Vca
  - 50/60 Hz
- Vérifiez si la prise de courant de sécurité pour l'installation est librement accessible. Il faut retirer la fiche de contact pour garantir la déconnexion du secteur.
- Lors du câblage, respectez les étapes indiquées dans le manuel. N'utilisez que les câbles correspondants aux spécifications indiquées dans ce manuel ou les câbles d'origine joints lors de la livraison. Dans le cas où vous utiliseriez d'autres câbles que ces derniers, la société BinTec Communications AG décline toute responsabilité pour des dommages éventuels ou pour tout défaut de fonctionnement pouvant en résulter. Dans de tels cas, la garantie est annulée.

- Pour le raccordement de l'appareil, respectez les indications du manuel. Lors de la mise en place des répartiteurs, veillez en particulier à ce que les broches ne soient pas tordues et que les vis du répartiteur enfiché soient tournées vers la droite, sinon l'interface risque de pas fonctionner et de subir des dégâts.
- 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.
- Ne raccordez à un **XCENTRIC** que des terminaux répondant aux critères généraux de sécurité pour les appareils de télécommunication. Les terminaux ayant une homologation CETECON (auparavant BZT) satisfont à ces exigences. Les terminaux RNIS à raccorder au **XCENTRIC** doivent être homologués euro-RNIS (DSS1) ; les terminaux analogiques doivent supporter la DTMF (tonalité multifréquence) et être réglés sur la numérotation à fréquences vocales.

Utilisation conforme, fonctionnement

- **XCENTRIC** est conçu pour l'utilisation dans les bureaux. En tant que router multiprotocole, **XCENTRIC** 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.
- **XCENTRIC** est conforme aux prescriptions de sécurité relatives aux équipements de la technique de l'information pour l'utilisation dans les bureaux.
- **XCENTRIC** est conçu pour être installé au mur et ne devra fonctionner qu'en étant suspendu. Eviter impérativement tout obstacle à l'aération.
- Le fonctionnement de ce système conformément aux normes CEI 950/ EN 60950 ne peut être garanti que si le boîtier métallique est complètement monté (refroidissement, protections anti-incendie et antiparasite).
- La température ambiante ne doit pas dépasser 40°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. Avant d'ouvrir l'appareil, retirez impérativement la fiche secteur. Une ouverture non autorisée et des réparations non conformes aux règles de l'art exposent l'utilisateur à des risques très graves (risque d'électrocution par ex.). 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.
- 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 **XCENTRIC** 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 **XCENTRIC** να λάβετε υπ' όψιν σας τις οδηγίες σχετικά με τις συνθήκες περιβάλλοντος (βλέπε Τεχνικά στοιχεία).
- Προσέχετε στην εγκατάσταση των εξωτερικών ISDN- συνδέσεων τους ισχύοντες κανονισμούς της χώρας σας.Ίσως χρειαστεί τεχνικός ο οποίος έχει την ανάλογη άδεια Πληροφορηθείτε για τις ιδιαιτερότητες των εθνικών διατάξεων, και προσέξτε την σχετική νομοθεσία κατά την εγκατάσταση.
- Ηλεκτροστατικά φορτία μπορούν να προκαλέσουν βλάβη στη συσκευή. Γι αυτό, πριν έρθετε σε επαφή με την ανοιχτή συσκευή ή τα ηλεκτρονικά στοιχεία θα πρέπει να φοράτε ένα αντιστατικό μανικέτι γύρω από το χέρι σας ή να αγγίζετε μία γειωμένη επιφάνεια. Αγγίζετε τις πλατίνες μόνο στις άκρες και μη πιάνετε καλώδια η εξαρτήματα.
- Εγκαταστείστε τα ηλεκτρονικά στοιχεία μόνο στις ειδικά γι' αυτά προορισμένες υποδοχές. Σε περίπτωση λανθασμένης εγκατάστασης μπορεί να προκληθεί βλάβη στα ηλεκτρονικά στοιχεία ή και σε ολόκληρη τη συσκευή.
- Ειδικά κατά την εγκατάσταση των στοιχείων ανύψωσης , πρέπει να προσέχετε ότι η υποδοχή 6 πρέπει να είναι πάντα εξοπλισμένη, και ότι στην υποδοχή 7 δεν πρέπει ποτέ να τοποθετούνται στοιχεία ανύψωσης, διαφορετικά μπορεί να προκληθεί βλάβη στα ηλεκτρονικά στοιχεία και στην συσκευή.
- Σκεπάζετε τις μη χρησιμοποιημένες προσθήκες των ηλεκτρονικών στοιχείων με το κάλυμμα, για να μη μπουν αντικείμενα στη συσκευή. Αν κατά την διάρκεια της λειτουργίας υπάρχουν στη συσκευή ξένα

αντικείμενα, υπάρχει κίνδυνος ηλεκτροπληξίας και βραχυκυκλώματος..

- Ένα ηλεκτρονικό στοιχείο 5-S0 στο οποίο οι γέφυρες τοποθετήθηκαν λανθασμένα, μπορεί να πάθει βλάβη όταν λειτουργεί. Τα ηλεκτρονικά στοιχεία έχουν ενσωματωμένες ασφάλειες που παρεμποδίζουν τέτοιες βλάβες. Παρόλα αυτά, πρέπει να προσέχετε όταν γίνεται η εγκατάσταση των γεφύρων. Επίσης θα πρέπει να προσεχτεί η κατάλληλη σύνδεση των αντίστοιχων διαρθρωμένων Units (εσωτερικών ή εξωτερικών).
- Κατά την καλωδίωση προσέξτε ώστε να μην καλύπτονται οι σχισμές εξαερισμού της συσκευής και να μην εμποδίζεται ο αερισμός. Από τον μειωμένο αερισμό του **XCENTRIC** μπορούν να προκληθούν ζημιές στην συσκευή. Οι βλάβες που προκύπτουν από ελλιπή αερισμό συνεπάγονται την απώλεια της εγγύσης.
- Μη ανοίγετε το ρευματολήπτη ούτε τη βασική συσκευή (συμπεριλαμβανομένου και του Modul TFE) και μην κάνετε μετατροπές στον ρευματολήπτη, διότι υπάρχει κίνδυνος θάνατος απο ηλεκτροπληξία. Μη βγάζετε της βίδες στερέωσης του ρευματολήπτη ή της βασικής συσκευής.
- 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.
- Εξετάστε αν η τάση του τοπικού ηλεκτρικού δικτύου συμφωνεί με την ονομαστική τάση του ρευματολήπτη. Η λειτουργία της συσκευής επιτρέπεται μόνο με τις ακόλουθες προϋποθέσεις:
  - 230 - 240 VAC
  - 50/60 Hz
- Βεβαιωθείτε πως η πρίζα σούκο της εγκατάστασης είναι προσιτή. Για την πλήρη αποσύνδεση από το ρεύμα πρέπει να βγάζετε το φις από την πρίζα.

- Κατά την καλωδίωση προσέξτε την σειρά που περιγράφεται στο εγχειρίδιο. Να χρησιμοποιείτε μόνον καλώδια που πληρούν τα χαρακτηριστικά στο εγχειρίδιο ή τα γνήσια που παραλάβατε. Αν χρησιμοποιείτε άλλα καλώδια, τότε η BinTec Communications AG δεν αναλαμβάνει καμία ευθύνη για ζημιές ή βλάβες στην λειτουργικότητα. Σε αυτές τις περιπτώσεις παύει να ισχύει η εγγύηση της συσκευής.
- Προσέξτε κατά την σύνδεση της συσκευής τις συμβουλές στο εγχειρίδιο. Προσοχή όταν τοποθετείτε τα στοιχεία σύνδεσης να μην κυρτώσουν οι πείροι και να μην δείξουν δεξιά οι βίδες του εφαρμοζόμενου στοιχείου σύνδεσης, διότι έτσι δεν λειτουργεί η διεπαφή και ίσως προκληθεί βλάβη.
- 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 βγάζετε τα καλώδια μεταφοράς δεδομένων, ούτε να τα ακουμπάτε.
- Συνδέστε στο **XCENTRIC** μόνο συσκευές που ανταποκρίνονται στους γενικούς κανόνες ασφαλείας για συσκευές επικοινωνίας. Τερματικές συσκευές με άδεια από την CETECON (πρώην BZT) ανταποκρίνονται σε αυτούς τους κανονισμούς. Οι συσκευές ISDN που συνδέονται στο **XCENTRIC** πρέπει να είναι εγκεκριμένες για το EURO-ISDN (DSS1), οι αναλογικές συσκευές πρέπει να υποστηρίζουν την διαδικασία επιλογής συχνότητας τόνου (DTMF) καθώς και να είναι ρυθμισμένες για αυτή τη διαδικασία.

Προβλεπόμενη χρήση, λειτουργία

- Το **XCENTRIC** προορίζεται για χρήση σε περιβάλλον γραφείου. Σαν Router πολλαπλών πρωτοκόλλων (Multi-Protokoll) το **XCENTRIC** σε εξάρτηση από την διαμόρφωση του συστήματος δημιουργεί συνδέσεις WAN. Για να αποφύγετε πρόσθετα τέλη θα πρέπει οπωσδήποτε να επιτηρείτε την συσκευή.
- Το **XCENTRIC** ανταποκρίνεται στις σχετικές διατάξεις ασφαλείας για εγκαταστάσεις τεχνολογίας πληροφοριών κατά τη χρήση σε περιβάλλον γραφείου.

- Το **XCENTRIC** είναι προορισμένο για την εγκατάσταση στον τοίχο και επιτρέπεται η λειτουργία μόνο κρεμαστά. Ο αερισμός να μην παρεμποδίζεται.
- Η καθορισμένη λειτουργία του συστήματος σύμφωνα με το IEC950/ EN60950 διασφαλίζεται μόνο με εγκαταστημένο περικάλυμμα (ψύξη, ασφάλεια πυρκαγιάς, εξάλειψη παρασίτων).
- Η θερμοκρασία περιβάλλοντος δε θα πρέπει να υπερβαίνει τους 40°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 μόνο απο ειδικά εκπαιδευμένο προσωπικό. Πριν το άνοιγμα της συσκευής θα πρέπει οπωσδήποτε να βγάλετε τον ρευματολήπτη. Αναρμόδιο άνοιγμα και λανθασμένη επισκευή της συσκευής προκαλεί μεγάλο κίνδυνο για τον χρήστη (Ηλεκτροπληξία). Συνιστάται η επισκευή της συσκευής να γίνεται μόνο στο σέρβις του BinTec. Που υπάρχει σέρβις κοντά σας το μαθαίνετε απο τον έμπορο σας.
- 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 **XCENTRIC** soltanto nell'imballaggio originale o in altro imballaggio adeguato a garantire protezione da urti e colpi.

