

BIANCA/BRICK-XL2

User's Guide

Hardware and Installation

Version 1.6
Document #71000G

November 2000

Copyright © 2000 BinTec Communications AG

All rights reserved

Purpose:

This manual explains the installation and configuration of BIANCA/BRICK-XL2 with the Software Release 4.9.4. Before installing and configuring your router, please note the security instructions described in your BIANCA/BRICK-XL2 User's Guide.

It is highly recommended that you read our Release Note containing the latest information and instructions for the most current Software Release – especially if you are performing a software update to a higher level. The latest Release Note is always available at www.bintec.de.

Liability:

While every effort has been made to ensure the accuracy of all information in this manual, BinTec Communications AG assumes no liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document. BinTec Communications AG is only liable within the scope of its terms of sales and delivery.

The information in this manual is subject to change without notice. Additional information, including changes and Release Notes for BIANCA/BRICK-XL2, can be retrieved at www.bintec.de.

As an ISDN multiprotocol router, BIANCA/BRICK-XL2 establishes ISDN connections in accordance with the system's configuration. To prevent unintentional charges accumulating, the product should be carefully monitored. BinTec Communications AG accepts no liability for incidental or consequential loss of data, unintentional connection costs and damages resulting from the unsupervised operation of the product.

Trademark:

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

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

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 the copyright owner. Also, an adaptation, especially a translation, of the document is inadmissible without the prior consent of BinTec Communications AG.

Declarations:

FCC Notice — Class A Computing Device

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to Part 15 of the FCC Rules and CSA Regulation C 108.8. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference which the user will be required to correct at his/her own expense.

CE Notice

The  symbol means that the BRICK-XL2 adheres to the EMV (89/336/EWG) and voltage (73/23/EWG) guidelines defined by the European Community.

Euro-Numeris

In addition to the guidelines defined by the EC, the BRICK-XL2 adheres to ISDN requirements in France and may be connected to Euro-Numeris.

GS

The GS (Geprüfte Sicherheit) symbol means that the BIANCA/BRICK-XL2 adheres to the standards defined by the German safety regulations.

Important Safeguards

This section describes the safety precautions the user should abide by when operating this equipment.

NOTICE: The safeguards listed here apply to all countries. A description of these safeguards in your local language can be found in Appendix A.

- As an ISDN multiprotocol router, BIAN-CA/BRICK-XL2 establishes ISDN connections depending on the system's configuration. To avoid extra charges, you should carefully monitor the product.
- Remove power before opening this device.
- Transport this equipment in its original packaging or by using appropriate materials to prevent against shock and impact.
- Before setting up this product for operation please make note of the accompanying environmental requirements.
- Slots and openings in the unit are provided for ventilation. To ensure reliable operation and to protect it from overheating these slots and openings must not be blocked or covered.
- Condensation may occur externally or internally if this equipment is moved from a colder room to a warmer room. When moving this equipment under such conditions, allow ample time for the equipment to reach room temperature and to dry before operating.
- Note that normal operation (in accordance with IEC 950/EN-60950) is only possible when the external housing is left in place (ventilation, fire prevention, and radio interference).
- Before supplying power, verify the power rating identified on the marking label complies with the local power source. This equipment may be operated under the following conditions:
 - 115 VAC/230 VAC
 - 60 Hz or 50 Hz
 - max. 6.0 A max. 3.0 A
- Do not allow anything to rest on any of the attached cables and do not locate the product where persons will walk or trip on the cables.
- Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type. Dispose of used batteries according to the manufacturer's instructions.
- Connect this equipment only to an approved, properly grounded, and accessible socket outlet (this product includes a safety tested power cable). To completely turn off this equipment you must remove the power cord from the system.
- Avoid connecting or disconnecting data lines during lightning storms.
- Follow the accompanying instructions when connecting the required cabling.
- Make sure no foreign objects or liquids come into contact with the internal components (danger of shock or short circuit).
- In an emergency (e.g., damaged external housing or internal elements, liquid spills) immediately remove the power cord and notify customer service.
- Use only the supplied cables. If you use other cables BinTec Communications cannot assume responsibility for any resulting damage.
- Electrostatic electricity can damage internal components. Ground yourself before touching any internal components.
- Never use water to clean this device. If water reaches the internal parts, extreme danger may result to the user or the equipment.
- Never use scouring or abrasive cleaning agents, or agents containing alkaline on this device. Damage to the device's exterior may result.
- Information for the Technician
- Remove the network cables before opening this equipment.

BIANCA/BRICK-XL2

*User's Guide
Version 1.6*

Contents

1. Introduction

How to contact BinTec Communications	1
How to get the latest software and documentation	2
About your User Documentation	2
Features	3
What's covered in this guide	5
Conventions used in this guide	6

2. Installing the BRICK

Connecting the BRICK to the LAN	8
Ethernet Installations	8
Token Ring Installations.....	10
Connecting the BRICK to the WAN	10
The ISDN Modules.....	10
The X.21 Module.....	11
Connecting the BRICK to a PC or terminal	11
The BOOT sequence	12
Logging in for the first time	14

3. Working with the BRICK

SNMP, MIBs, and BRICK System Tables	15
Configuration Files, Flash, and the TFTP	18
Physical and Software Interfaces	19
Setup Tool vs. SNMP Shell	20
Using Setup Tool	21
Menu Layout	21
Menu Structure	22
Special Menu Commands	24
Menu Navigation	25
List Navigation	26

4. Setup Tool Menus

Setup Tool Main Menu	31
Basic System Configuration	33
Hardware Interfaces	37
Partner Management	49
Configuring Protocols	66
System Administration	103

5. How Do I Configure ...

Hardware Interfaces	121
How do I configure an ISDN interface in general?	121
How do I configure a leased line connection?	122
How do I configure Dynamic Short Hold?	123
How do I configure my X.21 interface?	124
How do I configure my Fast Ethernet interface?	125
How do I configure my token ring interface?	126
How do I configure my primary rate interface?	127
IP Features	128
How do I configure dialup TCP/IP access for an ISDN partner?	128
How do I configure Dialup Access to CompuServe Online Services	130
How do I configure the BRICK to accept its IP address dynamically?	132
How do I configure the BRICK as a dynamic IP address server? ...	133
How do I configure Internet access for my LAN using NAT?	134

How do I configure the BRICK as a RADIUS Client?	137
How do I configure the BRICK as a BOOTP relay agent?.....	140
IPX Features	141
How do I connect my local and remote IPX networks over ISDN?	141
Modem and Fax Features	143
How do I configure my BRICK-XL2 as a Central Site Modem Server?.....	143
How do I enable outgoing modem calls?.....	145
Now the partner can also be called using one of your BRICK's modems.	146
How do I configure fax service from RVS-COM	146
Faxing from MS Applications via RVS Fax.....	149
Faxing from Microsoft Exchange.....	151
General	153
How can I retrieve accounting information (ISDN and TCP/IP)? ..	153
How can I Bridge two LANs over ISDN?.....	155
How can I improve security?	157
How can remote users access the BRICK's status page?.....	161

6. Troubleshooting

General Troubleshooting	167
Debugging Tools	168
Local SNMP Shell Commands.....	168
Remote Tools (UNIX and Windows).....	169
System Errors	169
Hardware Problems	171
X.21 (CM-X21) Interfaces.....	171
Fast Ethernet (CM-100BT) Interfaces	171
Primary Rate (CM-PRI) Interfaces.....	172
Token Ring Interfaces	173
Serial Console	173
Software Problems	174
IPX Routing	174
OSPF Routing	176
ISDN Connections	177

7. Command Reference

The SNMP shell commands 183
BRICKtools for UNIX Commands 196

8. Hardware/Firmware Configuration

Hardware 200
 Front Panel Indicators 200
 The Back Plane 202
 The Main Board 203
Firmware 205
 Upgrading System Software 205
 BOOTmonitor 205
 Automatic booting over TFTP 208
Communications Modules 209
 The LAN Modules..... 209
 The WAN Modules..... 214
Function Modules 222
 FM-8MOD Modem Module 222
 FM-STAC Compression Module 224
Installing Communications Modules 226
Installing the Modem Connection Kit 229
General System Specifications 235

A. Technical Data

Pin Assignments 236
 ISDN S₀ Interface(s) for CM-1BRI, CM-2BRI..... 236
 UTP Port for the BIANCA/CM-PRI 237
 TP Port for the CM-100BT 239
 Serial Port 240
 DB9 Port for the CM-TR 241
 Audio interface for the CM-1EBRI 242
 15 Pin Port for the CM-X21 243
Important Safety Information 244

B. Approvals

1

INTRODUCTION

What's covered

- How to contact BinTec Communications1
- How to get the latest software and documentation.....2
- About your User Documentation2
- What's covered in this guide5
- Conventions used in this guide.....6

How to contact BinTec Communications

Ways to contact BinTec	Telephone number or address
Telephone	+49 911 96 73 0
FAX	+49 911 688 07 25
Mail	BinTec Communications AG Südwestpark 94 D-90449 Nürnberg GERMANY
WWW	http://WWW.BinTec.DE

How to get the latest software and documentation

Please visit our WWW server for current information on all BinTec products. Via our WWW server BinTec provides you free of charge with the most recent versions of:

- User documentation for your BinTec software/hardware.
- System software for your BRICK (see section *Firmware* in chapter 8 on how to update the system software).
- Release notes for upgrading your BRICK's system software.
- Windows software and UNIXTools applications.

About your User Documentation

Your BRICK documentation consists of this *User's Guide*, the introductory *Getting Started* and *Los Geht's* manuals, and the online references *BRICKware for Windows*, *Extended Feature Reference*, *Software Reference*, and *The Management Information Base*.

This document includes information for users that are familiar with networking and telecommunications and describes the BIANCA/BRICK hardware, the available communications modules, and includes all the basic information you need to setup, configure, and administer your BRICK.

See the next section for an introductory list of features included with your new BRICK. Following that is an overview of what's covered in this guide.

Features

The BRICK-XL2 is the flagship of BinTec's family of BIANCA/BRICK multiprotocol routers. The system offers both power and flexibility though features not limited to the following:

- *Modem Pool*—the BRICK-XL2 can be outfitted with up to eight FM-8MOD modem modules allowing the BRICK-XL2's 56Kflex/V.90 modem pool to be expanded (in steps of 8) up to 64 modems.
- *Fast Ethernet*—support for 10/100 Mbit ethernet. Support for the CM-100BT module also includes auto-sensing mode allowing it to detect the fastest speed and mode (half/full duplex) of connected devices and configure the appropriate setting automatically.
- *Primary Rate ISDN*—built in support for Primary Rate Interface ISDN combined with an intelligent Dynamic Resource Allocation & Distribution (DRAD) system lets the BRICK-XL2 flexibly manage ISDN B-channels as pool of available resources.
- *RADIUS*—support for well known RADIUS software suppliers (Livingston, Merit, and Steel Belted Radius) lets you to maintain a common security model and administrative interface to network access. Additional BinTec-specific RADIUS extensions are also available for additional fine-tuning of RADIUS environments.
- *Accounting*—for user activity, ISDN charging, and attempted security breeches is possible through RADIUS accounting messages and the syslog protocol (UNIX hosts or Windows 95/NT systems).
- *Remote CAPI server*—many PC communication applications use the standardized CAPI interface to establish data connections—such as terminal sessions, T-Online, Eufofiletransfer, or fax—over the ISDN.
- Included on your BinTec ISDN Companion CD you'll find the *RVS-COM lite* communications software for Windows 95 and NT, which is a good and useful example of the power of CAPI applications. (To run *RVS-COM lite* a license must be purchased separately.)

- *Remote configuration*—configure your BRICK-XL2 from a remote site using the isdnlogin program (please refer to the *Getting Started* or *Los Geht's* manuals).
- *STAC compression*—BRICK-XL2 supports STAC compression according to RFCs 1974 and 1962 (PPP Stac LZS Compression Protocol and PPP Compression Control Protocol respectively) which—depending on the data—can increase performance to a factor of four.

The Stacker LZS algorithm is developed by Hi/fn Inc.

STAC compression on the BRICK-XL2 is also compatible with Cisco's proprietary STAC implementation which is automatically detected at connection time.

Extended Features

Additional, *extended features*, that are supported by your BRICK-XL2 include the following. Note that to take advantage of these features a supplemental software license (available from BinTec Communications or your local distributor) is typically required.

- *Token Authentication Firewall*—TAF is an advanced means of controlling access to central site computing resources that goes beyond the theoretical limitations of existing security mechanisms like Access Lists and Network Address Translation. TAF is a user verification system that is based on the established and well respected Token-Card-ACE/Server solution developed by Security Dynamics.
- *Virtual Private Networking*—Virtual Private Networking is a recent development in the networking field that allows you to both enhance connectivity and reduce communications costs while providing secure remote access to central site resources over the Internet. Using the BRICK as a VPN Server, client-to-LAN or LAN-to-LAN PPP connections (IP, IPX, or NetBEUI) can be “tunnelled” over the Internet. Allowing you to provide affordable yet secure remote access for distant or travelling workers, branch offices, or selected business partners.

What's covered in this guide

Chapter 1 Introduction is this chapter.

Chapter 2 Installing the BRICK describes physically installing the BRICK on your LAN.

Chapter 3 Working with the BRICK gives you a brief introduction to the BRICK and reviews some of the basic concepts that are central to working with the BRICK.

Chapter 4 Setup Tool Menus describes all the menus and variables you'll see when configuring BRICK features. This chapter is intended as a reference to the Setup Tool menus.

Chapter 5 How do I Configure ... answers the most common questions asked when configuring the BRICK. If you just want to know how to configure feature X, this is the first place to look.

Chapter 6 Troubleshooting is your guide to solving some of the most common problems you may encounter when administering the BRICK.

Chapter 7 Command Reference describes the shell commands available from the BRICK's SNMP shell.






Chapter 8 Hardware/Firmware Configuration describes the BRICK hardware, the available communications modules, and describes important tasks, such as installing new modules and upgrading system software.

Appendix A Technical Data contains technical specifications for the BRICK, its communications ports, and security information in different European languages.

Appendix B Approvals contains regulatory approval certificates.

Conventions used in this guide

To help you locate and interpret information easily, this manual uses the following visual clues and typographic conventions.

Visual Clues	
	Lets you know what information you'll need before you start to configure a feature.
	Marks the beginning of a list of steps required to configure a BRICK feature.
	References to information in other sections or documents that may be helpful.
	Points out additional information including useful tips and/or common pitfalls.
	Brings your attention to important safety precautions to help avoid injury.

Typographic Conventions	
	Bold constant width type represents characters or text that you must type in, exactly as shown.
	<i>Bold italic</i> type represents special system table names.
	Text enclosed in a box like this SYSTEM represents a submenu or menu command found in Setup Tool.

2

INSTALLING THE BRICK

What's covered

- Connecting the BRICK to the LAN8
 - Connecting the BRICK to the WAN10
 - Token Ring Installations10
 - Connecting the BRICK to a PC or terminal11
 - The BOOT sequence12
 - Logging in for the first time14
-


You may have already installed and setup your BIANCA/BRICK with the help of the accompanying *Getting Started* and *Los Geht's* manuals. In that case you can skip over this chapter.

In this chapter, we'll describe physically installing the BRICK on your LAN and attaching a serial console. Then we'll cover the brief BOOT sequence the BRICK goes through when starting up, and describe the login procedures you should use when logging in for the first time.

Connecting the BRICK to the LAN

This section explains how to connect the BRICK to your LAN. You can connect the BRICK-XL2 to your LAN (ethernet or token ring) using a variety of cabling methods. For ethernet installations, the CM-100BT communications module is available with a single Unshielded Twisted Pair, UTP (100baseTX) port. For token ring networks, the CM-TR Token Ring communications module is available with both a UTP and DB-9 port.


At boot time, and during normal operation mode, the BRICK automatically detects the appropriate interface (and speed, 10 or 100 Mbps, for ethernet interfaces) to use.


Caution:  Incorrect cabling of the LAN and ISDN interfaces could damage your router. Don't interchange the LAN and ISDN interfaces. Only connect the LAN interface of your router with the LAN interface of your PC/hub. Only connect the ISDN interface of your router with your ISDN outlet.

Ethernet Installations

The Fast Ethernet LAN Port

With the CM-100BT module installed (default hardware configuration) the BRICK-XL2's LAN port supports both 10 or 100 Mbps ethernet and determines the speed to operate in at boot time (auto-sensing mode). Since most sites are likely to prefer Fast Ethernet (100 Mbps) operation make sure of the following.

Note:  If you will be using the CM-BNCTP 10BaseT/10Base2 communications module please refer to the section [CM-BNCTP Ethernet Adapter](#) in Chapter 8 for special information.

-  1. Only use Category 5 STP (shielded twisted pair) cabling when attaching the BRICK to a network hub.

In most cases you can use a straight-through cable (i.e., each pin on one RJ-45 plug is wired to the same pin on the other end of the cable). The exact wire pairs shown in figure 1 below must be twisted.

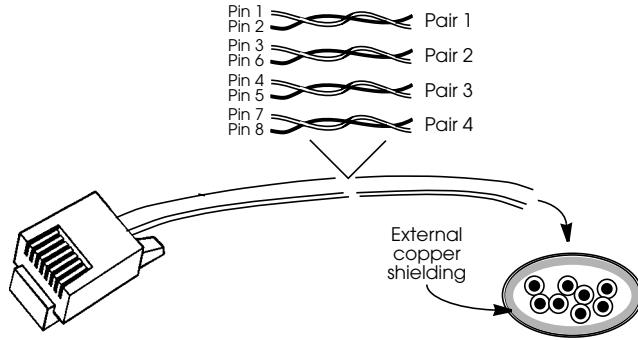


Figure 1: RJ-45 Western Plug with Twisted Pair cabling and External Shielding

2. Also note that for Fast Ethernet the maximum segment length from the BRICK to the next hub should not exceed 100 meters. (See IEEE's 802.3u Fast Ethernet standard)
3. If you are unable to establish connections with the BRICK via the ethernet, are using the appropriate cabling, and have not exceeded the segment length limitations log in via a serial console and check for error messages in Setup Tool's [Monitoring and Debugging][Messages] menu.
4. If you are still unable to establish connections via the LAN port it may help to manually configure ethernet port's speed/type as follows.

Log in via a serial console as the admin user.

Set the *biboAdmConnector* variable manually using one of the entries from the table shown below. Entering the following command from the SNMP shell prompt would configure the LAN port for 10 Mbit half-duplex operation.

```
biboABrdConnector:X=rj45_10mbit_hdup
```


Note that **x** in the above command must identify the number of the SBus slot where the CM-100BT module (typically slot 1) is installed.

5. After verifying that LAN connections can be established, save the manual settings by entering **cmd=save** from the shell prompt.

Token Ring Installations

If your BRICK-XL2 has a token ring module (CM-TR) installed, you can also connect your BRICK-XL2 to a MAU (medium access unit) on the ring with a lobe cable via the 10baseT or DB-9 port. If you use the 10baseT port on the token ring module make sure to attach a ferrite as shown on page 213. Pin assignments for CM-TR's ports are shown on page 241.

Connecting the BRICK to the WAN

Caution:  Incorrect cabling of the LAN and ISDN interfaces could damage your router. Don't interchange the LAN and ISDN interfaces. Only connect the LAN interface of your router with the LAN interface of your PC/hub. Only connect the ISDN interface of your router with your ISDN outlet.

The ISDN Modules

At boot time (and during normal operation) the BRICK-XL2 automatically detects which WAN modules are installed and adds appropriate entries in its internal configuration tables. If the communications module is connected to an ISDN subscriber outlet the BRICK will also detect the appropriate ISDN protocol that is being used.

Basic Rate Interface Modules

The BRICK-XL2 ISDN BRI communication modules can be connected to your ISDN subscriber outlet with the included ISDN cable or any standard 8 pin RJ-45 cable.



1. Attach the included ISDN cable (or any standard 8 pin RJ-45 cable) to an ISDN subscriber outlet.

2. Attach the other end of the cable to an available S₀ port of your CM-1BRI, CM-1EBRI, or CM-2BRI module.

Primary Rate Interface Modules

The BRICK-XL BIANCA/CM-PRI module should be connected to your ISDN primary rate interface. If you have any problems accessing ISDN services after booting the BRICK, see the section on PMX in Chapter 6.

You should also verify the correct cabling, see *UTP Port for the BIANCA/CM-PRI* in Appendix A. A note about installing NTs is also included there.

The X.21 Module

You can also connect the BRICK-XL2 to an X.25 data network using the X.21 module (CM-X21). Pin assignments for the CM-X21 module's 15 pin port are shown in *Appendix A* on page 243.

Connecting the BRICK to a PC or terminal

A PC or terminal can be connected directly to the BRICK using the 9 pin serial port on the backplane marked Serial Console. Please use the included laplink (serial) cable for this purpose. Do not use the port on the back plane, this is intended for other devices which will be supported in future releases. Initially use the following communications parameters.

Data Rate:	9600 bps
Data Bits:	8
Parity Bit:	None
Stop Bit:	1
Terminal Type:	VT100 (or ANSI)
SW Handshake:	XON/XOFF
HW Handshake:	none

The default data rate used by the BRICK can be set using the *BOOTmonitor* which is described in Chapter 8.

The BOOT sequence

Each time you power up the system, the BRICK moves between three different modes. The LEDs on the front panel correspond to stages within each mode. The section *Front Panel Indicators* in Chapter 8 describes their respective meanings.

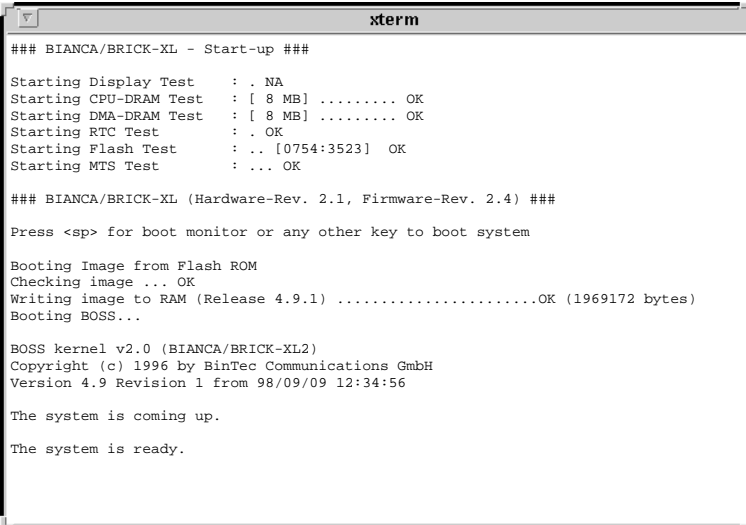
Power-up Mode BOOTmonitor Mode Normal Operation Mode

During **Power-up Mode**, the BRICK performs various self-tests designed to verify the integrity of the system and to ensure the internal circuitry is working properly.

In **BOOTmonitor Mode**, the BRICK waits 4 seconds for the user to press the spacebar which activates the BOOTmonitor. See *BOOTmonitor*, page 205, in Chapter 8 for information on using the BOOTmonitor.

Normal Operation Mode is entered once the BRICK is finished booting its internal system software.

Normally, the whole process only takes about 15 seconds. You can see the results of the various tests on your terminal display.



```
xterm
### BIANCA/BRICK-XL - Start-up ###

Starting Display Test   : . NA
Starting CPU-DRAM Test : [ 8 MB] ..... OK
Starting DMA-DRAM Test : [ 8 MB] ..... OK
Starting RTC Test      : . OK
Starting Flash Test    : .. [0754:3523] OK
Starting MTS Test      : ... OK

### BIANCA/BRICK-XL (Hardware-Rev. 2.1, Firmware-Rev. 2.4) ###

Press <sp> for boot monitor or any other key to boot system

Booting Image from Flash ROM
Checking image ... OK
Writing image to RAM (Release 4.9.1) .....OK (1969172 bytes)
Booting BOSS...

BOSS kernel v2.0 (BIANCA/BRICK-XL2)
Copyright (c) 1996 by BinTec Communications GmbH
Version 4.9 Revision 1 from 98/09/09 12:34:56

The system is coming up.

The system is ready.
```

After the system comes up, the BRICK detects which communications modules are installed, and starts various system daemons depending on which features are licensed on your BRICK. The system then presents a login prompt to the screen of a connected serial console.

Logging in for the first time

To log into the BRICK for the first time;

enter **admin** at the login prompt, then
enter **bintec** when prompted for a password.

Note that BRICK uses three different login names and passwords to grant various levels of access to configuration information. These user IDs correspond to "Community Names" used in the SNMP. For information on the differences between these user IDs or changing the default password settings, refer to Setup Tool's **SYSTEM** menu on page 34.

3

WORKING WITH THE BRICK

What's covered

- SNMP, MIBs, and BRICK System Tables15
- Configuration Files, Flash, and the TFTP18
- Physical and Software Interfaces19
- Setup Tool vs. SNMP Shell20
- Using Setup Tool21

In the previous chapter we explained physically installing the BRICK on your LAN. If you haven't already configured your BRICK for basic operation (covered in *Los Geht's* and *Getting Started*), you might like to read this chapter first.

With this chapter, we'd like to give you an introduction to working with the BRICK. First we'd like to explain a few basic concepts that make the BRICK such a diverse and powerful product. Of course if you're already familiar with the BIANCA/BRICK family of routers and the Setup Tool, feel free to skip this section.

Then we'll cover using Setup Tool (i.e., menu structure, key commands, etc.) on the BRICK. This section contains some important information including some of the finer points to using Setup Tool. You may decide to return to this section for future reference while using Setup Tool.

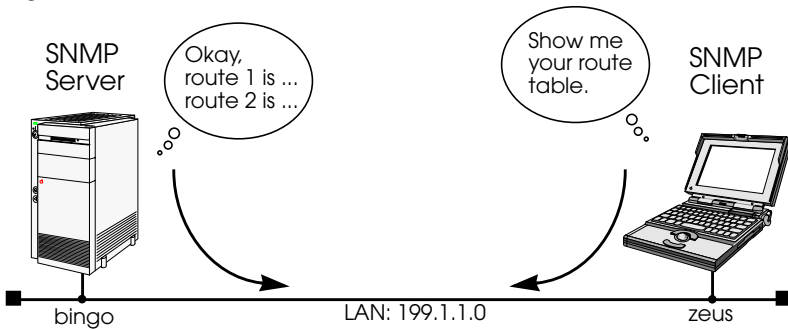
SNMP, MIBs, and BRICK System Tables

Remote access is one of the BRICK's most important features and means that as an administrator, you have just as much control of the BRICK from a telnet session as you do from an attached console. This section de-

scribes the underlying concepts such as SNMP, MIBs, and BRICK System Tables which make remote access possible.

SNMP stands for the Simple Network Management Protocol and defines the rules for the transfer of management information over IP networks. SNMP is implemented as a client-server system; the station "being managed" runs the server-process, and the management station the client-process.

For example, the administrator at host "zeus" could manage the router "bingo" using an SNMP management application such as Sun's Net-manager.



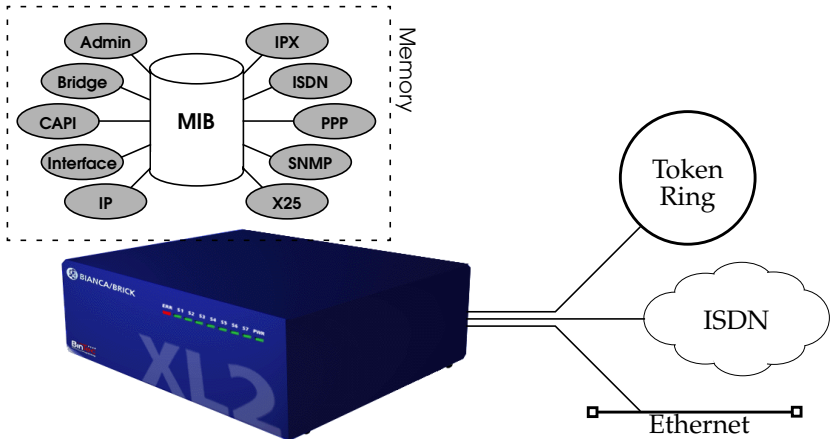
After booting, the BRICK starts a login shell. We sometimes refer to it as the SNMP shell because special commands can be entered from the shell which are given directly to the BRICK's SNMP server-process. This means that the BRICK's SNMP shell can be accessed from an SNMP client application, as well as simple text-oriented connections such as telnet, isdnlogin, or minipad.

But wait; before an SNMP management station can administer such stations, it first has to know a few things about it such as what type of station it is (router, printer, bridge, ...), what operating parameters can be changed, etc. This is where the **MIB** or Management Information Base comes in.

A MIB is a sort of database containing different variables (often referred to as objects), all of which combined, define how the BRICK operates as a whole. The BRICK implements different MIBs, including the standard IP MIB version 2, Novell and BinTec Enterprise MIBs. Our

SNMP client-process running on zeus shown above, would need to load MIB files locally from disk before contacting BRICK.

Upon booting, the BRICK starts an SNMP process, then reads its configuration file (covered next) and stores the information in memory. From the SNMP shell, these variables are represented by various **System Tables** which are arranged into functional groups. Entering the “g” command displays a list of groups while the “l” command shows a long list of all system tables.



These variables can be changed by editing the system tables; the BRICK then updates the respective variables in memory instantly. As mentioned earlier, the BRICK can be managed from any of its ports.

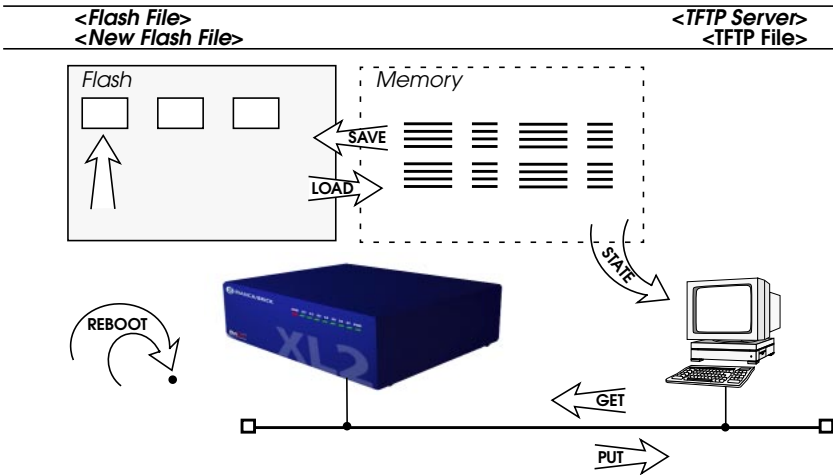
Note: As soon as a variable is changed in memory, the setting becomes effective immediately, the BRICK does not have to be rebooted nor do configuration files need be reloaded. Any changes made to memory not saved in a configuration file, however, are lost once the system is shut down.



Configuration Files, Flash, and the TFTP

As mentioned earlier, the BRICK reads its configuration information internally from a configuration file. This file is stored in **Flash EEPROM** (electronically erasable programmable read-only memory), which we just refer to as Flash. Actually, Flash can hold as many different files as you need; as long as there's enough room for them.

Think of Flash as a directory of configuration files. The files in this directory can be created, copied, moved, deleted. It's also possible to retrieve and transmit configuration files to/from remote hosts. These actions can be performed using the Configuration Management menu in Setup Tool or from the SNMP shell by using special commands. Refer to the description on this menu in Chapter 4 for more information on the various commands and parameters.



The transfer of configuration files between the BRICK and remote hosts is made possible by the **TFTP**, or Trivial File Transfer Protocol. Using TFTP, it's also possible for the BRICK to retrieve its boot-image (or system software) from a TFTP host. See the section on the **BOOT**monitor in Chapter 8.

Physical and Software Interfaces

One of the central concepts used on the BRICK is the idea of interfaces. This section briefly explains the idea of interfaces used on the BRICK.

As a central site router the BRICK-XL2 was designed to link your local and remote networks (or hosts) using WAN links such as ISDN dialup, leased line, and X.25 connections. To establish connections to these sites, the BRICK uses the Software Interfaces that you configure. By “Software Interface”, we simply mean that you create an interface by giving it a name and specifying the characteristics of the communications link such as:

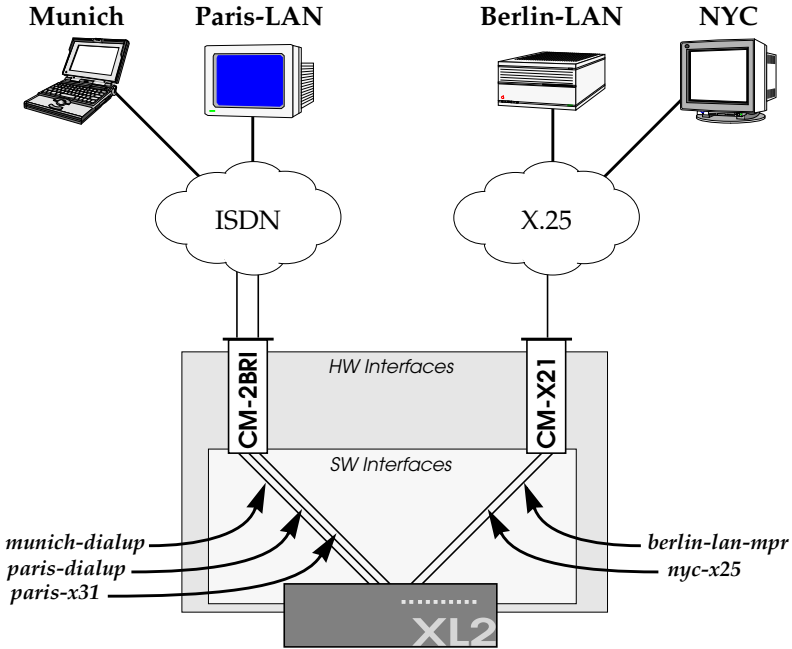
- **Type of Link** — what physical medium to use.
- **Supported Protocols** — what protocols do you want to route.
- **Encapsulation** — the format to use when transmitting data.
- **Connection security** — authentication at connect time?
- **Network security** — what types of traffic don’t you want routed.

The characteristics you configure for a software interface depend on the capabilities of the hardware (communications modules) installed on your BRICK. Software interfaces are easily added or changed using the BRICK’s Setup Tool under the WAN Partners menu. You can create as many software interfaces as you need. When routing, the BRICK maps software interfaces onto physical hardware interfaces.

Let’s consider the example shown on the following page. The BRICK-XL2 interconnects the central site office with 2 remote LANs, and provides remote access to hosts in Munich and NYC.

Suppose a host on the BRICK’s LAN segment generates intermittent bursts of traffic with a host on the Paris -LAN. We might create a “paris-x31” interface and configure X.31 (X.25 in the D-channel) allowing us to take advantage of volume-based charging in X.31. All other traffic could be routed over ISDN default dialup connections.

Traffic destined for the Berlin LAN or the database server in NYC would be routed over the same hardware interface (our X.21 module) but different software interfaces. “berlin-lan-mp” is our multiprotocol routing interface and supports IP, IPX, and Bridging traffic while “nyc-x25” only needs to handle X.25 packets from our remote database.



Setup Tool vs. SNMP Shell

As mentioned earlier, administering the BRICK's features involves managing the various system variables (or tables of variables) defined in the BRICK's MIB. Considering the close to 100 system tables and the various interdependencies of the resulting 1000 or more variables, this can be a daunting task when performed from the SNMP shell.

The BRICK's Setup Tool removes the complexity of administering the BRICK and allows you to configure the features you need using a simple character based menu system.

Keeping Setup Tool character oriented means you can administer the BRICK and its features remotely from simple character based connections such as telnet, terminal emulation programs, isdnlogin, and minipad.

This document describes administering the BRICK with Setup Tool. For info on using the SNMP shell see the *Software Reference Manual*.

Using Setup Tool

Setup Tool is an easy to use, intuitive menu-oriented program. After a few minutes, you'll have no problem finding your way around the various menus. In this section we'd like to point out a few things you should be aware of when using Setup Tool.

But first, let's look at Setup Tool's Menu Layout and Structure.

Menu Layout

Navigational Aid:
Tells you where you are in Setup Tool menu system.

BRICK's hostname:
Useful for sites with several routers.

```

BIANCA/BRICK-XL2 Setup Tool      BinTec Communications AG
[[P]][ROUTING]: IP Route Table      brick
  
```

The flags are: U (Up), D (Dormant), B (Blocked),
G (Gateway Route), I (Interface Route),
S (Subnet Route), H (Host Route)

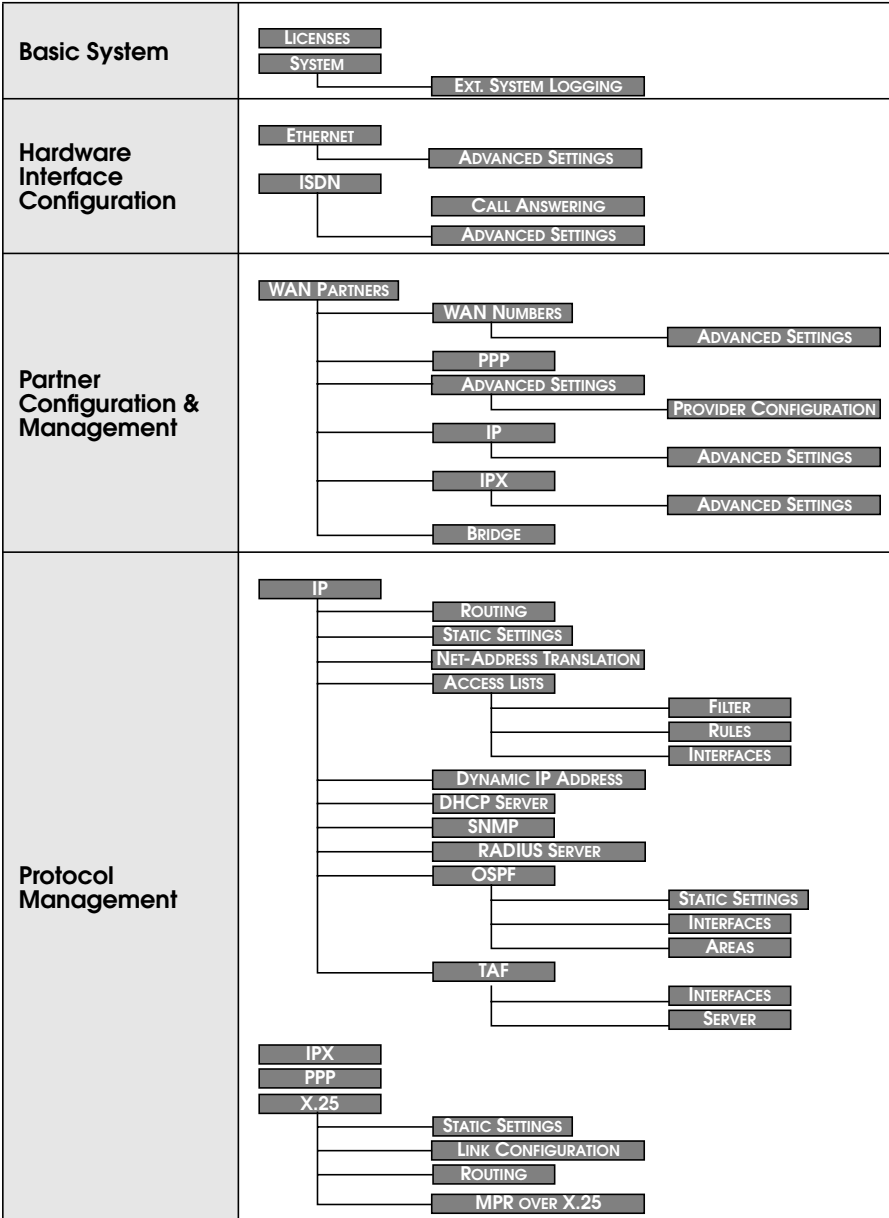
Destination	Gateway	Mask	Flags	Me	Interf/Partner	Pro
199.1.2.2	199.1.1.20	255.255.255.128	US	0	en1	loc
199.1.1.0	199.1.1.2	255.255.255.128	US	0	en1	loc

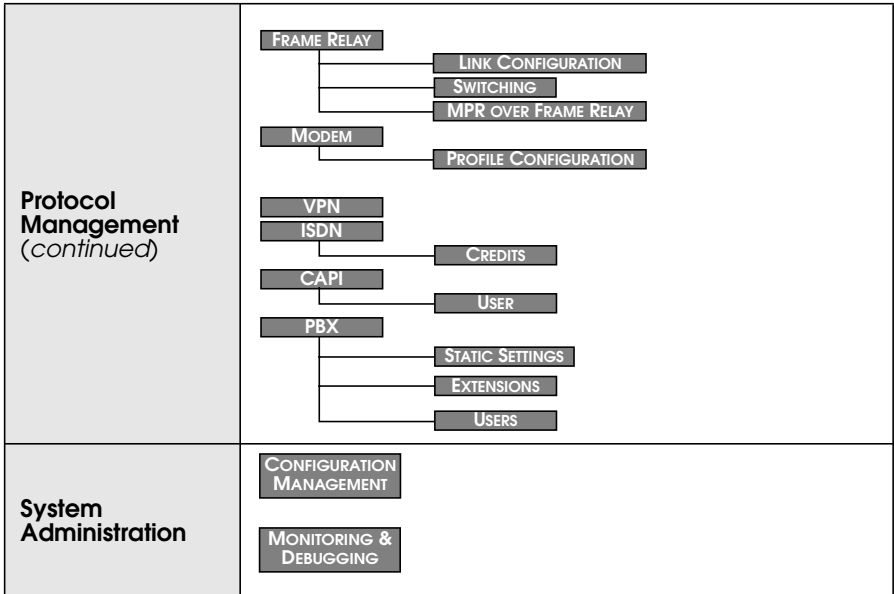
ADD DELETE EXIT

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

Help Line:
As you move the cursor between different fields the help line provides useful information.

Menu Structure





Info: Setup Tool's complete menu structure is displayed above; some sections are not available on certain products.

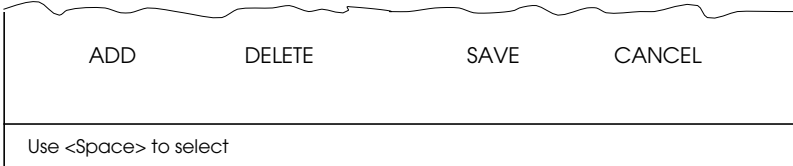


The menus available on your system will depend partly on Hardware (installed communications/feature modules) and Software (which features are licensed on your system).

When new hardware modules/software licenses are detected on your system, the BRICK automatically displays the respective menu items.

Special Menu Commands




















While using Setup Tool you will notice that some menus have different command options in the lower portion of the menu such as the "ADD" "DELETE" "SAVE" and "CANCEL" commands shown below. There are a few slight differences between these commands which you should be aware of.



Menu Command	Effect
ADD	Used to create or add an item to a list.
CANCEL	Discards all changes made within the current menu. Note: ONLY the current menu.
DELETE	This command deletes all entries tagged for deletion from a list. Changes are saved to memory and become effective immediately.
OK	The changes made in the current menu are marked, but are only saved to memory after a SAVE is activated in the next menu.
SAVE	All variables set in the current menu AND its submenus are saved to memory. The effect is that these changes become effective immediately.
EXIT	Simply return to the previous menu.

Menu Navigation

While using the Setup Tool the following keys can be used to navigate the various menus.

Key Combination	Meaning
 	Use the tab key to move to the next field entry. Use the Return key to enter a submenu or to activate a menu command (such as SAVE, EXIT, or DELETE).
 or 	Scroll backwards or forwards among a list of required entries.
 or 	Use the up and down cursor keys to move forwards or backwards among menu fields.
 	Entering the escape key two times successively aborts changes made and returns you to the previous menu.
	Use the spacebar to toggle the delete flag for special entries that may be deleted.
 - 	While holding down the Control-Key press L to redraw the screen.
 - 	While holding down the Control-Key press N to jump to the next item in a list.
 - 	While holding down the Control-Key press P to jump to the previous item in a list.
 - 	While holding down the Control-Key press B to scroll back a page in a long list. At the top right edge of the list there will be either a »=« (top of list) or a »^« (more to come).
 - 	While holding down the Control-Key press F to scroll forward a page in a long list. At the bottom right edge of the list there will be either a »=« (bottom of list) or a »v« (more to come).

List Navigation

Several Setup Tool menus contain lists of items, e.g. the **WAN PARTNER** → menu lists all the WAN partners which are currently configured, and the **IP** → **ROUTING** → menu lists all IP routes.

These lists are sorted alphabetically using the contents of the first field.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[WAN]: WAN Partners		brick	
Current WAN Partner Configuration			
Partnername	Protocol	State	
apollo-11	ppp	dormant	=
apollo-13	ppp	up	
apolonia	ppp	dormant	
bongo	x25_ppp	up	
T-online: 10432,7512	x75_ppp	up	
test-account	x25_ppp	down	
zapata	ip_lapb	down	v
ADD	DELETE	EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit			
Search: Te			

To search menu list items enter a valid search character (only printable characters). The cursor automatically jumps to the first match in the list. As long as the search is active subsequent characters entered are appended to the search string. The current search string is shown in the bottom portion of the terminal window. Entering a non-printable character resets the current search (and possibly performs an action; e.g. tab, space, etc.). The <backspace> key (and possibly <delete> depending on terminal settings) can be used to edit the search string. Search characters are case-insensitive (Entering the letter "t" matches both "t" and "T" characters).

Assuming the above **WAN PARTNER** → menu list the following key sequences would have the following effect:

Key Sequence	Resulting Effect
t, or T	Cursor jumps to the: T-Online 10432,7512 entry.

Key Sequence	Resulting Effect
te, TE, tE, Te	Cursor jumps to the: test-account entry.
a p o l o	Cursor jumps to: apollo-11 entry first then to: apolonia after the last "o".

Note also that a search can only be performed when the cursor is in a list field (and not when in an ADD, DELETE, EXIT, CANCEL, or SAVE field).

4

SETUP TOOL MENUS

What's covered

- Basic System Configuration.....33
 - Hardware Interfaces37
 - Partner Management49
 - Configuring Protocols66
 - System Administration103
-

In the previous chapter we gave you a brief overview of working with the BRICK and described how you can administer it using the SNMP shell, or Setup Tool.

In this chapter we'll cover all of the menus and settings you'll see while using Setup Tool. This chapter is divided into five sections which correspond to the Setup Tool Main Menu.

- Basic System Configuration
- Hardware Interfaces
- Partner Management
- Configuring Protocols
- System Administration

Each menu is identified according to its location in relation to the Main Menu such as **WAN PARTNER** → **ADD** → **IP** .

Caution



As an ISDN multiprotocol router, BIANCA/BRICK-XL2 establishes ISDN connections in accordance with the system's configuration. Incorrect or incomplete configuration of your product may cause unwanted charges. The conditions that lead to establishing connections are largely dependent on the respective network configuration.

- To avoid unintentional charges, it is essential that you carefully monitor the product. Observe the LEDs of your product or use the monitoring function in the Setup Tool.
- Use filters to deny certain data packets (cf. page 76). You should be aware that especially in a Windows network broadcasts may establish connections.
- Use the Credits Based Accounting System, as described on page 99, to define a maximum number of ISDN connections resp. the accounted charges allowed in a certain period of time and thus limit unwanted charges in advance.
- Use the checklist "ISDN connections remain open or are unwanted" on page 178 to prevent the most common causes of unintentional charges.

Setup Tool Main Menu

After entering **setup** from the shell prompt Setup Tool's Main Menu is displayed as below. Depending on your hardware setup and software configuration your BRICK's menu may differ slightly.

- LICENSES** Used for entering the serial number licensing information.
- SYSTEM** Contains basic administration information such as system name, security passwords, and system logging parameters.
- SLOT 1** Used for configuring specific hardware interfaces, depending on which slots your communications modules are installed in.
- through
- SLOT 7**

BIANCA/BRICK-XL2 Setup Tool				BinTec Communications AG			
[LICENSE]: Licenses				brick			
Licenses				System			
Slot 1:	CM-100BT, Ethernet			Slot 4:	CM-PRI, ISDN S2M		
Slot 2:	CM-2BRI, ISDN S0, Unit 0			Slot 5:			
	CM-2BRI, ISDN S0, Unit 1			Slot 6:			
Slot 3:	CM-2BRI, ISDN S0, Unit 0			Slot 7:	FM-MOD-56K/32		
	CM-2BRI, ISDN S0, Unit 1				MODEM VPN ISDN CAPI		
WAN Partner							
IP	IPX	PPP	X.25	FR			
Configuration Management							
Monitoring and Debugging							
Exit							
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit							

- WAN Partner** Used for adding/deleting ISDN partners.
- IP** Based on the information you provided in the Licenses menu, this area lists the protocols/features that can be configured on your system. Initially (before you install your license), only the IP, MODEM, and ISDN menus are available.
- IPX**
- PPP**
- X.25** If an X.25 license is installed, the X.25 menu will be available.

- FR** If a Frame Relay license is installed this menu this menu can be used to configure Frame Relay connections on the BRICK.
- MODEM** Here you can edit the parameters for the installed modems.
- VPN** Support for Virtual Private Networking also requires a separate license to be installed.
- ISDN** The ISDN menu is used for the managing the Credits Based Accounting system on your BRICK.
- CAPI** The CAPI menu is used for managing access to the Remote CAPI subsystem on your BRICK.

CONFIGURATION MANAGEMENT

Used for managing the BRICK's configuration files. For example you can save/delete files locally on the BRICK or on a remote IP host using TFTP.

MONITORING AND DEBUGGING

The Monitoring and Debugging submenus are useful in detecting problems on your network and allow you to monitor the BRICK's ISDN and X.25 interfaces, TCP/IP traffic by interface or protocol, Modem status, and syslog messages.

Basic System Configuration

LICENSES →

The upper portion displays a status for each of the BRICK's subsystems based on the installed licenses listed in the lower portion. Various subsystems are required for different features to operate on the BRICK.

Available subsystems and possible statuses include:

Subsystem	BRIDGE	CAPI	FR	IP	IPX
	OSPF	STAC	TAF	X25	VPN

Status	builtin	valid	not_valid
--------	---------	-------	-----------

Until a license is installed the list is empty and only IP is available (builtin).

BIANCA/BRICK-XL2 Setup Tool [LICENSE]: Licenses		BinTec Communications AG brick	
Available Licenses:			
IP (builtin), OSPF (valid), CAPI (valid), BRIDGE (valid), X25 (valid), IPX (valid)			
Serialnumber	Mask	Key	State
101546	287	88PNUPZ	ok
ADD	DELETE	EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit			

Select **ADD** to enter a new license.

Select **DELETE** to remove a license that has been marked for deletion (using the spacebar).

Select **EXIT** to accept the entries and return to the main menu.

SYSTEM →

The System menu contains the BRICK's basic system settings. Some fields are required for the IP and PPP protocols, and others are optional variables that contain administrative information.

BIANCA/BRICK-XL2 Setup Tool [SYSTEM]: Change System Parameters	BinTec Communications AG brick
System Name	brick
Local PPP ID (default)	brick
Location	building 14, 3rd floor, room f
Contact	Joe Brick (joe@brick.com)
admin Login Password/SNMP Community	bintec
read Login Password/SNMP Community	public
write Login Password/SNMP Community	public
HTTP Server Password	bintec
Syslog output on serial console	no
Message level for the syslog table	debug
Maximum Number of Syslog Entries	20
External System Logging >	
SAVE	CANCEL
Enter string, max length = 34 chars	

System Name = Defines the BRICK's system name and is used by IP as the hostname. If the system name is not set, the BRICK displays a warning message to the screen when the admin user logs in.

Local PPP ID = This field is required by the PPP to identify your BRICK at connection time for IP partners configured for PAP or CHAP authentication.

Location = (optional) The physical location of your BRICK.

Contact = (optional) Person responsible for this system. This text string must contain a valid email address if the system administrator is to be contacted from the BRICK's HTTP status-page.

Login Password/SNMP Community = These three fields define the passwords required for the admin, read, and write users. User restrictions are shown in the table below.

Note: The admin user has complete access to the all configuration information, thus the admin password should be protected.

User	Restrictions			
	Execute shell commands	Read System Vars	Set RW Vars	Save Config Files
admin	System, IP, IPX, ISDN, X.25	✓	✓	✓
write	IP, IPX, ISDN, X.25	✓ ¹	✓ ²	—
read	IP, IPX, ISDN, X.25	✓ ¹	—	—

1. Excluding password and license variables.
2. Changes only saved to memory (lost upon reboot).

HTTP Server Password = Required for viewing the HTTP status pages of your BRICK. Change this password from its default value of *bintec*.

Syslog output on serial console = Specifies whether to display system messages to the console and may be useful when debugging. Allowing syslog output to the console is not recommended for normal operation since it may affect system performance.

Message level for the syslog table = The priority level for messages sent to the console. Only system messages with a priority higher than or equal to this value are displayed. Priority levels include:

Highest priority	emerg	Emergency Messages
	alert	Alert Messages
	crit	Critical Messages
	err	Error Messages
	warning	Warning Messages
	notice	Notice Messages
	info	Info Messages
Lowest priority	debug	Debug Messages

Maximum Number of Syslog Entries = This field defines the maximum number of messages to save, older messages are discarded. The date, text, and time messages were sent can be seen in the

MONITORING AND DEBUGGING

MESSAGES

menu.



The External System Logging menu contains a list of Log Hosts to send system and/or accounting messages to.

Note: Generally it's not a good idea to send messages to hosts accessible over dialup ISDN interfaces.



Select **ADD** to create a new log-Host.

Select **DELETE** to remove a host which has been marked for deletion.

Select **EXIT** to accept the list and return to the system menu.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[SYSTEM][LOGGING]: External System Logging		brick	
Log Host	Level	Facility	Type
santorini	debug	local0	both
naxos-pc	info	local2	system
saxos-pc	err	local3	system
ADD	DELETE	EXIT	

For each host the following parameters must be set.

LogHost = An IP address of a host to send messages to.

Level = Defines the level of messages to send to this host. See "Message level for the syslog table" (p. 35) for info on message levels.

Facility = The facility on the log host, messages should be sent to. For UNIX hosts, this facility (level 0 – 7) must be configured appropriately. For PCs, you will need a separate application such as *DIME Syslog*.

Type = Type of messages to send to host (system, accounting, or both).

Hardware Interfaces

The Setup Tool Main Menu lists the communications modules detected on your system and shows which slots they are installed in. Since your system's hardware setup may be different, this section describes the menus you'll find according to communications module.

The BRICK-XL2 supports the following modules:

- CM-100BT, Fast Ethernet
- CM-1BRI, ISDN S0
- CM-TR, Token Ring
- CM-2BRI, ISDN 2xS0
- CM-X.21, X.21
- CM-2XBRI, ISDN 2xS0
- FM-MOD-56K/8
- BIANCA/CM-PRI, ISDN S2M
- FM-STAC
- CM-2UPO, ISDN 2xUPO

Slot 1 : **CM-100BT, FAST ETHERNET** →

This menu contains settings for the BRICK's CM-100BT interface. The Setup Tool Main Menu lists the communications modules detected on your system and shows which slots they are installed in. Since your system's hardware setup may be different, this section describes the menus you'll find according to communications module.

The BRICK-XL2 supports the following modules:

- CM-100BT, Fast Ethernet
- CM-1BRI, ISDN S0
- CM-TR, Token Ring
- CM-2BRI, ISDN 2xS0
- CM-X.21, X.21
- CM-2XBRI, ISDN 2xS0
- FM-MOD-56K/8
- BIANCA/CM-PRI, ISDN S2M
- FM-STAC
- CM-2UPO, ISDN 2xUPO

IP-Configuration

local IP-Number = The IP address for the BRICK's LAN interface.

local Netmask = The netmask to use for this interface.

BIANCA/BRICK-XL2 Setup Tool [SLOT 1 ETHERNET]: Configure Ethernet Interface	BinTec Communications AG brick																			
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding-left: 20px;">IP-Configuration</td> <td></td> </tr> <tr> <td style="padding-left: 40px;">local IP-Number</td> <td>199.1.1.2</td> </tr> <tr> <td style="padding-left: 40px;">local Netmask</td> <td>255.255.255.0</td> </tr> <tr> <td style="padding-left: 40px;">Encapsulation</td> <td>Ethernet II</td> </tr> <tr> <td style="padding-left: 20px;">IPX-Configuration</td> <td></td> </tr> <tr> <td style="padding-left: 40px;">local IPX-NetNumber</td> <td>0</td> </tr> <tr> <td style="padding-left: 40px;">Encapsulation</td> <td>none</td> </tr> <tr> <td style="padding-left: 20px;">Bridging</td> <td>enabled</td> </tr> <tr> <td style="padding-left: 20px;">Advanced Settings ></td> <td></td> </tr> <tr> <td style="text-align: center; padding-top: 10px;">SAVE</td> <td style="text-align: right; padding-top: 10px;">CANCEL</td> </tr> </table>	IP-Configuration		local IP-Number	199.1.1.2	local Netmask	255.255.255.0	Encapsulation	Ethernet II	IPX-Configuration		local IPX-NetNumber	0	Encapsulation	none	Bridging	enabled	Advanced Settings >		SAVE	CANCEL
IP-Configuration																				
local IP-Number	199.1.1.2																			
local Netmask	255.255.255.0																			
Encapsulation	Ethernet II																			
IPX-Configuration																				
local IPX-NetNumber	0																			
Encapsulation	none																			
Bridging	enabled																			
Advanced Settings >																				
SAVE	CANCEL																			
Enter IP address (a.b.c.d or resolvable hostname)																				

Encapsulation = Defines the type of header applied to IP packets sent over this interface; either "Ethernet II" and "Ethernet SNAP" may be used.

IPX-Configuration

local IPX-NetNumber = Defines the IPX network number assigned to the LAN connected to this interface.

Encapsulation = Defines the type of header applied to IPX packets sent over this interface.

IPX Encapsulation	Supports			
	IP	IPX	X.25	Bridging
Ethernet II	●	●		
Ethernet SNAP	●	●		
Ethernet 802.2 LLC		●	●	●
Novell 802.3		●		

Bridging = Setting to "enabled" allows bridging packets to pass over this interface. Set to "disabled" to disable.

CM-100BT, FAST ETHERNET → ADVANCED SETTINGS →

BIANCA/BRICK-XL2 Setup Tool. [SLOT 1 ETHERNET][ADVANCED]: Advanced Settings		BinTec Communications AG brick	
RIP Send	RIP V2		
RIP Receive	RIP V2		
IP Accounting	on		
Proxy Arp	off		
Back Route Verify	off		
SAVE		CANCEL	
Use <Space> to select			

RIP Send = Specifies which types of Routing Information Protocol (RIP) packets to send on this interface. When version 2 RIP packets are used, the BRICK also sends the netmask of propagated IP addresses. This allows the BRICK to propagate RIP packets to networks that do not use the default netmask for their respective network class.

RIP Receive = Specifies which types of RIP packets to accept (or ignore) from this interface.

IP Accounting = Turns IP accounting on or off for this interface. When turned on, accounting information for each TCP, UDP, or ICMP session routed over this interface is recorded in the ipSessionTable. Once a session is closed, an accounting record is generated and stored in the syslog table. Accounting records can be seen in the Setup Tool

MONITORING AND DEBUGGING → MESSAGES menu.

Proxy Arp = Turns proxy ARP for this interface to on or off. When turned on, the BRICK will answer ARP requests received on this interface with its own hardware address if 1. an IP route for the requested address exists, 2. the destination interface is different from the interface the ARP request arrived on, and 3. Proxy ARP has been enabled-

for the destination interface (to enable Proxy ARP for WAN interfaces see the **WAN PARTNER** → **IP** → **ADVANCED SETTINGS** menu).

Back Route Verify = This option allows the BRICK to discard packets with a potentially fake source address and can protect the BRICK from many »Denial-of-service« type attacks.

When set to “on” the BRICK will discard packets arriving on this interface that would not be routed back over the same interface if their source and destination addresses were exchanged.

Each time a packet is discarded, a syslog message is generated.

```
INFO/INET: backward route verify failed from if <ifindex> prot <prot>
<source IP address> -> <dest. IP address>
```

CM-TR, TOKEN RING →

The CM-TR is an LAN module with DB9 and UTP ports for access to the token ring. This section describes the settings specific to the token ring module. All settings not mentioned here are covered in the section CM-BNCTP on page 37.

Ring Configuration = Sets the speed of the BRICK’s token ring interface for high (16Mbit/s) or low speed rings (4Mbit/s). Early Token Release is only supported for high speed rings.

Default setting: 16Mbit/s + Early Token Release.

IP Configuration

Encapsulation = Defines the type of header applied to IP packets sent over this interface.

Token Ring Encapsulation	Supports		
	IP	IPX	X.25
Token Ring 802.5 SNAP	●	●	
Token Ring 802.5 LLC		●	●

IPX Configuration

Encapsulation = Defines the type of header applied to IPX packets sent over this interface. The same encapsulations are supported as for IP.

Slot 2 : **CM-1BRI, ISDN S0** →

This menu contains settings for the ISDN CM-1BRI module. The fields used in this menu are the same as those used for all Basic Rate Interfaces, with slight differences.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[SLOT 2 ISDN BR]: Configure ISDN Basic Rate Interface		brick	
Result of autoconfiguration:		Euro ISDN, point to multipoint	
ISDN Switch Type		autodetect on bootup	
D-Channel		dialup	
B-Channel 1		dialup	
B-Channel 2		dialup	
Incoming Call Answering >			
Advanced Settings>			
SAVE		CANCEL	
Use <Space> to select			

Result of autoconfiguration = The status of ISDN autoconfiguration for this interface. The autodetection procedure runs until a successful detection or the switch type (see below) is set manually.

ISDN Switch Type = Defines the switch type your ISDN provider uses. In most cases “autodetect on bootup” will detect the proper switch type. If the switch type is set manually, the autodetection feature is disabled for this interface.

The following protocols are supported for dialup and leased lines.

ISDN Dialup Lines	ISDN Leased Lines
<ul style="list-style-type: none"> • Euro ISDN • 1TR6 • AT&T 5ESS Custom ISDN • ISDN 1 AT&T NI1, EWSD NI1 • National ISDN 1 Northern Telecom DMS100 • Japan NTT INS64 	<ul style="list-style-type: none"> • leased line B1 channel (64S) • leased line B1+B2 channel (64S2) • leased line D+B1+B2 channel (TS02) • leased line B1+B2 different end-points¹

1. This type of leased line is called »Digital 64S mit Doppelanschaltung« in Germany.

D-channel = Most sites should leave these settings to their default values. However, if you have arranged special ISDN services from your provider the D-channel can (and must) be set to operate as DTE or DCE for the local side of a leased line connection. Note that the remote side must be configured opposingly.

B-channel 1 = Most sites should leave these settings to their default values. These settings should only be changed for sites requiring special configurations (as noted in D-channel above).


B-channel 2 = How to use the second B-channel. See above.

SPID B-Channel 1+2 = Required for the AT&T protocols and sets the SPID (Service Profile Identifier) to use for both B-channels.

SPID B-channel 1 = Required for the National ISDN 1 Northern Telecom protocol and sets the SPID to use for the first B channel.

SPID B-channel 2 = Required for the National ISDN 1 Northern Telecom protocol and sets the SPID to use for the second B channel.

Incoming Call Answering B1 = Under the National ISDN 1 Northern Telecom protocol, incoming call answering procedures must be specified for each B-channel.

See the  menu on page 43.

Incoming Call Answering B2 = See above.

CM-1BRI, ISDN S0 →

INCOMING CALL ANSWERING →

The settings in this menu are used to distribute incoming ISDN calls received on this interface to different service items. The BRICK distinguishes incoming calls based on the “Called Party’s Address” transmitted in ISDN.

For example you might want an incoming call from a particular ISDN station to automatically receive the login service. However, you’ll probably want most calls to be given to the routing service.

By default all incoming calls are dispatched to the login service.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[SLOT 2 ISDN BRI][INCOMING]: Incoming Call Answering		brick	
Item	Number	Mode	Username
ISDN Login	993031	right to left	
PPP (routing)	993030	right to left	
ADD	DELETE	EXIT	

The incoming call answering is handled by the entries in this list. At first the list will be empty. Choose **ADD** to create a new entry or select an existing entry and press <Return> to edit it. You will then get a new screen, where you can specify the Item, Number and Mode settings.

Item = the ISDN service you want to use for this call. You can select one of the following:

Value	Meaning
PPP (routing)	Default value, good for all PPP connection types listed below (except for the specific PPP Modem Profile 2 ... 8 settings) if the calls are signalled correctly (as is the case in most of Europe).
ISDN Login	login service
PPP 64k	64kbps PPP data connection
PPP 56k	56kbps PPP data connection
PPP Modem	selects Modem Profile 1 as configured in the [MODEM] menu
PPP DOVB	<u>d</u> ata transmission <u>o</u> ver <u>v</u> oice <u>b</u> earer; useful e.g. in the US where voice calls sometimes cost less than data connections
PPP V.110 (1200 - 38400)	bit-rate adaption according to V.110 (1200 bps, 2400 bps, ..., 38400 bps)
PPP Modem Profile 1 ... 8	selects Modem Profile 1 ... 8 as configured in the [MODEM] menu
CAPI 1.1 EAZ0 ... 9 Mapping	EAZ mapping for CAPI 1.1 applications

Number = the telephone number to use for this item.

Mode = the direction for matching the incoming telephone number (Called Party Number), either starting from the right (*right to left*, this is the default), or from the left (*left to right* (DDI), only useful for the Direct Dial In (DDI) feature of point-to-point ISDN accesses.¹

Username = Allows your to define a CAPI user to map the incoming call to. If this field is not defined, the incoming call will be offered to all CAPI applications.

Bearer = Allows you to additionally define the type of Bearer capability ("data" or voice") that was signalled with the incoming call.

1. Called »Anlagenanschluß« in Germany

CM-1BRI, ISDN S0 → ADVANCED SETTINGS →

BIANCA/BRICK-XL2 Setup Tool [SLOT 2 ISDN BRI][Advanced]: Advanced Settings		BinTec Communications AG brick
ISDN S0 Power Supply Detection on		
X.31 TEI Value	specify	
Specify TEI Value	0	
X.31 TEI Service	Packet Switch	
SAVE		CANCEL
Use <Space> to select		

ISDN S0 Power Supply Detection = Normally this should be left on to detect whether power is being received over the S₀ interface.

X.31 TEI Value = This is an optional field for sites that need to customize the TEI (Terminal Endpoint Identifier) used for this interface. The TEI value can be verified by your ISDN provider. To enable X.31 select “specify” and then specify your TEI.

X.31 TEI Service = Most sites will leave this settings to “Packet Switch”. May also be set to “CAPI” or “CAPI Default”.

CM-2BRI, ISDN S0 →

The Main Menu lists the slot location for each CM-2BRI module detected on the system. The CM-2BRI supports two Basic Rate Interfaces (i.e., 4 B-channels).

For each CM-2BRI, separate menu entries are present for each BRI (Unit 0 and Unit 1). Each BRI must be configured separately. See the section CM-1BRI on page 41 to configure each unit of your CM-2BRI module.

CM-2XBRI, ISDN S0 →

The CM-2XBRI supports two Basic Rate Interfaces (i.e., 4 B-channels) and has either two or four 33.6K fax/modems mounted on separate daughter cards.

for the CM-2XBRI module, separate menu entries are present for each BRI interface. Each ISDN stack must be configured separately. See the section CM-1BRI on page 41 to configure each unit of your CM-2XBRI module. The [MODEM] menu can be used to configure “profile” settings for incoming modem connections.

CM-2UP0, ISDN UPO →

With the exception of the “Power Supply Detection” option, the configuration menu for the CM-2UP0 module is identical to the Basic Rate Interface settings described on page 41.

Slot 3: **CM-PRI, ISDN S2M** →

BIANCA/BRICK-XL2 Setup Tool [SLOT 3 ISDN PRI]: Configure S2M Interface		BinTec Communications AG brick
Result of autoconfiguration: autoconfiguration disabled		
ISDN Switch Type	leased line B1..B30	
ISDN Line Framing	standard (CRC4)	
Incoming Call Answering >		
SAVE	CANCEL	
Use <Space> to select		

Result of autoconfiguration = Displays the results of autodetection for this interface. Autodetection runs until a successful detection or the switch type is set manually.

ISDN Switch Type = Sets the switch type, dialup or leased for this PRI. In most cases “autodetect on bootup” will detect the correct type, but may be configured manually. The following types are supported:

ISDN Dialup Lines	ISDN Leased Lines
<ul style="list-style-type: none"> • Euro ISDN S2M user profile (TE) • Euro ISDN S2M user profile (NT) • 1TR6 S2M user profile (TE) • 1TR6 S2M user profile (NT) 	<ul style="list-style-type: none"> • leased line B1..B30 • leased line, 1 Hyperchannel • leased line, chann. E1, 31 diff. endpoints¹ • back to back

1. This type of leased line is called »aggregated kilostream« in the UK.

ISDN Line Framing = Mosts sites will use the default “standard (CRC4)”. Some sites in Sweden and France connected to PBXs may require special framing.

CM-PRI, ISDN S2M → **INCOMING CALL ANSWERING** →

This menu is the same for all ISDN interfaces, see Incoming Call Answering on page. 43.