Installazione e azionamento

- Prima di installare ed usare **XCENTRIC** fare attenzione alle istruzioni sulle condizioni ambientali (cfr. Dati tecnici).
- Durante l'installazione dei collegamenti base ISDN esterni ci si deve attenetere agli ordinamenti generali vigenti del vostro Paese. Può essere necessario rivolgersi ad un tecnico, che dispone della licenza adeguata. Informarsi sulle particolarità degli ordinamenti nazionali e tenere conto dei principi su cui si basano durante l'installazione.
- Le cariche elettrostatiche possono causare danni all'apparecchio. Indossate perciò un polsino elettrostatico sull'articolazione della mano oppure toccare una superficie con messa a terra, prima di entrare in contatto con l'apparecchio aperto o con uno dei moduli. Toccare sempre la scheda madre solo sui bordi e non prendere in mano cavi o elementi costruttivi.
- Installare i moduli solo negli slot previsti a tale scopo. Un'installazione im--propria può causare dei danni al modulo o all'intero apparecchio.
- In particolar modo durante l'installazione dei moduli hub ci si deve assicurare che lo slot 6 sia sempre occupato e che non sia inserito alcun modulo hub nello slot 7, dato che ciò potrebbe danneggiare il modulo o l'intero apparecchio.
- Chiudere gli slot dei moduli non utilizzati con le coperture, affinché nessun oggetto entri all'interno dell'apparecchio. La presenza di corpi estranei nell'apparecchio durante il funzionamento costituisce pericolo di scosse elettriche e di corto circuito.
- Un modulo 5-S_0 su cui i ponti sono applicati impropriamente può essere danneggiato durante il funzionamento. I moduli dispongono fino a un certo punto di dispositivi di protezione integrati al fine di evitare tali danni; è consigliabile tuttavia operare attentamente quando si installano tali ponti. Ass-

icurarsi assolutamente che le unità appositamente configurate (interne o esterne) siano ben collegate.

- Durante il collegamento dei cavi occorre accertarsi che le fessure di ventilazione dell'apparecchio non vengano coperte e che la ventilazione non sia ostacolata. L'impedimento della ventilazione di **XCENTRIC** può danneggiare l'apparecchio. Danni provocati dalla carenza di ventilazione causano la perdita del diritto di garanzia.

- Non aprire né il convertitore né l'apparecchio base (compreso il modulo TFE) e non intraprendere alcuna manipolazione dell'alimentatore poiché sussiste pericolo di morte a causa di scosse elettriche. Non estrarre nessuna vite dall'attacco dell'alimentatore e dell'apparecchio base.

- 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

- Assicurarsi che la tensione di rete locale corrisponda ai voltaggi nominali dell'alimentatore. L'apparecchio funziona alle seguenti condizioni:
  - 230 - 240 V c. a.
  - 50/60 Hz

- Accertarsi che la presa con contatto di terra dell'installazione sia accessibile. Per la completa separazione dell'apparecchio dalla rete di alimentazione è necessario estrarre la spina.

- Per il cablaggio si deve seguire la sequenza descritta nel manuale. Utilizzare soltanto i cavi rispondenti alle specifiche riportate in questo manuale o quelli originali forniti in dotazione. Se si utilizzano altri cavi, la BinTec Communications AG non risponde dei danni o della riduzione di funzionalità che ne risultano. In questi casi decade la garanzia per l'apparecchio.

- Quando si collega l'apparecchio si devono seguire le istruzioni del manuale. Nel momento in cui si allacciano i connettori si deve evitare che le punte vengano distorte e fare in modo che le viti dei connettori precedentemente inseriti siano rivolte verso destra, altrimenti il circuito di interfaccia non funziona e può subire danni.

- 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.
- Collegare **XCENTRIC** soltanto ad apparecchi terminali che rispondono ai requisiti di sicurezza generali richiesti per gli apparecchi di comunicazione. Apparecchi terminali con un'omologazione del CETECON (già BZT) soddisfano questi requisiti. Gli apparecchi terminali ISDN che vengono collegati a **XCENTRIC** devono essere omologati per Euro-ISDN, mentre quelli analogici devono supportare il procedimento di selezione della frequenza/DTMF ed essere impostati per lo stesso.

Utilizzazione conforme alla destinazione, funzionamento

- **XCENTRIC** è concepito per l'impiego negli uffici. Come Router per reti multiprotocollo **XCENTRIC** stabilisce collegamenti WAN in rapporto alla configurazione del sistema. Per evitare canoni indesiderati, si consiglia di controllare assolutamente il prodotto.
- **XCENTRIC** è conforme alle relative disposizioni di sicurezza per impianti della tecnica informatica impiegati in ambiente d'ufficio.
- **XCENTRIC** è ideato per il montaggio a parete e deve operare solo se agganciato. La ventilazione non deve essere ostacolata in nessun caso.
- Il funzionamento regolamentare del sistema secondo le disposizioni IEC 950/EN 60950 è garantito (raffreddamento, protezione antincendio, schermatura contro radiodisturbi) solo se è completamente montato l'involucro di lamiera.
- La temperatura ambiente non dovrebbe superare i 40°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 solamente da personale altamente specializzato. Prima di aprire l’apparecchio estrarre assolutamente la spina di alimentazione. Un’apertura non autorizzata e delle riparazioni improprie possono costituire dei pericoli considerevoli per l’utilizzatore (ad esempio scossa elettrica). Lasciare che le riparazioni all'apparecchio vengano eseguite unicamente da un centro di assistenza autorizzato BinTec. Il rivenditore di fiducia può fornire informazioni sulle sedi di questi centri.
- 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, detergenti 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 **XCENTRIC** 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 **XCENTRIC** op de instructies voor de omgevingsvoorwaarden (vergelijk technische gegevens).
- Bij de installatie van externe ISDN-basisaansluitingen de afzonderlijke bepalingen in acht nemen die voor uw land gelden. Eventueel moet er een technicus aan te pas komen die een desbetreffende vergunning heeft. Informeer u bij de installatie over bijzondere nationale voorschriften en neem de wettelijke basis hiervan in acht.
- Elektrostatische opladingen kunnen schade aan de toestellen veroorzaken. Draag daarom een antistatische manchet om de pols of raak geaard oppervlak aan voordat u het geopende toestel of een van de modules aanraakt.Platines principieel alleen aan de rand aanraken en niet aan leidingen of bouwdelen komen.
- Installeer de modules alleen in de daarvoor bestemde slots. Bij een verkeerde montage kan schade aan de module of aan het hele toestel ontstaan.
- Vooral bij de installatie van de Hub-modules moet erop gelet worden dat slot 6 nooit leeg mag zijn en geen enkel Hub-module in slot 7 mag steken, omdat anders schade aan de module of aan het hele toestel kan ontstaan.
- Module-openingen, die niet worden gebruikt, met beschermingsafdekkingen afsluiten zodat er geen vreemde delen in het toestel kunnen komen. Als zich vreemde delen in het toestel bevinden terwijl het in werking is bestaat gevaar voor stroomstoten en kortsluiting.
- Een 5-S_0-module, waar bruggen verkeerd op zijn gestoken kan beschadigd worden als hij in werking wordt gezet. De modules bezitten beperkte geïntegreerde veiligheidsmaatregelen om dergelijke schade te voorkomen, maar toch dient u nauwkeurig te werk te gaan als u bruggen op de module

steekt. Zorg er absoluut voor dat overeenkomstig geconfigureerde (intern of extern) units ook passend verbonden worden.

- Zorg er bij de bedrading voor dat de ventilatie-openingen van het toestel niet afgedekt worden en de ventilatie niet gehinderd wordt. Door het hinderen van de ventilatie van de **XCENTRIC** kan het toestel beschadigd worden. We kunnen geen garantie geven voor schade die veroorzaakt werd door een gebrekkige ventilatie.

- Het netdeel en het basistoestel (inclusieve TFE-module) nooit openen en nooit manipuleren aan het netdeel, omdat er anders gevaar voor stroomstoten bestaat. Geen schroeven van de bevestiging van het netdeel of van het basistoestel losmaken.

- 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 milieuvoorschriften in de technische gegevens in acht.

- Ga na of de plaatselijke netspanning overeenstemt met de nominale spanningen van het netdeel. Het toestel mag onder de volgende voorwaarden in werking worden gesteld:
  - 230 - 240 VAC
  - 50/60 Hz

- Zorg ervoor dat de veiligheidscontactdoos van de installatie vrij toegankelijk is. Om het toestel helemaal van het net te scheiden moet de netstekker uitgetrokken worden.

- Let bij de aansluiting van de kabels op de volgorde, zoals in het handboek wordt beschreven. Gebruik enkel kabels die aan de specificaties in dit handboek voldoen of die meegeleverd werden. Indien u andere kabels gebruikt, is BinTec Communications AG niet aansprakelijk voor mogelijke schade of het slecht functioneren van het toestel. In dit geval vervalt de garantie.

- Bij de aansluiting van het toestel de voorschriften in de handleiding in acht nemen. Bij het vaststeken van de klemschragen vooral erop letten dat de stiften niet worden verbogen en de schroeven van de vastgestoken klem-

schraag naar rechts staan omdat anders de scheidslijn niet functioneert en beschadigd kan worden.

- Leg de kabels zodanig, dat zij geen gevaarsbron (struikelgevaar) vormen en niet worden beschadigd.
- Tijdens een onweer de datatransmissielijnen niet aansluiten, uittrekken of aanraken.
- Sluit aan **XCENTRIC** alleen maar eindtoestellen aan, die voldoen aan de algemene veiligheidsvoorschriften voor communicatie-toestellen. Eindtoestellen die door het CETECON (vroeger BZT) zijn toegelaten voldoen aan deze eisen. ISDN-eindtoestellen, die aan **XCENTRIC** worden aangesloten, moeten voor het Euro-ISDN (DSS1) zijn toegelaten, analoge eindtoestellen moeten met de DTMF-/audiofrequentie-keuzemethode werken en ingesteld zijn op audiofrequentie-keuzemethodes.