Slot 4 : **CM-X21, X.21** →

This menu contains the settings for the CM-X21 communications module.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[SLOT 4 X.21]: Configure X.21 Interface		brick	
Layer 1 Mode	dce		
Speed	2048 kbit/s		
Layer 2 Mode	auto		
	SAVE		CANCEL
Use <Space> to select			

Layer 1 Mode = The mode the BRICK operates in for Layer 1 (dte or dce). Select DTE (Data Terminal Equipment) if the BRICK is connected to a public data network (such as Datex-P in Germany). DCE (Data Circuit-Terminating Equipment) is used if the BRICK is operating as the network provider (always required by one side of a private X.25 data network).

Speed = If the BRICK is set to operate as DCE, for Layer 1, the speed for the link must also be specified here. Link speed is scalable from 2400 bits/second up to 2048 Kbits/second.

Layer 2 Mode = The mode the BRICK operates in for Layer 2 (dte, dce, or auto) For X.21 leased lines one side of the link must be configured as dte, the other dce. Sites accessing public data networks can leave this field set to auto.

Partner Management

WAN PARTNER →

This menu lists all ISDN partners currently configured on your system. The list displays each partner's name, the protocol used, and the current state, i.e. active (connected) or dormant (disconnected).

BIANCA/BRICK-XL2 Setup Tool [WAN]: WAN Partners		BinTec Communications AG brick
Current WAN Partner Configuration		
Partnername	Protocol	State
partnerbrick1	ppp	up
2	ppp	dormant
partnerbrick3	ppp	up
partnerbrick4	ppp	dormant
ADD	DELETE	EXIT
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit		

To edit an existing partner from the list, first highlight the partner, then enter <Return>.

Select **ADD** to create a new ISDN partner interface.

Select **DELETE** to remove a partner interface that has been marked for deletion (Using the spacebar).

Select **EXIT** to accept the partner list and return to the main menu.



This menu is where you add (or change) ISDN partner configurations. If you are editing an existing partner, the current settings are displayed. If you're adding a new ISDN partner, the default values for a dialup IP partner are shown.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[WAN][ADD]: Configure WAN Partner		brick	
Partner Name	test-partner		
Encapsulation	PPP		
Compression	none		
Encryption	none		
Calling Line Identification	no		
WAN Numbers >			
PPP >			
Advanced Settings >			
IP >			
IPX >			
BRIDGE >			
	SAVE	CANCEL	
Enter string, max length = 25 chars			

Partner Name = Enter a unique name to identify your partner. If the ISDN partner is a BIANCA/BRICK, this should be set to the BRICK's hostname.

Encapsulation = Defines the type of encapsulation to use over this link. The table shown below displays the different encapsulations and the link compression/encryption options which may be used.

Also note that encapsulations using STAC compression are only available if STAC is licensed on your BRICK or an FM-STAC module has been installed.

WAN Partner Link Encapsulation

Protocol			Encapsulation ¹	Compression			Encryption		
				STAC	V.42bis	MPPC ²	MPPE40	MPPE128 ³	
IP	IPX	Bridge	PPP	✓		✓	✓	✓	
			Async PPP over X.75	✓		✓	✓	✓	
			Async PPP over X.75/T.70/BTX	✓		✓	✓	✓	
			Multi-Protocol LAPB Framing		✓				
			Multi-Protocol HDLC Framing						
			Frame Relay						
				HDLC Framing (only IP)					
				LAPB Framing (only IP)		✓			
		X.25	X.25_PPP	✓		✓	✓	✓	
			X.25						
			X.25 PAD						
			X.25 No Configuration						
			X.25 No Signalling						
			X.25 No Configuration, No Signalling						
	X31 B-Channel								

1. The X.25 encapsulations can only be used in connection with a valid X.25 license.
2. The MPPC compression can only be used with an FM-STAC module (BRICK-XM, BRICK-XL2) installed.
3. If you use MPPE128 encryption be sure that your partner also supports MPPE128 encryption. Otherwise you will be disconnected.

Compression = Determines the type of compression to attempt to use (negotiate) with this partner. MPPC, STAC, V42bis, and MS-STAC are currently supported.

Encryption = Determines the type (if any) of encryption to use with this partner. MPPE compression using 40 bit or 128 bit keys are supported.

Calling Line Identification = This determines whether calls from this partner must be identified using the Calling Party's Number in ISDN. This field is set automatically depending on the type of ISDN number (either "incoming (CLID)" or "both (CLID)") that is configured in the WAN Numbers submenu.



This menu lists the telephone or modem numbers this WAN partner can be reached at. If you're configuring a new partner the list is empty.


BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[WAN][ADD][WAN NUMBERS]: WAN Numbers ()		brick	
WAN Numbers for this partner:			
WAN Number		Direction	
9302		incoming	
ADD	DELETE	EXIT	

Select **ADD** to add a new WAN number. In the subsequent dialogue, enter a WAN number (e.g. ISDN telephone number, analog modem number) this partner can be reached at.

In the WAN Number field, you may use wildcards to define entries that match multiple numbers. Note, however, that the wildcards are used differently for incoming and outgoing calls.

Wildcard	Example	Outgoing Calls	Incoming Calls
*	1234*	is ignored, e.g 1234	matches zero or any string, e.g 1234 or 123467
?	1234?	is replaced by 0, e.g. 12340	matches any single digit, e.g. 12349, 12347

Wildcard	Example	Outgoing Calls	Incoming Calls
[a-b]	123[5-9]	first digit in the range, e.g. 1235	denotes the range of possible digits to match, e.g. 12345, 12346
[^a-b]	123[^0-5]	range of digits not allowed, first possible digit inserted, e.g. 1236	denotes the range of excluded digits to match, e.g. 12346, 12347
{ab}	{00}1234	inserted for outgoing calls, e.g. 001234	optional string to match, e.g. 001234, 1234

Note:  If the Calling Party's Number from the incoming call matches a WAN Number entry with wildcards and an entry without wildcards, the entry without wildcards is always used.

Direction = Here you can specify whether the ISDN number(s) should be used for outgoing calls, incoming calls, or both.

ISDN Ports to use = If multiple ISDN stacks are available on your system this field can be used to select which ISDN interfaces may be used to establish connections with this partner. The list only displays the ISDN D-channel stacks that are currently available.

Select **DELETE** to remove an entry that has been tagged (using the spacebar) for deletion.

Select **EXIT** to accept the list of WAN number(s) and return to the previous menu.

To change an existing number, highlight the entry and enter <Return>.



The Advanced Settings submenu currently contains the Closed User Group option for this ISDN number. You must be receiving this service from your ISDN provider to utilize this option.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[WAN][ADD][WAN NUMBERS][ADVANCED]: Advanced Settings ()		brick	
Closed User Group		none	
OK		CANCEL	

Closed User Group = To specify a particular Closed User Group select "specify" using the spacebar and enter an integer between 1 and 9999 in the additional field. By default "none" is defined here.

Select **OK** to accept the number for the Closed User Group and return to the previous menu.

Select **CANCEL** to discard any changes made here and return to the previous menu.



This menu is only available if a PPP compatible encapsulation is being used for this partner. This menu contains Partner-specific PPP settings for this partner.

BIANCA/BRICK-XL2 Setup Tool [WAN][ADD][PPP]: PPP settings ()	BinTec Communications AG brick														
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; padding: 5px;">Authentication</td> <td style="width: 50%; padding: 5px;">CHAP + PAP</td> </tr> <tr> <td style="padding: 5px;">Partner PPP ID</td> <td style="padding: 5px;">none</td> </tr> <tr> <td style="padding: 5px;">Local PPP ID</td> <td style="padding: 5px;">brick</td> </tr> <tr> <td style="padding: 5px;">PPP Password</td> <td style="padding: 5px;">none</td> </tr> <tr> <td style="padding: 5px;">Keepalives</td> <td style="padding: 5px;">off</td> </tr> <tr> <td style="padding: 5px;">Link Quality Monitoring</td> <td style="padding: 5px;">off</td> </tr> <tr> <td style="padding: 20px 5px 5px 5px;">OK</td> <td style="padding: 20px 5px 5px 5px;">CANCEL</td> </tr> </table>		Authentication	CHAP + PAP	Partner PPP ID	none	Local PPP ID	brick	PPP Password	none	Keepalives	off	Link Quality Monitoring	off	OK	CANCEL
Authentication	CHAP + PAP														
Partner PPP ID	none														
Local PPP ID	brick														
PPP Password	none														
Keepalives	off														
Link Quality Monitoring	off														
OK	CANCEL														
Use <Space> to select															

Authentication = Specifies the authentication protocol(s) to use when authenticating this partner at connect time. If Calling Line IDentification is not being used, at least one authentication mechanism must be used. You can choose from the following protocols/combinations:

WAN Partner PPP Authentications	CHAP
	PAP
	CHAP + PAP
	CHAP + PAP + MS-CHAP
	MS-CHAP
	none
	LAPB Framing (only IP)
	LAPB Framing (only IP) + Compression

Partner PPP ID = This is the caller's PPP ID. The remote side must identify itself using this ID at connection time.

Local PPP ID = The PPP ID your BRICK should use for this partner. When creating a new partner the Local PPP ID from the **SYSTEM** is displayed here as a default setting. Be careful of leading/trailing blank spaces here, they will be written to the *biboPPPTable* entry.

PPP Password = The password this partner uses at connection time.

Keep Alives = When this option is set the BRICK sends LCP echo requests to the remote partner every three seconds. After five unanswered requests the PPP interface's *ifOperStatus* is set to "down". PPP keep alives is most useful (and by default, set to "on") for leased line interfaces. The transmission of echo requests does not affect the Short Hold timer.

Link Quality Monitoring = This option allows you to tell the BRICK to gather PPP Link Quality statistics for a specific PPP partner. When enabled, link statistics are continuously written to the BRICK's *biboPP-PLQMTable* (viewable from the SNMP shell), when a connection is established with this partner.



This menu is used to enable special features for the respective partner.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG
[WAN][ADD][ADVANCED]: Advanced Partner Settings ()		brick
Callback	no	
Static Short Hold	20	
Idle for Dynamic Short Hold (%)	0	
Delay after Connection Failure	300	
Channel-Bundeling	dynamic	
Total Number of Channels	2	
Layer 1 Protocol	ISDN 64 kbps	
Provider Configuration >		
OK		CANCEL
Use <Space> to select		

Callback = Your BRICK supports a number of different callback options.

Setup Tool	SNMP Shell	Explanation
no	disabled	no Callback possible
expected (awaiting callback)	expected	wait for a call back from a partner
yes	enabled	accept callback requests and call back immediately
yes (delayed)	delayed	accept callback requests and call back after <i>RetryTime</i> seconds ¹
yes (PPP negotiation)	ppp_offered	accept callback requests and negotiate the callback number inband

- Note that delayed callback currently only works for calls identified out-band by their CLID.
The *biboPPPRetryTime* can be configured from the SNMP shell.

Static Short Hold = Defines the number of seconds to wait before closing all data channels to this partner once the line becomes silent.

Note: Using CLID (see Identify by Calling Number in the previous menu) avoids incurring charges for the initial call, but is a less secure means of authentication when used without PAP and or CHAP.



Idle for Dynamic Short Hold (%) = Sets the idle timer to the given percentage of the last charging interval. As soon as the charging interval lengths change—e.g. when switching from daytime to nighttime tariff—the idle timer changes accordingly (see “How do I configure Dynamic Short Hold?” on page 123).



To be able to use Dynamic Short Hold you must be receiving the AOCD (advice of charge during the call¹) service from your provider.

Delay after Connection Failure = The number of seconds to wait before allowing new connections with this partner after a connection failure. Upon failures the interface is blocked for this many seconds.

Channel-Bundeling = The type of channel-bundeling to use for this partner. The number of channels (N in the table below) is defined by the next field “Total Number of Channels”.

Type	Open extra channels based on throughput	Channels to open initially	Max # of channels
static	No	N	N
dynamic	Yes	1	N
no	No	1	1

“static” means always keep N channels open for connections to this partner. When a connection is established with this partner, N channels are opened, and remain open until the link is closed.

“dynamic” means monitor throughput, and open additional ISDN channels to this partner only when needed. Initially, 1 ISDN B-channel is opened.

1. Called »Übermittlung der Tarifeinheiten während der Verbindung« in Germany

Total Number of Channels = Defines the max # of channels to have open with this partner. If static channel-bundeling is being used, this also defines the # of channels to open at connection time.

Layer 1 Protocol = This entry only has an effect on outgoing calls to this partner and on incoming calls which are identified by their calling party number. For an outgoing modem connection you should select one of the eight modem profiles.

The Layer 1 Protocol for incoming calls *not* identified by their calling party number—which will probably be the case for most incoming modem connections, as they usually originate from the analogue telephone network, where no calling party numbers are supplied with the calls—is taken from the **INCOMING CALL ANSWERING** settings.

The following table shows the possible values for the *Layer 1 Protocol* entry.



Note that most entries correspond to similar entries in the *Item* field of the menu explained On the BRICK-XL index numbers are broken down as follows: on page 43.

Value	Meaning
ISDN 64kbps	64kbps ISDN data connection
Modem	selects Modem Profile 1 as configured in the [MODEM] menu
V.110 (1200 - 38400)	bit-rate adaptation according to V.110 (1200 bps, 2400 bps, ..., 38400 bps)
Modem Profile 1 ... 8	selects Modem Profile 1 ... 8 as configured in the [MODEM] menu

To change an existing WAN number, highlight the entry and then enter <Return>.



You can use this menu to configure dialup IP connections to CompuServe Online Services and is only available after selecting the “Async PPP over X.75” or “Async PPP over /T.70/BTX” encapsulation in the main WAN Partner menu.

The user access information provided in this menu is used to generate *biboPPPLinString* used at connection time.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[WAN][EDIT][ADVANCED][PROVIDER]: Provider Configuration(cis)		brick	
Provider	CompuServe Network		
Host	CIS		
User ID	12345,6789		
Password	secret		
OK		CANCEL	
Use <Space> to select			

Provider = Defines the type of access to CompuServe and may be one of the following:

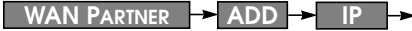
Online Provider	Encapsulation in WAN Partner menu
not defined	(default value, i.e. do not use this option)
CompuServe via T-Online	async PPP over X.75/T.70NL/T-Online ²
CompuServe Corporate Network	async PPP over X.75 ¹
	async PPP over X.75/T.70NL/T-Online ²
CompuServe Network	async PPP over X.75 ¹

1. For direct access.
2. For indirect access via the T-Online gateway.

Host = The CompuServe hostname to dial into.

User ID = The CompuServe Member ID to use for the connection.

Password = The password to use for the User ID specified above.



Use this menu to set this partner's IP address and netmask.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG
[WAN][ADD][IP]: IP Configuration ()		brick
IP Transit Network		yes
local ISDN IP Address		10.0.0.1
Partner's ISDN IP Address		10.0.0.2
Partner's LAN IP Address		192.168.55.0
Partner's LAN Netmask		255.255.255.0
Advanced Settings >		
	SAVE	CANCEL
Use <Space> to select		

Transit Network = Specifies whether to use a transit network between the BRICK and this partner's LAN. Most sites will not require a transit network and can leave this set to "no".

If you use a transit net ("yes"), you'll also have to set the ISDN IP addresses for both sides of the connection.

Assigning "dynamic-client" means that the BRICK will receive its IP address from this partner at connection time.

Assigning "dynamic-server" means that the BRICK will assign this remote partner an IP address at connection time.

local ISDN IP Address = The BRICK's IP address on the transit network (on if you said "yes" to using a transit network).

Partner's ISDN IP Address = The partner's IP address on the transit network (on if you said "yes" to using a transit network).

Partner's LAN IP Address = The partner's IP on the remote LAN. (Not required if dynamic-client/server is set in IP Transit Network).

Partner's LAN Netmask = The netmask to use for the remote LAN. If left blank, a standard netmask for the respective network class is used. (Not required if dynamic-client/server is set in IP Transit Network).



This menu is used to enable special features for the respective partner.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG
[WAN][ADD][IP][ADVANCED]: Advanced Settings ()		brick
RIP Send	none	
RIP Receive	none	
Van Jacobson Header Compression	off	
Dynamic Name Server Negotiation	yes	
IP Accounting	off	
Back Route Verify	off	
Route Announce	up or dormant	
Proxy ARP	off	
OK		CANCEL
Use <Space> to select		

RIP Send = Which types of RIP packets to send to this partner. If RIPv2 packets are sent, the BRICK also sends the netmask of the propagated IP address, which allows the BRICK to propagate RIP packets to networks that do not use the default netmask for their respective network class.

RIP Receive = Which types of RIP packets (see above) to accept (or ignore) from this partner.

Van Jacobson Header Compression = If turned "on" the TCP/IP packet headers are compressed according to RFC 1144, resulting in a better data-to-overhead-ratio, especially when using smaller packet sizes.

Dynamic Name Server Negotiation = This option controls how (and if) the BRICK negotiates IP addresses for the primary/secondary Domain Name and WINS servers. The respective DNS and WINS IP addresses defined in the **IP** → **STATIC SETTINGS** menu are negotiated as follows:

Value	With respect to DNS/WINS Addresses, the BRICK:
off	does not offer or accept WINS/DNS server IP addresses.
yes	offers the currently configured WINS and DNS addresses.
client (receive)	requests the WINS/DNS server addresses.
server (send)	if requested, provides the WINS/DNS server addresses .

IP Accounting = If IP Accounting is turned “on” accounting messages will be stored for each TCP, UDP, or ICMP session routed between this partner.

See the section on the **MONITORING AND DEBUGGING** → **MESSAGES** menu for information on the format of accounting messages.

Back Route Verify = This option allows the BRICK to discard packets with a potentially fake source address and can protect the BRICK from many »Denial-of-service«-type attacks.

When set to “on” the BRICK will discard packets arriving on this interface that would not be routed back over the same interface if their source and destination addresses were exchanged.

Each time a packet is discarded, a syslog message is generated.

```
INFO/INET: backward route verify failed from if <ifindex> prot <prot>
<source IP address> -> <dest. IP address>
```



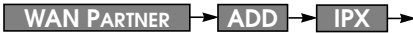
Please note that in cases where packets should take an asymmetric path—i.e. be received via one interface, but transmitted via a different interface—you have to switch *Back Route Verify* **off**, otherwise these packets are also discarded.

Route Announcement = This option allows you to control when IP routes defined for this interface will be propagated. This is dependent upon the interface’s *ifOperStatus* (in the *ifTable*) as follows:

Value	Routes are propagated:
“up only”	only when the operational status of the interface is up.
“up or dormant”	when the operational status of the interface is up or dormant.

Value	Routes are propagated:
"always"	always, regardless of the current link's operational status.

Proxy ARP = Proxy ARP (Address Resolution Protocol) for WAN links is disabled, or "off" by default. When enabled ("up only" or "up or dormant") requests are answered in dependence of the *ifOperStatus* of the link.



This menu is available if the IPX protocol is enabled for this WAN partner.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[WAN][ADD][IPX]: IPX Configuration ()		brick	
Enable IPX	yes		
IPX NetNumber	0		
Send RIP/SAP Updates triggered + piggyback(on changes, per. if link active)			
Update Time	60		
Age Multiplier	4		
OK		CANCEL	
Enter integer value			

Enable IPX = When IPX is enabled for this partner, the following fields can be configured as described.

IPX NetNumber = This is the IPX network number of the WAN link and is required by some IPX routers.

Send RIP/SAP Updates = Determines how often RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) packets are sent to this remote partner.

In IPX networks, RIP and SAP packets are broadcast to adjacent networks to inform them of current routes and services. The traffic

generated by RIP and SAP is okay for LANs but for adjacent networks connected over WAN interfaces, consideration must be made.

The following table shows the types of updates that can be configured for IPX partners.

	Open new link?	Send changes?	Send Periodic updates?	Drawback
timed update	always	yes	yes	May lead to higher ISDN costs.
piggyback	never	yes	yes	At least 1 static route/service must be configured for partner
triggered + piggyback	only for changes	yes	yes	default setting (sufficient in most cases)
triggered	only for changes	yes	no	Less traffic but is less reliable than triggered + piggyback.
passive triggered	never	yes	no	At least 1 static route/service must be configured for partner
off	never	no	no	All routes/services must be configured statically.

Update Time = Determines how often periodic updates are sent.

Age Multiplier = Used only for aging of existing routes/services.

Routes and services not updated within

<update time> x <age Multiplier> seconds are removed.

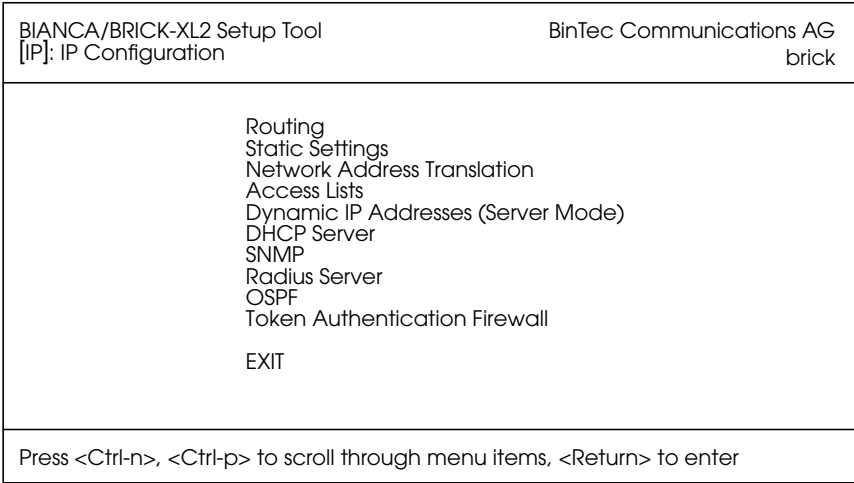


Enable Bridging = To enable bridging with this PPP partner set this field to "yes".

Configuring Protocols

IP →

The IP menu consists of several submenus which contain global settings for the IP and some special IP-related features. Most of the menus contain optional settings, specific to a particular feature.



ROUTING contains the BRICK's IP routing table.

STATIC SETTINGS contains some required parameters such as the BRICK's domain name, as well as IP addresses for optional servers.

Network Address Translation is used to configure different interfaces for Network Address Translation.

ACCESS LISTS is used to configure different access lists which can be used to control access to/from hosts on the connected networks.

DYNAMIC IP ADDRESSES is used to manage the pool of IP addresses the BRICK uses when operating as an IP address server.

DHCP SERVER contains resources the BRICK will use when acting as a Dynamic Host Configuration Protocol server.

SNMP contains basic settings required for the SNMP.

RADIUS SERVER is used to configure one or more RADIUS servers for your BRICK..

OSPF contains settings required for the OSPF routing protocol. For a description of these menus please refer to the *BIANCA/BRICK Extended Features Reference* (included on the Companion CD).

TOKEN AUTHENTICATION FIREWALL is used to configure interfaces for use with Token Authentication Firewall services, or TAF. TAF is separately licensed on the BRICK; for a detailed description of these menus please refer to the *Extended Features Reference* (contained on the Companion CD) for details on configuring/using TAF with the BRICK.

IP → **ROUTING** →

This menu displays the current IP routing table. From this menu you can edit existing IP routes or add new ones. Note that IP routes learned through the RIP can't be changed, only deleted.

For the most part, the columns are self explanatory:

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG			
[[IP]][ROUTING]: IP Routing		brick			
<p>The flags are: U (Up), D (Dormant), B (Blocked), G (Gateway Route), I (Interface Route), S (Subnet Route), H (Host Route)</p>					
Destination	Gateway	Mask	Flags	Met.	Interf./Partner
199.1.1.0	199.1.1.2	255.255.255.0	US	0	en1 loc
ADD		DELETE		EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit					

To add a new IP route select **ADD**.

To edit an existing route, highlight the entry and enter <Return>.

To remove one or more IP routes, mark the entries for deletion using the spacebar, then select **DELETE**.

Select **EXIT** to accept the entries and return to the **IP** menu. Note that the changed routing table becomes effective immediately.



Use this menu to add (or make changes) to the IP routing table.

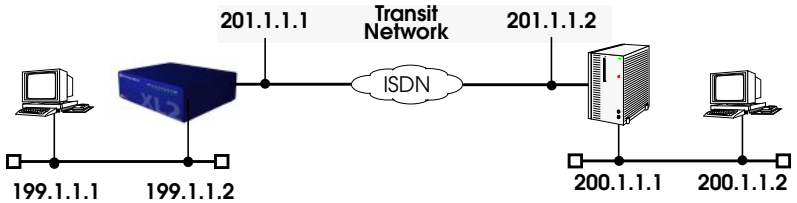
BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[IP][ROUTING][ADD]: Add or Change IP Route		brick	
Route Type	Host route		
Network	WAN without transit network		
Destination IP-Address	200.1.1.2		
Partner / Interface	partnerbrick		
Metric	1		
SAVE		CANCEL	
Use <Space> to select			

Route Type = The type of IP route you're adding, i.e. a route to a single host or network. If a default route is specified it will only be used when no other matching routes are found.

Network = Use LAN for hosts (or nets) directly attached to the BRICK. For routes that use WAN interfaces, specify whether the route includes transfer network. If "discard" is used the BRICK disregards all packets matching this route.

Transit Networks = Some sites may require an intermediate transit network (mainly sites using routing equipment from different manu-

facturers). As shown below, each host on the transit network is accessible via two different addresses.



Destination IP-Address

= IP address of the remote host or network. If this route uses a WAN link with a transfer network, enter the IP address of the ISDN side of the partner's router. See diagram above.

Netmask = Only for network-routes. If left blank, a standard netmask for the appropriate network class will be used.

Partner / Interface = For routes using a WAN link without a transfer network, scroll through the list of WAN partners using the spacebar.

Gateway IP-Address = The host the BRICK should forward packets to for this route, often called the "Next-Hop".

Metric = The metric value for this route. Metric values with a lower priority have precedence.



Use the Static Settings to configure basic IP settings on the BRICK.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[IP][STATIC]: IP Static Settings		brick	
Domain Name		bricks.com	
Primary Domain Name Server		199.1.1.99	
Secondary Domain Name Server			
Primary WINS			
Secondary WINS			
Time Protocol		TIME/UDP	
Time Offset (seconds)		0	
Time Update Interval (seconds)		86400	
Time Server		199.1.1.99	
Remote CAPI Server TCP port		2662	
Remote TRACE Server TCP port		7000	
RIP UDP port		520	
BOOTP Relay Server			
Unique Source IP Address			
HTTP TCP port		80	
SAVE		CANCEL	
Enter string, max length = 35 chars			

Domain Name = Sets the BRICK's IP domain name.

Primary Domain Name Server = The IP address of the BRICK's domain name server.

Secondary Domain Name Server = An alternate name server.

Primary WINS Server = The IP address of the primary WINS (or NBNS NetBios Name Server).

Secondary WINS Server = The address for an alternate WINS server.

Note: See page 62 for information on automatic WINS/DNS address negotiation.

Time Protocol = The protocol to use to retrieve current time. The following protocols are possible. Since the BRICK-XL has an internal

real-time clock this field is optional. If a timeserver is configured, the time provided by the server overrides the internal clock.

Protocol	Explanation
time_udp	Time Service (RFC 868) via UDP
time_tcp	Time Service (RFC 868) via TCP
time_sntp	SNTP (Simple Network Time Protocol, RFC 1769) via UDP
isdn	ISDN D-Channel (stack 0 only)
none	Disable time retrieval altogether

Time Offset (seconds) = The time in seconds to add/subtract to the retrieved time. Values between -24 and +24 are assumed to be hours and are appropriately converted to seconds. Note that when time is retrieved from ISDN the offset must be set to zero.

Time Update Interval (seconds) = The interval in seconds at which current time should be updated/retrieved. Similar to Time Offset values between 1 and 24 are assumed to be hours and converted to seconds. For Protocol=time_udp, time_tcp, or time_sntp new requests are sent every *Time Update Interval* seconds. When isdn is used the current time will be retrieved from the next ISDN connection established after *Time Update Interval* seconds.

Time Server = The IP address of the BRICK's timeserver.

Remote CAPI Server TCP port = The port number to use for CAPI connections. Default value: 2662

Remote TRACE Server TCP port = The port number the BRICK uses for TRACE requests. Default value: 7000

RIP UDP port = The port number used on the BRICK for RIP. Default setting is 520. RIP can be disabled by assigning port 0.

BOOTP Relay Server = The BOOTP server's IP address. If configured the BRICK will relay all BOOTP requests received on any LAN interface to the server. BOOTP responses received from the server are returned to the requesting client.

Unique Source IP Address = This is not the BRICK's IP address. The BRICK normally uses the IP address of the first LAN interface as the source address in IP frames. If this is not desired, this field defines the IP address that will always be used instead.

HTTP port = The port number used on the BRICK for HTTP requests. By default TCP port number 80 is used. Access to the BRICK's status-page can be disabled by assigning port number 0 here.

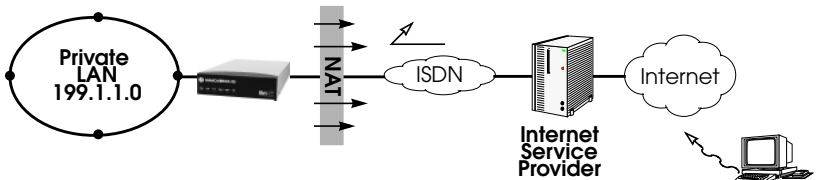
IP → **Network Address Translation** →

This menu lists all IP interfaces that may be configured for NAT. The BRICK supports both **Forward** and **Reverse** NAT.

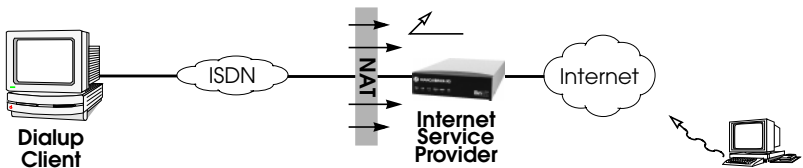
BIANCA/BRICK-XL2 Setup Tool [IP][NAT]: NAT Configuration	BinTec Communications AG brick
Select IP Interface to be configured for NAT en1 partnerbrick1 partnerbrick2 partnerbrick3 partnerbrick4 EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select	

To configure an interface highlight it and enter <Return>.

Forward NAT means, allow all traffic destined (moving-forward) on this interface. Arriving traffic is only accepted if explicitly allowed¹.



Reverse NAT means, allow all traffic arriving on this interface. Traffic destined for this interface is only accepted if explicitly allowed¹.



1. Or the traffic is return data from a session initiated internally.



The NAT Configuration menu lists session profiles that define which sessions are allowed over this NAT interface. From this menu you can add, change, or delete session profiles.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[IP][NAT][CONFIG]: NAT Configuration (en1)		brick	
Network Address Translation off			
Configuration for sessions requested from outside			
Service	Destination	Source Dep.	Dest. Dep. Port Remap
ADD	DELETE	SAVE	CANCEL
Use <Space> to select			

Network Address Translation = The type of NAT to perform for this interface: “on” for forward NAT, “reverse” for reverse NAT, and “off” to disable NAT completely.


To edit an existing session, highlight the entry and enter <Return>.

To configure a new session profile for this interface select **ADD**.

To delete a session, mark the entry for deletion using the spacebar, then select **DELETE**.

Select **SAVE** to accept the session list and return to the previous menu.

Select **CANCEL** to discard all changes made since the last SAVE and return to the previous menu.

Note:  Once saved, any changes made here become effective immediately. Be aware of this when configuring NAT from a remote site.



This menu is used to add or change session profiles for a NAT interface. Sessions configured here define the types of IP session(s), that are explicitly allowed over this NAT interface. The session profile configured here applies to a specific host.

BIANCA/BRICK-XL2 Setup Tool [IP][NAT][CONFIG][ADD]: Edit NAT Configuration (en1)		BinTec Communications AG brick
Service Protocol Port (-1 for any)	user defined icmp -1	
Destination		
	SAVE	CANCEL
Use <Space> to select		

Service = The service to allow on the internal host. Several services are already defined. To define other services, set to “user-defined” and set the Protocol and Port fields appropriately.

Protocol = The protocol to allow for user-defined services.

Port = The port number to allow. Use “-1” to allow all ports for the specified protocol. If a specific port is set, it must match the port number used by the internal host.

Destination = IP address of the internal host to allow connections to. Leaving this field empty identifies the BRICK as the destination host.

Select **SAVE** to accept the session profile and return to the previous menu.

Select **CANCEL** to abort the entries made so far and return to the previous menu.



Access Lists on the BRICK are based upon a concept of Rules, Filters, and so-called Chains. This menu displays three submenus where IP Access Lists are configured.

BIANCA/BRICK-XL2 Setup Tool [IP][ACCESS]: IP Access Lists	BinTec Communications AG brick
Filters Rules Interfaces EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select	

The **FILTERS** menu is used to configure filters. Each filter describes a subset of IP traffic and may be address, protocol, source or destination port based.

The **RULES** menu is used to configure rules. Rules can be ordered, or “chained” to control the order in which the filters are applied.

The **INTERFACES** menu is used to define which rule is used first for traffic arriving on that interface.

Access List Methodology

An Access Filter simply describes a subset of IP traffic and may be based upon one or more of the following attributes.

- Source and/or Destination IP address.
- Source and/or Destination Port.
- Source and/or Destination Protocol.
- A current TCP Connection State.

An Access Rule defines an:

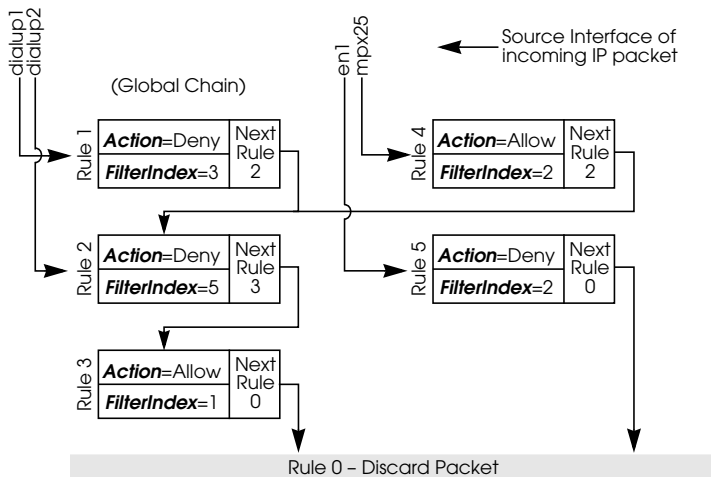
1. Access Filter to compare the packet to.
2. Action to take if a packet matches/doesn't-match a filter.
3. Index of the next rule to use if no action was taken.

Each Rule references a NextRule allowing different *Chains* (sequence of Rules) to be defined. For each interface a separate starting rule must be defined (via the *ipExtIfRuleIndex* field) that determines which Rule chain is applied. Rule 1 has special meaning; it is used by default for all newly created interfaces.

Rules are applied until one of the following events occur:

- The packet matches and the **Action** is “match” based OR the packet doesn't match and the **Action** is “if_not” based.
- The packet is discarded if the end of the chain or Rule 0 is reached.

In the diagram below, packets arriving via the “dialup1” interface are compared to Rules 1–2–3 while packets arriving on the “mpx25” are applied to Rules 4–2–3.





This menu lists the currently configured IP Access Filters and shows the Index number, Description, and Conditions for each filter. In the Conditions column abbreviations (explained in the menu) are used to describe the type of filter (i.e., address or port based filter).

To add a new filter select **ADD**. The menu shown below will be displayed.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG
[IP][ACCESS][FILTER][ADD]: Configure IP Access Filter		brick
Description	no http	
Index	4	
Protocol	tcp	
Connection State	established	
Source Address	192.168.50.5	
Source Mask	255.255.255.0	
Source Port	any	
Destination Address		
Destination Mask		
Destination Port	specify	
Specify Port	80	
	SAVE	CANCEL
Enter integer range 0..65535		

Description = A text string can be entered here to describe the filter. Note that in other menus only the first 15 characters of the description may be displayed.

Index = The index field can't be changed. The BRICK assigns a new filter number here automatically as new filters are added.

Protocol = Select a predefined protocol; "any" matches all protocols, "tcp" matches only TCP sessions, etc.

Connection State = When the protocol field is set to "tcp", you can use this field to define filters based on the TCP connection state. When set to "established" a filter is defined that will match all TCP packets that, when routed, would not force (initiate) a new connection.

Source/Destination Address = (optional) Enter the source (or destination) IP address to match IP packets from.

Source/Destination Mask = (optional) Apply an optional mask.

Source/Destination Port = The range of port numbers to apply. Use “specify” to select a specific port number, “specify range” to select a range of port numbers by entering the first and the last port to be included in the range, “any” to match all ports numbers, or one of the predefined ranges, as explained in the table below.

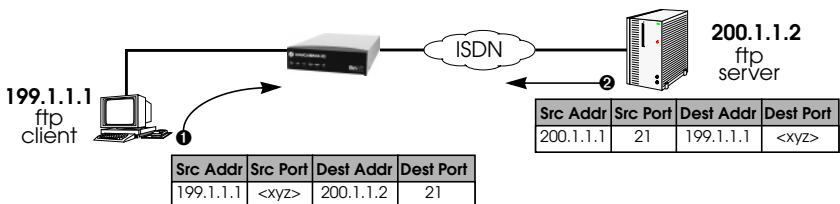
Source Port Ranges

0 ... 1023	1024 ... 4999	5000 ... 32767	32768 ... 65535
privileged	unprivileged		
server	clients	server	clients
specify / specify range			

Specify Port = If “specify” or “specify range” is set in the previous field the port number or port number range must be set here.

Using Source and Destination Port Numbers

Along with the source and destination addresses, the Internet Protocol uses source and destination ports numbers, to identify data connections uniquely. The client side generates a number (xyz) which is used as the source port, for the destination port it uses the number the server offers the service on. The server sends IP packets with the port numbers reversed in respect to the client. A simplified ftp connection might look like this.





This menu lists configured Rule Chains (individual chains are separated by a line). For each rule the Rule Index, Filter Index, Next Rule Index, Action, Filter, and Conditions are shown.

If a Rule (i.e., a link in the chain) is deleted from the list all neighbouring rules in the chain are automatically relinked.

Select **ADD** to create new rules. The menu below will be displayed. For each rule an Action and Filter must be defined that defines what to do when a packet matches that filter.

Select **DELETE** to remove an existing Rule that has been marked for deletion (Using the spacebar).

Select **REORG** to reorganize the order of the rules in a chain. See the following page.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[[IP]][ACCESS][RULE][IP]: Configure IP Access Rules		brick	
Index	Insert behind Rule	R2	F5 (no telnet)
Action	deny M		
Filter	no ftp (1)		
SAVE		EXIT	
Use <Space> to select			

Index = This value can not be changed but is displayed when editing an existing rule. When creating new rules this field is empty until the rule is saved.

Insert behind Rule = (only shown when creating new rules) Use the scrollbar to select the location in the chain where this new rule should be inserted. For example: If you already have a global rule chain 1-3-2-0, selecting 3 here results in the chain 1-3-4-2-0.

To start a new (separate) rule chain use the scrollbar and select “none” in this field.

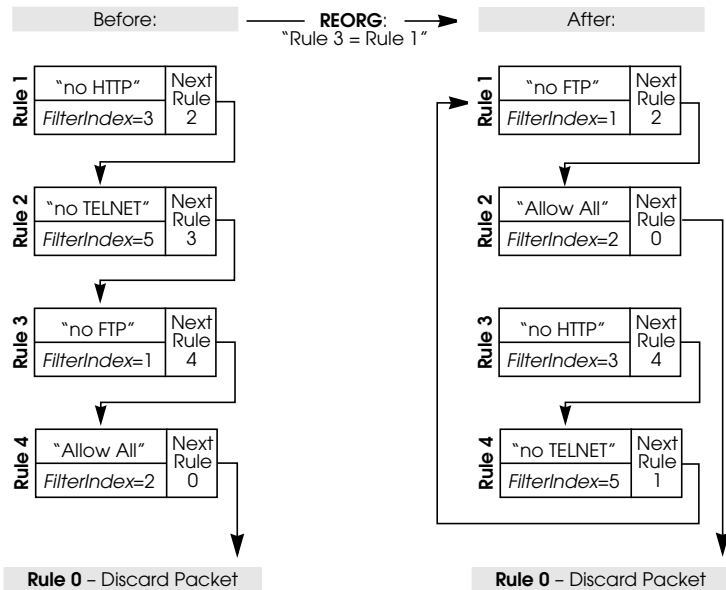
Action = The action field defines whether to allow or discard the packet based on whether or not the packet matches the filter (defined in the following field) or not.

Filter = The Filter to test IP packets against; use the spacebar to scroll through the list of currently configured filters.

Reorganizing Rules in a Chain

The **REORG** menu allows you to change the order of Rules in an Access Rule chain.

After selecting the Rule that should be placed at the beginning of the chain (the “Index of Rule that gets Index 1” field), remaining Rules are automatically relinked. The appropriate Rule Index and Next Rule Index numbers are reassigned in the *ipRuleTable* and the interface-specific Start Rules are updated in the *ipExtIfTable*.



Note: The appropriate indicies are renumbered but the access semantics remain the same.





This menu is used to control which Rule Chain(s) are used for packets arriving via the BRICK interface. This menu lists all IP capable interfaces and the First Rule that is currently being used for this interface.

To change the First Rule for any interface highlight the entry and hit Return key; otherwise select **Exit** to accept the displayed settings.

Note: By default Rule 1 is always used for newly created interfaces.

BIANCA/BRICK-XL2 Setup Tool [IP][ACCESS][INTERFACES]: Configure First Rules	BinTec Communications AG brick																		
Configure first rules for interfaces																			
<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Interface</th> <th style="text-align: left;">First Rule</th> <th style="text-align: left;">First Filter</th> </tr> </thead> <tbody> <tr> <td>en1</td> <td>0 (no access rules)</td> <td></td> </tr> <tr> <td>en2</td> <td>0 (no access rules)</td> <td></td> </tr> <tr> <td>sales1</td> <td>2</td> <td>3 (all else)</td> </tr> <tr> <td>sales2</td> <td>2</td> <td>3 (all else)</td> </tr> <tr> <td>sales2</td> <td>2</td> <td>3 (all else)</td> </tr> </tbody> </table>	Interface	First Rule	First Filter	en1	0 (no access rules)		en2	0 (no access rules)		sales1	2	3 (all else)	sales2	2	3 (all else)	sales2	2	3 (all else)	
Interface	First Rule	First Filter																	
en1	0 (no access rules)																		
en2	0 (no access rules)																		
sales1	2	3 (all else)																	
sales2	2	3 (all else)																	
sales2	2	3 (all else)																	
EXIT																			
Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select																			

In the EDIT/ADD menu the following fields are displayed.

Interface = This value can not be changed but is displayed for reference.

First Rule = Use the scrollbar to select the Rule to use first for packets arriving on this interface. Setting this field to “none” disables the Access List mechanism for this interface.


Note: If the referenced Rule doesn't exist (in ipRuleTable) then all packets arriving on this interface will be allowed.





This menu should be used to create a pool of IP addresses the BRICK may use when operating as a Dynamic IP address server.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[IP][DYNAMIC]: Dynamic IP Addresses (Server)		brick	
Pool	first IP Address	last IP Address	Range
0	192.168.10.5	192.168.10.9	5
1	10.5.5.1	10.5.5.35	35
ADD	DELETE	EXIT	

Note: Existing host routes always take priority over available IP addresses from the Address Pool.
 i.e., After an incoming call is authenticated, the BRICK first checks for a host route for the caller. If a host route does not exist, the caller is assigned an address from the address pool if one is available.

Select **ADD** to add a block of addresses to the pool. You may add single IP addresses, or a complete block of addresses. In the following menu define one or more address blocks using these fields:

Pool ID = A unique number to identify the pool.

IP Address = Enter the first number of the address block.

Number of consecutive addresses = Enter the number of addresses in the block including the first number.

Select **DELETE** to remove a block of addresses marked for deletion.

Select **EXIT** to return to the **IP** menu.



The BRICK supports the Dynamic Host Configuration Protocol which can be used to assign local (or remote) hosts IP addresses. This menu is used to control which IP addresses can be assigned and how long the address is valid.

BIANCA/BRICK-XL2 Setup Tool [IP][DHCP]: DHCP Server			BinTec Communications AG brick	
Interface	IPAddress	Count	Lease Time (Min.)	MAC Address
en1	192.168.1.70	9	30	
en1	199.168.1.85	5	120	
en1	192.120.130.144	1	480	00a0f90046e7
tr6-snap	200.1.2.50	4	120	
ADD	DELETE	EXIT		
Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select				

The BRICK acts as a DHCP Server. Client machines (PCs running Windows 95/NT) that support DHCP are generally configured to retrieve their IP address from the server and adjust their configurations appropriately. With DHCP the retrieved IP address is only valid for a specified time period, known as the "Lease Time". Once the lease time has run out, the server is free to reassign the IP address when needed. The DHCP server also informs clients of the appropriate nameserver (*biboAdmNameServer* is used) and default gateway.

Select **ADD** to add a new range of addresses; or highlight an entry and enter <Return> to change an existing entry. In the subsequent menu you'll need to enter information for the following fields.

Interface = Associates a BRICK interface with a set of IP addresses. The BRICK will assign an available IP address from the appropriate

set of addresses depending on which interface it received the address-request on.

IP Address = Defines the first IP address in the set.

Count = Defines the number of addresses in the set (including the first address).

Lease Time (Minutes) = Defines the time in minutes addresses from this set are valid. Addresses become available for reassignment once the lease time runs out.

MAC Address = Specifies which device—identified by its unique MAC address—should get the IP address given above.

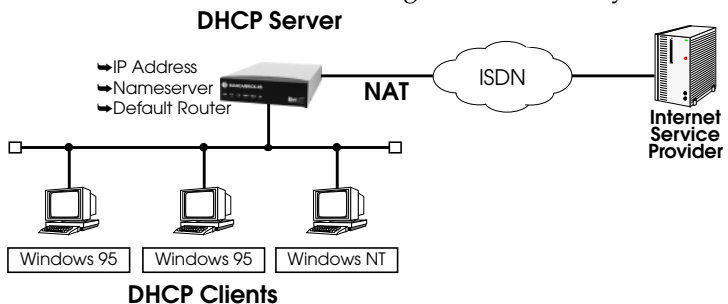
This only works, if *Number of consecutive addresses* is set to 1.

Select **SAVE** to add the entry to the list and return to the previous menu.

Note that existing entries can not be edited by selecting them, you must delete the entry by tagging the entry for deletion (with the spacebar), and selecting **DELETE**. To configure new parameters, select **ADD** again.

Internet Access for the LAN using DHCP and NAT

DHCP can be used in combination with Network Address Translation to provide easy Internet access for a complete LAN. The main advantage is that PCs on the LAN don't need to be configured individually.



A simplified configuration using this setup would involve:

1. Configuring Network Address Translation on the BRICK (only one official IP Address is required).
2. Configure BRICK as DHCP Server.



Use this menu to change the basic settings for the SNMP, or Simple Network Management Protocol.

BIANCA/BRICK-XL2 Setup Tool [IP][SNMP]: SNMP Configuration	BinTec Communications AG brick
SNMP listen UDP port 161 SNMP trap UDP port 162 SNMP trap broadcasting off SNMP trap community snmp-Trap	
SAVE	CANCEL
Enter integer range 0..65535	

SNMP listen UDP port = Defines the UDP port the BRICK uses for receiving SNMP requests.

SNMP trap UDP port = Defines the UDP port the BRICK sends SNMP traps to when SNMP trap broadcasting is turned on.

SNMP trap broadcasting = When turned **on** the BRICK broadcasts SNMP traps over its LAN interface.

SNMP trap community = By default, the snmp-trap community is used.

Select **SAVE** to accept the these settings and return to the previous menu.

Select **CANCEL** to abort the entries made so far and return to the previous menu.



This menu lists all the RADIUS Servers currently configured. You can add, edit, or delete list entries in the usual fashion.

For each Radius Server you can configure the following parameters:

BIANCA/BRICK-XL2 Setup Tool [IP][RADIUS][EDIT]: Configure Radius Server		BinTec Communications AG brick
Protocol	auth	
IP Address	44.55.66.77	
Password	blubb	
Priority	0	
Policy	authoritative	
Port	1812	
Timeout	1000	
Retries	1	
State	active	
	SAVE	CANCEL
Use <Space> to select		

Protocol = Use this RADIUS Server for authentication purposes (**auth**) or for accounting ISDN connections (**acct**).

When you configure a RADIUS Server for accounting, the BRICK transmits Start and Stop Radius packets for each ISDN connection to this server.

Default value: auth

IP Address = IP Address of the RADIUS Server.

Password = Shared secret between RADIUS Server and BRICK.

Priority = 0 ... 7. When there are several RADIUS Server entries, the server with the lowest priority entry is used first. If there is no reply from this server, the server with the next lowest priority entry is used, and so forth, i.e. servers with *Priority=0* have the highest priority.

Default value: 0

Policy = can be set to **authoritative** or **non-authoritative**. If set to authoritative, a negative answer to a request will be accepted. This is not

necessarily true when set to **non-authoritative**, where the next radius server will be asked until there is finally an **authoritative** server configured.

Default value: authoritative

Port = TCP port to use for RADIUS data. According to RFC 2138 the default ports are 1812 for authentication (was 1645 in older RFCs) and 1813 for accounting (1646 in older RFCs).

Default value: 1812

Timeout = 50 ... 50000, number of milliseconds to wait for an answer to a request.

Default value: 1000 (1 second)

Retries = number of retries if a request is not answered. If after *Retries* attempts still no answer was received, the server *State* is set to **inactive**. The BRICK then tries to contact the Server every 20 seconds, and once the Server replies, the *State* is changed to **active** again.

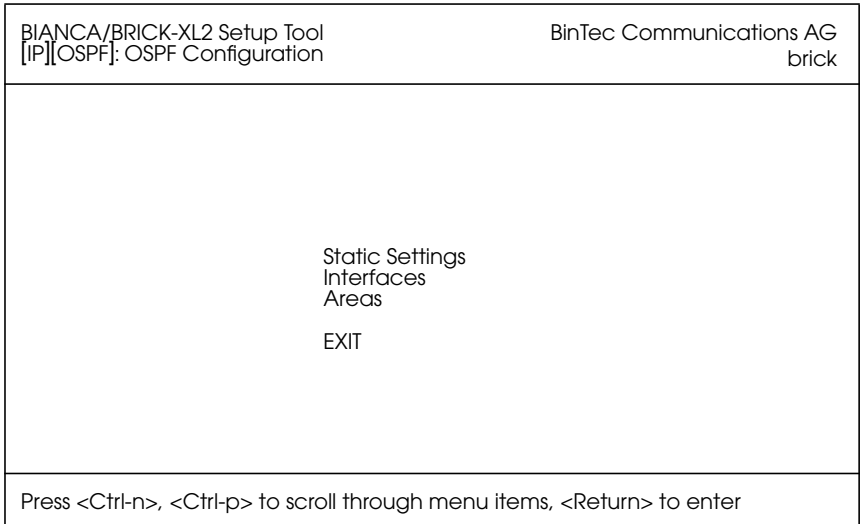
Default value: 1

State = the state of the RADIUS Server. In normal operation mode this is either **active** (server answers requests) or **inactive** (server does not answer; see *Retries* above). You can also set *State*=**disabled**, to temporarily disable requests to a certain RADIUS Server.

Default value: active



OSPF on the BRICK can be configured from Setup Tool using the three menus available here.



STATIC SETTINGS contains global OSPF parameters. This is where OSPF is enabled on the BRICK.

INTERFACES lists all OSPF capable BRICK interfaces and is used for configuring interface-specific settings.

AREAS lists all known OSPF areas and used for adding/configuring area-specific settings.

For a detailed description of these menus please refer to the *Extended Features Reference* (contained on the Companion CD).

IPX →

The IPX Configuration menu is used to set global parameters for the IPX protocol. These settings apply to all IPX interfaces.

BIANCA/BRICK-XL2 Setup Tool [IPX]: IPX Configuration	BinTec Communications AG brick
Local System Name	brick
Internal Network Number	f9000e91
enable IPX spoofing	yes
enable SPX spoofing	yes
NetBIOS Broadcast replication	yes
SAVE	CANCEL
Enter string, max length = 35 chars	

Local System Name = Defines the IPX system name used by the BRICK. The name may not contain underscores or dots, and must be in uppercase.

Internal Network Number = The BRICK's internal network number. This value must be unique among all network numbers and defaults to the last 4 bytes of the BRICK's MAC address. Change only if this value conflicts with a remote IPX router's net number.

enable IPX spoofing = Set to "yes" or "no" to enable/disable NCP session watchdog spoofing and handling of 'broadcast message waiting' packets.

enable SPX spoofing = Set to "yes" or "no" to allow/disallow spoofing of SPX session watchdog packets. Enable this if you are using SPX sessions over WAN links.

NetBIOS Broadcast replication = Defines how NetBIOS packets are used.

“yes” all NetBIOS hosts in your network can be accessed, however WAN links may be opened frequently.

“on LAN only” only NetBIOS hosts attached to the BRICK via LAN interfaces can access each other. WAN links won’t be opened for NetBIOS packets.

“no” NetBIOS hosts in different LANs can not access each other.

Selecting **SAVE** accepts the entries and returns to the main menu.

Selecting **CANCEL** discards all changes made in this menu and returns to the main menu.

PPP →

The PPP menu allows you to configure default (non-partner specific) PPP settings. The PPP settings configured in this menu are only used when negotiating an incoming call that could not be identified via Calling Line ID.

BIANCA/BRICK-XL2 Setup Tool [PPP]: PPP Profile Configuration	BinTec Communications AG brick
Authentication Protocol RADIUS Server Authentication PPP Link Quality Monitoring	CHAP + PAP + MS-CHAP inband none
SAVE	CANCEL
Use <Space> to select	

The possible “default” PPP settings available in this menu include:

Authentication Protocol = Defines the type of PPP authentication protocol to offer the caller first. Possible values include: none, PAP, CHAP, CHAP + PAP, MS-CHAP, and CHAP + PAP + MS-CHAP.

RADIUS Server Authentication = This entry is used to configure possible RADIUS authentication on incoming calls. When set to “inband” (the default) only inband RADIUS requests (PAP, CHAP) are sent to the defined RADIUS server. When set to “Calling Line ID” outband requests are sent to the server. When set to “both”, both requests are sent. Setting to “none” disables RADIUS requests.

PPP Link Quality Monitoring = Defines whether link quality monitoring is performed for PPP links. When set to “yes”, link statistics are written to the SNMP shell’s *biboPPPLQMTable*.

X.25 →

The X.25 menu contains several submenus used to configure the X.25 protocol on the BRICK.

BIANCA/BRICK-XL2 Setup Tool [X.25]: X.25 Configuration	BinTec Communications AG brick
Static Settings Link Configuration Routing Multiprotocol over X.25 EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter	

STATIC SETTINGS contains the BRICK's X.25 address.

LINK CONFIGURATION lists all X.25-compatible interfaces on the BRICK, and is used to configure them respectively.

ROUTING contains the BRICK's X.25 routing table.

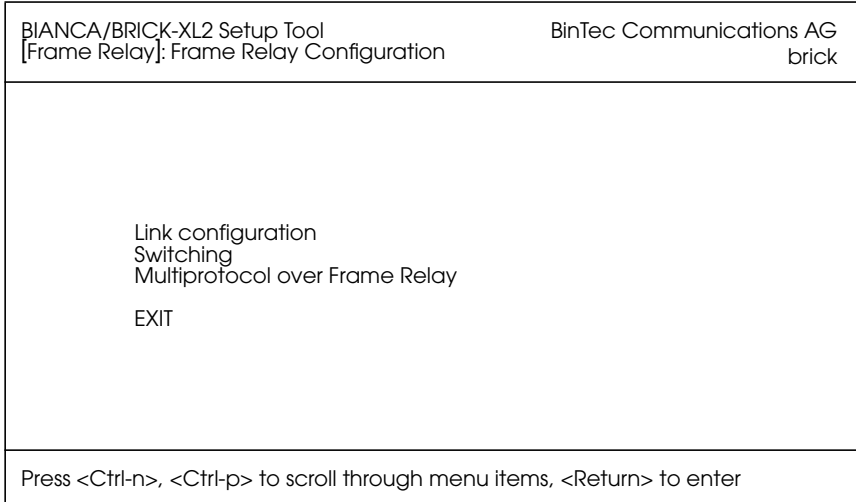
MULTIPROTOCOL OVER X.25 is used to configure the Multiprotocol Routing over X.25 (MPX25) feature.

Select **EXIT** to return to the main menu.

For a detailed description of these menus please refer to the *BIANCA/BRICK Extended Feature Reference* (contained on the Companion CD).

FR →

The Frame Relay menu contains several submenus used to configure support for Frame Relay on the BRICK.



LINK CONFIGURATION contains settings relative to layer 2 of the Frame Relay interface.

SWITCHING contains settings for each Frame Relay Virtual Circuit.

MULTIPROTOCOL OVER FRAME RELAY contains settings for all MFPR interfaces currently configured on the BRICK.

For a detailed description of these menus please refer to the *BIANCA/BRICK Extended Feature Reference* (contained on the Companion CD).

MODEM →

This menu is available if one or more modems have been detected on your system.

BIANCA/BRICK-XL2 Setup Tool [MODEM]: Modem Configuration	BinTec Communications AG brick
<p>Profile Configuration</p> <p>EXIT</p>	
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter	

The **PROFILE CONFIGURATION** submenu, contains settings for the eight modem profiles.

MODEM → **PROFILE CONFIGURATION**

The modem profiles can be associated with the Called Party's Number of incoming calls in the [CM-1BRI] [*Incoming Call Answering*] menu. Thus, using your available MSNs, you can create separate profiles to support the analog equipment your remote access users (dial-up clients) will be calling from.

In theory you could use only one profile, where all values are set to maximum—or auto, where applicable—and let the calling modem negotiate the values it needs.

This will work in most cases—only older modems will be unable to negotiate the necessary values—but will require more time to negotiate the connection parameters at connect time. After starting the Setup Tool, go to the [MODEM] [*Profile Configuration*] menu, and select *Profile 1*.

You must ensure that the modem settings correspond to the type of fax/modem provided by your BRICK. The settings are shown below should be fine for 56000 modems.

BIANCA/BRICK-XL2 Setup Tool [MODEM][PROFILE][EDIT]: Configure Profile		BinTec Communications AG brick
Name	Profile 1	
Description	Default User	
Modulation	K56flex	
Error Correction	auto	
Automode	on	
Min Bps	300	
Max Receive Bps	33600	
Max Transmit Bps	56000	
V.42bis Compression	auto	
MNP5 Compression	auto	
SAVE		CANCEL
Enter string, max length = 48 chars		

The fields in this menu have the following meanings:

Name = Profile 1...8. Cannot be changed.



Note that Profile 1 is used as the *default profile* for modem connections, if no other profile is explicitly specified.

Description = descriptive string for this profile.

Modulation = modem standard to use, select with the space bar. Values range from K56flex down to Bell 103. Make sure you select a modulation that your feature board's modem supports; K56flex or below for 56000 modems, V.34 or below for 33600 modems, V32bis or below for 14400 modems.

Error Correction = select the type of error correction to use.

Value	Meaning
none	Do not use any error correction.
required	First tries LAPM and then MNP5 error correction. If both fail, the modem will hang up.
auto	First tries LAPM and then MNP5 error correction. If both fail, the modem will not use error correction.
LAPM	Selects LAPM error correction. If this fails, the modem will hang up.
MNP	Selects MNP4 error correction. If this fails, the modem will hang up.

Automode = enable (*on*) or disable (*off*) negotiation of speed and modulation parameters.

Min Bps = the minimum baudrate you want to use with this profile. You can set any speed supported by the current modulation (i.e. standard). The connection is released, if it cannot negotiate a baud rate \geq to this speed.

Max Receive Bps = the maximum baudrate you want to use with this profile. You can set any speed supported by the current modulation (i.e. standard). Note that the value set in Max Transmit Bps will be used if its $<$ the value set here.

Max Transmit Bps = only used in conjunction with the *K56flex* modulation. Sets the maximum transmit baudrate (*»downstream«*, server to client) you want to use with this profile. K56flex modulation is not supported for your feature module.

V.42bis Compression = enable (*auto*) or disable (*off*) negotiation for using V.42bis compression.

MNP5 Compression = enable (*auto*) or disable (*off*) negotiation for using MNP5 compression.



Note that data compression only works if you use any error correction and the remote site also supports the same type of error correction. In general, it's best to use the auto settings for error correction.

VPN →

The VPN menu is used to configure Virtual Private Networking interfaces on the BRICK. The structure of the VPN menu is consistent with Setup Tool's WAN partner menus with slight differences.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[VPN]: Configure VPN Interfaces		brick	
Partner Name	VPN1		
Encapsulation	PPP		
Compression	none		
Encryption	none		
PPP >			
Advanced Settings >			
IP >			
IPX >			
SAVE		CANCEL	
Enter string, max length = 25 chars			

Support for Virtual Private Networking on the BRICK requires a separate license. For detailed information on setting up Virtual Private Networks please refer to the Extended Features Reference (contained on the Companion CD).

ISDN →

The ISDN menu contains settings for the Credits Based Accounting System which gives BRICK administrators the ability to control charges. It allows BRICK administrators to watch and limit the number of connections, the connection time and the accounted charges of every subsystem during a specified period of time. If the limit is exceeded the BRICK can't make further connections during that time period.

Syslog messages are generated to give you information about credits, when the 90% or 100% mark for each limit and each subsystem is reached. Also, each time a call is rejected a syslog message is generated.

To configure the Credits Based Accounting System, you will need to enable surveillance of one or more subsystems on the BRICK in the **ISDN** → **Credits** → submenu.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG
[[ISDN]][[CREDITS]: Configure Credits		brick
Select Subsystem		
Subsystem	Surveillance	
capi	off	
ppp	off	
isdnlogin	off	
EXIT		
Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select		

Select the BRICK subsystem you wish to control and enter <Return>. In the subsequent submenu set the Surveillance field to "on"; you can then define the controls for the respective subsystem.

Note: Only the settings for the CAPI subsystem are shown below. The default settings for the PPP and ISDNLOGIN subsystems are the same.

ISDN →
 CREDITS →
 CAPI →

BIANCA/BRICK-XL2 Setup Tool [ISDN][CREDITS][EDIT]: Configure ppp Credits	BinTec Communications AG brick
Surveillance	on
Measure Time (sec)	86400
Maximum Number of Incoming Connections	on 2
Maximum Number of Outgoing Connections	on 20
Maximum Charge	off
Maximum Time for Incoming Connections (sec)	on 28800
Maximum Time for Outgoing Connections (sec)	on 28800
SAVE	CANCEL
Use <Space> to select	

Surveillance = Determines whether or not accounting for ppp connections is activated. If you set Surveillance on, you are able to determine the following parameters.

Measure Time (sec) = The observation interval in seconds. Enter an integer from 0 to 2147483647. Default value is 86400 seconds, which is 24 hours.

Maximum Number of Incoming Connection = The number of allowed incoming connections during the measure time. Once enabled, you can enter an integer from 0 to 2147483647. Default value is off.

Maximum Number of Outgoing Connections = The number of allowed outgoing connections during the measure time. Once enabled, you can enter an integer from 0 to 2147483647. Default value is 100 calls.

Maximum Charge = The maximum allowed charge information during the measure time. Once enabled, you can enter an integer from 0 to 2147483647. Default value is off.

Maximum Time for Incoming Connections (sec) = The maximum allowed time in seconds for incoming connections during the measure

time. Once enabled, you can enter an integer from 0 to 2147483647. Default value is 28800 seconds, which is 8 hours.

Maximum Time for Outgoing Connections (sec) = The maximum allowed time in seconds for outgoing connections during the measure time. Once enabled, you can enter an integer from 0 to 2147483647. Default value is 28800 seconds, which is 8 hours.

Once one or more BRICK subsystems have been enabled for surveillance you can then monitor accounting statistics via Setup Tool's **MONITORING AND DEBUGGING** → **ISDN CREDITS** menu as shown on page 108.

CAPI →

The CAPI menu is used to configure CAPI users for use with BinTec's CAPI User Concept. This user concept has been implemented to give you greater control of access to the BRICK's CAPI subsystem.

Each network user that attempts to access the BRICK's CAPI subsystem must first be authenticated using a user name and password which has been configured on the local system here. Only if authentication is successful, the user can receive incoming calls or establish outgoing connections via the Remote CAPI.

The CAPI menu is seemingly straight forward; simply select ADD in the **CAPI** → **USER** → submenu to add/modify existing CAPI users.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG
[CAPI][User]: Configure CAPI Users		brick
Name default	Password	CAPI enabled
ADD	DELETE	EXIT

If this menu (*capiUserTable*) is empty at boot time, a default entry (as shown above) is automatically added. The default user is enabled and no password is required.

In the subsequent ADD menu define the following fields:

Name = Specifies the user name (up to 16 characters) to enable/disable CAPI access for.

Password = Specifies the password this user must authenticate with when accessing the CAPI subsystem.

CAPI = Determines whether the CAPI service is "enabled" or "disabled" for this user.

System Administration

CONFIGURATION MANAGEMENT →

This menu is used to manage configuration files. Files may be stored (or retrieved) locally in Flash, or on remote hosts which support TFTP. For an overview of configuration management see Configuration Files, Flash, and the TFTP in Chapter 3.

BIANCA/BRICK-XL2 Setup Tool [CONFIG]: Configuration Management		BinTec Communications AG brick
Operation	put	(FLASH -> TFTP)
TFTP Server IP Address	200.1.1.99	
TFTP File Name	test1.cf	
Name in Flash	boot.new	
Type of last operation	put	(FLASH -> TFTP)
State of last operation	done	
START OPERATION		EXIT
Use <Space> to select		

Operation = Select the operation to perform.

Operation	Meaning/Effect
save	Save all settings in memory to a configuration file <Name in Flash> will be overwritten/created.
load	Load configuration from Flash into memory (settings read from <Name in Flash> take effect immediately)
move	Rename Flash file <Name in Flash> to <New Name in Flash>.
copy	Copy Flash file <Name in Flash> to <New Name in Flash>.
delete	Delete Flash file <Name in Flash>.

Operation	Meaning/Effect
put	If successful ¹ , overwrites/creates <TFTP File Name> on host at <TFTP Server> with contents of <Name in Flash>.
get	If successful ¹ , overwrites/creates <Name in Flash> in Flash with contents of <TFTP File Name> retrieved from host at <TFTP Server>. Since this information is not saved to memory a subsequent load command is required.
state	If successful ¹ , overwrites/creates <TFTP File Name> on host at <TFTP Server > with contents of memory ² .
reboot	Reboot the system; settings not previously saved are lost.

1. Host must support TFTP, file must exist and be writeable.
2. Variables that contain password information (**bintecsec**, **biboPPPAuthSecret**, **radiusSrvSecret**, **tafServerNodeSecret**) are saved as "*****" in TFTP file

Name in Flash = Filename to read from (or write to).

TFTP Server IP Address = The IP address of the TFTP host (or PC running *DIME Tools*) to transmit/request a configuration file to/from.

TFTP File Name = Filename to write (or read from) on the TFTP host.

Name in Flash = Select the name of a file in Flash to read from or enter a filename to write to.

New Name in Flash = Filename in Flash to create.

Type of last operation = Last operation performed since last reboot.

State of last operation = Status of the last operation which may be:

State	Meaning
todo	The operation has not been started.
running	The command is currently running.
done	The operation is done.
error	The operation could not be completed.

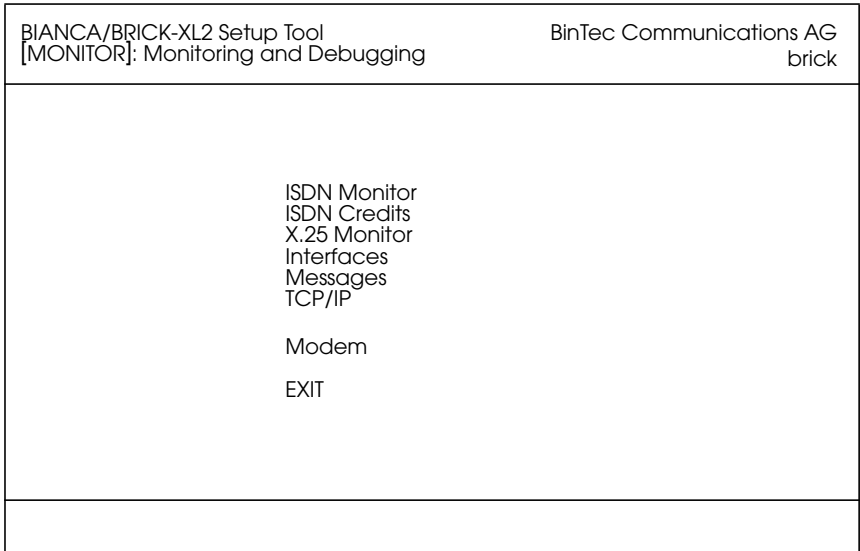
If the "error" state is reported Setup Tool's message monitoring menu, **MONITORING AND DEBUGGING** → **MESSAGES** may contain a possible cause

Select **START OPERATION** and hit <Return> to perform operations.

Select **EXIT** to return to the previous menu.

MONITORING AND DEBUGGING →

This menu consists of several submenus which allow you to monitor the BRICK's operational status (and debug problems) in different ways.



ISDN MONITOR lets you track incoming and outgoing ISDN calls.

ISDN CREDITS lets you track statistics for the Credits Based Accounting System.