Doelmatig gebruik, bedrijf

- **XCENTRIC** is enkel voor het gebruik in een bureau-omgeving geschikt. Als multi-protocol-router bouwt **XCENTRIC** afhankelijk van de systeemconfiguratie WAN-verbindingen op. Om ongewenste kosten te vermijden, moet het product absoluut gecontroleerd worden.
- **XCENTRIC** voldoet aan de gebruikelijke veiligheidsbepalingen voor inrichtingen van informatietechniek voor toepassing in een kantooromgeving.
- **XCENTRIC** is gepland voor de montage aan de muur en mag alleen hangend in werking worden gesteld. De ventilatie mag in geen enkel geval worden gestoord.
- De reglementaire werking volgens IEC950/EN60950 van het systeem is alleen gegarandeerd bij een volledig gemonteerde blikken omhulling (koeling, brandbeveiliging, ontstoring.
- De omgevingstemperatuur mag niet hoger zijn dan 40°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 stroomverzorging en neemt u contact op met de service-dienst.

Reiniging en reparatie

- Het toestel mag alleen door geschoold vakkundig personeel worden geopend. Voor het openen van het toestel in elk geval de netstekker uittrekken. Door onbevoegd openen en ondeskundige reparaties kan groot gevaar voor de gebruiker ontstaan.(bijv. stroomstoten). Reparaties aan het toestel alleen door een door BinTec geautoriseerde servicedienst laten uitvoeren. Waar zich deze servicedienst bevindt, weet uw handelaar.
- 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 **XCENTRIC** i originalemballasjen eller i en annen egnet emballasje som beskytter mot støt og slag.

Oppstilling og ibruktaking

- Før oppstilling og drift av **XCENTRIC** må du ta hensyn til henvisningene når det gjelder omgivelsesbetingelsene (sml. tekniske data).
- Ved installasjon av eksterne ISDN-Basistilknytninger så skal det tas hensyn til de til enhver tid gjeldende rammebetingelser for landet utstyret befinner seg i. Likedan kreves det en teknikker som har tillatt adgang til utstyret. Gjør deg kjent med de viktige nasjonale bestemmelsene og vær oppmerksom på deres rettslige grunnlag ved installasjon.
- Elektrostatiske oppladninger kan resultere i skader på apparatet. Ta på deg en antistatisk mansjett på håndleddet, eller benytt en jordet overflate før du åpner apparatet, eller tar på en av modulene. Du skal bare ta på platinen på kantene, og ikke berøre ledninger eller andre deler.
- Modulene skal bare installeres i de angitte slotene. Ved feil montasje kan modulen bli ødelagt eller hele apparatet kan bli skadet.
- Ta spesiell hensyn ved installasjon av hub-moduler, at det alltid sitter noe i slot 6, og at ingen enkelt moduler sitter i slot 7, ellers kan dette resultere i beskadigelse av modulen eller hele apparatet.
- Ikke dekk til benyttede modul-innlegg med blinddeksler. Hvis det skulle befinne seg fremmedlegemer i apparatet, så kan dette resultere i elektrisk støt - og kortslutning.
- Hvis en 5-S0-Modul, blir satt inn feil på broen, så kan denne bli skadet når den settes i drift. Modulene besitter begrensede integrerte sikkerhetsanordninger for å forhindre slike skader, men man må allikevel gå forsiktig fram når broene bestykkes. Pass nøye på at konfigurerte (intern eller eksterne) enheter også blir riktig forbundet.
- Under tilkoplingen må du passe på at apparatets ventilasjonsåpninger ikke blir tildekket og at ventilasjonen ikke blir hindret. Ved nedsatt ventilasjon av

XCENTRIC kan det oppstå skader på apparatet. Skader som oppstår på grunn av manglende ventilasjon fører til tap av garantien.

- Du må verken åpne nettdelen eller basisapparatet (inkludert TFR-modul) og ikke forta noen form for manipulering av nettdelen, ellers kan dette resultere i livsfare på grunn av elektrisk støt. Ikke fjern skruene som er festet til nettdelen og basisapparatet.
- 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 at den lokale nettspenningen er i overensstemmelse med nettdelens merkespenning. Apparatet kan settes i drift under følgende betingelser.
  - 230 - 240 VAC
  - 50/60 Hz
- Kontroller at det er fri tilgang til installasjonens jordete stikkontakt. Nettstøpselet må trekkes ut for at apparatet skal være fullstendig frakoplet nettet.
- Følg den rekkefølgen som er beskrevet i håndboken under tilkopling. Bruk kun kabler som svarer til spesifikasjonene i denne håndboken eller som fulgte med i original i leveringen. Hvis du bruker andre kabler, påtar seg BinTec Communications AG intet ansvar for eventuelle skader eller nedsatt funksjonalitet. Garantien på apparatet oppheves i slike tilfeller.
- Følg instruksene i håndboken ved tilkopling av apparatet. Pass ved festingen av klemklossene spesielt på at stiftene ikke er/ blir bøyd og at skruene på de påsatte klemklossene peker mot høyre, ellers er ikke grensesnittet funksjonsdyktig og kan dermed bli skadet.
- 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.

- Kople til **XCENTRIC** bare sluttapparater som stemmer overens med de alminnelige sikkerhetskravene for kommunikasjonsapparater. Sluttapparater med godkjennesle fra CETECON (tidligere BZT) oppfyller disse kravene. ISDN-apparater som **XCENTRIC** koples til må være godkjent for Euro-ISDN (DSS1). Analoge sluttapparater må understøtte DTMF-/lydfrekvensvalg og være innstilt på lydfrekvensvalg.

Forskriftsmessig bruk, drift

- **XCENTRIC** er beregnet på bruk i et kontorlandskap. I egenskap av multiprotokoll-router bygger **XCENTRIC** opp WAN-forbindelser, avhengig av systemkonfigurasjonen. Det er tvingende nødvendig å overvåke produktet for å unngå utilsiktede gebyrer..
- **XCENTRIC** oppfyller gjeldende sikkerhetsbestemmelser for innretninger innen informasjonsteknikk for bruk i kontorlanskapp.
- **XCENTRIC** er beregnet for montering på veggen og skal bare settes i drift når den henger. Ventilasjonen skal absolutt ikke forhindres.
- Forskriftsmessig bruk IEC950/EN60950 av systemet er kun gitt ved komplett montert metalldeksel (kjøling, brannbeskyttelse, radio-støydempning).
- Omgivelsestemperaturen bør ikke overstige 40°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 skal bare åpnes av fagpersonell. Før du åpner apparatet er det nødvendig å dra ut nettstøpselet. Ved forbudt åpning og usakkyndige reparasjoner kan det oppstå alvorlige risikoer for brukeren (f.eks. elektrisk støt). Reparasjoner av apparatet skal bare gjennomføres av autoriserte BinTec-autoriserte serviceverksteder. Din forhandler kan fortelle deg hvor nærmeste serviceverksted er.

- 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 **XCENTRIC** 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 **XCENTRIC** tenha em conta as indicações relativas às condições ambientais (cf. Dados técnicos).
- Respeite as condições básicas em vigor no seu país aquando da instalação de contactos externos de base RDIS. Se necessário, a instalação deverá ser efectuada por um técnico que disponha de licença para tal. Informe-se sobre as particularidades dos regulamentos nacionais e respeite o seu fundamento legal aquando da instalação.
- As cargas electrostáticas podem causar danos nos aparelhos. Por conseguinte, use um punho antiestático à volta do pulso ou então toque numa superfície ligada à terra antes de mexer no aparelho aberto ou num dos módulos. Toque apenas nos bordos das placas de circuitos impressos e não toque nos condutores ou nos componentes.
- Instale os módulos apenas nas slots previstas para o efeito. Uma montagem incorrecta pode causar danos no módulo ou em todo o aparelho.
- Aquando da instalação dos módulos de curso, certifique-se de que a slot 6 está sempre ocupada e de que não há nenhum módulo de curso individual na slot 7, o que poderia causar danos no módulo ou em todo o aparelho.
- Feche os módulos não utilizados com as coberturas cegas, de modo a que não possa entrar qualquer objecto no interior do aparelho. Se, durante o funcionamento, houver algum objecto estranho dentro do aparelho, existe perigo de choque eléctrico e de curto-circuito.
- Um módulo 5-S_0 em que as pontes tenham sido mal inseridas poderá sofrer danos aquando da colocação em funcionamento. Os módulos possuem medidas de protecção integradas para evitar danos deste tipo. No entanto, deve introduzir as pontes com cuidado. Certifique-se de que as unidades

(internas ou externas) devidamente configuradas também são ligadas adequadamente.

- Durante a cablagem, tenha atenção para que as ranhuras de ventilação do aparelho não fiquem tapadas e a ventilação não seja obstruída. A obstrução da ventilação do **XCENTRIC** pode causar danos no aparelho. Os danos causados por uma ventilação insuficiente têm como consequência a perda da garantia.

- Não abra o equipamento de alimentação de rede, nem o aparelho base (inclusíve o módulo TFE), e não mexa no equipamento de alimentação de rede, uma vez que existe perigo de morte devido a choque eléctrico. Não retire quaisquer parafusos de fixação do equipamento de alimentação de rede e do aparelho base.

- 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 de rede local corresponde às tensões nominais do equipamento de alimentação de rede. O aparelho pode ser operado nas seguintes condições:
  - 230 - 240 VAC
  - 50/60 Hz

- Certifique-se de que a tomada de contacto de segurança da instalação está acessível. Para desligar completamente a corrente do aparelho, retire a ficha de rede.

- Ao proceder à cablagem, respeite a sequência tal como está descrita no manual. Utilize unicamente cabos que correspondam às especificações contidas neste manual ou cabos originais que tenham sido fornecidos. Se usar outros cabos, a BinTec Communications AG não se responsabiliza por danos daí decorrentes ou por limitações de funcionamento. Nestes casos, a garantia do aparelho é anulada.

- Aquando da conexão do aparelho, respeite as indicações constantes do manual. Quando encaixar os blocos de aperto, certifique-se de que não entorta os pinos e de que os parafusos do bloco de aperto encaixado apontam para a direita, caso contrário o interface não está operacional e pode ser danificado.
- Instale os cabos de maneira a não constituírem uma fonte de perigo (perigo de tropeçar) nem se danificarem.
- Em caso de trovoada, não ligue, retire ou toque nos cabos de transmissão de dados.
- Ligue ao **XCENTRIC** apenas terminais que preencham os requisitos gerais de segurança dos aparelhos de comunicação. Os terminais homologados pela CETECON (antiga BZT) preenchem os referidos requisitos. Os terminais RDIS que são conectados ao **XCENTRIC** devem estar homologados para a RDIS europeia (DSS1), e os terminais analógicos devem suportar o processo de selecção de frequência de som / DTMF e ser ajustados de acordo com o processo de selecção de frequência de som.