X.25 MONITOR lets you track incoming and outgoing X.25 calls.

INTERFACES lets you monitor traffic by interface.

MESSAGES displays system messages generated by the BRICK's system logging and accounting mechanisms.

TCP/IP menu lets you monitor IP traffic by protocol.

OSPF menu lets you monitor OSPF related information.

MODEM menu lets you monitor the status of your modems.

Select **EXIT** to return to the main menu.

MONITORING AND DEBUGGING

ISDN MONITOR

Initially this menu displays all ISDN calls currently established (incoming and outgoing) on the BRICK.

Enter one of the menu commands (c, h, d, or s) listed at the bottom of the screen to list different statistics relating to ISDN call information.

BIANCA/BRICK-XL2 Setup Tool				BinTec Communications AG		
[MONITOR][ISDN CALLS]: ISDN Monitor - Calls				brick		
Dir	Remote Number	Charge	Duration	Stack	Channel	State
EXIT						
(c)alls		(h)istory		(d)etails		(s)tatistics

The **(c)alls** listing shows a list of all currently established ISDN calls:

Dir	Remote Number	Charge	Duration	Stack	Channel	State
in	2		2910	0	B1	active
out	3		106	0	B2	disc_req

For each established call you can also monitor transfer activity. Select a call from the list and enter “s” (statistics). Enter “d” to see details for this call.

The **(h)istory** listing shows a list of the last 20 completed calls (incoming and outgoing connections) since the last system reboot.

Dir	Remote Number	Charge	Starttime	Duration	Cause
in	2		14:16:29	6	(0x90) normal call clear
in	3		14:21:02	7	(0x90) normal call clear

Detailed information for both completed and active calls can be seen under the (d)etails listing. To see more information for a completed call, select an entry from the (h)istory list, then enter “d”.

The **(d)etails** listing shows specific information for both completed and active ISDN calls.

Remote Number:	2	Direction:	out	State:
Cause	(0x90) normal call clearing			
Local Cause	(0x0)			
Local Number	2			
Dispatch Item	routing			
Stack	0			
Channel	B1			
Charging Info				
SIN	data_transfer			

The **(s)tatistics** listing shows transfer activity for established ISDN calls.

Remote Number:	442	Direction:	out	State:	active
Duration	971				
Send:		Receive:			
Packets	1555	Packets	1552		
Bytes	10032	Bytes	20999		
Errors	0	Errors	0		
Packets/s	0	Packets/s	0		
Bytes/s	0	Bytes/s	0		
Load(%)	0	Load(%)	0		

MONITORING AND DEBUGGING

ISDN CREDITS

Initially this menu displays all ISDN calls currently established (incoming and outgoing) on the BRICK.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[MONITOR][CREDITS][STATS]: Monitor isdnlogin Credits		brick	
	Total	Maximum	% reached
Time till end of measure interval (sec)	7794	86400	91
Number of Incoming Connections	0	2	0
Number of Outgoing Connections	0	20	0
Time of Incoming Connections	4	28800	0
Time of Outgoing Connections	13	28800	0
Charge	0		
EXIT			

Time til end of Measure interval (sec) = The seconds left in the current observation interval.

Number of Incoming Connections = The number of established incoming connections during the current measure time.

Number of Outgoing Connections = The number of established outgoing connections during the current measure time.

Time of Incoming Connections = The accounted time for incoming connections during the current measure time.

Time of Outgoing Connections = The accounted time for outgoing connections during the current measure time.

Charge = The number of charge informations received during the current measure time.

MONITORING AND DEBUGGING

X.25 MONITOR

The X.25 Monitor menu initially display all active X.25 connections. These calls include leased and dialup connections made through X.25 public networks or over ISDN.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG			
[MONITOR][X.25 CALLS]: X.25 Monitor		brick			
From	To	Calling Addr		Called Addr	Duration
xi3	local	1	0	0	591
EXIT					
(c)alls	(h)istory	(d)etails	(s)tatistics		

For a detailed description of these menus please refer to the *BIANCA/BRICK Extended Feature Reference* (contained on the Companion CD).

MONITORING AND DEBUGGING → **INTERFACES**

The Interface Monitoring display can be used to monitor statistics for any interface configured on the system. The menu is divided vertically into two parts, so that two interfaces can be monitored simultaneously.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[MONITOR][INTERFACE]: Interface Monitoring		brick	
Interface Name	en1	partner1	
Operational Status	up	dormant	
	total	per second	total per second
Received Packets	5512	0	0 0
Received Octets	920664	0	0 0
Received Errors	0		0 0
Transmit Packets	9	0	0 0
Transmit Octets	1193	0	0 0
Transmit Errors	0		0 0
Active Connections	N/A	0	
Duration	N/A	0	
EXIT	EXTENDED	EXTENDED	
Use <Space> to select			

Interface Name = Select the interface to display statistics for.

Operational Status = The current state of this interface; may be up, down, blocked, or dormant.

The **Received/Transmit** fields actively display the amount of traffic being routed over the respective interface.

Active Connections = For ISDN interfaces, displays the number of B-channels currently in use.

Duration = For ISDN interfaces, the duration of the connection in seconds.

The **EXTENDED** command displays additional information about an interface, and can be used to quickly change the status of an interface.

Select **EXIT** to return to the previous menu.

MONITORING AND DEBUGGING →**INTERFACES** →**EXTENDED** →

This menu displays additional information about a selected Interface. In the upper portion of the menu transmission statistics for all traffic passing over this interface are shown. For WAN interfaces, the lower portion actively display call information for the B-channels currently in use.

BIANCA/BRICK-XL2 Setup Tool				BinTec Communications AG		
[MONITOR][INTERFACE][EXTENDED]: Extended Interface Monitoring				brick		
OperSt	InPkts	InOctets	OutPkts	OutOctets	ActCalls	IP-Address
up	5670	947856	9	1192	N/A	199.2.2.2
Calls:						
Stk Ch	Dir	Remote Number	Local	DspItem	RPckts	TPcktsCharge Duration
EXIT	Operation >reset			START OPERATION		

Select **EXIT** to return to the previous menu.

You can also move this interface to the up or down state. Move to the **OPERATION** field and choose an operation to perform, then select the **START OPERATION** command and enter <Return>.



The Syslog Messages menu actively displays system messages generated on the BRICK. System Logging messages are listed here with newer messages being appended to the bottom of the list.

The number of messages shown here depends on the “Maximum Number of Syslog Entries” configured under **SYSTEM** on page 35.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG
[MONITOR][MESSAGE]: Syslog Messages		brick
Subj	Lev	Message
SNMP	DEB	sent TRAP(linkUp,0) 115 bytes to circindex 10001 Port 36880
SNMP	DEB	sent TRAP(linkUp,0) 115 bytes to 199.1.1.13 Port 162
EXIT	RESET	
Press <Ctrl-n>, <Ctrl-p> to scroll		

Select **EXIT** to return to the previous menu.

Select **RESET** to delete all System Logging messages.

Note: If the number of messages displayed here exceeds your terminal's output, you can scroll up to previous messages using the up-arrow key or Ctrl-P. Scroll forward with Ctrl-N.



MONITORING AND DEBUGGING →

TCP/IP →

The IP Statistics Menu can be used to monitor different statistics relating to the ICMP, IP, UDP, and TCP protocols routed by the BRICK. Initially, the menu displays information relating to the IP. Use the menu commands (c, i, u, and t) shown at the bottom of the screen, to see other information relating to a particular protocol.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG	
[MONITOR][IP]: IP Statistics		brick	
InReceives	3912	OutNoRoutes	0
InHdrErrors	0	ReasmTimeout	500
InAddrErrors	0	ReasmReqs	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			
(C)MP		(I)P	
		(U)DP	
		(T)CP	

Note: Information shown in the various menus reflects the combined number of ICMP, IP, UDP, or TCP packets, octets, etc., passing through the BRICK. For the meanings of individual fields shown in these menus, please refer to the Management Information Base.



MONITORING AND DEBUGGING

OSPF

The OSPF monitor is divided horizontally in three sections and displays information relating to OSPF Interfaces, Neighbours, and Areas.

BIANCA/BRICK-XL2 Setup Tool [MONITOR][OSPF]: OSPF Monitor			BinTec Communications AG brick		
Interface	DR	BDR	Admin Status	State	
en1	192.168.30.1	192.168.30.0	active	BDR	
brickxs	0.0.0.0	0.0.0.0	active	PTP	
Neighbor	Router ID	Interface	Retx Queue	State	
192.168.30.1	10.0.1.1	en1	0	full	
12.0.0.2	11.0.0.2	brickxs	0	full	
Area	Type	Link State ID	Router ID	Sequence	Age
0.0.0.0	Summary Net	10.0.0.0	10.0.1.1	0x80000003	1641 =
0.0.0.0	Network Link	192.168.30.1	10.0.1.1	0x80000001	361
11.0.0.0	Router Link	11.0.0.2	11.0.0.2	0x80000009	1
11.0.0.0	Summary Net	0.0.0.0	192.168.40.3	0x80000001	2 v
EXIT					
Press <Ctrl-n>, <Ctrl-p> to scroll					

For a detailed description of these menus please refer to the *BIANCA/BRICK Extended Feature Reference* (contained on the Companion CD).

MONITORING AND DEBUGGING

MODEM

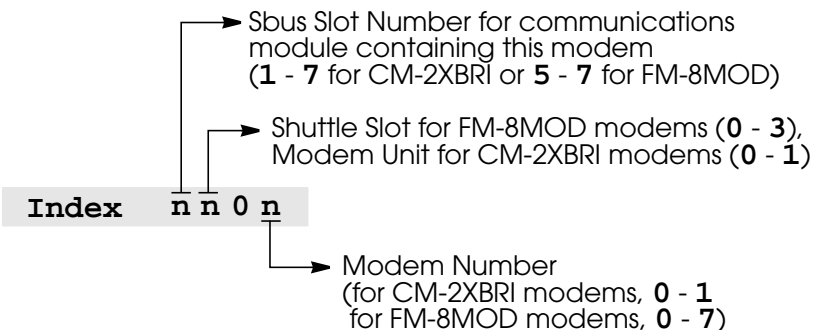
This menu allows you to monitor the status of each modem installed on your BRICK. Depending on how many modems are installed in your BRICK (via FM-8MOD modem boards and/or CM-2XBRI feature modules) there will always be exactly one entry listed here for each modem. The individual fields shown below correspond to the SNMP table entries in the *mdmTable*.

BIANCA/BRICK-XL2 Setup Tool		BinTec Communications AG							
[MONITOR] [MODEM]: Modem Calls		brick							
Index	Action	Type	State	Mode	Modu- lation	Err Corr	ComprTX	RX Speed	ifindex/ BChan
3000	enabled	csm336	idle	none	unknown	none	none	0 0	0/0
3001	enabled	csm336	connected	fax	v17	none	none	9.6K 9.6K	3000/2
3100	enabled	csm336	connected	ppp	v34	none	none	33K 28K	3000/1
3101	enabled	csm336	idle	none	unknown	none	none	0 0	0/0
7000	enabled	csm56K	connected	modem	unknown	none	none	56K 56K	2000/21
7001	enabled	csm56K	idle	none	unknown	none	none	0 0	0/0
7002	enabled	csm56K	idle	none	unknown	none	none	0 0	0/0
7003	enabled	csm56K	idle	none	unknown	none	none	0 0	0/0
7004	enabled	csm56K	idle	none	unknown	none	none	0 0	0/0
7005	enabled	csm56K	idle	none	unknown	none	none	0 0	0/0
7006	enabled	csm56K	idle	none	unknown	none	none	0 0	0/0
7107	enabled	csm56K	idle	none	unknown	none	none	0 0	0/0

EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll

Index = The index field identifies exactly which modem the list entry applies to. On the BRICK-XL index numbers are broken down as follows:



Action = This field will display one of: reboot, disabled or, enabled, with the latter being the default. Action corresponds to the *mdmTable*'s *mdmAction* object, which is the only editable object in this table. i.e., Assigning this object to one of the stated values (from the SNMP shell), results in "rebooting" a (hung) modem, "disabling" availability of this modem, or "enabling" availability of this modem in the modem pool.

Type = This field describes the type of modem detected in your BRICK. The following table shows which modem types are used in each BRICK / BinGO! product.

BRICK/BinGO! Product:	Modem Types			
	mdm144	mdm336	Csm336	Csm56K
BinGO! Plus	-	-	-	-
BinGO! Professional	✓		-	-
BIANCA/BRICK-XS Office	✓	-	-	-
BIANCA/BRICK-XM	-	-	✓ ^{1/2}	-
BIANCA/BRICK-XMP	-	-	-	✓
BIANCA/BRICK-XL2	-	-	✓ ¹	✓ ²

1. Via an installed CM-2XBRI module.
2. Via FM-8MOD modules.

State = The current status of the modem which may be as follows:

booting	The init phase (after a system boot).
idle	The modem is available for use.
calling	An outgoing call has been initiated.
called	An incoming call is being processed.
connected	An incoming/outgoing call has been established.
hangup	The current connection is being terminated.
stopped	This modem is not longer available.

Mode = The mode the modem is currently in.

modem	Modulation mode.
ppp	Modulation mode + asynchronous HDLC framing.

fax	A FAX is being sent or received.
dtmf	Sending or receiving DTMF touchtones.
none	The modem is currently not in use.

Modulation = The modulation standard that was negotiated by the sending and receiving modems. Depending on the type of modem installed in your BRICK has one of the following values will be present .

bell103	bell212	v21	v22	v22bis
v23	v32	v32bis	v34	k56flex
vfc	v90	unknown		

Error Correction = The type of error correction negotiated by the calling/called modems.

none	Error correction is not being performed.
alt	MNP error correction.
lapm	LAPM error correction.

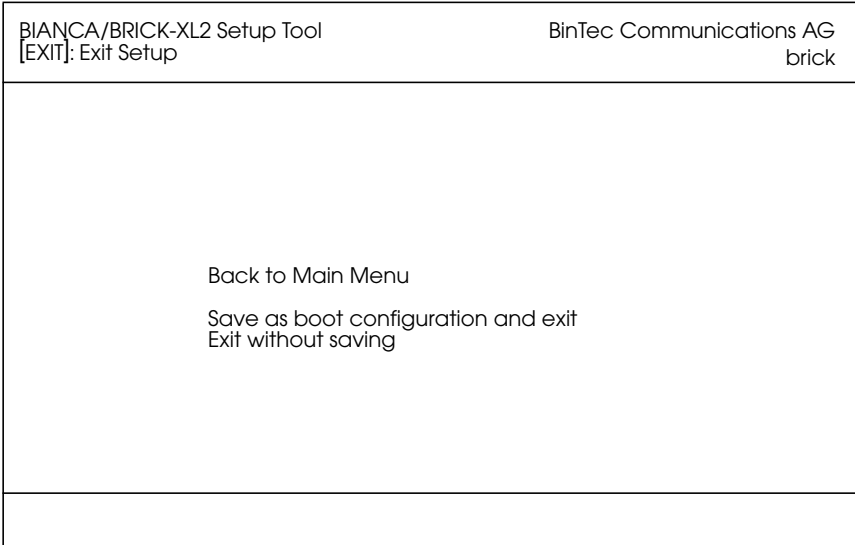
TX Speed = The transmit speed negotiated by the modems. This will always be the same as the RX Speed, except for **csM336** and **csM56K** modems.

RX Speed = The receive speed negotiated by the modems. As stated above, this is always the same as the TX Speed, except for **csM336** and **csM56K** modems.

lindex/BChannel = If a connection has been established, this field identifies the lindex and B-channel the (incoming or outgoing) connection has been established on.

Exit


From this menu three options are available.



Back to Main Menu = Simply returns you to the Main Menu.

Save as boot configuration and exit = All settings (or changes) made in this session will be saved to Flash and will be named *boot*. After creating the Flash file, you are returned to the SNMP shell prompt.

Exit without saving = Closes this setup session and returns you to the SNMP shell prompt.

Note:  If changes have been made in a submenu and were subsequently saved, these changes are currently active in memory and are not removed upon exiting Setup Tool.

If you want to save your current settings to a different configuration file, refer to the **CONFIGURATION MANAGEMENT** menu.

Alternatively, you may want to reload your existing boot configuration file. This can also be done from the Configuration Management menu

5

HOW DO I CONFIGURE ...




What's covered

- Configuring the BRICK's features
 - Hardware Interfaces 121
 - IP Features 128
 - IPX Features 141
 - Modem and Fax Features 143
 - General 153
-

In the previous chapter we described the many menus you'll find when using Setup Tool to configure and administer your BRICK.

Now we'll explain explicit, step-by-step, how to configure those features you want to use. We've organized this chapter into major topics and present the information in a quick-answer format to help answer some of the most common questions you'll have.

Within each section, look for the following symbols:

-  This section lets you know what information you'll need before you begin to configure a feature.
 -  This section explains step-by-step instructions on how to configure the BRICK's features.
 -  This section contains references to other information you may find helpful when configuring a particular feature (i.e., tips on testing features, troubleshooting, or general background information).
- (p. 50) Since we'll be referring to Setup Tool's menus we've included the page reference in the left margin where the description of the menu can be found in Chapter 4.

Caution



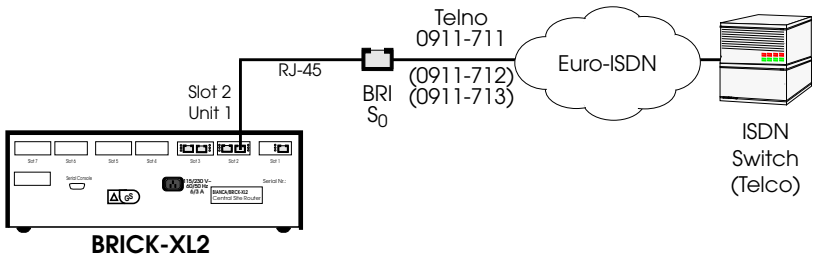
As an ISDN multiprotocol router, BIANCA/BRICK-XL2 establishes ISDN connections in accordance with the system's configuration. Incorrect or incomplete configuration of your product may cause unwanted charges. The conditions that lead to establishing connections are largely dependent on the respective network configuration.

- To avoid unintentional charges, it is essential that you carefully monitor the product. Observe the LEDs of your product or use the monitoring function in the Setup Tool.
- Use filters to deny certain data packets (cf. page 76). You should be aware that especially in a Windows network broadcasts may establish connections.
- Use the Credits Based Accounting System, as described on page 108, to define a maximum number of ISDN connections resp. the accounted charges allowed in a certain period of time and thus limit unwanted charges in advance.
- Use the checklist "ISDN connections remain open or are unwanted" on page 178 to prevent the most common causes of unintentional charges.

Hardware Interfaces

How do I configure an ISDN interface in general?

Configuring an ISDN interface on the BRICK involves telling the BRICK a few things about the ISDN service you're receiving from your carrier and how to answer calls it receives on this line. After the BRICK knows the basic information about this interface, you can begin to configure different ISDN partners the BRICK can establish connections with.



This information is configured for each installed communications module. The settings for our CM-2BRI module shown above would be configured in Setup Tool as follows:

Slot 2: **CM-2BRI, ISDN S0, UNIT 1** → Here's where we tell the BRICK what type of ISDN service we're receiving over this line.

BRICKResult of autoconfiguration: In most cases, the BRICK detects the correct D-channel protocol at boot time (and during normal operation) and displays the results here.

ISDN Switch Type: Normally this is set to allow auto detection. Only if auto detection is incorrect, unsuccessful, or you need to configure the switch type manually, set the switch type and channel fields.

For Leased Lines set the appropriate number of channels to use.

For Dialup Lines specify the ISDN protocol used on the D-channel.

Slot 2: **CM-2BRI, ISDN S0, UNIT 1** → **INCOMING CALL ANSWERING** → Here's where we tell the BRICK how to answer incoming calls on this line. This allows you take advantage of the different telephone numbers provided by your carrier. The BRICK answers or dispatches calls to different services based on the number called (known as the Called Party's Number or CPN in ISDN).

To dispatch incoming calls based on the CPN, in this menu you add an entry to tell the BRICK which "Item" to use for a specific ISDN "Number". Our shown above is connected to Euro-ISDN and includes three different MSNs. We might configure the BRICK to dispatch calls received for 0911-713 to the Login service and have other calls be given to Routing service.

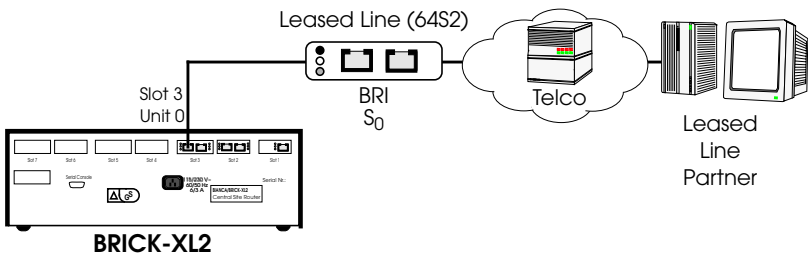
Slot 2: **CM-2BRI, ISDN S0, UNIT 1** → **ADVANCED SETTINGS** → *BIANCA/BRICK-XL* These settings aren't normally required since the BRICK detects this information automatically.

This is all that's required to configure an ISDN (hardware) interface. ISDN partners can now be configured to establish networking connections using this physical interface.

How do I configure a leased line connection?

Configuring an ISDN leased line interface on the BRICK is similar to the basic procedure mentioned on page 121, for ISDN interfaces in general.

After setting the basic information about the physical interface you need to configure the WAN partner attached to the other end of the line. The BRICK automatically creates a temporary WAN partner interface named according to the slot and unit the leased line was configured for. For our leased line interface below, a temporary WAN partner named "Leased Line, Slot 3 (0)" would be created.



To edit the settings for this partner locate the appropriate "Leased Line" partner interface from the **WAN PARTNER** → menu. Information on the WAN partners menu is found on page 128.

How do I configure Dynamic Short Hold?



Before you begin

ISDN calls are normally not charged according to the exact length of the connection in seconds, but rather according to a coarser grid of charging units—which can be anything from a few seconds to several minutes in length, depending on the target you are calling, the time of day, etc.—the fixed solution mentioned above is not flexible enough to adapt the Short Hold timer to the changing charging unit lengths.

You can, however, configure your BRICK to adapt the short hold timer dynamically depending on the actual lengths of the call charge units (*Dynamic Short Hold*).

Info: To be able to use the Dynamic Short Hold your ISDN access must have the AOCD (advice of charge during the call^a) feature activated.



If you are not sure whether AOCD is activated for your ISDN access, there is an easy way to verify it.

Go to the [*Monitoring and Debugging*][*ISDN Monitor*] menu of the Setup Tool while an outgoing ISDN call is active. If the *Charge* field for this call remains empty until the end of the call, no advice of charge was received during the call.

a. Called “Übermittlung der Tarifeinheiten während der Verbindung” in Germany



Configure it

(p. 57) **WAN PARTNER** → **ADD** → **ADVANCED SETTINGS** → **Set Percentage**

Dynamic Short Hold is activated by specifying a percentage of the charge unit length (*ChargeInterval*).

As a default, Dynamic Short Hold is *not* active (0%).

- For *interactive connections* (e.g. telnet) you should specify a rather high Dynamic Short Hold percentage (e.g. 80-90) to avoid frequent disconnects due to short periods of inactivity.
- For *internet connections* (WWW, http, etc.) you should specify a medium to high Dynamic Short Hold percentage (e.g. 50-80) to avoid frequent disconnects due to waiting periods.

- For *data connections* (e.g. ftp) you should specify a low Dynamic Short Hold percentage (e.g. 10-40) to avoid unnecessarily waiting—and incurring charges—once a transfer is complete.



If configured, the Static Short Hold timer will *always* take precedence over Dynamic Short Hold to avoid permanent connections.

Make sure to set the Static Short Hold to a value greater than the length of a charging unit if you want Dynamic Short Hold to have any effect.


For example, in Germany there are different maximum charging unit lengths for different tariff zones (City = 4 minutes, long distance calls = 2 minutes), so you can set the *Static* Short Hold to 245 (>4 minutes) for City connections, and to 125 (>2 minutes) for long distance calls, to avoid nullifying your Dynamic Short Hold settings.

Once the Dynamic Short Hold inactivity time is reached, the connection will be kept up until shortly before the next advice of charge is expected, thus maximizing the connection time without any additional cost.

This mechanism will not work properly for the first charging unit with a radically changed length once a new tariff zone is entered, which may result in a few inefficiently used longer charging units.

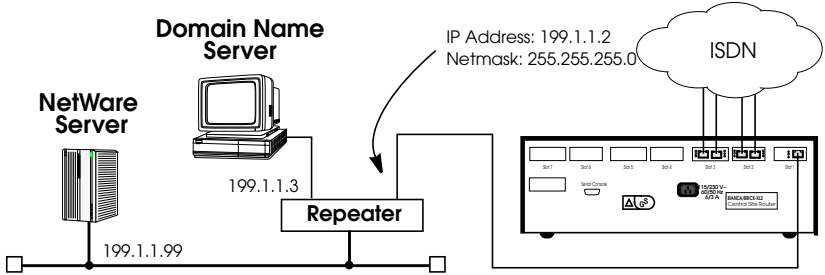
How do I configure my X.21 interface?

The CM-X.21 communications module can be used to access a public (Datex-P in Germany) or private X.25 networks. Configuring the X.21 hardware interface simply involves settings the mode, DTE (Data Terminal Equipment) or DCE (Data Circuit-Terminating Equipment) the BRICK should operate in at Layers 1 and 2.

This setting to use here will depend on the type of network this interface is connected to. The  menu shown on page 48 is used to configure these settings.

How do I configure my Fast Ethernet interface?

Configuring the BRICK's Fast Ethernet interface is straight forward and involves telling the BRICK a few things about the LAN attached to this interface. This will include the IP address and netmask to use and the type of header to apply to ethernet frames.



Before you begin

You'll need to know the following information about your LAN.

- IP address and netmask the s LAN port will be assigned.
- Domain name and IP address of your Domain Name Server.



Configure it

(p110)

MONITORING AND DEBUGGING

MESSAGES

Auto-Config

First, verify that no error messages regarding the ethernet interface appear shortly after bootup. Look for system messages beginning with "**Ether: slot X...**" (where X is the slot where the slot for your CM-100BT module). The CM-100BT's UTP port supports both 10 or 100 Mbps ethernet. In most cases the BRICK will be able to determine the best speed to operate in automatically.

If problems occurred detecting/configuring the LAN port refer to Chapter 2 ([Connecting the BRICK to the LAN](#)) for more information.

(p. 39)

CM-100BT, FAST ETHERNET

IP Address and Subnet Mask

In the IP-Configuration section you'll need to set the following:

local IP-Number
local Netmask
Encapsulation

<IP address on the Ethernet>
<subnet mask used on this LAN>
Ethernet II

Only configure the settings in the IPX-Configuration section if you will be using the BRICK as an IPX router. The Bridging option can also be enabled if the BRICK will be bridging traffic between this LAN and dialup network connections.

(p. 39) **CM-100BT, FAST ETHERNET** → **ADVANCED SETTINGS** → **RIP Settings**

The types of Routing Information Protocol packets sent/received by the BRICK should be defined here. (The type of RIP support can be configured independently for each interface.)

RIP Send	<type(s) of RIP packets to send>
RIP Receive	<type(s) of RIP packets to accept >
IP Accounting	off
Proxy ARP	off
BackRoute Verify	on

Do not enable IP Accounting for the LAN interface if you intend to log accounting information with a host accessible via this interface.

The Back Route Verify option in this menu can be optionally enabled to protect the BRICK from packets sent with a potentially fake source address. Select **SAVE** and return to the main menu.

(p. 70) **IP** → **STATIC SETTINGS** → **Nameserver Settings**

Here you'll need to set the BRICK's domain name and IP address of the primary (and optionally a secondary) nameserver.

Domain Name	<BRICK's Domain Name>
Primary Domain Name Server	<numeric IP address of primary>
Secondary Domain Name Server	<numeric IP address of secondary>

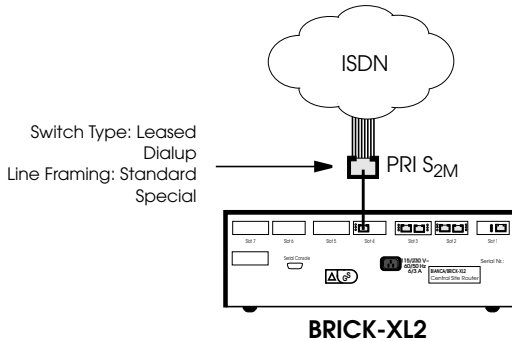
For information on the other fields shown in this menu, refer to Chapter 4.

How do I configure my token ring interface?

Configuring the CM-TR token ring module is almost identical to configuring ethernet interfaces as mentioned above. For token ring interfaces however, the Ring Configuration must additionally be set. This defines the speed the ring operates at and whether to use Early Token Release.

How do I configure my primary rate interface?

For the BRICK to access the ISDN via a primary rate interface (PRI) the router must be outfitted with a BIANCA/CM-PRI communications module. Only two settings are required to configure the hardware interface for the BIANCA/CM-PRI. These include the Switch Type and the Line Framing to use.



Info: In most cases the appropriate switch type and the proper Line Framing to use are automatically configured by the BRICK at boot time and don't need to be set manually

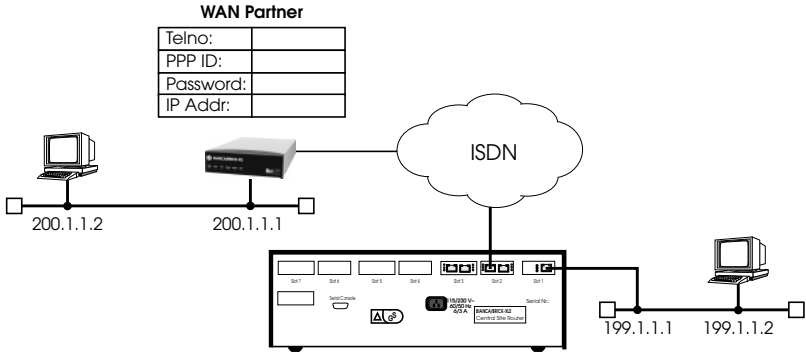
The Switch Type and ISDN Line Framing parameters are configured in the **CM-PRI, ISDN S2M** → menu.

Once the hardware interface is configured (or autoconfigured at boot time) you can begin to configure ISDN WAN partners that can use the B-channels provided by your PRI to establish networking connections. Information on configuring WAN partners is found on page 128.

IP Features

How do I configure dialup TCP/IP access for an ISDN partner?

This is the most common task for sites wanting to connect a remote IP host or LAN via a dialup ISDN line. The remote WAN partner may be an IP host or router/bridge and is configured in Setup Tool as follows.



Before you begin

You'll need the following information about your WAN partner.

- ISDN telephone number to use.
- If PAP or CHAP authentication is used: The partner's PPP ID and PPP password the BRICK will use for authentication.
- IP Address and Netmask (if non-standard mask is used)



Configure it

(p. 50) **WAN PARTNER** → **ADD** →

Create Partner Interface

First, you'll need to define a unique name to identify this dialup partner and select a compatible encapsulation protocol depending on the type of traffic the BRICK will route over the link. (See the table on page 29 for a list of encapsulations and supported protocols).

Partner Name	testPartner
Encapsulation	PPP
Calling Line Identification	<yes or no>

The Calling Line Identification field is set automatically, once an “incoming” (or “both”) ISDN number is configured in the next step.

(p. 52) **WAN PARTNER** → **WAN NUMBERS** → **Configure WAN Number**

Now, in the WAN Numbers submenu, select ADD to configure the dial-up partner’s ISDN telephone number that should be used for establishing the link.

Number	78345
Direction	both (CLID)
Advanced Settings >	
ISDN Ports to use	<X> Slot 2, ISDN S0<X> Slot 3, ISDN S0

If multiple ISDN stacks are available on your system (CM-2xBRI, CM-PRI, etc) then you must also define which ISDN interfaces may be used for calls to or from this partner. The select SAVE, then EXIT to return to the main WAN Partner menu.

(p. 55) **WAN PARTNER** → **PPP** → **PPP Settings (partner-specific)**

Next, edit the fields in the WAN Partner’s PPP submenu to define the PPP Setting to use with the new partner.

Authentication	CHAP + PAP
Partner PPP ID	<remote partner’s PPP ID>
Local PPP ID	<BRICK’s PPP ID>
PPP Password	<remote partner’s password>

Then select OK, and return to the main WAN Partner menu.

(p. 61) **WAN PARTNER** → **IP** → **IP Settings (partner-specific)**

Here, we need to configure the IP address for the WAN partner interface. A static address (with or without a transit network) or a dynamic address may be configured.

Transit Network	no
Partner’s LAN Address	192.168.54.0
Partner’s LAN Netmask	255.255.255.0

“Dynamic client” specifies that the BRICK accepts it’s own address for this interface from the remote partner. If the BRICK should assign this partner an address dynamically, select “dynamic server” under

Transit Network and make sure there are IP addresses configured for the Pool ID specified in the **ADVANCED SETTINGS** → submenu.

See page 83 for information about creating IP Address Pools. For sites that need to use a transfer network, please see page 68 for more information.

More Info

There are several partner-specific features that can be configured under the **WAN PARTNER** → **ADVANCED SETTINGS** → menu such as Short Hold, Channel Bundling, and Callback Support. Using these features is optional and fairly straight forward. See the menu descriptions beginning on page 57 in Chapter 4 for more detailed information.

How do I configure Dialup Access to CompuServe Online Services

To allow for dialup connections to CompuServe Online Services two additional encapsulation methods have been added to the *biboPPP*Encapsulation variable:

- x75_ppp** async PPP over X.75
- x75btX_ppp** async PPP over X.75/T.70/BTX (T-Online)

These settings can be used to enable the BRICK to dial into a CompuServe Network Node directly (*x75_ppp*) or to access CompuServe indirectly through T-Online's CompuServe Gateway (*x75btX_ppp*).

Configure it

(p. 50) **WAN PARTNER** → **ADD** →

Create Partner Interface

- | | |
|---------------|---------------------|
| Partner Name | cis |
| Encapsulation | Async PPP over X.75 |
| Compression | none |
| Encryption | none |

(p. 52) **WAN PARTNER** → **WAN NUMBERS** →

Configure WAN Number


- | | |
|------------|--------------------------|
| WAN Number | <CIS's telephone number> |
| Direction | outgoing |

Then select SAVE, then EXIT to return to the main WAN Partner menu.

(p. 60) **WAN PARTNER** → **ADVANCED SETTINGS** → **PROVIDER CONFIGURATION** → **CIS**

Provider	Compuserve Network
Host	CIS
User ID	<your CIS member ID>
Password	<your CIS password>

Note that this information is required and is used to generate the *biboPPPLoginString* variable automatically .

Info:  When accessing CompuServe through the T-Online Gateway using the “Async PPP over X.75/T.70/BTX” encapsulation make sure to use the ISDN number 01910 to get local charging tariff.

Then select OK twice to return to main WAN Partner menu.

(p. 61) **WAN PARTNER** → **IP** → **IP Settings**

To allow the BRICK to accept it’s IP address dynamically from CompuServe Network, make sure “dynamic client” is set here.

IP Transit Network	dynamic client
--------------------	----------------

(p. 60) **WAN PARTNER** → **ADVANCED SETTINGS** → **Short Hold Timer**

Because call setup and negotiation with some online providers may take longer, you may want to increase the ShortHold timer to 100 seconds (20 is the default) or more.

Static Short Hold (sec)	20
-------------------------	----

How do I configure the BRICK to accept its IP address dynamically?

The BRICK can be configured to accept its IP address dynamically (i.e. client mode) from an ISDN dialup partner that acts as the IP address server. ISPs (Internet Service Providers) commonly assign their customers' IP addresses dynamically at connection time, allowing them to reduce their required address space.

! Configure it

(p. 61) **WAN PARTNER** → **ADD** →

Configure WAN Partner

The WAN partner that assigns the BRICK an IP address is configured just like any other WAN partner. First define the encapsulation type to use, and whether compression and/or encryption will be used over the link.

Define the partner's ISDN number in the **WAN NUMBERS** → submenu. Configure the relevant PPP settings in the **PPP** → submenu.

(p. 61) **WAN PARTNER** → **IP** →

Dynamic IP Address Setup

To allow the BRICK to accept its IP address dynamically from the remote side of the link, make sure "dynamic client" is set here.

IP Transit Network dynamic client

Select SAVE to return to the main WAN partner menu.

(p. 68) **IP** → **ROUTING** → **ADD** →

Add a Default Route

Next, create a default route for the WAN partner interface.

Route Type	Default route
Network	WAN without transit network
Partner / Interface	<partner interface name>

In the Partner/Interface field you should be able to select (using the spacebar) the partner interface created in the previous step. Select SAVE and then EXIT.

? More Info

In most cases configuring the BRICK to accept its IP address dynamically is helpful when NAT is being used. To configure NAT (with or without dynamic IP address assignment) see page 134.

How do I configure the BRICK as a dynamic IP address server?

The BRICK can be configured as an IP address server that assigns IP addresses to ISDN dialup partners at connection time. Upon accepting a dialup connection from a client, the BRICK assigns the host an IP address from a pool of pre-configured addresses. Then a host route is added to the IP route table. Once the dialup connection closes, the IP address is returned to the pool, and the IP route is deleted.



Before you begin

You'll need the following information.

- One or more IP addresses to put in an address pool.



Configure it

(p. 83) **IP** → **DYNAMIC IP ADDRESSES** → **ADD** → **Address pool**

Define the set of IP addresses the BRICK should use for dialup clients.

Pool ID	0
IP Address	<1st address in the block>
Number of consecutive addresses	<total # of addresses>

If you don't have a complete block of available addresses you'll have to assign each address individually.

(p. 50) **WAN PARTNER** → **ADD** → **Dialup Clients**

Here you'll need to set:

Partner Name	<Unique Partner Name>
Encapsulation	<select an IP compatible method>

(p. 52) **WAN PARTNER** → **WAN NUMBERS** → **Configure WAN Number**

WAN Number	<partner's ISDN telephone number>
Direction	both (CLID)

Select SAVE, then EXIT to return to the main WAN Partner menu.

(p. 55) **WAN PARTNER** → **PPP** → **PPP Settings (partner-specific)**

Next, edit the fields in the WAN Partner's submenu to define the PPP Setting to use with the new partner.

Authentication	CHAP + PAP
Partner PPP ID	<remote partner's PPP ID>

Local PPP ID	<BRICK's PPP ID>
PPP Password	<remote partner's password>

Select OK, and return to the main WAN Partner menu.

(p. 61) **WAN PARTNER** → **IP** → **Dynamic IP Address Setup**

To have the BRICK assign this caller an available IP address at connection time, make sure "dynamic server" is set here.

IP Transit Network	dynamic server
--------------------	----------------

(p. 62) **WAN PARTNER** → **IP** → **ADVANCED SETTINGS** → **Specify Pool ID**

The BRICK will retrieve a free IP address from the Pool specified here. This should be the same pool you created in the first step.

Select OK and then SAVE to return to the main WAN partner menu.

How do I configure Internet access for my LAN using NAT?

Using NAT, or Network Address Translation, the BRICK can connect your LAN to the Internet using a single IP address. This IP address can be a static address or dynamically assigned by your Internet Service Provider (ISP) at connection time. The beauty of using NAT is that you don't need an official IP address for every host on the LAN and NAT provides you a built-in firewall that protects your LAN from intruders.



Before you begin

You'll need the following information provided by your ISP.

- Your ISP's ISDN telephone number.
- The PPP ID of the system your BRICK will dial into.
- The BRICK's PPP Password.
- An IP address (not needed if assigned dynamically).



Configure it

(p. 50) **WAN PARTNER** → **ADD** → **Configure ISP interface**

First configure a new PPP interface. Here you'll need to set:

Partner Name	<Name of Internet Service Provider>
Encapsulation	PPP

(p. 52) **WAN PARTNER** → **WAN NUMBERS** → **Configure WAN Number**

Add the ISDN number to use for setting up the link to this partner.

WAN Number	<partner's ISDN telephone number>
Direction	outgoing

Select SAVE, then EXIT to return to the main WAN Partner menu.

(p. 55) **WAN PARTNER** → **PPP** → **PPP Settings (partner-specific)**

Configure the PPP settings for the PPP link here.

Authentication	CHAP + PAP
Local PPP ID	<BRICK's PPP ID>
PPP Password	<remote partner's password>

Select OK, and return to the main WAN Partner menu.

(p. 61) **WAN PARTNER** → **IP** → **Dynamic IP Address Setup**

Here, configure the IP address assigned by your ISP. If your address is assigned dynamically all you need to do here is set IP Transit Network to "dynamic client". Otherwise set the fields as follows:

IP Transit Network	yes
Local ISDN IP Address	<BRICK's static IP address>
Partner's ISDN IP Address	<BRICK's static IP address>

Select SAVE and return to the main WAN Partner menu.

Select SAVE again to add the new partner interface to the system.

(p. 73) **IP** → **Network Address Translation** → **Enable NAT**

In this menu select the ISP interface you just configured from the list and enter <Return>. With the spacebar enable NAT for this interface.

Network Address Translation on

Now configure the types of incoming connections you want to allow. Under **ADD** specify the internal host, and services to allow. You might want to allow access to an FTP server on the LAN.

Service	ftp
Destination	<IP address of your FTP server>

Select SAVE. When you are finished adding sessions select SAVE again, and then EXIT to Setup Tool's main menu.

(p. 68) **IP** → **ROUTING** → **ADD** →

Setup IP Routing

All that's left to do now is to add a default route to your ISP.

Route Type	Default route
Network	WAN without transit network
Partner / Interface	<ISP interface name>

? More Info

Additional Routing Settings: Note that routing settings on some workstations on your LAN may need to be modified to include a default route that specifies the BRICK's LAN address. Check your operating system's instructions to see what changes need to be made.

- On most UNIX workstations, you can add the route with:
`route add default <BRICK's LAN Address> 1`
This may not be needed if the workstation understands RIP. It will learn about new routes from the BRICK every 30 seconds.
- On Windows 95 systems with Microsoft TCP/IP change "Properties–Systemcontrol–Network–TCP/IP-Properties–Gateway" and add the BRICK as the primary gateway.

Another option is to use Proxy ARP on the LAN. This can be configured under: **CM-100BT, FAST ETHERNET** → **ADVANCED SETTINGS**

How do I configure the BRICK as a RADIUS Client?

RADIUS (Remote Authentication Dial In User Service) is a client/server protocol originally developed by Livingston Enterprises. RADIUS provides a security system that allows you to exchange authentication and configuration information between a Network Access Server, such as the BRICK, and a RADIUS Server, a PC or UNIX machine running a RADIUS daemon process. The RADIUS server maintains a database of user authentication data and configuration information.



Before you begin

You'll need the following information

- The IP address of your RADIUS server.
- The RADIUS Client Key (or password).
- The UDP port number for the server's authentication service.



Configure it

(p. 87)



Create RADIUS Server Entry

This menu contains one or more RADIUS servers. Select <ADD> to create a new RADIUS server entry.

Protocol	auth
IP Address	<RADIUS Server's IP Address>
Password	<Password from /etc/radb/clients>
Priority	<0 for highest priority, 7 for lowest>
Policy	<authoritative or non-authoritative>
Port	<Server's UDP port number>
Timeout	1000
Retries	1

The BRICK is now configured as a RADIUS client and can exchange authentication and configuration information with this server. When an incoming caller can't be identified via a locally defined partner interface the RADIUS server is polled. If the server authenticates the caller, a new interface is created on demand, otherwise the connection is terminated. The characteristics of the dynamic interface must be configured on the RADIUS server (typically this is done in */etc/radb/users*). The BRICK also adds a static route for the partner. Once the

connection is closed, the interface and route are deleted. Accounting data is only sent to servers configured with *Protocol* set to "acct".

? More Info

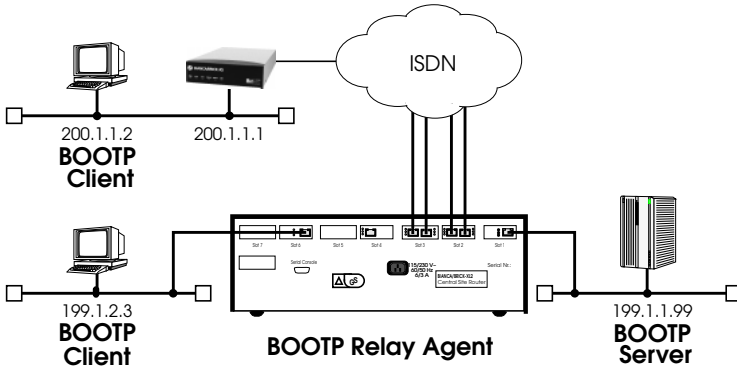
Additional information regarding RADIUS is contained in the *Extended Feature Reference* on the Companion CD. As a quick reference the BRICK supports the following RADIUS attributes which can be used in the RADIUS server's user database. For configuration information relating to your RADIUS server refer to you local documentation.

RADIUS Attribute	Type	R / A	Remark
User-Name	string	REQ	User name, mandatory inband: PPP partner name outband: PPP partner telephone number
User-Password	string	REQ	Password for PAP authentication
CHAP-Password	string	REQ	Password for CHAP authentication
NAS-Identifier	string	REQ	sysName of the BRICK
Service-Type	integer	ANS	Framed (for PPP) Callback-Framed (for PPP with Callback)
Framed-Protocol	integer	ANS	inband: PPP outband: PPP, X25, X25-PPP, IP-HDLC, IP-LAPB, MPR-LAPB MPR-HDLC, FRAME-RELAY, X31-BCHAN, X75-PPP, X75BTX-PPP, X25-NOSIG, X25-PPP-OPT
Framed-IP-Address	ipaddr	ANS	Partner IP address
Framed-IP-Netmask	ipaddr	ANS	Partner IP netmask
Framed-Routing	integer	ANS	None, RIPV1-Broadcast, RIPV1-Listen, RIPV1-Broadcast-Listen
Framed-Compression	integer	ANS	None, Van-Jacobson-TCP-IP
Framed-Route	string	ANS	You can create a route of the format 'ipaddr[/netmask bits] gateway' [metric1]...[metric5] e.g.: 192.2.3.4/24 193.141.54.1 1

RADIUS Attribute	Type	R / A	Remark
Idle-Timeout	integer	ANS	Shorthold
Port-Limit	integer	ANS	Number of B channels (== MaxConn)
Reply-Message	string	ANS	outband: ifDescr is set to this name (instead of using the telephone number)
Callback-Number	string	ANS	telephone number for Callback

How do I configure the BRICK as a BOOTP relay agent?

BOOTP, the Bootstrap Protocol, defines how a host on a TCP/IP network can get its IP address and other information required at startup from another computer. The requesting host is the BOOTP client, the computer providing the information is the BOOTP server. Since the server only hears requests on directly connected LAN segments its sometimes useful to have a BOOTP relay agent forward requests/responses between the clients and server.



Before you begin

To configure the Relay Agent all you need is the server's IP address.



Configure it

(p. 70) **IP** → **STATIC SETTINGS** →
BOOTP Relay Server

Set BOOTP Server Address

<server's IP Address>

The BRICK will now forward all BOOTP requests received over any of its interfaces (WAN or LAN) to the server.

(p. 50) **WAN PARTNER** → **ADD** →

(optional) WAN Partner

If the server or client is accessible via a dialup link, the appropriate WAN partner must also be configured before the BRICK can contact or respond to the server or client.

IPX Features

How do I connect my local and remote IPX networks over ISDN?

IPX (Internet Packet Exchange protocol) was developed by Novell and is a network layer protocol similar to IP in the TCP/IP world. An IPX network allows DOS/Windows PCs (or stations) to share networked services and devices. Stations on IPX networks are classified as a server or client.



Before you begin

Before you start you'll need the following information.

- A unique IPX System Name for the BRICK.
- IPX Network Numbers for the local LAN, and if required by the remote router, a network number for the WAN link.
- Your remote IPX router's telephone number.
- Remote router's PPP ID and Password if authentication is used.
- An Internal IPX Network Number for the BRICK if the default value is already in use.



Configure it

(p. 33) **LICENSES** →

Verify License

Verify the IPX subsystem is valid.

(p. 39) **CM-100BT, FAST ETHERNET** →

Configure LAN interface

Enter the IPX Network Number of the LAN attached to this interface.

Local IPX-NetNumber <IPX Network Number>

Info: Normally, your LAN module is installed in slot 1. Select the appropriate hardware interface depending on your local installation.



(p. 50) **WAN PARTNER** → **ADD** →

Create new WAN Partner

Create a new WAN partner for the remote IPX router the BRICK should call.

Make sure the IPX protocol is enabled and select an appropriate encapsulation method; in most cases "PPP" will be fine.

(p. 64) **WAN PARTNER** → **ADD** → **IPX** → **Partner specific IPX settings**

Set the IPX specific settings for this interface.

Enable IPX	yes
IPX NetNumber	0
Send RIP/SAP Updates	triggered + piggyback
Update Time	60

Info: Set the WAN link's IPX Network Number if the remote router requires it. This is not required if the remote side is also a BRICK.



Set the RIP/SAP update behaviour here. In most cases the default settings (triggered + piggybacked updates at 60 seconds) should be fine.

(p. 90) **IPX** → **Global IPX protocol Settings**

Define the BRICK's Local System Name for IPX. To save on ISDN charges it is recommended that you enable IPX/SPX SPX spoofing and set NetBIOS Broadcast replication.

Local System Name	BRICK
enable IPX spoofing	yes
enable SPX spoofing	yes
NetBIOS Broadcast replication	on LAN only

Info: If the default Internal Network Number used by the BRICK is already in use by another router, change its value here. (see the 'ipx internal net' command on your NetWare server).



? More Info

The ipxping command is available from the SNMP shell and can be used to test routing connections between the BRICK and remote IPX servers.

If you're having problems with routing or ISDN connections relating to your IPX networks, refer to the section IPX Routing in Chapter 6 Troubleshooting.

Modem and Fax Features

How do I configure my BRICK-XL2 as a Central Site Modem Server?

In this example we will show you how to set up your BRICK as a modem server for *incoming* connections, where the callers receive their IP addresses and name servers from the BRICK.

Info: This example—of course—only works, if you have at least one FML-8MOD modem module installed in your BRICK.



Before you begin

Before you start you'll need the following information.

- Your communications partners' PPP IDs.
- The PPP password for each partner.
- The ISDN telephone number of your BRICK to use for incoming modem calls.



Configure it

(p. 50) **WAN PARTNER** → **ADD** →

Create Partner Entry

Here you'll need to set:

Partner Name	<Unique Partner Name>
Encapsulation	PPP

(p. 55) **WAN PARTNER** → **PPP** →

PPP Settings (Dial-In Users)

Configure the PPP settings for the PPP link here.

Authentication	CHAP + PAP
Partner PPP ID	<WAN partner's PPP ID>
Local PPP ID	<BRICK's PPP ID>
PPP Password	<remote partner's password>

Select SAVE and continue.

(p. 57) In the **ADVANCED SETTINGS** → submenu, and change the following settings (leave the rest at their default values).

Callback	no
Static Short Hold (sec)	3600

Confirm the settings with *OK* to return to the WAN Partners menu.

(p. 62) In the **IP** → submenu, set IP Transit Network field to “dynamic server”.

IP Transit Network	dynamic server
--------------------	----------------

(p. 62) In the **IP** → **ADVANCED SETTINGS** → submenu, change the following settings (leave the rest at their default values).

RIP Send	none
RIP Receive	none
Van Jacobson Header Compr.	on
IP Address Pool	<any Pool with free addresses>

Info: The Pool ID specified must be contain one or more addresses. Page 82 contains information on configuring IP Address Pools.



Confirm your settings with *OK* and then *SAVE*.

(p. 95) **MODEM** → **PROFILE CONFIGURATION** → **(optional) New Modem Profile**

This step sets up a separate modem profile for callers with fast K56flex modems. If all (or most) of the callers use V.34 modems (up to 33,600 bps) you can simply use the default profiles, which will carry out automatic speed and modulation negotiations.

Select Profile 2. Leave Profile 1—which is the default profile for all modem connections where no specific profile is defined—as it is for the time being. For a K56flex profile change the following entries.

Description	K56flex hi-speed
Modulation	K56flex
Error Correction	auto
Min Bps	300
Max Receive Bps	33600
Max Transmit Bps	56000

[*SAVE*] the profile.

You can also modify the other profiles to fit your demands.

(p. 47) **CM-PRI, ISDN S2M** → **INCOMING CALL ANSWERING** → **Call Dispatching**

Select ADD to create a new entry.

Item	PPP Modem Profile 2
Number	<your BRICK's ISDN number>
Mode	left to right (DDI)

Info: S_{2M} access plus the dial-in number you want to use for this modem profile.



SAVE the entry. ADD another using a *different* Number for Modem Profile 3. Callers with K56flex modems can now use the first number, and all other callers can use the second number.

How do I enable outgoing modem calls?

To enable outgoing modem connections to certain partners, e.g. for use with the Callback feature, go to Setup Tool's

(p. 50) **WAN PARTNER** → **EDIT** → **Modify WAN Partner**

Edit the existing WAN partner configuraion.

In the **WAN NUMBERS** → submenu select ADD to add an outgoing number where this partner can be reached at for modem calls.

Select SAVE, and then EXIT.

Then go to the **ADVANCED SETTINGS** submenu, and enable the features you need, e.g. enable Callback if desired, or reduce the Static Short Hold time, so that outgoing connections do not need one hour to time out, etc.

Lastly, select an appropriate modem profile ("Modem Profile 1" ... Modem Profile 8") you want to use with this partner in the "Layer 1 Protocol" field.

Select OK, and then SAVE to exit to the main WAN partner's menu.

Now the partner can also be called using one of your BRICK's modems.

How do I configure fax service from RVS-COM

Note: If you want to install RVS-COM Lite, contact RVS Datentechnik GmbH as you require a separately purchased license. You can retrieve the address from RVS-COM Lite's online help.



Info: If you work with the softfax solution when faxing with your router and RVS-COM Lite, the fax software must always be started when you want to receive faxes. On installing RVS-COM Lite, RVS-COM is stored in the Windows Taskbar – as long as you do not close the program, RVS-COM is available at all times.



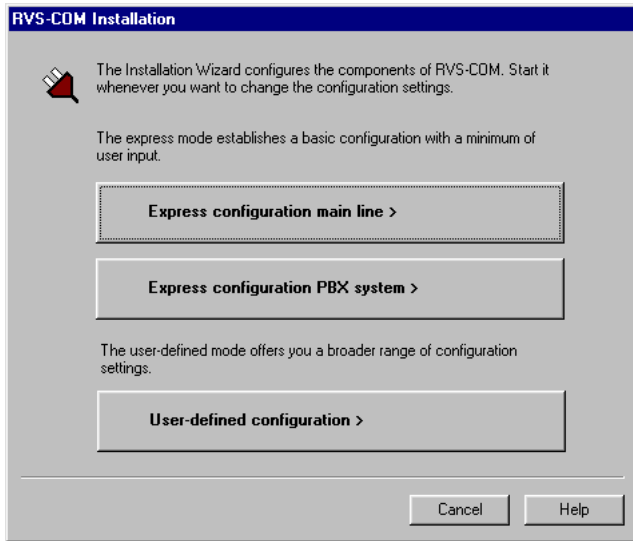
On BRICK XL2 systems you may disable the Softmodem option in the RVS CommCenter and use hardware fax with the corresponding fax hardware.

TIP: Since this solution involves adding the RVS Fax service as an additional e-mail transport service, the Windows e-mail system should already be installed and configured.

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

1. First, install RVS-COM Lite and BRICKware for Windows to your PC from the Companion CD. The Remote CAPI client must also be configured and involves assigning the TCP port and IP address of your BRICK.
2. From the RVS-COM for Windows and Windows 95 program group, start the Installation Wizard. The Wizard guides you

through setting up RVS-COM components on the PC.



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

- make sure your router is connected to your ISDN connection.
 - make sure your Remote CAPI configuration is configured as described.
3. Choose an installation method, for example **User-Defined Configuration**.
 4. If a message appears saying you should change the dialing properties (e.g. area code, exchange number), adjust the settings.
 5. Continue until you will be asked to enter the telephone numbers used by your BRICK with an MSN. Specific RVS-COM services are

associated with these numbers in the next dialog in the User-Defined Configuration. Click Next>.

RVS-COM Installation: ISDN Phone Numbers

Please enter your ISDN phone numbers which will be used to accept calls with RVS-COM.
Do not enter country or area codes.

Enter the corresponding MSN for each phone number, if the MSN is not the the full number.

Phone number MSN1:	<input type="text" value="9723"/>	MSN:	<input type="text" value="1"/>
Phone number MSN2:	<input type="text" value="9724"/>	MSN:	<input type="text" value="2"/>
Phone number MSN3:	<input type="text" value="9725"/>	MSN:	<input type="text" value="3"/>

In most cases the MSN is the full phone number; you can then leave the MSN fields empty. However, for some PBX systems you need only specify the extension, and not the full number.

Please consult the manufacturers' manual of your ISDN adapter and ask for information about the special features of your ISDN line, if necessary.

< Back Next > Cancel Help

6. Associate the MSNs defined above with a specific service. This is required so that incoming calls dispatched by the BRICK can be automatically answered by the appropriate RVS-COM service on your PC. As noted in the dialog, you can only activate 1 analog and 1 digital service for each available MSN.

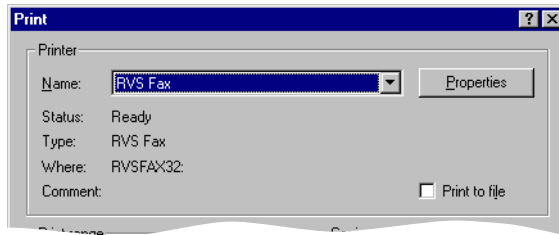
Click Next>. The ISDN Phone Numbers component is configured.

7. Now you need to enable the RVS Inbox or another E-Mail Service. Incoming and outgoing faxes are saved as messages that can be displayed by the RVS Inbox or by the mail reader. Note that some mail programs may need to be restarted before the RVS FAX driver is acknowledged.

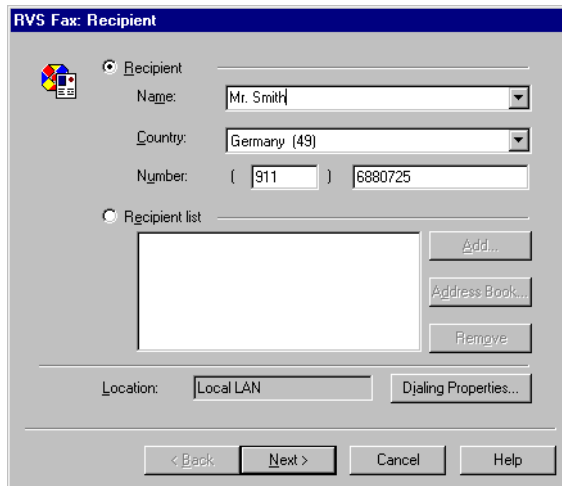
Faxing from MS Applications via RVS Fax

Once the RVS-COM components are configured outgoing faxes can be sent from any MS application that has access to the Windows printing system. From the application the document to be faxed as follows.

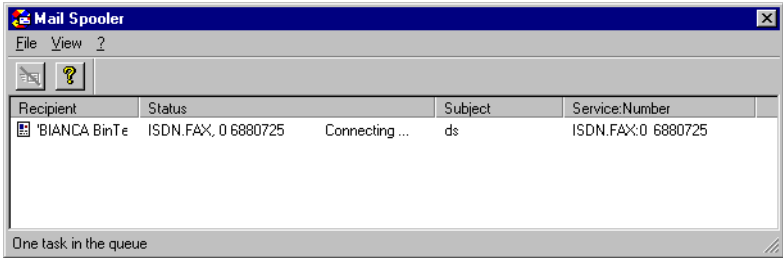
1. From the application menu select the File option then Print...
2. In the Printer section of the print setup dialog, select the printer name **RVS Fax**.



3. The RVS Fax Assistant is then started. The parameters for this fax can be defined here.



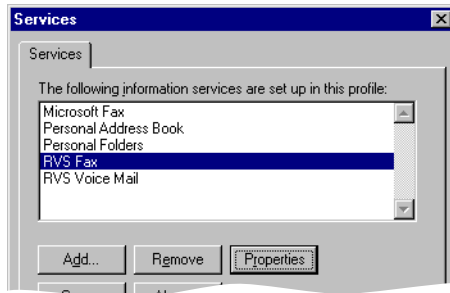
4. The new fax is then spooled to the Mail Spooler which shows the status of the fax transmission.



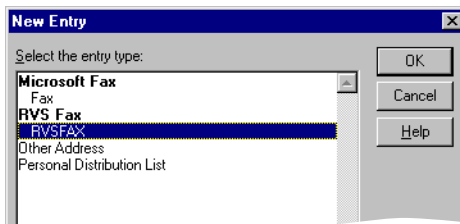
Faxing from Microsoft Exchange

With the RVS-COM components configured as noted above, faxes can also be sent directly from Microsoft Exchange. By creating the appropriate addressbook entries (shown below) fax messages from Exchange are sent just like sending email messages.

1. In Microsoft Exchange's Services menu the following services should be listed. Verify that RVS Fax service is available here.



2. An AddressBook entry can be created by selecting: Tools→Addressbook→New Entry from Exchange's main menu. Select RVS Fax and click OK



3. Select the RVS Fax tab to associate a Fax number with this addressbook entry. When email messages are sent to this addressbook en-

try the messages will be spooled to the mail spooler where the connection status of the fax transmission is displayed.

The image shows a Windows-style dialog box titled "New RVSFAX Properties". It has four tabs: "Business", "Phone Numbers", "Notes", and "RVSFAX - Fax". The "RVSFAX - Fax" tab is selected. The dialog is divided into two main sections: "Name" and "Faxnummer".

In the "Name" section, there are two text input fields: "Vorname:" containing "BIANCA" and "Nachname:" containing "BinTec".

In the "Faxnummer" section, there is a "Land:" dropdown menu set to "Germany (49)" and a "Nummer:" field containing "(911)" followed by "6880725".

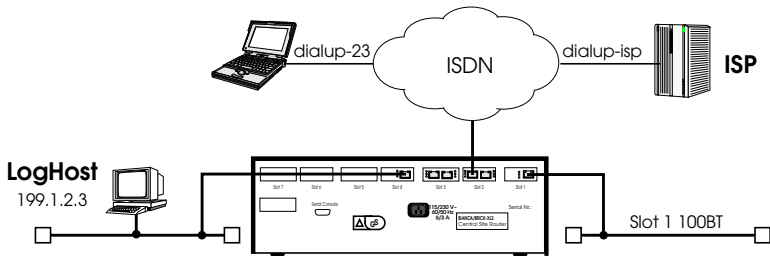
At the bottom of the dialog, there are four buttons: "OK", "Cancel", "Apply", and "Help".

General

How can I retrieve accounting information (ISDN and TCP/IP)?

Various system messages are generated on the BRICK based on different events. Accounting messages are a subset of these messages. The BRICK can be configured to forward accounting messages (as well as other messages) to remote Log Hosts (PCs or UNIX systems). Two types of accounting messages are currently used.

- **ISDN Accounting**—contains information relating to ISDN connections such as duration of call, called and calling number, charging information, and error causes.
- **IP Accounting**—contains information relating to IP sessions such as source and destination addresses, IP protocol and port numbers, session duration, and amount of traffic sent/received.



Before you begin

To forward accounting messages to a remote Log host all you need is:

- The IP address of the LogHost.



Configure it

(p. 39) **CM-100BT, FAST ETHERNET** → **ADVANCED SETTINGS** → **LAN Interfaces**

Turn on IP accounting for each LAN interface you want the BRICK to generate IP accounting messages for.

IP accounting on

(p. 57) **WAN PARTNER** → **IP** → **ADVANCED SETTINGS** → **WAN Interfaces**

Turn on IP accounting for each IP-capable WAN interface you want the BRICK to generate IP accounting messages for.

IP Accounting on

(p. 36) **SYSTEM** → **EXTERNAL SYSTEM LOGGING** → **Add Log Host**

Here's where you add (or change) remote hosts the BRICK should send system messages to.

Loghost	<IP address of host>
Level	info
Facility	<syslog facility used by log host>
Type	accounting

If the Log Host is a PC running Windows, then DIMETools must be installed there. See your BRICKware documentation for info on DIME Syslog. For UNIX hosts this facility must correspond to the syslog facility (local 0 – 9) configured there. See the man pages for syslog.conf.

Info: Do NOT turn IP accounting on for interfaces that you are sending system logging messages over. Since the sending of a message requires a UDP connection this must be heeded to avoid an endless cycle of connections.



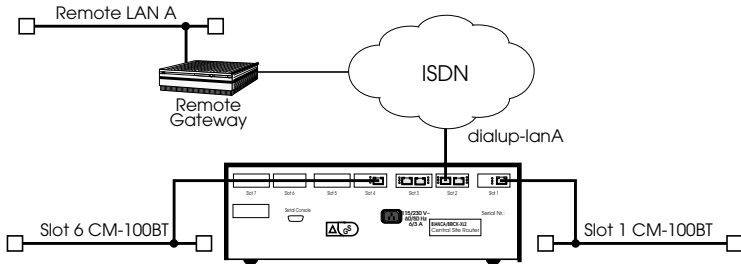
? More Info

You don't have to configure individual Log Hosts to actually see accounting messages. If you just want to browse accounting messages you can begin to see accounting messages accumulate under Setup Tool's

MONITORING AND DEBUGGING → **MESSAGES** listing once one or more interfaces are turned on. Accounting messages are identified by the **ACCT** string under the **Subj** column.

How can I Bridge two LANs over ISDN?

The BRICK can be configured to operate as a Bridge that forwards all packets from one LAN interface to another LAN. The destination LAN may be accessible over ISDN via a remote router or bridge, or directly connected to the BRICK.



Before you begin

To bridge two LAN segments over ISDN you will need the following:

- The remote gateway's IP address.
- The remote gateway's ISDN telephone number.
- The remote gateway's PPP ID (only if PAP or CHAP is used).
- The BRICK's PPP Password (only if PAP or CHAP is used).



Configure it

(p. 50) **WAN PARTNER** → **ADD** →

Configure Gateway

Configure the remote gateway as a new WAN partner.

Partner Name <unique interface name>
Encapsulation PPP

Then, in the **WAN NUMBERS** → submenu set

WAN Number <gateway's ISDN number>
Direction both (CLID)
ISDN Ports to use <specify which ISDN portsto use>

(p. 55) In the **PPP** → submenu configure the PPP parameters for authenticating connections with the remote gateway.

Authentication	CHAP + PAP
Partner PPP ID	<gateway's PPP ID>
Local PPP ID	<BRICK's PPP ID>
PPP Password	<gateway's password>

Then select OK, and return to the main WAN Partner menu.

(p. 65) And in the **BRIDGE** → submenu, enable bridging for this partner.

Enable Bridging	yes
-----------------	-----

(p. 39) **CM-100BT, FAST ETHERNET** → **Enable LAN interfaces**

Next, enable one or more LAN interfaces you want the BRICK to forward packets from.

Bridging	enabled
----------	---------

Once the local interface is enabled the BRICK can begin to learn MAC addresses from remote LANs and begins to fill its forwarding table. This is particularly important when bridging over ISDN links so that unnecessary ISDN charges can be avoided.

More Info

Additional control of bridged traffic is available using special bridge filters which are similar to the Access List mechanism described on page 76. Currently, this must be configured from the SNMP shell using the *dot1dStaticAllowTable* and *dot1dStaticDenyTable*.

How can I improve security?

The BRICK offers a wide variety of features that make internetworking and remote access as easy as possible. Though providing access to your remote sites is important it's just as important to ensure your networks are secure. This section outlines some of the things to consider when looking to improve security.

Passwords

Until these settings are changed (and saved in a configuration file) the BRICK uses the following default passwords for the three logins.

- admin bintec
- write public
- read public

The write and read users have restricted powers but can still make temporary changes (see page 35). Once your system is configured you should change these settings and protect the passwords.

Dial-in Partner Authentication

When adding ISDN dialup partners in the **WAN PARTNER** → **ADD** menu it is recommended that you configure an "incoming" number (or "both") to take advantage of the **Calling Line ID** feature of ISDN. When this is done, the "Identify by Calling Number" field is set to "yes".

In addition to CLID the CHAP and PAP authentication protocols are available from the **WAN PARTNER** → **PPP** menu.

Login access via isdnlogin

The isdnlogin program can be used to login to the BRICK from a remote ISDN site depending on the Local Number you assigned to the *ISDN Login* item under **INCOMING CALL ANSWERING**.

Note that if there are no **INCOMING CALL ANSWERING** entries, OR the routing item is assigned and the *isdnLoginOnPPPDDispatch* variable (only accessible from the SNMP shell) is set to "allow", then login calls are also accepted.

Login access via X.25 PAD calls

Remote login on the BRICK is possible using PAD applications such as minipad. To disable login access via PAD calls enter the following:

From the SNMP shell enter: `x25LocalPadCall=dont_accept`

Detecting Intruders

Though it's hard to catch intruders in the act, there are a few places to look for clues. One place to look is in the BRICK's **SysLog Messages**.

The BRICK stores a limited number of messages. The best way is to setup an external Log Host and have the BRICK forward all messages to it. A LogHost can be a UNIX host (using Syslogd) or a PC (using BRICKware). Configuring the BRICK to forward messages to a LogHost is described on page 153.