Utilização conforme com as especificações, Operação

- O **XCENTRIC** destina-se à utilização em escritórios. Como Router de protocolos múltiplos, o **XCENTRIC** constrói ligações WAN de acordo com a configuração do sistema. Para evitar custos indesejados, controle o produto.
- O **XCENTRIC** corresponde às normas de segurança habituais relativas a dispositivos de informática para utilização em escritórios.
- O **XCENTRIC** está previsto para instalação na parede e só pode ser operado na posição suspensa. A ventilação não pode de modo algum ser obstruída.
- Só é possível assegurar o funcionamento adequado do sistema em conformidade com IEC950/EN60950 se a caixa de chapa estiver completamente montada (refrigeração, protecção contra incêndio, supressão de interferências).
- A temperatura ambiente não pode exceder os 40°C. Evite expor o aparelho à luz solar directa.

- Tenha o cuidado de não deixar entrar objectos (por ex. clipes) 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 técnicos especializados. Antes de abrir o aparelho é indispensável retirar a ficha de rede. A abertura não autorizada e as reparações inadequadas podem representar riscos graves para o utilizador (por ex. choque eléctrico). Mande efectuar as reparações do aparelho apenas nos serviços de assistência técnica BinTec autorizados. O seu fornecedor indicar-lhe-á a localização dos referidos serviços.
- 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 bezpieczeñstwa w jêzyku polskim

Poniżej podano zasady bezpieczeństwa, których należy bezwzględnie przestrzegać przy obchodzeniu się z routerem.

Transport i magazynowanie

- Urządzenie XCENTRIC należy transportować i magazynować wyłącznie w opakowaniu oryginalnym lub innym nadającym się do tego celu opakowaniu, zapewniającym ochronę przed obiciami i uderzeniami.

Ustawianie i uruchamianie

- Przed ustawieniem i uruchomieniem urządzenia XCENTRIC należy zastosować się do wskazówek dotyczących warunków otoczenia (por. Parametry techniczne).
- Przy instalacji zewnętrznych przyłączy bazowych ISDN należy przestrzegać obowiązujących w danym kraju przepisów i ustaleń branżowych. W niektórych przypadkach przyłączenia może dokonać wyłącznie technik posiadający odpowiednie uprawnienia. Przed przystąpieniem do instalacji zasięgnijcie Państwo informacji o szczegółach regulacji prawnych obowiązujących w Waszym kraju.
- Elektrostatyczna różnica potencjałów może doprowadzić do uszkodzenia urządzenia. Przed przystąpienim do pracy należy założyć na przegub ręki antyelektrostatyczną opaskę zabezpieczającą lub dotknąć uziemionej powierzchni zanim dojdzie do kontaktu dłoni z otwartym urządzeniem lub jednym z jego modułów. Płytki drukowane należy chwytać zawsze na obrzeżach; nie dotykać bezpośrednio ścieżek drukowanych oraz elementów elektronicznych.
- Poszczególne moduły mogą być zainstalowane wyłącznie w przeznaczonych dla nich cokołach. Nieprawidłowe zabudowanie może doprowadzić do uszkodzenia modułu lub całego urządzenia.
- Zwłaszcza przy instalacji modułów typu Hub należy przestrzegać zasady, że cokół 6 musi być zawsze zajęty, a jednego jedynego modułu nie wolno instalować w cokole 7. W przeciwnym przypadku może dojść do uszkodzenia modułu bądź też całego urządzenia.
- Nie używane cokoły dla modułów należy zaopatrzyć w zaślepki zabezpieczające zapobiegające dostaniu się do wnętrza urządzenia niepożądanych przedmiotów. Obecność obcych elementów w urządzeniu w

czasie jego eksploatacji stanowi zagrożenie porażenia prądem lub prowadzi do spięcia elektrycznego.

- Moduł typu 5-S0- nieprawidłowo zmostkowany może zostać uszkodzony przy włączeniu urządzenia. Moduły są wyposażone w wewnętrzne systemy zabezpieczające o ograniczonym zakresie mające zapobiegać tego rodzaju uszkodzeniom, jednakże przy mostkowaniu zalecana jest szczególna staranność. Koniecznie należy zwrócić uwagę, że tylko odpowiednio skonfigurowane (wewnętrznie i zewnętrznie) jednostki (units) mogą być ze sobą łączone.
- Okablowanie powinno być tak prowadzone, żeby szczeliny wentylacyjne i otwory w obudowie nie zostały przysłonięte i w konsekwencji nie doszło do zakłócenia właściwego chłodzenia urządzenia. Niewystarczające przewietrzanie XCENTRICmoże doprowadzić do awarii urządzenia. Uszkodzenia wynikające z niedostatecznej wentylacji mogą wiązać się z utratą reklamacji.
- Otwieranie zarówno zasilacza prądowego jak i urządzenia głównego (włącznie z modułem TFE) jest niewskazane; pod żadnym pozorem nie dozwolone jest dokonywanie manipulacji w układzie elektrycznym zasilacza – niebezpieczeństwo śmiertelnego porażenia prądem. Zabronione jest odkręcanie z zasilacza i urządzenia podstawowego śrub mocujących.
- 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.
- Konieczne jest sprawdzenie zgodności napięcia lokalnej sieci zasilającej z napięciem znamionowym zasilacza prądowego. Urządzenie może być eksploatowane pod następującymi warunkami:
  - 230 - 240 VAC
  - 50/60 Hz
- Należy upewnić się, czy gniazdko kontaktu bezpieczeństwa instalacji elektrycznej jest łatwo dostępne. Aby przerwać w pełni zasilanie prądem, wtyczka musi być wyciągnięta z gniazdka.

- Przy przyłączaniu przewodów należy przestrzegać kolejności opisanej w instrukcji obsługi. Należy używać tylko takich kabli których specyfikacje odpowiadają danym z niniejszej instrukcji obsługi lub też są dostarczone wraz z urządzeniem. W przypadku zastosowania innych przewodów firma BinTec Communications AG nie ponosi odpowiedzialności za poniesione szkody. Tym samym umowa gwarancyjna staje się nieaktualna.
- Podczas podłączania urządzenia do sieci należy przestrzegać wskazówek zawartych w instrukcji obsługi. Przy zabudowywaniu bloków zaciskowych należy zwracać szczególną uwagę na to, żeby kołki kontaktowe nie zostały zgięte, a śruby założonego bloku skierowane były na prawo – w przeciwnym przypadku złącze nie będzie funkcjonowało i może zostać uszkodzone.
- Przewody należy ułożyć tak, aby nie występowało niebezpieczeństwo potykania się o nie oraz ich uszkadzania.
- Podczas burzy nie wolno podłanczać przewodów przenoszenia danych, ani też dotykać ich lub wyłanczać.
- Do XCENTRIC mogą być podłączone wyłącznie urządzenia końcowe odpowiadające ogólnym wymogom bezpieczeństwa dla urządzeń komunikacyjnych. Urządzenia końcowe dopuszczone do użytku przez CETECON (były BZT) odpowiadają tym wymaganiom. Urządzenia ISDN podłączone do XCENTRIC , muszą posiadać dopuszczenie Euro-ISDN (DSS1), analogowe urządzenia końcowe muszą być wyposażone w opcję DTMF-/dźwiękowe wybieranie numerów i na tą opcję nastawione.

Zgodne z przeznaczeniem stosowanie, eksploatacja

- XCENTRIC przeznaczona jest do pracy w otoczeniu biurowym. Jako Multi-Protokoll-Router buduje XCENTRIC niezależnie od konfiguracji systemowej połączenia WAN. Aby zapobiec nieprzewidzianym opłatom, powinno się go strzec.
- Urządzenie XCENTRIC spełnia obowiązujące zasady bezpieczeństwa dla urządzeń informatycznych przeznaczonych do stosowania w otoczeniu biurowym.
- XCENTRIC jest przeznaczony do montażu na ścianie i może być eksploatowany wyłącznie w pozycji wiszącej. Przewietrzanie chłodzące nie może być w żadnym stopniu utrudnione.

- Zgodna z przeznaczeniem eksploatacja systemu zgodnie z IEC950/EN60950 jest zagwarantowana tylko w przypadku kompletnie zamontowanej obudowy blaszanej (chłodzenie, ochrona przeciwpożarowa, eliminacja zakłóceń w eterze).
- Temperatura otoczenia nie powinna przekraczać 40°C. Należy unikać bezpośredniego działania promieni słonecznych.
- Należy uważać, aby do wnętrza urządzenia nie wnikały 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 zostać otwarte tylko przez przeszkolonego fachowca. Przed otwarciem obudowy koniecznie wyjąć wtyczkę z gniazdka sieciowego. Otwarcie przez osoby nieupoważnione i niefachowo przeprowadzone naprawy mogą pociągnąć za sobą powstanie poważnych zagrożeń dla użytkownika (np. porażenie prądem). Naprawy mogą być wykonywane tylko przez autoryzowany przez BinTec warsztat naprawczy. Adresy warsztatów serwisowych można uzyskać w placówkach handlowych.
- 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 **XCENTRIC** 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 **XCENTRIC**, observe las instruc-ciones acerca de las condiciones ambientales (ver ”Datos técnicos”).
- Observe Vd., al instalar conexiones de base ISDN externas, las respectivas condiciones de principio de su país. Dado el caso, deberá recurrirse a un técnico que dispone de la autorización necesaria. Infórmese sobre las particularidades de los reglamentos nacionales y tenga en cuen-ta las bases jurídicas durante la instalación.
- Cargas electrostáticas pueden ocasionar daños en los aparatos. Lleve Vd., por consiguiente, un puño antiestático alrededor de la muñeca o toque una superficie puesta a tierra, antes de tocar el aparato abierto o uno de los módulos. Toque Vd. las placas de circuitos impresos por principio sólo en los bordes y no toque cables ni componentes.
- Instale Vd. los módulos sólo en las ranuras previstas para este fin. En caso de un montaje erróneo puede producirse un daño en el módulo o en el aparato completo.
- Especialmente debe ponerse atención, al instalar los módulos de ele--vación, en que la ranura 6 debe estar siempre dotada y que no debe estar enchufado ningún módulo de elevación individual en la ranura 7 puesto que, en caso contrario, podría resultar un daño en el módulo o en el aparato completo.
- Cierre Vd. unidades enchufables de módulo no utilizadas con las cubiertas ciegas para que no puedan penetrar ningunos objetos en el interior del aparato. Si durante el servicio se encontraran objetos extraños en el aparato, existiría el peligro de electrocuciones y de cortocircuitos.
- Un módulo 5-S_0, sobre el cual se enchufaron erróneamente puentes, podría ser dañado durante la puesta en servicio. Los módulos tienen

medidas de protección integradas en límites para evitar tales daños, debería procederse, no obstante, con cuidado al enchufar puentes. Ponga de todos modos atención en que unidades correspondientemente configuradas (internas o externas)sean también unidas de un modo ap-ropiado.