Examine your BRICK's SysLog Messages from time to time to see what's happening on your system (access list violations, problems, charging information, etc).

While the BRICK is routing you can track external connections by the type of connection (ISDN or X.25 Call), interface, or by IP protocol using the **MONITORING AND DEBUGGING** → menus. See Chapter 4 beginning on page 105.

CAPI Port

You can also control access to the BRICK's CAPI port by changing the TCP port number (default 2662) or by disabling CAPI altogether. To disable CAPI

From the SNMP shell enter: `biboAdmCAPItcpPort=0`

Under Setup Tool see the **IP** → **STATIC SETTINGS** → menu.

Alternatively you can configure a separate access list to protect this port. See page 76 for configuring Access Lists.

Trace Port

Information transmitted over the BRICK's ISDN B and D-channels can be traced using bricktrace and DIME Trace. The default (7000) TCP port number can be set to 0 to disable access to the BRICK's trace port.

From the SNMP shell enter: `biboAdmTracetcPport=0`

Under Setup Tool see the **IP** → **STATIC SETTINGS** → menu.

SNMP Port

Access to the BRICK's SNMP port number can also be changed (default = 161) or disabled by setting to 0. To disable the SNMP port:

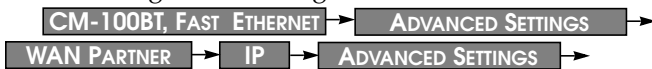
From the SNMP shell enter: `biboAdmSNMPport=0`

Under Setup Tool see the **IP** → **SNMP** → menu.

This will disable remote SNMP sessions. Configuration over telnet connections are still possible and must be controlled using Access Lists.

RIP Information

The Routing Interior Protocol is used by routers to learn (and teach) IP routes. You can control which interfaces the BRICK learns about new IP routes using the **RIP Receive** field for both Ethernet and WAN Partner interfaces using the following menus.



Even though small, outgoing RIP packets contain information about your internal networks. You can restrict the interfaces the BRICK broadcasts RIP information on using the **RIP Send** fields on the above mentioned menus. Another alternative is to disable RIP altogether by setting the RIP port (from its default value of 520) to 0.

From the SNMP shell enter: `biboAdmRipUdpPort=0`

Under Setup Tool see the **IP** → **STATIC SETTINGS** → menu.

NAT

Network Address Translation is an excellent method of controlling access to an internal network. You can configure NAT for each WAN partner interface that connects your LAN to an “unsecure” network (i.e. Internet).

Access Lists

If NAT can't be used or simply isn't enough you can always use Access Lists (with Allow and Deny Lists) to control the types of traffic to restrict

on a per-interface basis. Separate Access Lists can be used for IP, IPX, and Bridging traffic. See page 76 for information on using IP access lists.

RADIUS

Many sites use a separate RADIUS server for more advanced authentication procedures. The BRICK can be configured as a RADIUS client that polls the RADIUS server at connection time. See page 87.

Identification of ISDN dialup X.25 partners

A special Rewriting Rule for X.25 calls can be used to verify X.25 callers. This must be configured from the SNMP shell using the *x25RouteTable* and the *x25RewriteTable* as follows.

If the *RewritingField* is set (default is 0) in the *x25RouteTable*, then the X.25 route is rewritten using the respective Rule defined in the *x25RewriteTable*. The special rule is this:

If the respective *SrcAddress* field is set to "# " then the caller's X.25 address will be replaced with the ISDN Calling Party's Number.

How can remote users access the BRICK's status page?

The BRICK provides status information about its operational state (installed licenses, available ISDN channels) in HTML. The status page is primarily intended for end users on the BRICK's LAN that are having problems connecting to remote sites. From this page users can then inform the system administrator via email if a problem exists.

To access the status-page point a WWW browser (Netscape Navigator or Microsoft's Internet Explorer) at the BRICK using a URL of the format.

http://<SysName>:< HTTP Port Number>

SysName is the name set for System Name in the **SYSTEM** → menu.

HTTP Port Number is only required if the BRICK's HTTP port number has been changed from its default value of 80. This is set in the HTTP port field in the **IP** → **STATIC SETTINGS** → menu.

As seen on page 164, the BRICK's status page consists of three tables.

System Description

This information is retrieved from the BRICK's *admin* table. If a valid email address is detected in the SysContact field the BRICK underlines the address. When this address is clicked the browser opens a new compose message window using this address.

Software Options



This information is retrieved from the BRICK's *biboAdmLicInfoTable* and displays the status of the BRICK subsystems.

Hardware Interfaces

This table displays the current state of the BRICK's hardware interfaces. Column three displays the state of the resource; possible states are described below:

Module Type	Displayed State	Possible Causes
LAN	o.k.	Normal operation.
	inactive	Cable not connected.

Module Type	Displayed State	Possible Causes
ISDN	o.k.	Normal operation.
	inactive	No B-channels currently in use.
	unconfigured	Cable not connected or incorrect D-channel protocol is being used.
X.21	o.k.	An X.21 link is currently open.
	inactive	X.21 interface is configured but no links are active.
	unconfigured	Cable not connected or X.21 interface is not configured.
all	empty	No module installed in this slot.
	unknown	Module of unknown type was detected.

Info: Access to the BRICK's status page can be disabled by setting the HTTP port to 0. See the HTTP port field in the  **IP** →  **STATIC SETTINGS** → menu.

Column four of the Hardware Interfaces table displays the current state of the ISDN B-Channels and analog/digital modems for the respective slot. A red LED identifies an ISDN B-Channel (or modem) that is currently in use while a white LED indicates a B-Channel (or modem) that is currently available.


For modems, if you move the mouse pointer over the red LED, the rate for receiving and transmitting data in bps is displayed. The ISDN channel currently connected to the respective modem is also displayed using four digits XYZZ which stand for the slot (X), the unit (Y) and the ISDN channel used (ZZ).

Netscape: BIANCA: System Information

File Edit View Go Communicator Help

Bookmarks Go To: <http://bianca>

System Information: BIANCA



System description

Type of System	BIANCA/BRICK-XL2
System Name	BIANCA
Location	Documentation Department
Contact	bianca@brick.com
Software	V 4.9 Rev. 1 from 98/09/18 12:34:54
System state	up and running for 14d 6h 47min

Software options

IP	OSPF	TAF	TUNNELING	STAC	CAPI	BRIDGE	X25	FRAME_RELAY	IPX
o.k.	o.k.	o.k.	o.k.	o.k.	o.k.	o.k.	o.k.	o.k.	o.k.

Hardware Interfaces

Slot	Interface	Status	Details
Slot 1	Fast Ethernet	o.k.	
Slot 2, Unit 0	ISDN S0	o.k.	ISDN: used 1, available 1 Modem 33.6: used 0, available 2
Slot 2, Unit 1	ISDN S0	o.k.	ISDN: used 1, available 1 Modem 33.6: used 1, available 1
Slot 3	X.21	o.k.	
Slot 4	ISDN S2M	active	used 12, available 18
Slot 5	empty		
Slot 6	Token Ring	o.k.	

You can [update](#) this page, see a list of [system tables](#), or [login](#) to the router.

For more information about BinTec products see <http://www.bintec.de>

Go to the Home page

SNMP-Table Browsing

The contents of the BRICK SNMP tables can be browsed via HTTP browsers using the "SNMP Tables" link from the BRICK main Status-Page. Initially this link displays a list of all system tables found on the BRICK. From there, individual system tables can be selected; the BRICK creates the appropriate HTML pages on-the-fly.

CGI Program: `htmlshow`

The contents of BRICK SNMP tables and variables can also be selectively displayed to any WWW browser using the internal `htmlshow` program. The BRICK authenticates `htmlshow` queries using the HTTP user name and HTTP Server password once per browser session. The initial settings are:

`http` as user name
`bintec` as password

The user name cannot be changed. However for security reasons the HTTP Server password must be changed on your BRICK in the **SYSTEM** → menu.

The syntax for using `htmlshow` adheres to the CGI (Common Gateway Interface) standard and can be referenced as follows:

separates CGI program
name from parameters

`http://<SysName>/htmlshow?<option=val>&<option=val>`

separates
parameter strings

where possible options may include:

`oid=snmp_oid`

This option is mandatory and specifies an SNMP object identifier (OID) to display. `snmp_oid` is not case-sensitive.

An OID may be specified in one of the following ways:

1. A symbolic object identifier, e.g.
`.iso.org.dod.internet.mgmt.mib-2.interfaces.ifEntry.ifTable`
2. An numerical object identifier, e.g.
`.1.3.6.1.2.1.2.2.1`
3. A unique MIB-2 or BinTec MIB table or variable name, e.g.
`iftable`

Object identifiers starting with a period (“.”) are taken to be absolute object identifiers; otherwise a relative object identifier is assumed. Relative object identifiers are searched for relative to MIB-2, i.e. .iso.org.dod.internet.mgmt.mib-2 or .1.3.6.1.2.1.

refreshtime=interval

If interval is specified the display is updated every *interval* seconds. Entering 0 in the resulting text field disables automatic refresh updates.

orientation=mode

Defines the orientation of the output.

“portrait” (default) or “landscape” mode may be specified.

If more than one object identifier is specified, the resulting tables or columns are printed side-by-side. For example, the following URL was used to display the selected system variables shown below:

```
http://mybrick/htmlshow?oid=isdnchisdnifindex&
oid=isdnchstate&oid=isdnchreceivedoctets&
oid=isdnchtransmitoctets&oid=isdnchreceivederrors
&refreshtime=10
```

The screenshot shows a web browser window with the following content:


Address bar: `http://mybrick/htmlshow?refreshtime=10&orientation=portrait&oid=isdnchisdnifindex&oid=isdnchstate&oid=isdnchreceivedoctets&oid=isdnchtransmitoctets&oid=isdnchreceivederrors`

Page Title: **isdnchisdnifindex / isdnchstate / isdnchreceivedoctets / isdnchtransmitoctets / isdnchreceivederrors**

Refresh time: Orientation:

isdnchisdnifindex	isdnchstate	isdnchreceivedoctets	isdnchtransmitoctets	isdnchreceivederrors
isdnifindex	State	ReceivedOctets	TransmitOctets	ReceivedErrors
0 2000	0 not_connected	0 0	0 0	0 0
1 2000	1 not_connected	1 0	1 0	1 0
2 2000	2 not_connected	2 0	2 0	2 0

Go to the list of [system tables](#), or back to the [home page](#)

Info:  References to HTML pages generated by the BRICK htmlshow program can be “bookmarked” for future reference. This will spare you the time of having to type long htmlshow queries (all htmlshow options will be saved in the bookmark, except for SNMP passwords of course).

Login

The login link will open a telnet session to your BRICK which can e.g. be used for quick configuration changes via the Setup Tool.

BinTec

The final link on the main page will take you to our WWW server where you can get the latest information on our products as well as current system software and documentation for your BRICK.

6

TROUBLESHOOTING

What's covered

- General Troubleshooting 167
 - Debugging Tools..... 168
 - System Errors..... 169
 - Hardware Problems..... 171
 - Software Problems..... 174
 - ISDN Connections 177
-

General Troubleshooting

In general, if you are having problems, it may be helpful to briefly enable debugging output from the SNMP shell. This can easily be done by logging into the BRICK and then entering the `177` command:

```
debug all
```

All debugging information will be written to your terminal's display.

If you want to survey debugging output over a longer time period it is best to configure a log host and have the BRICK forward system messages to the remote host. Log hosts can be configured from Setup Tool's **SYSTEM** → **EXTERNAL SYSTEM LOGGING** menu.

System messages can also be saved locally on the BRICK as events occur. In Setup Tool's **SYSTEM** menu set:

```
Maximum Number of Syslog Entries      30  
Message level for the syslog table    debug
```

You can then review the system messages as they occur from Setup Tool's **MONITORING AND DEBUGGING** → **MESSAGES** menu.

If you're connected via the serial console you can also set

```
syslog output on serial console      yes
```

in the **SYSTEM** menu and let the messages scroll to the screen.

Debugging Tools

Local SNMP Shell Commands

debug

The debug command can be used from the SNMP shell to debug one or more BRICK subsystems. See Chapter 7 for help on using debug.

isdnlogin

To verify that an ISDN connection can be made you can use the isdnlogin program. A brief description of this program is in Chapter 7. To establish an ISDN connection use the **isdnlogin** program as follows:

```
isdnlogin isdn-number telephony
```

where the *isdn-number* parameter is the telephone number of a telephone in your local office where you can audibly verify the call. The *isdn-service* parameter should specify the ISDN "telephony" service. You can also verify the call by viewing the *isdnCallHistoryTable* as explained in the next section.

trace

The trace command can be used from the BRICK's SNMP shell to trace and interpret ISDN messages (D and B channels) or packets sent or received over the LAN. A detailed description of the trace command, as well as a couple of usage examples, is contained in Chapter 7.

This command displays ISDN messages travelling over the next B-channel that is opened:

```
trace -ip next
```

This command dumps raw packets sent from the BRICK's MAC address to the host with MAC address 0:a0:f9:d:5:a.

```
trace -x -s me -d 0:a0:f9:d:5:a 0 0 1
```

Remote Tools (UNIX and Windows)

bricktrace

You can use the **bricktrace** utility (included with *BRICKtools for UNIX*) to inspect and disassemble the data being sent over the ISDN channels. The bricktrace command will attach to TCP/IP port 7000, so you must specify the IP address for the host you wish to trace. This is done with the **-H** *hostID* parameter or by using a TRACE_HOST environment variable. For additional information on using the bricktrace utility see chapter 7.

DIME Tracer

The DIME Tracer program is a component of *BRICKware for Windows* that allows you to trace your BRICK's ISDN channels from a remote PC where DIME Tools has been installed. Refer to your *BRICKware for Windows* documentation (included on the Companion CD) for information on installing and using DIME Tools.

System Errors

If you are having problems in regaining control of the system due to configuration errors or forgotten passwords, you may want to return the BRICK to its initial configuration state as it arrived. This can be done from the BOOTmonitor at startup.

I can't reach the BRICK via the network.

- If the BRICK can not be reached over a network connection, you may need to attach a terminal (or computer running a terminal emulation program) to it directly.

Login is only possible via the console.

- If you can still login as the admin user on the console (connection over the serial port) you can move the boot configuration file as mentioned above. Then restart the system and begin again with the basic configuration.

Login not possible

- If you do not receive a login prompt or do not have the admin password, first attempt to delete the BRICK's boot configuration using the BOOTmonitor. If using the BOOTmonitor does not succeed in regaining control of the system there is an emergency recovery procedure. This procedure will leave your BRICK in the initial configuration state as it arrived. You must then restart with the basic configuration.

1. Remove all modules from the BRICK. See Chapter 8.
2. Restart the system with no modules installed.
3. You can then log in as **admin** using the "bintec" password.
4. From the shell delete the configuration file with the following:

```
cmd=delete path=boot
```

5. Shut down the system, reinstall your modules, and reboot again.
- If you do not get a login prompt, even when no modules are installed, check the console for possible errors during the internal self test and system power-up procedures.

Hardware Problems

X.21 (CM-X21) Interfaces

If you are having problems establishing connections (X.25, PPP) over an X.21 interface the bricktrace tool can be helpful in determining the problem. To trace X.25 data being sent over an X.21 interface use:

```
bricktrace -3 -H <host> 0 0 <slot>
```

For PPP traffic the `-p` option is used, and for IP the `-i` option.

Fast Ethernet (CM-100BT) Interfaces

If you have problems establishing LAN connections via the BRICK-XL2's CM-100BT module verify:

- You're using Category 5 Twisted Pair cabling with External shielding.
- Pairs 1-2, 3-6, 4-5, and 7-8 of your cabling are twisted. (refer to the cable specifications in *Appendix A* on page 239.)
- The maximum segment lengths haven't been exceeded.

If you continue to have problems at 100Mbps, try configuring the port (via *biboAdmBoardConnector*) for 10Mbps operation.

Fast Ethernet Syslog messages

If your cabling and network topology is compliant check the *biboAdmSyslogTable* for syslog messages generated from the "Ether" subsystem.

<i>biboAdmSyslogMessage</i>	<i>~Level</i>
Ether: slot <n>: Excessive collisions (Transm. aborted).	Debug
Ether: slot <n>: Excessive Deferral (Transmission aborted)	Warning
Ether: slot <n>: No Carrier Sense - Cable problem?	Warning
Ether: slot <n>: Late Collisions (Invalid fullduplex mode?)	Warning
Ether: slot <n>: CD Heartbeat lost	Warning

<i>biboAdmSyslogMessage</i>	<i>~Level</i>
Ether: slot <n>: Auto-negotiation failed <mode> <i>mode</i> displays an incompatible neg. mode	Err
Ether: slot <n>: Wrong negotiation protocol <code> hub/switch doesn't support 802.3u auto-neg.	Err
Ether: slot <n>: No auto-negotiation hub/switch doesn't support auto-negotiation	Info
Ether: slot <n>: Auto-negotiation done <speed:mode> <i>speed</i> = 10baseT or 100baseTx <i>mode</i> = halfdup or fulldup	Info

Primary Rate (CM-PRI) Interfaces

If your having problems accessing ISDN services over your Primary Rate Interface (CM-PRI module) it often helps to check the Layer1State field in the pmlfTable. One of the following values will be displayed.

Layer1State	Meaning
active	active, framing and synchronisation is o.k. This is the only state where transmission is possible
remote-alarm	receipt of an RAI, remote alarm indication, from the remote side; The remote-alarm is also known as yellow alarm or distant alarm
no-signal	no signal is received, RAI will be transmitted. NOS is also known as red alarm.
no-sync	signal is received but synchronisation is not possible, RAI will be transmitted The received signal may also consist of continuous ones.
crc-error	signal and synchronisation are o.k. but signal has heavy crc errors, RAI will be transmitted.
power-on	initial state after power was switched on (transient)
resync	Setting Layer 1 State to resync can be used to force resynchronisation.

Token Ring Interfaces

At boot time, the BRICK's token ring module performs a self test before linking itself to the token ring. This procedure normally takes about 10 seconds. The self test is complete when the *tokenringIfState* variable changes to "done".

Self test is done, still can't access token ring.

If your BRICK still can't access the token ring there may be a configuration or cabling problem.

- Verify the token ring cabling, especially if you are using the RJ-45 port of your token ring interface.
- Verify the appropriate *RingRate* is set in the *tokenringIfTable*.
- Verify the *ifAdminStatus* field for the tr-llc and tr-snap interfaces are set to "up".

Serial Console

On the BRICK-XL2 make sure you are using appropriate terminal settings. Your terminal settings must use:

9600 bps, 8 data bits, no parity, 1 stop bit

If you changed the default settings in the BOOTmonitor, you may have to test various settings until a connection can be established.

Software Problems

IPX Routing

This section covers some of the problems you may encounter when configuring IPX routing and suggests where to look first for possible solutions.

- First, verify that your license is properly set for IPX by displaying the *biboLicInfoTable* (Or the **LICENSES** menu under Setup Tool).

A server exists on a remote LAN (over ISDN), but is 'invisible' to client stations on the local LAN.

The server may become "invisible" to client stations if SAP packets are not being received from this server.

Possible reasons include:

- The SAP protocol has been turned "off" for the ISDN interface and there are no entries in the *ipxStaticServTable*. (Verify *sapCircState* for each interface in the *sapCircTable*)
- SAP packets are being filtered out by one of the intermediate routers.
- The ISDN connection can't be established.
- The service is being removed through aging, see the *Update* and *AgeMultiplier* fields on page 65. These settings must be compatible with the settings used by the servers on the BRICK's LAN.
- The Network Number for the BRICK's LAN interface is either not set (in *ipxCircNetNum*) or could not be obtained from the server. If this is the case, the BRICK can't send SAP packets over the LAN. The client never learns of the servers presence.

The client waits for a long time and eventually disconnects when trying to connect to a server on a remote network accessible via PPP.

In some cases, the local router may inform the client that a server is available but in reality isn't available any more. Possible reasons include:

- The server has crashed and the Aging interval has not expired yet.

- The server and router on the remote network may have gone down at the same time (e.g. due to loss of power). Although the router has rebooted, it can't inform the BRICK of the change since it doesn't know the server exists yet. The BRICK can't acknowledge the change either if the aging mechanism has been disabled for the PPP interface.

Suggestion: Briefly set the *ifAdminStatus* for this interface to "down" then back to "dialup". This will force all routes and services, available over this interface, to be deleted.

Can't change to a network drive from the client station.

- The file server may be "invisible" to the client, see above.
- The number of user licenses on the server as been exceeded. This is not a routing problem.

ISDN connections constantly reconnecting.

In general, RIP/SAP packets do not force ISDN to be established on the BRICK.

- Is there an entry in the *ipxDenyTable* that is preventing Novell serialization packets from being sent over the dialup interface?
- Is SPX spoofing enabled (see *ipxAdmSpxSpoofing*)? Also, if the remote SPX router does not support SPX spoofing, then the BRICK will disable SPX spoofing (as long as the interface is up).
- Is IPX spoofing enabled? (see *ipxAdmIpxSpoofing*)
- Is RCONSOLE running somewhere with a constantly changing screen (e.g., MONITOR, IPXCON, TCPCON, a screensaver, etc.)?
- Is somebody using NetBIOS over IPX (Windows for Workgroups, NT, Win95)? You may need to set *ipxAdmNETBIOSRepl* to "off" or "lan_only".
- Are NDS Replica Synchronization running?
(For Netware 4.1 servers)
- Set the *biboAdmSyslogLevel* = debug and check the syslog table. The IPX messages sent to the *biboAdmSyslogTable* will tell you why (by packet type and socket) a connection is being established. It may be possible to filter these packets.

***ipxAdmSpXConns* shows more connections than are actually present.**

The BRICK may not be receiving SPX disconnect messages from the server.

- Using the command “reset router” on the console of the respective server, any inactive connections between the server and the BRICK are closed.
- If the disconnect for the client is lost, the connection will eventually timeout and close. Until the timeout, the connection is displayed in the *ipxAdmSpXConns*. Once the connection does close, SPX sends a message to the server informing it that the connection is closed.

OSPF Routing

This section lists some of the things to check first when troubleshooting your OSPF configuration. Note that in general, most errors are logged to the *biboAdmSyslogTable*. OSPF protocol specific errors are also logged the *ospfErrTable* and *ospfStatTable*.

- Verify a valid OSPF license is installed by displaying the *biboAdmLicInfoTable* (Or the **LICENSES** menu under Setup Tool).
- Verify that OSPF is enabled. The *ospfAdminStat* variable must be set to “enable”.
- Have all OSPF Areas been configured? Check the *ospfAreaTable*.
- Are all OSPF interfaces assigned to the desired areas? Check each interface’s *IfAreaId* in the *ospfIfTable*.
- Is the Admin Status of each interfaces configured properly? Check the value of *ipExtIfOspf* for the interface.
- Have all OSPF neighbour routers been identified?
OSPF neighbour routers identified via the HELLO protocol should appear in the *ospfNbrTable*.
- If other OSPF routers are present on the network but haven’t been identified. Verify the interface parameters are the same for all routers in the area. Check: *ipRouteMask*, *ospfIfAreaID*, *ospfIfHelloInterval*, *ospfIfRtrDeadInterval*, *ospfIfAuthKey*, *ospfIfAuth-*

Type). Also, verify the area parameters are the same for all routers in the area. Check: *ospfImportAsExtern*.

- Has the DR and BDR been elected for broadcast nets? Check the addresses set in the *ospfIfDesignatedRouter* and *ospfIfBackupDesignatedRouter* objects.
- Are OSPF syslog messages appearing in *biboAdmSyslogTable*? First set *biboAdmSyslogTableLevel* to “debug”.
- Is NAT turned off for all OSPF interfaces? Check the *Nat* field in *ipExtIfTable*. It must be “off”.

ISDN Connections

This section covers some of the problems you may encounter when configuring ISDN connections and suggests where to look first for possible solutions. The following sections give instructions on using the available utilities and programs to check your ISDN configurations.

Outgoing calls do not connect.

- Verify the call is connected by viewing the back plane LEDs. Refer to Chapter 8 for specific modules.
- Check to see if outgoing calls are possible by using the **isdnlogin** program.

Check the *isdnCallHistoryTable*.

- Was an outgoing call logged at all?
- Was the dialled number correct (see *biboDialTable*)?
- Was the call connected (duration > 0)?

Check the *biboAdmSyslogTable*.

- Check for syslog messages from ISDN with a “disconnect cause”.

Check the *biboPPPTTable* (IP routing and bridging)

- Is encapsulation identical for both sides?
- Is authentication identical for both sides?

- Verify what is being sent over the channels using the **bricktrace** program from a remote host on your local network.

Check the *isdnStkTable*.

- Does the *Status* field show “loaded”?

Entries in the *isdnDispatchTable* have an effect on the local number field of outgoing calls.

Incoming calls do not connect

- Verify the incoming call was initially received by viewing the back plane LEDs. Refer to Chapter 8 for specific modules.

Check the *isdnCallHistoryTable*.

- Was an incoming call logged at all?
- If the call was not connected, check for possible error causes (*DSS1Cause*, *1TR6Cause*, *LocalCause*).
- Does the incoming caller's number match an appropriate entry in *biboDialTable*?

Check the *isdnDispatchTable*.

- Is there a corresponding entry (*Item*, *Stack*, *LocalNumber*, ...) for the incoming call?

Check the *biboPPPTable*. (IP routing and Bridging)

- Is encapsulation identical for both sides?
- Is authentication identical for both sides?

ISDN connections remain open or are unwanted



Use the credits based accounting system as described on page 99. You can thus set a limit for connections with BRICK to prevent unnecessary charges from accumulating as a result of mistakes made during configuration.

- Using debug *all* or *trace*, check if a PC in the LAN is using a different netmask from the one entered on BRICK.

- Using `debug all` or `trace`, check if a PC in the LAN is configured for Remote CAPI with an incorrect IP address (destination port 2662).
- Check in **SYSTEM** → **EXTERNAL SYSTEM LOGGING** if BRICK is configured to send syslog messages to a host outside the LAN (destination port 514).
- Check in the MIB table *biboAdmTrapHostTable* if BRICK is configured to send SNMP traps to a host outside the LAN (destination ports 161, 162).
- Check if, due to different loads of traffic, frequent opening and closing of a B-channel is occurring for connections with dynamic channel bundling.
- Using `debug all` or `trace`, check if a PC in the LAN is configured with an incorrect IP address for the WINS server (destination ports 137-139). If necessary, configure the PC properly or enter the corresponding filters.
- Using `debug all` or `trace`, 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). Do not try to resolve NetBIOS names with DNS!
- Using `debug all` or `trace`, check if an application on a PC in the LAN is trying to resolve names that the name server at the Internet provider does not know (it is accessed from a client port to destination port 53). Install a local HOSTS file in the Windows directory that can facilitate name resolution
- Using `debug all` or `trace`, check if NetBIOS over IP is configured on a PC in the LAN (it is accessed from source port 137 to destination port 53). The attempt is thus made to resolve NetBIOS names over DNS. Disable NetBIOS over IP or insert filters (configuration of filters can be found on page 76) or use the simple NetBIOS filter of the Configuration Wizard.
- Check if you have configured Callback as described on page 57 and in doing so entered an incorrect dial number (Number under **WAN PARTNER** → **EDIT** → **WAN NUMBERS** → **EDIT**).

- If you have configured Callback, check if your partner denies your initial call using `debug all` or `trace` (D channel). For example, if your dial number is not being transmitted over the ISDN during the initial call, your partner firstly takes the call to identify the caller before a callback is being established.
- Check if you left running a trace program over an ISDN-PPP connection. That would cause the constant sending of packets over ISDN, the connection would remain permanently open.
- In the **Configuration** menu of the DIME Tools check under **Options** if **DNS Name Resolution** is activated for the Syslog daemon. That would cause an ISDN connection if the DNS server is outside your LAN. For example, if you configured Internet access with your router, usually the DNS server of your Internet Service Provider is used for name resolution.
- For X.25 connections check in **X.25** → **LINK CONFIGURATION** → **EDIT** if you set the *Layer 2 Behaviour* to *always active*. (Corresponds with a value of -1 for the variable *L2IdleTimer* in the *X25LinkPresetTable*.) The connection could remain open permanently.
- If RIP packets are continually routed over ISDN, check if there is a loop in the local network or a directly connected network. Verify the network configuration or disable RIP with *biboAdmRipUdpPort=0*.

Unable to establish a connection

If a connection can not be established, you should first inspect the information being transmitted over the D-channel. This would be done from a remote host where the bricktrace utility has been installed. Assuming your ISDN module is installed in slot 2, the bricktrace utility could be used as follows. The *host* parameter can specify either a hostname or IP address. The output is redirected to a file, which can be inspected later.

```
bricktrace -HhostID -h23pi 0 0 2 > dchan &
```

Then kill the running process and inspect file "dchan" to verify what was actually transferred over the D channel.

Connection established: Tracing the B channels

If a connection has been established you can inspect the appropriate B channels using the same procedure mentioned above, but specifying a 1 or 2 (channels B1 and B2) in the channel parameter.

The following procedure could be used to obtain tracing data for an ISDN connection between two BRICKs (system A and B). This example assumes each system has one ISDN module with one BRI interface installed in slot 2.

1. Trace the D channel of system A in the background, and redirect the output to a file.

```
bricktrace -HsystemA 0 0 2 >chD-sysA &
```

2. Trace the B channels of system A in the background and redirect the output to a file.

```
bricktrace -HsystemA -h2pi 1 0 2 >chB1-sysA &
```

```
bricktrace -HsystemA -h2pi 2 0 2 >chB2-sysA &
```

3. Trace the D channel of system B in the background, and redirect the output to a file.

```
bricktrace -HsystemB 0 0 2 >chD-sysB &
```

4. Trace the B channels of system B in the background, and direct the output to a file.

```
bricktrace -HsystemB -h2pi 1 0 2 >chB1-sysB &
```

```
bricktrace -HsystemB -h2pi 2 0 2 >chB2-sysB &
```

5. All tracers have been started, start an activity on the target host.

```
telnet host id
```

6. Wait at least 30 seconds. Close the telnet session, kill the six bricktrace processes started earlier, and inspect the trace data.

```
kill pid1 ... pid6  
vi *sysA *sysB
```

7

COMMAND REFERENCE

What's covered

- SNMP Shell Commands
 - telnet 183
 - ping 183
 - ipxping 184
 - trace 184
 - rtlookup 186
 - tracert 187
 - lfstat 187
 - netstat 188
 - isdnlogin 188
 - minipad 189
 - date 190
 - update 190
 - modem 190
 - setup 192
 - debug 192
 - p 193
 - t 193
 - ifconfig 194
 - halt 194
 - ospfmon 195
- BRICKtools for UNIX Commands
 - bricktrace 196
 - capitrac 196

The SNMP shell commands

The BRICK contains several preinstalled programs, ready for use from the SNMP client shell. A short description of these programs and their usage is as follows:

telnet

telnet [-f] <host> [<port>]

The telnet program can be used to communicate with another host. Telnet requires the host parameter (IP address or hostname) and has an optional port parameter.

The -f option specifies that the telnet connection should be transparent. This option is especially useful for establishing connections to *non-telnet* ports such as uucp or smtp.

ping

ping [-c <count>] <host> [<size>]

Ping can be used to test communication with another host. Ping sends ICMP echo_request packets of length *size* to *host*.

You can limit the number of packets to be sent by using the **-c** option; *<count>* sets the number of packets..

Info:



Without the **-c** option ping will continue to send packets until you stop it (e.g. by pressing Ctrl-C).

Host is a required parameter which takes an IP address or a host-name. *Size* is optional and sets the length of the packets to use.

ipxping

ipxping [**-c** *<count>*] [**-d** *<delay>*] [**-s**] *<internal-netnumber>* [*<node>*]

The ipxping command can be used to test communication between the BRICK and an IPX server. Ipxping takes the following arguments:

-c *count* Specifies the number of packets to send.

-d *delay* Specifies the delay between packets in seconds.

-s Sends 10000 packets.

internal-netnumber

Specifies the server's Internal Network Number (mandatory).

node Specifies the destination node (xx:xx:xx:xx:xx:xx)

trace

For WAN interfaces:

trace [**-h23aFAtpiNxx**] [**next**] [**-T** *<tei>*] [**-c** *<cref>*]
<channel> *<unit>* *<slot>*

For LAN interfaces:

trace [**-h23iNxxl**] [**-d** *<destination MAC filter>*]
[**-o**] [**-s** *<source MAC filter>*] **0 0** *<slot>*

The trace program can be used from the SNMP shell to trace and interpret ISDN messages (D and B channels) or LAN packets sent or received via the BRICK's interfaces. Command line parameters are:

-h	hexadecimal output
-2	layer 2 output
-3	layer 3 output
-a	asynchronous HDLC (B-Channel only)
-F	FAX (B-Channel only)
-A	FAX + AT Commands (B-Channel only)
-p	PPP (B-Channel only)
-i	IP output (B-Channel only)
-N	Novell IPX output (B-Channel only)
-t	ASCII text output (B-Channel only)
-x	raw dump mode
-X	asynchronous PPP over X.75 (B-Channel only)
-T <i><tei></i>	set TEI filter (D-Channel only)
next	only display info for the next B-channel that is opened (B-Channel only)
-c <i><cref></i>	set callref filter (D-Channel only)
-d <i><MAC filter></i>	set destination MAC address filter (LAN only)
-s <i><MAC filter></i>	set source MAC address filter (LAN only)
-o	combine two or more -s or -d filters with a logical OR operation

<MAC filter> **me** = BRICK's MAC address
bc = broadcast packets
<MAC address> (xx:xx:xx:xx:xx:xx)

<channel> 0 = D-Channel or X.21 Interface
1..31 = Bx-Channel

<unit> 0..1

<slot> 1..2

The *<MAC filters>* deserve some further explanation. You can combine an -s and a -d filter with a logical AND operation by simply specifying them both (see example *LAN AND filter* below). Now only packets with matching source AND destination address are displayed.

To combine two or more -s or -d filters with a logical OR operation, you specify the first filter, followed by -o, then specify the next filter, and so on (see example *LAN OR filter* below).

Examples

ISDN B-Channel

```
trace -h23i 1 0 2
```

PPP Interface

```
trace -ip <ifcname>
```

next used B-Channel

```
trace -ip next
```

LAN AND filter (packets from my BRICK to the specified MAC address)

```
trace -2iN -s me -d 0:a0:f9:d:5:a 0 0 1
```

LAN OR filter (broadcast packets OR packets from my BRICK)

```
trace -d bc -o -d me 0 0 1
```

rtlookup

```
rtlookup [-isuvotp] <destination IP address>
```

The *rtlookup* (route lookup) command will output the destination interface an IP packet would be routed to.