- Al instalar los cables, preste atención a no cubrir las rendijas de ventilación del aparato para no impedir la ventilación. Si la ventilación de **XCENTRIC** resultase afectada, podrían ocasionar daños en el aparato. Los daños producidos a causa de una ventilación insuficiente conllevan la pérdida de garantía.

- No abra ni la fuente de alimentación ni el aparato de base (incluso el módu--lo TFE) y no haga ningunas manipulaciones en la fuente de alimentación, puesto que en caso contrario existiría peligro de muerte por una elec--trocución. No retire ningunos tornillos de la fijación de la fuente de alimen--tación y del aparato de base.

- 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 de la red local coincide con las tensiones nominales de la fuente de alimentación. El aparato puede funcionar bajo las siguientes condiciones:
  - 230 - 240 VAC
  - 50/60 Hz

- Asegúrese de que no quede obstaculizado el acceso a la caja de enchufe con puesta a tierra de la instalación. Para desconectar totalmente el aparato de la red es necesario desenchufar el enchufe de la red.

- Al instalar los cables respete el orden descrito en el manual. Utilice únicamente cables que cumplan las especificaciones expuestas en este manual o que hayan venido incluidos en el volumen de suministro. Si utiliza otros cables, BinTec Communications AG no se hará responsable en el caso de que se produzcan daños o una merma en el funcionamiento. En estos casos la garantía pierde su validez.

- Al conectar el aparato, observe las indicaciones hechas en el manual. Ponga especialmente atención, al enchufar los bloques de bornes, en que las clavijas no se doblen y que los tornillos del bloque de bornes enchufado señalen a la derecha, puesto que, en caso contrario, el interface no sería capaz de funcionar y podría ser dañado.
- Coloque los cables de manera que no constituyan un peligro (tropezones) y no puedan ser deteriorados.
- Durante una tormenta, no enchufe ni desenchufe los conductos de transmisión de datos, ni los toque.
- Conecte al **XCENTRIC** sólo aparatos terminales que corresponden a los re-querimientos generales de seguridad para aparatos de comunicación. Aparatos terminales con una aprobación por el CETECON (anteriormente BZT) corresponden a estas exigencias. Aparatos terminales ISDN, que se conectan al **XCENTRIC**, deben ser admitidos para el Euro-ISDN (DSS1), aparatos terminales análogos deben favorecer el procedimiento DTMF/de selección a distancia por frecuencia vocal y estar ajustados al procedimiento de selección a distancia por frecuencia vocal.

Utilización prevista, servicio

- **XCENTRIC** está concebido para ser utilizado en oficinas. Como router multiprotocolo, **XCENTRIC** establece conexiones WAN dependiendo de la configuración del sistema. Para evitar que se produzcan gastos de conexiones indeseadas, es absolutamente necesario vigilar el producto.
- **XCENTRIC** corresponde a las disposiciones de seguridad pertinentes para equipos informáticos utilizados en oficinas y despachos.
- **XCENTRIC** está previsto para el montaje en la pared y debe funcionar sólo en estado suspendido. En ningún caso, debe ser estorbada la ventilación.
- El servicio correspondiente al destino según IEC 950/EN 60950 del sistema está sólo asegurado al estar montada completamente la caja de chapa (refrigeración, protección contra incendios, antiparasitaje).
- La temperatura ambiental no debe superar los 40°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. Antes de abrir el aparatos debe sacarse de todos modos el enchufe con la red. El abrir y reparar el aparato sin autorización puede conllevar un peligro considerable para el usuario (p.ej. electrocución). Por lo tanto, realice las posibles reparaciones del aparato solamente a través de un servicio técnico autorizado por BinTec. Su vendedor le informará de la dirección del servicio técnico.
- 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.
- El símbolo CE significa que XCENTRIC corresponde a las siguientes directivas de la Comunidad Europea: EMV (89/336/EWG) y tensión de la red (73/23/EWG).

Allmänna säkerhetsanvisningar på svenska

Beakta alltid nedanstående säkerhetsanvisningar för användning av apparaten.

Transport och förvaring

- **XCENTRIC** 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 **XCENTRIC** installeras och startas.
- Beakta gällande bestämmelser för installation av externa ISDN-basanslutningar. Eventuellt måste installationen utföras av en behörig tekniker. Beakta även alla andra relevanta bestämmelser vid installationen.
- Elektrostatisk uppladdning kan förorsaka skador på apparaten. Bär därför en antistatisk manschett runt handleden, eller rör alltid vid en jordad yta innan Du vidrör den öppna apparaten eller någon modul. Tag endast på kretskortens kanter, vidrör aldrig ledningarna och komponenterna.
- Installera modulerna endast på härför avsedda instickslatser. Felaktigt montage kan medföra skador på modulen och på hela apparaten.
- Särskilt viktigt vid insättning av anslutningsboxmodulerna; instickslats 6 måste alltid vara bestyckad och det får inte sitta en ensam anslutningsboxmodul på instickslats 7. Annars kan modulen eller hela enheten skadas.
- Täck över ej använda modulurtag med täckskivorna så att inga främmande föremål kan komma in i apparaten. Risk för strömstötar och kortslutning om främmande föremål finns i apparaten under drift.
- En 5-S_0-modul med felaktigt insatta bryggor kan skadas vid idrifttagandet. Modulerna har inbyggda skyddsfunktioner som inom vissa gränser skyddar dem mot sådana skador; sätt trots det alltid in bryggorna ytterst noggrant. Beakta att alla enheter (interna resp externa) ansluts enligt resp konfiguration.
- Säkerställ, under kabeldragningen, att apparatens ventilationsslitsar inte täcks över och att ventilationen inte påverkas. En reducerad ventilationseffekt kan medföra skador på **XCENTRIC**. Tillverkaren övertar inget garantiansvar för skador som uppstår p g a bristfällig ventilation.

- Öppna varken nätdelen eller basenheten (inklusive TFE-modulen), utför inga som helst förändringar på nätdelen; risk för strömstötar, livsfara. Tag inte bort några skruvar på nätdelens eller basenhetens fästanordningar.
- 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 spänningen på plats överensstämmer med nätdelens märkspänning. Under följande villkor får apparaten användas:
  - 230 - 240 VAC
  - 50/60 Hz
- Säkerställ att det jordade vägguttaget alltid är fritt tillgängligt. För separering från nätet måste nätkontakten dras ut.
- Utför kabeldragningen i den ordningsföljd som anges i handboken. Använd endast medlevererade originalkablar eller kablar som överensstämmer med specifikationerna i denna handbok. BinTec Communications AG påtar sig inget ansvar för eventuella skador eller brister på apparaten om den används tillsammans med andra kablar. I detta fall gäller inte garantin längre.
- Beakta anvisningarna i handboken vid anslutning av apparaten. Beakta, vid insättning av anslutningsplintarna, att stiften inte deformeras och att skruvarna på den insatta anslutningsplinten pekar mot höger. Annars är gränssnittet inte funktionsdugligt och kan ta skada.
- 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.
- Anslut endast sådana slutapparater till **XCENTRIC**, som uppfyller de allmänna säkerhetskraven för kommunikationsutrustning. Slutapparater med godkännande från CETECON (tidigare BZT) uppfyller dessa krav. ISDN-slutapparater som ansluts till **XCENTRIC** måste vara godkända för Euro-ISDN (DSS1), analoga slutapparater måste stödja DTMF-/tonfrekvensringning och vara inställda på tonfrekvensringning.

Ändamålsenlig användning, drift

- **XCENTRIC** är avsedd för användning i kontorslokaler. **XCENTRIC** är en multi-protokoll-router som, beroende på systemkonfiguration, upprättar WAN-förbindelser. Produkten bör övervakas så att inte onödiga kostnader uppstår.
- **XCENTRIC** uppfyller kraven i alla relevanta säkerhetsbestämmelser för informationsteknikutrustning i kontorslokaler.
- **XCENTRIC** är avsedd för väggmontage och får endast användas hängande. Ventilationen får inte täckas över eller påverkas på något annat sätt.
- Ändamålsenlig användning av systemet enligt IEC 950/EN 60950 säkerställs endast om plåthöljet är komplett monterat (kylning, brandskydd, radioavstörning).
- Omgivningstemperaturen bör inte vara högre än 40°C . Undvik direkt solljus.
- Säkerställ att det inte kan komma in några föremål (t ex häftklammer) eller någon vätska i apparaten (strömstötar, 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. Drag alltid ut nätkontakten innan apparaten öppnas. Obehörigt öppnande resp ej sakkunniga reparationer på apparaten kan medföra fara för användaren (t ex elektriska stötar). Reparationer får bara utföras av en av BinTec auktoriserad serviceverkstad. Återförsäljaren tillhandahåller information om närmaste serviceverkstad.
- 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

- **XCENTRIC** cihazı sadece orjinal ambalajı içinde veya çarpmaya ve darbeye karşı koruyan uygun başka bir ambalajla taşıyıp depolayınız.

Kurulması ve Çalıştırılması

- **XCENTRIC** cihazını kurup çalıştırmadan önce çevre koşulları hakkındakı bilgileri dikkate alınız (bak. Teknik Bilgiler)
- Harici ISDN temel bağlantılarının montajı için ülkenizde geçerli olan çerçeve hükümlerini dikkate alınız. Gerekirse, ilgili izinlere sahip olan bir tekniker görevlendirilmelidir. Ulusal yönetmelikler hakkında bilgi edininiz ve montaj sırasında bunların kanuni esaslarını dikkate alınız.
- Elektrostatik yüklenmeler cihazın zarar görmesine neden olabilir. Bu yüzden el bileğinize antistatik bir manşet takınız veya açılmış cihaza yada modüllerden birine dokunmadan önce topraklı bir yüzeye dokununuz. Platinleri yalnız kenarlarından tutunuz, hatlara veya yapı parçalarına dokunmayınız.
- Modülleri sadece bunlar için öngörülmüş slotlara monte ediniz. Hatalı montaj durumunda modülün veya tüm cihazın hasar görmesi mümkündür.
- Modül yada bütün cihaz zarar görebileceği için, özellikle kaldırma modülünün montajında, slot 6'nın dolu olması ve slot 7'ye tek bir tane kaldırma modülünün dahi sokulmamış olmasına dikkat edilmeli
- Cihazın içine yabancı cisimlerin girmesini engellemek için kullanılmayan modül girişlerini körtapalarla kapatınız. Kullanım esnasında cihazın içinde yabancı cisimler bulunuyorsa, elektrik çarpması ve elektrik bağlantılarının kısa devre yapma tehlikesi bulunmaktadır.
- Üzerinde köprülerin hatalı takıldığı bir 5-S $_0$ modülü, çalışma esnasında hasar görebilir. Modüller, bu tür hasarları engellemek için sınırlarına entegre edilmiş koruma tedbirlerine sahiptir. Ancak köprüler takılırken gene de özen gösterilmelidir. Uygun konfigürasyonlu (dahili veya harici) birimlerin doğru olarak bağlanmasına mutlaka dikkat ediniz.

- Kabloları yerleştirirken, cihazın havalandırma deliklerinin kapanmamasına ve havalandırmanın engellenmemesine dikkat ediniz. **XCENTRIC** cihazının havalandırması engellendiği takdirde cihaza zarar gelebilir. Yetersiz havalandırmanın yol açtığı zararlar, cihazın garanti hakkının kaybına sebeb verir.
- Elektrik çarpması sonucunda hayati tehlike bulunduğundan, ne şebeke parçasını ne de temel cihazı (TFE modülü dahil) açmayınız, şebeke parçasında da herhangi bir işlemde bulunmayınız şebeke parçasının ve temel cihazın sabitleyicisinin vidalarını sökmeyiniz.
- 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.
- Yerel şebeke geriliminin, şebeke parçasının nominal gerilimine uygun olup olmadığını kontrol ediniz. Cihaz, aşağıdakı koşullar doğrultusunda çalıştırılabilir:
  - 230 - 240 VAC
  - 50/60 Hz
- Koruyucu kontak prizinin montaj için rahatlıkla ulaşılabilecek durumda olmasını sağlayınız. Şebekeden tamam kopmak için, elektrik fişinin prizden çekilmeşi gerekir.
- Kabloları takarken el kitapcığındaki sıralamaya dikkat ediniz. Sadece el kitapcığında belirtilen verilere uygun veya cihazla birlikte gönderilen kabloları kullanınız. Başka kablo kullandığınız takdirde, BinTec Communications AG meydana gelen hasar veya fonksiyonlardaki olumsuz etkilerden dolayı sorumluluk üstlenmez. Bu durumlarda garanti hakkı ortadan kalkar.
- Cihazı bağlarken el kitapcığındaki açıklamalara dikkat ediniz. Özellikle sıkma topuzu takarken çubukların eğilmemesine ve takılı olan sıkma topuzunun vidalarının sağ tarafı göstermesine dikkat ediniz. Aksi takdirde kesitler çalışmaz ve hasar görebilir.
- Kabloları, tehlike kaynağı olamayacak ve zarar görmeyecek şekilde (takılma tehlikesi) döşeyiniz.

- Fırtına esnasında veri iletişim hatlarını ne bağlayınız, ne çıkartınız, ne de bunlara dokununuz.
- **XCENTRIC** cihazına sadece iletişim cihazları için olan genel güvenlik taleplerine uygun cihazlar bağlayınız. CETECON (önceden BZT) tarafından müsaade edilen cihazlar, bu taleplere uymaktadır. **XCENTRIC** cihazına bağlanacak olan ISDN-cihazlar, Euro-ISDN (DSS1) için müsaade edilmiş olmalıdır, analog cihazlar DTMF/ses frekansı seçme sürecini desteklemeli ve ses frekansı seçme sürecine ayarlanmış olmalıdır.

Belirlenmiş şekilde kullanım, işletim

- **XCENTRIC** cihazı büro ortamında kullanım için tasarlanmıştır. Multi-Protokol-Router olarak **XCENTRIC** cihazı sistem konfigurasyonuna bağlı olarak WAN-bağlantıları kurmaktadır. Istenmeyen masrafları önlemek için, ürünü mutlaka kontrol altında tutunuz.
- **XCENTRIC** cihazı, büro ortamında kullanılan enformasyon teknik donanımları için geçerli olan güvenlik talimatnamelerine kesinlikle uymaktadır.
- **XCENTRIC** cihazının duvara monte edilmesi öngörülmüştür ve sadece asılı durumda çalıştırılmalıdır. Havalandırma hiç bir surette engellenmemelidir.
- IEC 950/EN 60950 uyarınca, sistemin belirlenmiş şekilde kullanımı sadece saç kasnağı tamamiyle monte edildiğinde sağlanabilir (soğutma, yangın önleme, parazit giderme).
- Çevre sicaklığı 40°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. Cihazı açmadan önce, mutlaka elektrik fişini prizden çekiniz. Müsaade edilen

işlemler dışında açılması ve uygun olmayan şekilde tamir edilmesi, kullanıcı için büyük tehlikeler doğurabilir (örneğin elektrik çarpması). Cihazın tamiratını sadece BinTec yetkili servisi tarafından yaptırınız. Yetkili servis yerlerini nerede bulabileceğinizi satıcınızdan öğrenebilirsiniz.

- 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 XCENTRIC csak az eredeti vagy egy más, arra alkalmas csomagolásban szállítandó és tárolandó, amely lökések és ütések ellen védelmet biztosít.

Felállítás és üzembe helyezés

- Az XCENTRIC felállítása és üzembe helyezése előtt vegye figyelembe a környezeti feltételekre vonatkozó utsításokat (v.ö. a műszaki adatokkal).
- A külső ISDN-alapcsatlakozás telepítésekor vegye figyelembe az adott országban érvényes szabályzatokat és feltételeket. Adott esetben egy a megfelelő engedéllyel rendelkező műszaki szakemberre van szükség. Tájékozódjon az adott országban érvényes ide vonatkozó szabályzatokról, és vegye figyelembe azokat a telepítés során.
- Az elektrosztatikus töltések kisülése a berendezés meghibásodásához vezethet. Ennek megelőzése érdekében viseljen földelt csuklópántot, vagy érintsen meg egy földelt felületet, mielőtt a nyitott készüléket vagy annak valamelyik modulját megérintené. A platinákat mindig csak a szélükön érintse meg, sose érjen vezető vonalakhoz vagy alkatrészekhez.
- A modulokat csak az arra kijelölt slotra csatlakoztassa. Hibás csatlakoztatás a modulok vagy az egész készülék meghibásodását okozhatja.
- Különösen a hub-modulok telepítésekor ügyeljen arra, hogy a 6-os slot mindig foglalt legyen, és a 7-es sloton ne legyen egyedüli hub-modul, különben ez a modul vagy a teljes készülék meghibásodását okozhatja.
- Fedje le a használaton kívüli slotokat vakfedéllel, hogy ne kerülhessen idegen tárgy a készülék belsejébe. Amennyiben idegen tárgyak kerülnek a készülék belsejébe, áramütés és rövidzárlat veszélye áll fenn.
- 5-S_0-modulok hibás jumperelés esetén üzembe helyezéskor meghibásodhatnak. Ezek a modulok rendelkeznek bizonyos integrált védőintézkedésekkel az ilyen típusú hibák ellen, a jumperelésnél ennek ellenére különös gonddal járjon el. Feltétlenül ügyeljen arra, hogy a konfigurált egységek (belső vagy külső) ennek megfelelően legyenek csatlakoztatva.
- A vezetékezésnél ügyeljen arra, hogy a készülék szellőzőnyílásai ne legyenek letakarva, a szellőzés zavartalanul működjék. A nem megfelelő szellőzés az

XCENTRIC meghibásodásához vezethet. A nem megfelelő szellőzés miatt fellépő károk esetében garanciaigénye megszűnik.

- Ne nyissa ki se a tápegység, se a készülék (beleértve a TFE modult) burkolatát, és ne végezzen semmilyen átalakítást a tápegységen, mert ezáltal életveszélyes áramütés veszélye áll fenn. Ne távolítsa el a tápegység vagy a készülék rögzítő csavarjait.
- 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 helyi hálózati feszültség megegyezik-e a tápegység névleges feszültségével. A készülék az alábbi feltételek mellett üzemeltethető:
  - 230 - 240 VAC
  - 50/60 Hz
- Gondoskodjon róla, hogy a védőérintkezős csatlakozó aljzat a telepítésnél hozzáférhető legyen. A hálózatról való teljes leválasztáshoz húzza ki a hálózati csatlakozót.
- A vezetékezés során vegye figyelembe a kézikönyvben megadott sorrendet. Csak olyan vezetékeket alkalmazzon, amelyek a kézikönyvben megadott specifikációknak megfelelnek, vagy amelyek a készülék szállítási terjedelmében találhatók. Amennyiben más vezetékeket alkalmaz, az emiatt fellépő károkért vagy a működésben fellépő változásokért a BinTec Communications AG nem vállal felelősséget. Ebben az esetben megszűnik a garanciajogosultsága.
- Vegye figyelembe a készülék csatlakoztatásánál a kézikönyvben leírt ide vonatkozó utasításokat. Különös figyelemmel kezelje a sokpólusú csatlakozók csatlakoztatását, nehogy egy-egy tűjük elgörbüljön, csavarjaiknak csatlakoztatott állapotban jobbfelé kell mutatniuk, ellenkező esetben az interfész nem működőképes, és meghibásodhat.
- A vezetékeket úgy fektesse le, hogy azok ne lehessenek veszélyek forrásai (botlásveszély), azokban pedig kár ne keletkezhessen.

- Az adatátvivő vezetékeket vihar esetében ne csatlakoztassa, ne húzza le, ne érintse meg.
- Az XCENTRIC készülékre csak olyan végkészülékeket csatlakoztasson, amelyek a kommunkációs készülékekre vonatkozó általános biztonsági előírásoknak megfelelnek. A CETECON (egykori BZT) által engedélyezett készülékek megfelelnek ezeknek a követelményeknek. Azoknak az ISDN-végkészülékeknek, amelyeket az XCENTRIC készülékhez csatlakoztat, Euro-ISDN (DSS1) engedéllyel kell rendelkezniük, az analóg végkészülékeket DTMF-hangfrekvenciás választási módra kell beállítani.

Rendeltetésszerű alkalmazás, üzemeltetés

- Az XCENTRIC irodai környezetben való alkalmazásra készült. Az XCENTRIC, mint multi-protokoll-router, a rendszerkonfigurációtól függően a WAN-összeköttetésekre épül. A nem kívánt telefondíjak elkerülése végett, a terméket feltétlenül tartsa megfigyelés alatt.
- Az XCENTRIC megfelel az idevágó - irodai környezetben való használatra alkalmas információtechnikai berendezésekre vonatkozó - biztonsági előírásoknak.
- Az XCENTRIC fali készüléknek készült, és csak függő állapotban üzemeltethető. A szellőzés működését semmi esetre sem akadályozza.
- A rendszer rendeltetésszerű üzemeltetése az IEC 950/EN 60950 szabályzatnak megfelelően csak a teljesen összeszerelt fémburkolattal biztosítható (hűtés, tűzvédelem, zavarszűrés).
- A környezeti hőmérséklet nem haladhatja meg a 40 °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.
- Az 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 készülék felnyitása előtt feltétlenül húzza ki a hálózati csatlakozót. A készülék jogtalan felnyitása és a helytelen javítás révén a felhasználó számára jelentős

veszélyforrások keletkezhetnek (pl. áramütés). A készüléken szükséges javításokat ezért csak a BinTec által feljogosított szervizekkel végeztesse. A szervizek címét érdeklődje meg a szakkereskedőjénél.

- 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

- XCENTRIC 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 XCENTRIC přihlížejte k pokynům, které se týkají podmínek okolního prostředí (srovn. Technické údaje).
- Při instalaci externích základních přípojek ISDN přihlížejte k příslušným platným rámcovým podmínkám Vaší země. Eventuálně bude třeba přizvat technika s příslušným povolením. Informujte se o zvláštních ustanoveních národních vyhlášek a předpisů a při instalaci přihlížejte k jejich právní podstatě.
- Elektrostatické náboje mohou způsobit poškození přístroje. Použijte proto antistatickou manžetu přiloženou kolem zápěstí anebo se nejprv dotkněte některé uzemněné plochy, než se budete dotýkat otevřeného přístroje nebo některého modulu. Platiny se zásadně dotýkejte pouze na okrajích a nesahejte na vodivé spoje nebo součásti.
- Moduly instalujte pouze do příslušných slotů. V důsledku chybné montáže se může poškodit modul nebo kompletní přístroj.
- Speciálně při instalaci modulů hub se musí dbát na to, aby byl stále obsazen slot 6 a aby ve slotu 7 nebyl zasunut jednotlivý modul hub, jinak se může poškodit modul nebo kompletní přístroj.
- Nepoužívané modulové zásuvky uzavřete záslepkami tak, aby do vnitřku přístroje nemohly vniknout cizí předměty. Pokud se během provozu v přístroji nacházejí cizí předměty, hrozí nebezpečí zasažení elektrickým proudem nebo zkratu.
- Modul 5-S_0, na kterém jsou nesprávně zasunuty můstky, se při uvedení do provozu může poškodit. Moduly mají omezená integrovaná ochranná opatření, kterými se má takovýmto poškozením zabránit, při zasouvání můstků byste přesto měli postupovat pozorně. Zásadně dbejte na to, aby byly vhodně spojeny příslušně konfigurované jednotky (interně nebo externě).

- Při kabeláži dbejte na to, aby nedošlo k zakrytí větracích otvorů přístroje a aby nebyla omezována funkce větrání. V důsledku omezení větrání XCENTRIC by mohlo dojít k poškození přístroje. Škody vzniklé v důsledku nedostatečného větrání vedou ke ztrátě nároků z ručení.
- Neotevírejte ani síťový zdroj ani základní přístroj (včetně TFE modulu) a síťový zdroj nepodrobujte žádným manipulacím, jinak hrozí životní nebezpečí zasažením elektrickým proudem. Neodstraňujte žádné šrouby u upevnění síťového zdroje a základního přístroje.
- 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.
- Kontrolujte, zda se napětí místní sítě shoduje s hodnotami jmenovitého napětí síťového zdroje. Přístroj lze provozovat za těchto podmínek:
  - 230 - 240 VAC
  - 50/60 Hz
- Postarejte se o to, aby zásuvka s ochranným kontaktem byla při instalaci volně přístupná. Pro úplné odpojení od sítě je třeba vytáhnout síťovou zástrčku.
- Při propojování dbejte na pořadí tak, jak je popsáno v příručce. Používejte pouze kabely, jež odpovídají specifikacím v této příručce anebo dodané originální kabely. Pokud použijete jiné kabely, odmítá BinTec Communications AG ručení za vzniklé škody nebo za omezenou funkčnost. Ručení za přístroj v těchto případech zaniká.
- Při připojování přístroje dbejte na pokyny uvedené v příručce. Dbejte zejména při nasazování svorkových bloků na to, aby nedošlo k ohnutí kolíků a aby šrouby nasazeného svorkového bloku ukazovaly doprava, jinak není rozhraní schopné provozu a může se poškodit.
- Vedení ukládejte tak, aby se nestala zdrojem nebezpečí (např. zakopnutím) a aby se nepoškodily.
- Během bouřky nepřipojujte vedení na přenos dat, neodpojujte je a ani se jich nedotýkejte.

- Na XCENTRIC připojujte pouze koncové přístroje, které odpovídají všeobecným bezpečnostním požadavkům pro komunikační přístroje. Koncové přístroje se schválením CETECON (dřívější BZT) těmto požadavkům vyhovují. ISDN koncové přístroje, které se připojují na XCENTRIC, musí mít schválení pro Euro-ISDN (DSS1), analogové koncové přístroje musí podporovat DTMF/tónovou volbu a musí být na tónovou volbu nastaveny.

Použití, provoz podle stanoveného účelu

- XCENTRIC je určen pro použití v kancelářském prostředí. Jako MultiProtocol Router sestavuje XCENTRIC v závislosti na systémové konfiguraci spojení WAN. Chcete-li zabránit účtování nežádoucích poplatků, měli byste výrobek bezpodmínečně hlídat.
- XCENTRIC odpovídá příslušným bezpečnostním předpisům pro zařízení informační techniky používaná v kancelářském prostředí.
- XCENTRIC je určen pro nástěnnou montáž a smí se používat pouze v zavěšeném stavu. Funkce větrání zásadně nesmí být omezována.
- Provoz systému odpovídající stanovenému účelu podle IEC 950/EN 60950 je zaručen pouze při kompletní montáži plechového krytu (chlazení, protipožární ochrana, odrušení).
- Teplota okolí by neměla překročit 40°C. Zabraňte přímému ozáření sluncem.
- Dbejte na to, aby do vnitřku přístroje nemohly vniknout žádné předměty (např. kancelářské svorky) anebo kapaliny (elektrický výboj, zkrat). Dbejte na dostatečné chlazení.
- V nouzových případech (např. poškozená skříň anebo ovládací prvek, vniknutí kapaliny nebo cizích těles) okamžitě přerušte přívod proudu a informujte servis.

Čištění aopravy

- Přístroj smí otvírat pouze školený odborný personál. Před otevřením se přístroj zásadně musí odpojit od sítě (vytáhnout zástrčku). Nepovolaným otevíráním a neodbornými opravami se uživatel vystavuje značnému ohrožení (např. zasažení elektrickým proudem). Provedením oprav přístroje pověřujte pouze autorizovaný servis firmy BinTec. Adresu servisu Vám sdělí Váš obchodník.

- 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 **XCENTRIC** 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 **XCENTRIC** opstilles og tages i brug (se Tekniske data).
- Ved installation af eksterne ISDN-basistilslutninger skal de aktuelt gældende, nationale rammebetingelser overholdes. I givet fald skal der tilkaldes en tekniker med den nødvendige autorisation. Søg oplysning om specielle forhold i de nationale regler og overhold de deri fastlagte bestemmelser ved installationen.
- Statisk elektricitet kan medføre apparatskader. Bær derfor en antistatisk manchet om håndleddet eller rør ved en flade med jordforbindelse, inden du rører ved det åbne apparat eller et af modulerne. Berør kun printkort i kanten og tag ikke fat om konstruktionsdele eller ledninger.
- Modulerne må kun installeres i de dertil beregnede slots. Forkert montage fører til beskadigelse af modulet eller hele apparatet.
- Specielt ved installationen af hub-modulet skal du være opmærksom på, at slot 6 altid skal være bestykket, og at der ikke må sættes et enkelt hub-modul i slot 7, da dette kan medføre beskadigelse af modulet eller hele apparatet.
- Luk de ubenyttede modulpladser med blindafdækninger, så der ikke kan komme genstande ind i apparatets indre. Hvis der kommer fremmede genstande ind i apparatet, er der fare for elektriske stød og kortslutninger.
- Et 5-S_0-modul, hvor jumperne er anbragt forkert, kan blive beskadiget ved ibrugtagningen. Modulerne er inden for visse grænser udstyret med integrerede beskyttelsesforanstaltninger for at forhindre sådanne beskadigelser, men du bør alligevel være påpasselig ved anbringelsen af jumperne. Sørg ubetinget for, at konfigurerede enheder (interne eller eksterne) bliver korrekt forbundet.

- Ved ledningsføringen skal du sørge for, at apparatets udluftningsslidser ikke dækkes til og at der ikke skabes hindringer for ventilationen. Begrænsning af ventilationen for **XCENTRIC** kan medføre skader på apparatet. Skader, som skyldes manglende ventilation, dækkes ikke af garantien.
- Undlad at åbne såvel netdelen som basisapparatet (inklusiv TFE-modul) og foretag ingen manipulationer med netdelen, da der ellers kan opstå livsfare ved elektriske stød. Fjern ingen af netdelens og basisapparatets fastgørelsesskruer.
- 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.
- Kontroller, om den lokale netspænding stemmer overens med netdelens mærkespænding. Apparatet må anvendes under følgende betingelser:
  – 230 - 240 VAC
  – 50/60 Hz
- Kontrollér, at der er fri adgang til installationens jordede sikkerhedsstikkontakt. For at opnå fuld afbrydelse fra strømnettet skal netstikket trækkes ud.
- Følg den rækkefølge, der angives i denne håndbog, for tilslutningen af kablerne. Brug kun kabler som opfylder specifikationerne i denne håndbog eller de originale, medfølgede kabler. BinTec Communications AG hæfter ikke for evt. skader eller funktionsbegrænsninger ved brug af andre kabler. I sådanne tilfælde bortfalder apparatets garanti.
- Overhold henvisningerne i denne håndbog mht. apparatets tilslutning. Ved anbringelsen af klemmeblokkene skal du især passe på, at stifterne ikke bliver bøjede, og sørge for at den monterede klemmebloks skruer peger mod højre, da interfacet ellers ikke fungerer og kan blive beskadiget
- 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 tordenvejr, og undlad at berøre dem.

- Kun terminaludstyr, som opfylder de generelle sikkerhedskrav for telekommunikationsudstyr, må sluttes til **XCENTRIC**. Terminaludstyr med en godkendelse fra CETECON (tidligere BZT) opfylder disse krav. ISDN-terminaludstyr, som sluttes til **XCENTRIC** , skal være godkendt til Euro-ISDN (DSS1), analogt udstyr skal understøtte DTMF-/tonefrekvensopkaldsmetode og være indstillet på tonefrekvensopkald.

Bestemmelsesmæssig anvendelse, brug

- **XCENTRIC** er beregnet til anvendelse i kontormiljø. Som multiprotokolrouter etablerer **XCENTRIC** WAN-forbindelser afhængigt af systemkonfigurationen. For at forebygge uønskede afgiftsbetalinger bør du ubetinget overvåge produktet.
- **XCENTRIC** opfylder de gældende sikkerhedsbestemmelser for informationsteknisk udstyr til kontorer.
- **XCENTRIC** er beregnet til montering på væggen og må kun anvendes i ophængt tilstand.
- Bestemmelsesmæssig anvendelse af systemet iht. IEC_950/EN_60950, er kun sikret, når metalkabinettet er monteret komplet (køling, brandsikkerhed, radiostøjdæmpning).
- Omgivelsestemperaturen må ikke overstige 40°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 uddannet, faglært personale. Træk altid netstikket ud, før kabinettet åbnes. Uautoriseret åbnning og reparationer, som ikke er faglig korrekte, kan medføre betydelige farer for brugeren, (f.eks. elektriske stød). Lad kun et BinTec-autoriseret serviceværksted udføre reparationer på apparatet. Din forhandler kan oplyse dig serviceværkstedets adresse.
- 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.

CLIR Calling Line Identification Restriction

BRICKware 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**.

Direct dialing range — See ➤➤ **extension numbers range**

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.

DNS — Domain Name System

Each device in a ➤➤ **TCP/IP network** is usually located by its ➤➤ **IP address**. Because ➤➤ **host names** are often used in networks to reach different devices, it is necessary for the associated IP address to be known. This task can be performed by a Domain Name Server (DNS), which resolves the host names into IP addresses. Alternatively, name resolution can also take place over the HOSTS file, which is available on all PCs.

Domain A domain refers to a group of devices in a network, whose host names share a common suffix, the domain name. Thus, in the ➤➤ **Internet**, a part of a naming hierarchy (e.g. bintec.de).

Downstream Data transmission rate from the ➤➤ **Internet Service Provider** to the client.

DSL/xDSL Digital Subscriber Line

Data transmission technique that enables high transmission rates to be achieved on normal telephone lines.
The data rate is dependent on the distance to be covered and the quality of the line and therefore varies.

xDSL is used as a bookmark for the different DSL variants, such as ➤➤ **ADSL**, ➤➤ **RADSL**, ➤➤ **VDSL**, ➤➤ **HDSL**, ➤➤ **SDSL**, ➤➤ **U-ADSL**, etc., which are part of the family of DSL techniques.

DSS1 Digital Subscriber Signalling System.

A common D-channel protocol used in the Euro ISDN.

DTE Data Terminal Equipment

Data Terminal Equipment (see ➤➤ **V.24**)

DTMF Dual Tone Multi Frequency (tone dialing system)

Dialing method for telephony systems. In this method, pressing a key on the telephone keypad generates two simultaneous tones, which are correspondingly evaluated by the PABX or exchange.

E1/T1 E1: European variant of the 2.048 Mbps ➤➤ **ISDN** ➤➤ **Primary Rate Interface**, which is also called the E1 system.

T1: American variant of the ISDN Primary Rate Interface with 23 basic channels and one D-channel (1.544 Mbps).

EAZ Terminal Selection Digit

Is only used in the ➤➤ **1TR6** system and designates the last digit of an extension number. It is used for dialing various terminals connected to the ISDN Basic Rate Interface (e.g. fax). This occurs by attaching one digit between 0 and 9 to the actual ISDN telephone number. In Euro ISDN (DSS1), the complete extension number, ➤➤ **MSN**, is transferred instead of the EAZ.

Encapsulation Encapsulation of ➤➤ **data packets** in a certain protocol for transmitting the packets over a network that the original protocol does not directly support (e.g. NetBIOS over TCP/IP).

Encryption Refers to the encoding of data, e.g. ➤➤ **MPPE**.

Ethernet A local network that connects all devices in the network (PC, printers, etc.) via a twisted pair or coaxial cable.

Extension An extension is an internal number for a terminal or subsystem. In ➤➤ **point-to-point ISDN accesses**, the extension is usually a number from the ➤➤ **extension numbers range** assigned by the telephone provider. In point-to-multipoint connections, it can be the MSN or a part of the MSN.

Extension numbers range (direct dialing range)

A **point-to-point ISDN access** includes a ➤➤ **PABX number** and an extension numbers range. The PABX number is used to reach the PABX. The extension numbers range is a group of numbers used for selecting terminals within the ➤➤ **PABX**.

Filters A rule that defines a set of packets that should or should not be transmitted by the router.

Firewall Designates the whole range of mechanisms to protect the local network against external access. **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 ➤➤ **S_0 bus**.

ISDN BRI ISDN Basic Rate Interface

➤➤ **ISDN Basic Rate Interface**, also ➤➤ **S_0 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.

Layer 1 Layer 1 of the ➤➤ **ISO/OSI reference model**, physical layer.

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.

Local prefix See ➤➤ **trunk prefix**.

MAC address Every device in the network is defined by a fixed hardware address (MAC address). The network card of a device defines this internationally unique address.

Main number A ➤➤ **point-to-point ISDN access** includes a main number and an ➤➤ **extension numbers range**. The main number is used to reach the PABX. A certain terminal of the PABX is then dialed via one of the extension numbers of the extension numbers range.

MIB Management Information Base

The MIB is a database that describes all the manageable devices and functions connected to a network. All MIBs (including the BinTec MIB) contain objects specific to the manufacturer. ➤➤ **SNMP** is based on MIB.

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 ➤➤ **S_0 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 (➤➤ **S_0 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 (➤➤ **S_0 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 ➤➤ **S_0 interface** and ➤➤ **1TR6** or other manufacturer-specific ➤➤ **D-channel protocols** on the subscriber side.

An ISDN PABX is used to set up an internal telephone infrastructure allowing internal connections between the PABX extensions without the need to connect to the telephone service provider. Not all BinTec routers include an exchange.

PABX number A point-to-point ISDN access includes a PABX number and an ➤➤ **extension numbers range**. The PABX number is used to reach the PABX. A certain terminal of the ➤➤ **PABX** is then dialed via one of the numbers of the extension numbers range.

PAP Password Authentication Protocol

Authentication process for connecting over ➤➤ **PPP**. Functions like ➤➤ **CHAP**, except that the user name and password are not encoded before being transmitted to the partner.

Ping Packet Internet Groper

Command that can be used to determine the range to remote network components. Ping is also used for test purposes to determine if the remote device can actually be reached at all.

Point-to-multipoint Feature of a connection that is permanently connected between three or more data stations or set up via switching systems.

Point-to-multipoint connection ➤➤ **Point-to-multipoint**)

Several different terminals can be connected to a point-to-multipoint connection. The individual terminals are addressed via certain extension numbers (➤➤ **MSN**s).

Point-to-point Feature of a connection between two data stations only. The connection can be permanently switched or set up via switching systems.

Point-to-point ISDN access A point-to-point ISDN access is used for the connection of a ➤➤ **PABX**. The PABX can forward calls to a number of terminals. A point-to-point access includes a ➤➤ **PABX number**, via which the PABX is reached from outside and a group of numbers (➤➤ **extension numbers range**), with which the terminals connected to the PABX can be dialed.

Port Input/output

The port number is used to decide to which service (telnet, WWW) an incoming data packet should be sent.

POTS Plain Old Telephone System

The traditional analog telephone network.

PPP Point-to-Point Protocol

A protocol suite for authentication of the connection parameters of a ➤➤ **point-to-point connection**. PPP is used to connect local networks over the ➤➤ **WAN**. Multiprotocol packets are encapsulated (➤➤ **encapsulation**) in a standard format before transmission. Establishing a connection involves a number of other components and subprotocols, such as the authentication mechanisms ➤➤ **PAP/CHAP**.

PPP authentication Security mechanism. A method of authentication using passwords in ➤➤ **PPP**.

PPPoE Point to Point Protocol over Ethernet

The PPP-over-Ethernet (PPPoE) protocol permits Internet access over Ethernet via an ➤➤ **xDSL** modem or xDSL router.

Prefix See ➤➤ **trunk prefix**.

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.

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).

S_0 bus All ISDN sockets and the ➤➤ **NTBA** of an ISDN point-to-multipoint connection. All S_0 buses consist of a four-wire cable. The lines transmit digital ISDN signals. The S_0 bus is terminated with a terminating resistor after the last ISDN socket. The S_0 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 S_0 bus at any one time, as only two ➤➤ **B-channels** are available.

S_0 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).

Slot A slot is the physical position into which a hardware module is inserted.

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.

TAPI Telephony Applications Programming Interface

Standard Microsoft software interface used by many telephony programs. Telephony programs enable database-supported telephoning on the PC. An example is the Windows utility or the BinTec program CTI Phone, which can be found on the BinTec Companion CD. TAPI services are only supported by routers with an integrated ➤➤ **PABX**.

All the users of a network can use TAPI services via BinTec's Remote TAPI.

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).

TE Terminal Equipment

Terminal equipment for subscriber access, e.g. telephone, fax or PC.

TEI Terminal Endpoint Identifier

The TEI in ➤➤ **ISDN** is an address field in layer 2 that is used for identifying a certain terminal.

Telematics Telematics is a combination of telecommunication and computer technology and describes data communication between systems and devices.

Telnet Protocol from the ➤➤ **TCP/IP protocol suite**. Telnet enables communication with a remote device in the network.

Terminal Terminal equipment

A terminal refers to equipment such as ISDN and analog telephones connected to **X1000**, as well as to subsystems such as router, CAPI and ISDN Login.

TFE Door intercom

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.

Trunk Refers to an exchange line in ➤➤ **ISDN**.

Trunk prefix Refers to the sequence of digits that may have to be dialed to obtain an exchange line for making an outside call (trunk prefix) or an internal connection (local prefix). Prefixes are also used for cascading **X1000**s.

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.42bis Data compression procedure.

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.

Numerics

A