You can input the destination IP address and the following parameters:

-i <source ifindex>

-s <source IP address>

-u <source port>

-v <destination port>

-o <tos / type of service>

-t <ttl / time to live>

-p <protocol> (where <protocol> is one of the possible values for *ipExtRtProtocol*. The most common protocols are **icmp** (1), **tcp** (6), and **udp** (17).)

Examples


```
brick:> rtlookup 123.45.35.34
```

```
Matches ipRouteTable, inx = 0
```

```
Using ifindex 1000 nexthop 123.45.35.35
```

```
brick:> rtlookup -i 1000 -p tcp 1.2.3.4
Denied
```

```
brick:> rtlookup 123.45.35.61
Local destination
```

Info:  Make sure to specify a *source ifindex* if you are testing security features, because otherwise the »packet« will be treated as if it was generated locally on the BRICK, thus nullifying the effect of most security features, e.g. access lists.

Please note, that the current operating status of the interfaces specified in the *rtlookup* command will not be affected, i.e. if you issue a *rtlookup* for a dormant ISDN interface it will correctly be reported to be »not available«.

traceroute

```
traceroute [-m <maxhops>] [-p <port>] [-q <nqueries>]
              [-w <waittime>] <host> [<packetsize>]
```

The traceroute program prints the route packets take to arrive at a network host. The only mandatory parameter is the destination host name or IP number.

ifstat

```
ifstat [-lur] [<ifcname>]
```

The ifstat command displays status information for the system's interfaces, based on the contents of the *ifTable*. Ifstat takes the following parameters:

- l** Displays the full length of the interface descriptions (normally the description is only displayed up to the 12th character).
 - u** Only displays information on interfaces which are in the **up** state.
 - r** Displays the Access Rules that apply to the specified interface(s).
- <ifcname>* Only displays information on interfaces whose description starts with the given characters (e.g. **ifstat en1** will display information on the interfaces en1, en1-llc, and en1-snap).

netstat

```
netstat [[-i | -r | -p [interface]] | -d <dest. IP addr.>]
```

The netstat command can be used to display a quick list of interfaces, routing table entries, or ISDN partners, using the **-i**, **-r**, and **-p** options respectively.

With the *<interface>* parameter details about interfaces, routes, and partners can be limited to a selected interface. For *<interface>* a numeric *ifIndex* or *ifDescr* may be used.

The **-d** option can be used to display IP routes to a destination address (specified in *<dest. IP addr.>*).

Info: The **-d** option should not be confused with the **rtlookup** command. The **-d** option simply performs a string match against all *ipRouteTable* entries and returns all routes whose *ipRouteDest* field starts with *<dest. IP addr.>*.



isdnlogin

```
isdnlogin [-c <stknumber>] [-C] [-s <service>] [-a <addinfo>] [-b <bits>] isdn-number [isdn-service | layer1-protocol]
```

The isdnlogin program enables you to start a remote login shell on the BRICK over ISDN. This is made possible by the **isdnlogind** which is started in the background at boot time. (See the sample bootup session in Chapter 2.)

The options have the following meanings:

- c <stknumber>**
Selects the ISDN stack to use for this login.
- C**
Try to use compression (V.42bis).
- s <service>**
1TR6 service code for outgoing calls
- a <addinfo>**
1TR6 additional info code for outgoing calls
- b <bits>** Use only *<bits>* bits for transmission (e.g. for 7bit ASCII transmissions use **-b 7**).

Using the *isdn-number* and *isdn-service* parameters, you select the ISDN partner to login to, and the ISDN service to use. Valid *isdn-service-identifiers* include: data, telephony, faxg3, faxg4, and btx.

Through D-channel signalling, *isdnlogin* can also accept incoming calls with V.110. Connections to V.110 stations can also be established with *isdnlogin* when the appropriate layer 1 protocol is supplied on the command line, for example:

The following layer 1 protocols can be used with *isdnlogin* command.

```
v110_1200  v110_2400  v110_4800  v110_9600
v110_19200 v110_38400  modem      dovb56k
telephony
```

minipad

```
minipad [-7] [-p <pktsz>] [-w <winsz>] [-c <cug>]
          [-o <outgocug>] [-b <bcug>] <x25address>
```

The *minipad* program is a basic PAD (Packet Assembler/Disassembler) program that can be used to provide a remote login services for remote X.25 hosts. *Minipad* takes the following arguments:

- 7** Use 7 bit data bytes only.
- p** <pktsz>
Open data connection with packet size <pktsz>.
- w** <winsz>
Open data connection with window size <winsz>.
- c** <cug> Closed user group. Possible values for <cug>: 0-9999.
- o** <outgocug>
Closed user group with outgoing access.
Possible values for <outgocug>: 0-9999.
- b** <bcug>
Bilateral Closed user group.
Possible values for <bcug>: 0-9999.
- <x25address>
Either a standard X.121 address or an extended address.

Minipad is also useful for testing X.25 routes. To diasble X.25 connections to the minipad, *x25LocalPadCall* must be set to "dont_accept".

date

date [-i] [YYMMDDHHMMSS]

The BRICK has a real-time clock and a software clock. Entering **date** by itself from the SNMP shell reads the real-time clock and displays the current time. The **-i** option is used to read and display the software clock. Using **date** followed by a date string (YYMM-DDHHMMSS) sets both clocks to the specified year, month, day, hour, minute, and second.

update

update [-v] <IP address> <filename>

The update command can be used on a running system (from the SNMP command prompt), to upgrade the internal software using TFTP. The host at *ipaddress* can be a UNIX system or a PC and must be configured as a TFTP host. The *filename* specifies the image to load into flash ROM.

Note that performing a software update on a running system via the update command requires a contiguous block of free memory, greater than or equal to the size of the new software image. If there is not enough memory available to load the complete image into RAM you will be offered an incremental update which loads the image file via TFTP in 64 KB blocks and write the image directly to Flash ROM. Before performing an incremental update, it is recommended that you verify the image using the -v option first (the file is not written to flash) and then, assuming the file verifies, restart the update command and perform an incremental update.

modem

modem [**update** <TFTP server> <image file name>
| **status**
| **cmd** <modemno> **off** | **boot**]

The modem command can be used on a running system (from the SNMP command prompt) to update the system software of your FM-MODI2 modem connector module, to display the current oper-

ating status of all modems, or to switch off or reboot a single modem.

modem update *<TFTP server> <image file name>*

There are two prerequisites for performing a software update for your modem connector module:

(1) You must have configured a TFTP host for your BRICK (for instructions on how to do so please refer to section *System Administration* on page 103).

(2) The new modem software image (available from our WWW server) must be located in the TFTP directory of your TFTP host.

<TFTP server> is either the IP address or hostname of the TFTP host, *<image file name>* is the name of the modem software image (e.g. **cs_m_461.csm**)

If you supplied the correct TFTP host and file name you will see some screen output concerning the loading and verifying of the image file. The update application will automatically detect your modem connector module and offer you to update it.

Perform update for BIANCA/FM-MODI-56K in slot 7 (y or n)?

If you reply with »y« the update will be performed. This will take approximately 60 seconds. After the update is complete you should reboot your BRICK if you immediately want to use the new modem software.

modem status

This command displays the status of all modems installed in your BRICK. This will get you a display similar to the one below.

No	State	OBytes	IBytes	LastMessage
00	IDLE	280	2704	CONNECT 115200/K56/LAPM/NONE/38000:TX/31200:RX
01	IDLE	278	2701	CONNECT 115200/V34/LAPM/V42BIS/33600:TX/33600:RX
02	IDLE	18481	22233	CONNECT 115200/K56/LAPM/NONE/40000:TX/31200:RX
03	CALLING	0	0	
04	CONNECTED	59635	64330	CONNECT 115200/V34/LAPM/NONE/33600:TX/33600:RX
05	CONNECTED	407	79	CONNECT 115200/K56/LAPM/V42BIS/36000:TX/31200:RX
06	CALLED	0	0	
07	IDLE	0	0	

The following table explains the possible modem states.

State	Description
IDLE	no modem activity
CALLING	outgoing call being set up
CALLED	incoming call being processed
CONNECTED	connection established,

modem cmd *<modemno>* **off** | **boot**

This command lets you switch off or reboot a single modem, specified by *<modemno>* (0..31).

setup

setup

The setup command is used from the SNMP shell to start the BRICK Setup Tool. Setup Tool provides a menu oriented interface to configuring the BRICK and its major features, and administering/monitoring its operational state. For an introduction to using Setup Tool see *Using Setup Tool* in Chapter 3. A description of all menus is contained in Chapter 4, *Setup Tool Menus*. Information on configuring specific features can be found in Chapter 5, *How do I Configure*

debug

debug [**show**] | [[**-t**] **all** | **acct** | **system** | *<subs>* [*<subs>* ...]]

The debug command is available from the SNMP shell. The debug command can be used to selectively display debugging information originating from one or more of the BRICK's various subsystems. Command line parameters are used as follows:

- show** Show all possible subsystems that can be debugged.
- t** Print a timestamp before each debugging message.
- all** Display debugging information for all subsystems.
- acct** Display debugging information for the accounting subsystem.

system Display debugging information for all subsystems *except* for the accounting subsystem.

<subs> One or more subsystems separated by whitespace can be entered to display only debugging information from these subsystems.

p

p [**high** | **low**]

The **p** (priority) command sets the priority (high or low) of the BRICK's SNMP shell with respect to other system processes.

The specified priority becomes effective for the current shell and all sub-processes started from this shell. If no options are specified, the current priority is displayed.

By default, the SNMP shell has a lower priority than routing processes which means that an interactive configuration session (**setup**) does not affect performance on systems with many WAN partners.

t

t [*<seconds>*]

The **t** (auto-logout timer) command defines the number of seconds to wait (once terminal input is idle) before closing the current login session. When the BRICK closes the login shell, all programs (**setup** session, **trace**, etc) started during the session that are currently running are also closed.

Each time a user logs in the timeout is set to **900** seconds by default.

The auto-logout feature can be disabled completely (for the current login session only) by setting the timer to **0**.

Info: This feature is primarily intended for security/cost-control reasons. If you expect a long, non-interactive terminal session (**setup** tool monitoring, ISDN trace session, etc.) you should disable the timer.



ifconfig

```
ifconfig <interface> [destination <destaddr>]
           [<address>] [netmask <mask>]
           [up | down | dialup] [-] [metric <n>]
```

The ifconfig command can be used to assign an address to a network interface and/or to configure network interface parameters and change the respective routing table entries.

When only the required interface parameter is used, ifconfig displays the current settings for the interface.

Options and their respective *ipRouteTable* entries are as follows:

<interface> Interface name (ifDescr)

destination <destaddr>

Destination IP address of a host for adding host routes. (ipRouteDest, ipRouteMask)

<address> BRICK's IP address for this interface (ipRouteNextHop).

netmask <mask>

Netmask of interface (ipRouteMask).

[**up** | **down** | **dialup**]

Set the interface to one of these states.

- Don't define own IP address (i.e. ipRouteNextHop = 0.0.0.0).

metric <n>

Sets route metric to *n* (ipRouteMetric1).

halt

halt

The halt command halts the system and reboots using the default boot configuration file. The halt command has the same effect as simply powering the system off and on again.

Info: The preferred method of rebooting the system is to assign the value "reboot" to the *biboAdmConfigCmd* object from the SNMP shell by entering: **cmd=reboot**.



ospfmon

ospfmon db [rtr | net | sum | asbr | ext | stat] <options>

The ospfmon application can be used from the SNMP shell to display the contents of the BRICK's OSPF Link State Database. Note that only LSA header information is stored in the MIB system tables, this application can be used to dump the complete contents of the database. The various parameters can be used to selectively display specific types of database entries.

Only one of the six identifiers can be used at time to display a cross section of the database.

rtr	Show all Router links.
net	Show all Network links.
sum	Show all Summary links.
asbr	Show all AS Border Router links.
ext	Show all External Links.
stat	Show OSPF database statistics.

Additional options may also be used to further identify more specific types of entries and include.

area <id>	Show database entries for area <id>.
rtrid <id>	Show entries generated by router ID <id>.
lsid <id>	Show database entry with link state ID <id>.

makekey [-g]

The makekey command can be used to show the current public key (stored on the *biboAdmPublicKey* variable), or—when invoked with the **-g** option—to generate a new pair of keys (public and private).

You will only need to use **makekey -g** once before starting to configure TAF for the first time.

shtaf

The **shtaf** command can be used to test the TAF authentication procedure. The BRICK will prompt you for an ACE/Server user name and a passcode (the Token currently displayed on this user's Token Card).

If the authentication was successful, it will give you a normal BRICK login prompt. After logging in to the BRICK you can terminate *shtaf* by typing **exit**.

BRICKtools for UNIX Commands

bricktrace

```
bricktrace [-h23aeFpiNtxs] [-T <tei>] [-c <cref>] [-r <cnt>]
           [-H <host>] [-P <port>] <channel> <unit> <slot>
```

The *bricktrace* program, included with *BRICKtools for UNIX*, enables tracing and interpretation of ISDN messages (D and B channels). Command line parameters are:

-h	hexadecimal output
-2	layer 2 output
-3	layer 3 output
-a	asynchronous HDLC (B-Channel only)
-e	ETS300075 (EuroFileTransfer) output (B-channel only)
-F	FAX (B-Channel only)
-p	PPP (B-Channel only)
-i	IP output (B-Channel only)
-N	Novell(c) IPX output (B-Channel only)
-t	ascii text output (B-Channel only)
-x	raw dump mode
-T <tei>	set TEI filter (D-Channel only)
-c <cref>	set callref filter (D-Channel only)
-r <cnt>	receive only <i>cnt</i> bytes
-H <host>	specify trace host (BRICK's name or IP address)
-P <port>	specify trace tcp port (default: 7000)
-s	scan Brick for available trace channels
<channel>	0 = D-Channel or X.21 Interface 1..31 = Bx-Channel
<unit>	0..1
<slot>	1..2

capitrace

```
capitrace [-h][-s][-1]
```

The *capitrace* program, included with *BRICKtools for UNIX*, enables tracing and interpretation of CAPI messages and displays all CAPI messages sent and received by the BRICK. The environment variable `CAPI_HOST` must be set to the IP address of the BRICK to trace CAPI messages on.

Command line parmaters are:

- h** hexadecimal output (default)
Print a hexdump of the entire CAPI message. This option is activated by default (if no options are specified).
- s** short output
Only print at the end of the information line the application ID and a connection identifier in the form "(application/identifier)" and the name of the CAPI message.
- l** long output (default)
Give a detailed interpretation of each parameter included in the CAPI message.
This option is activated by default.

Each message displayed is preceded by a line containing the following information:

- Timestamp ("seconds.miliseconds" in localtime)
- Sent/Received Flag ('X' = sent, 'R' = received)
- CAPI-Message-Name (ASCII string)
- CAPI-Message-Command
(0xABXY (AB = <subcommand> XY = <command>))
- Tracer-Message-Number (#<decimal>)
- CAPI-Message-Length (len=<decimal>)
- Application-ID (appl=<decimal>)
- CAPI-Message-Number
(messno=0x<hexadecimal>)
- Connection-Identifier
(ident=0x<hexadecimal> (short output only))

eft

eft [-l <username>][-p <password>][-c <controller>]
[-C <configfile>][-i <telephonenumber> command command args...]

-i starts the eft client in command prompt mode

Eft enables file transfer over ISDN to and from a Eurofile transfer server (EFT server for short). Data transfers are handled using the EFT standard protocol, ETS 300075. The configuration for the eft client is normally stored in the users ~/ .eft.cf file. A sample configuration file is included on the Companion CD.

Upon starting up, EFT will load its configuration file from the user's .eft.cf file if available; if it is not available standard, default values will be used. Note however, if the environment variables CAPI_HOST and CAPI_PORT are available in the user's shell environment, these values always take precedence.

eftd

eftd [-c <configfile>][-l <logfile>]

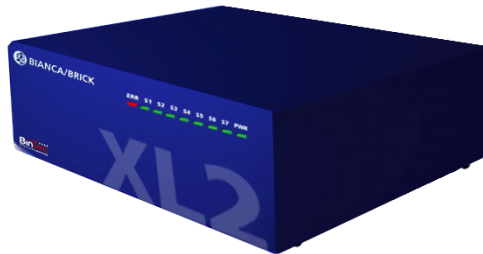
Eftd is an eft daemon that allows eft client file transfers to and from the host station over ISDN using the standard EFT protocol, ETS 300075. The configuration for the eftd server is stored in the eftd.cf file. A sample configuration file, as well as UNIX man pages are included on the Companion CD. This file must be present in the same directory as the eftd program.

8

HARDWARE/FIRMWARE CONFIGURATION

What's covered

Hardware	200	Communications Modules.....	209
Front Panel Indicators.....	200	The LAN Modules	209
The Back Plane.....	202	The WAN Modules.....	214
The Main Board.....	203	Function Modules.....	222
Firmware	205	Installing Communications Modules....	226
Upgrading System Software	205	Installing the Modem Connection Kit..	229
BOOTmonitor.....	205		
Automatic booting over TFTP	208		

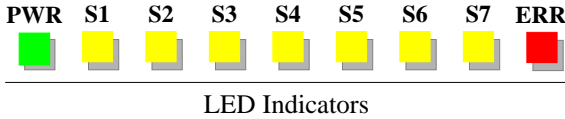


The BRICK-XL2 is the flagship of BinTec's BIANCA/BRICK family of routers and is designed as a central-site router for mid to large sized corporations.

In this chapter we'll cover the BRICK hardware, the available communications modules, and some important tasks you may need to perform in future such as installing communications modules and upgrading system software.

Hardware

Front Panel Indicators



There are nine front panel indicators (LEDs) that display status information about your BRICK-XL2. The various LEDs have different meanings depending on which mode the BRICK-XL2 is in. Upon booting the BRICK-XL2 moves between three different operational modes.

- Power Up Mode
- BOOTmonitor Mode
- Normal Operation Mode

Meanings for the nine LEDs in the different modes are shown below.

Power Up Mode

(duration: approximately 5 seconds)

LED	State	Meaning
PWR	On	Power is being supplied.
S1	On	Performing Display test.
S2	On	Performing DRAM test 1.
S3	On	Performing DRAM test 2.
S4	On	Performing RTC test.
S5	On	Performing Flash test.
S6	On	Performing MTS test.
ERR	Off	All tests completed.

BOOTmonitor Mode

(duration: 4 seconds)

LED(s)	State	Meaning
PWR	On	Power is being supplied.
S1 ... ERR	On	BOOTmonitor is in use (or is awaiting keyboard input).
	Blinking	BOOTmonitor is decompressing boot image.

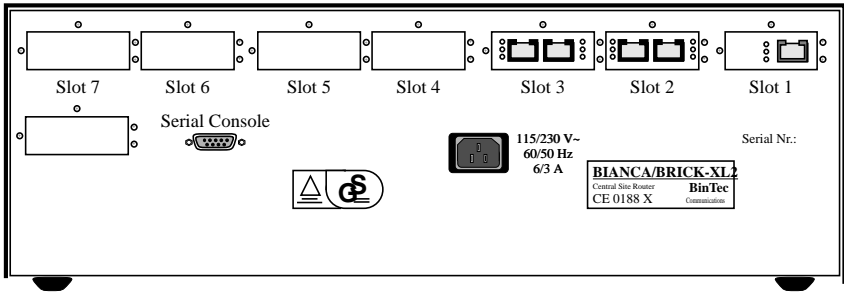
Normal Operation Mode

PWR is on when power is being supplied to the system. ERR (error) is normally off but may blink when a cabling problem exists or a collision has occurred; when ERR remains on an internal fan has stopped.

Depending on which slots your communications modules are installed the LEDs for slots 1 through 7 (S1 ... S7) are as follows:

	Modules	State	Meaning
LAN Modules	CM-AUI CM-BNCTP CM-TR	On	Sending or receiving a packet.
	CM-1BRI CM-1EBRI	On	1 B-channel in use.
		Blinking	2 B-channels in use.
WAN Modules	CM-2BRI CM-2XBRI	On	1 B-channel in use.
		Blinking	More than 1 B-channel in use.
	CM-PRI	On	1 or more B-channels in use.
	CM-X21	On	Sending or receiving a packet.

The Back Plane



The Power Socket

The BRICK-XL2 is capable of operating at 230 VAC, 50 Hz, max. 3.0 A or 115 VAC, 60 Hz, max. 6.0 A. A universal power supply senses the incoming voltage and adjusts accordingly. Depending on which country you purchased your BRICK-XL2 in you should be able to use the included power cord.

Note: Before supplying power to the BRICK-XL2, please verify the power rating identified on the marking label complies with your local power source.



Serial Port

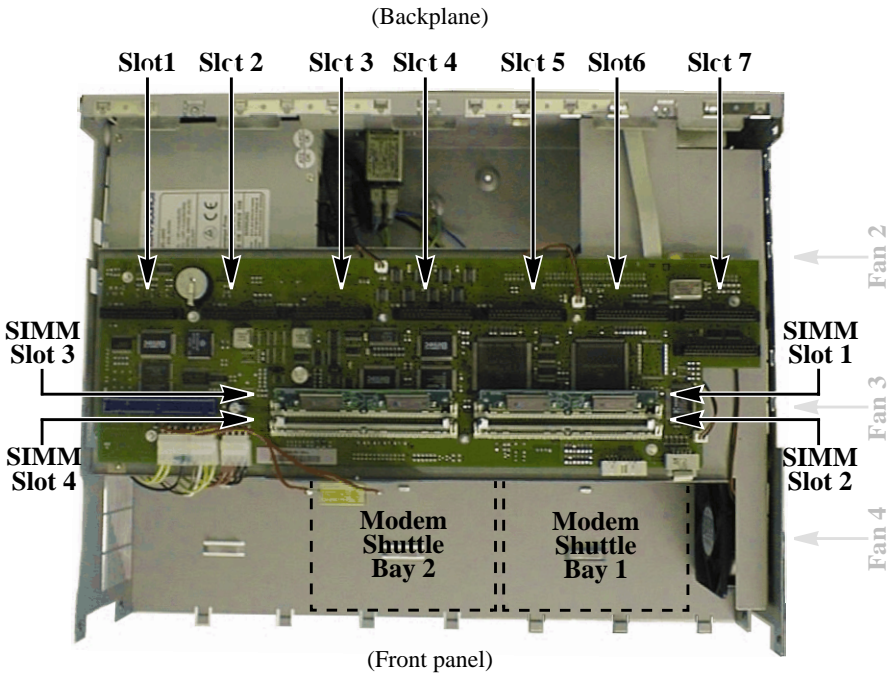
The 9 pin serial port is located on the back plane below slot 6. To allow for compatibility with a wider variety of terminals, the pin assignments for the serial port have been modified. Individual pin assignments for the 9 pin serial port are listed in *Appendix A* (page 240). See Chapter 2, for information on Connecting the BRICK to a PC or terminal.

The Network Ports

Which network ports are available on your system will of course depend on which communications modules are installed in your BRICK-XL2. Refer to the section, *Installing Communications Modules*, later in this chapter for information on removing or installing your modules.


The Main Board

The BRICKhas seven slots for LAN and/or WAN communications modules. Two bays are located below the main board for installing optional FM-MODI2 modem shuttles. The system is powered by a 33 MHz (MC68EC040) Motorola processor. Memory is scalable via 4 SIMM slots on the main board. Configuration information and code are stored in Flash-ROM which provides 2 MB of separate space.



System Memory


The BRICK-XL2 ships with 16 MB of system memory which is split among two 8 MB SIMMs. Memory is scalable to a maximum of 96 MB and can be upgraded at any time by purchasing additional memory modules directly from BinTec Communications or your local distributor. When upgrading memory, always make sure you fill the primary slot of the respective bank first (i.e. slots 1 and 3).

Note:  Using memory modules supplied by parties other than BinTec Communications or its authorized distributors will nullify your warranty.

Bank	Slot	Primary/Secondary	Usage
1	1	Primary	Reserved for CPU (central processing unit). Maximum 64 MB in bank 1 using: 4, 8, 16, or 32 MB modules.
	2	Secondary	
2	3	Primary	Reserved for DMA (direct memory access) for modules. Maximum 32MB in bank 2 using: 4, 8, or 16 MB modules.
	4	Secondary	

Cooling Fan

Three cooling fans are located below the BRICK-XL2's mainboard along the right side (identified as Fan 2, 3, and 4 as shown on the previous page). These fans ensure that the proper amount of air is circulated internally in the BRICK-XL2. This is very important on systems with FM-8MOD modems modules installed.

Note:  If the BRICK-XL2 is not mounted in a 19" rack and is left free-standing please ensure that the ventilation grids along the right side of the housing are not blocked.

By default the cooling fans adjust speeds automatically according to the internal temperature detected inside the BRICK-XL2. The fans can be configured to be on at all times by setting the *sysConfigFanControl* variable to "high" via SNMP or the SNMP shell.

The operational status of each cooling fan (i.e, whether the fan is actually turning) can be verified by checking the contents of the *sysConfig* table via SNMP or the SNMP shell. The respective variables *sysConfigFan2*, *sysConfigFan3*, and *sysConfigFan4* may report either and "on" or "off" status.

Firmware

Upgrading System Software

You may decide to upgrade your BRICK's internal system software in the future to take advantage of new and enhanced features developed at BinTec. System software upgrades are available via BinTec's FTP server via the WWW at <http://www.bintec.de>. There you'll also find current information about new software releases.

After obtaining the newest software you can perform the upgrade using any of the methods mentioned below:

- BOOTmonitor (pressing the spacebar during bootup)
- update command (while the system is running)

Another option is configure the BRICK so that it always retrieves its BOOT image via a remote host on your LAN via TFTP. With this method you can easily test new software releases and keep older system software images on hand in a central location. To do this you'll need to:

- Setup a TFTP Server
To use a Windows PC refer to your *BRICKware* documentation, to setup a UNIX host refer to Chapter 5 of the *Software Reference Manual*.
- Set the BRICK's default BOOT parameters in BOOTmonitor.
(See Default BOOTmonitor Parameters below.)

BOOTmonitor

After the internal self test has been successfully completed, the BRICK switches into BOOTmonitor mode and displays a BOOTmonitor prompt to the screen, if a terminal is connected. Using the BOOTmonitor, you can easily perform firmware upgrades, test a new software release, or remove configuration files on your system.

To activate the BOOTmonitor the spacebar must be pressed within the first 4 seconds, otherwise the system continues with its normal boot procedure and switches into normal operation mode. Pressing the spacebar activates the BOOTmonitor as shown in Figure 2 below. As long as the

BOOTmonitor is active (or awaiting keyboard input), all nine LEDs (PWR, S1 -S7, ERR) will remain on.

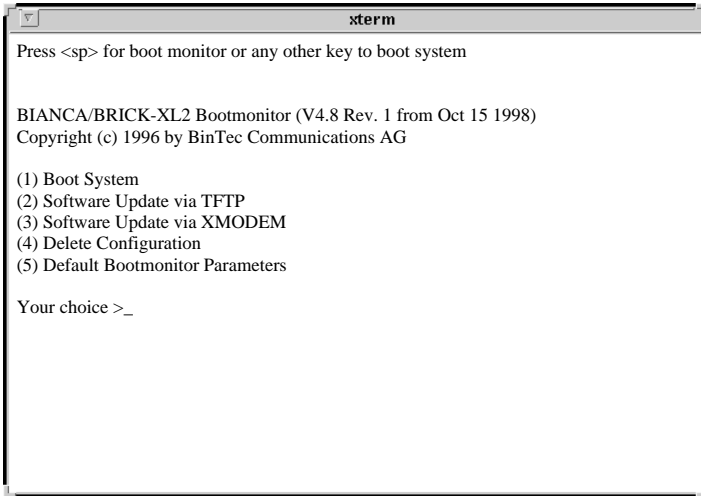


Figure 2: BOOTmonitor

The commands from the BOOTmonitor menu are self guiding, informing/prompting you for confirmation along the way.

Boot System

Selecting menu item (1) loads the compressed boot image (if one is present) from Flash ROM into RAM. This is the normal procedure performed by the BRICK when powered up.

Software Updates

To upgrade the BRICK firmware, first select either option (2) or (3) to specify how the new image should be transferred to the BRICK. If transferring over TFTP you will be prompted for IP addresses for the sending/receiving stations and the file name of the new image. If the transfer is

performed using XMODEM, you will be prompted for a baud rate for the transfer first.

Once you have entered the name of the image and it has been retrieved you will be asked to confirm the update. Here, you have two options:

1. Update Flash ROM
2. Write image to RAM and boot it.

Note:



Note that option (2) only loads the image into RAM and does not remove your existing boot image stored in Flash. In this way, you can test the new software release without removing your existing boot image. If the BRICK is turned off, your old software release will be used upon a subsequent reboot.

Delete Configuration

You can select option (4) to return the BRICK to its factory settings, as it arrived. All configuration files and BOOTmonitor settings (see *Default BOOTmonitor Parameters* below) will be removed.

Default BOOTmonitor Parameters

By selecting option (5) from the menu you can set or change the default settings used by the BOOTmonitor. The following default settings can be defined:

- The baud rate used for connecting a terminal.
- The ethernet connector type to use; “auto” by default, or: 10/100 Mbit ethernet in either Half-/Full-Duplex mode¹
- Which LAN interface to use for TFTP file transfers (when more than 1 is present).
- The IP address for the BRICK
- The IP address for the TFTP server

1. If the BRICK can't boot via TFTP (ethernet), verify the ethernet connector setting here.

- The image file to load/retrieve
- Automatic boot file retrieval over TFTP

The IP address settings defined here are used strictly for the BOOTmonitor and are not used for any IP routing functions on the BRICK.

Note: If you change the baud rate, be sure that your terminal supports this rate, otherwise you may not be able to connect to the BRICK. The default setting is set at 9600 baud, which is supported by practically all terminals.



Automatic booting over TFTP

The BRICK can load its boot file over TFTP automatically at boot time by defining the appropriate settings in menu item (5). After setting the local and remote IP addresses, and the name of the image file to retrieve answer “yes” to the question:

Do you want to boot automatically from the TFTP server (y or n):

to have the BRICK automatically retrieve its boot image via TFTP.

Note: If this file transfer is not successful (TFTP server not responding, image file not found, etc.) the system will halt.



Communications Modules

The BIANCA/BRICK-XL2 can link your local area network (LAN) to a wide area network (WAN) by serving as a router, bridge, or both. To access the networks, a variety of communications modules are available for both the LAN and WAN sides. The following sections describe the LAN and WAN modules currently available.

The LAN Modules

CM-AUI Ethernet Adapter

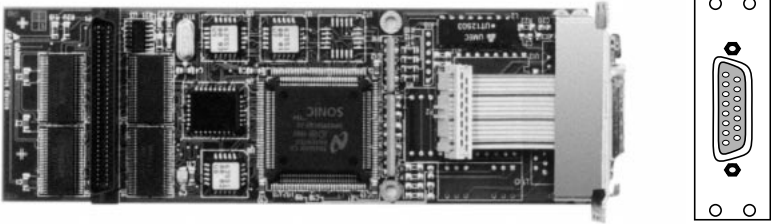


Figure 3: CM-AUI Adapter

Specially designed for the BIANCA/BRICK the CM-AUI is a 32 bit ethernet communications module. The CM-AUI module has a standard AUI interface which connects directly to your LAN. There are no jumper settings required.



CM-100BT Fast Ethernet Adapter

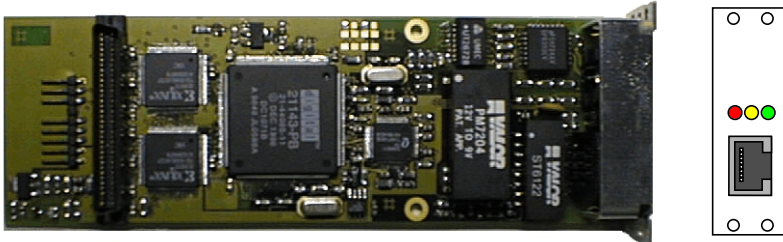


Figure 4: CM-100BT Adapter

The CM-100BT is a dual 10/100 Mbps ethernet module designed with flexibility in mind for sites that are moving, or have moved to Fast Ethernet networks. The back plane offers a twisted pair port on the back plane for the attachment of a switch or hub using Category 5 STP cable.

Pin assignments for the UTP port are shown in *Appendix A*. There are three status indicators located on the back plane. The LEDs indicate various status conditions, as follows:

CM-100BT back plane LEDs:

Colour	State	Meaning
Red	On	Receiving packets.
Amber	On	Transmitting packets.
Green	On	10 Mbps mode enabled.
	Blink	100 Mbps mode enabled.
	Off	Network interface down.

CM-BNCTP Ethernet Adapter



Figure 5: CM-BNCTP Adapter

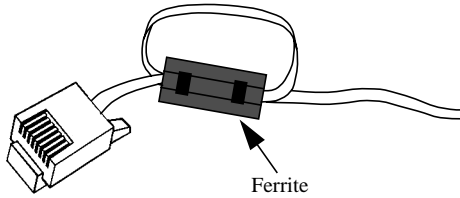
The CM-BNCTP is an ethernet communication module designed for the BRICK. It offers both a BNC port and a twisted pair port on the back plane. The back plane of the BNCTP also has three status indicators. They have the following meanings:

CM-BNCTP back plane LEDs:

Colour	State	Meaning
Red	On	Receiving packets.
Amber	On	Transmitting packets.
Green	On	Network interface is up.

Note: When using the UTP port a ferrite must be attached as follows.

1. Make sure the system is powered off.
2. Make a small loop in your twisted pair cable as close as possible to the BRICK and attach a ferrite as shown.



3. Attach the cable to the CM-BNCTP's UTP port.
4. Attach the other end of the cable to an available input port on your concentrator or hub.

CM-TR Token Ring Adapter

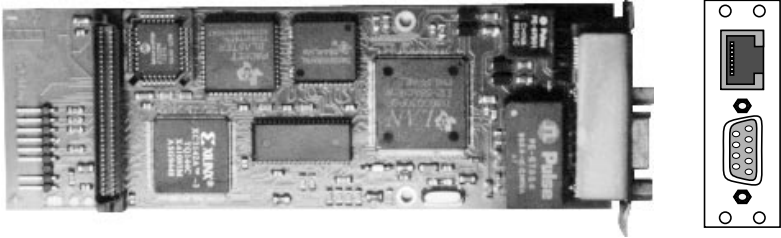


Figure 6: CM-TR Adapter

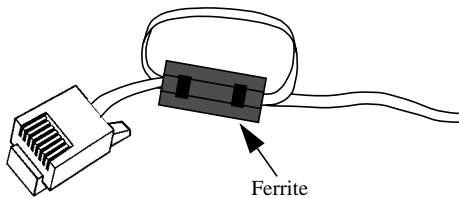
The CM-TR is a communication module designed for connecting the BRICK-XL2 to a Token Ring network. The CM-TR module can operate at both 4Mbits or 16Mbits and supports Early Token Release in accordance with IEEE standard 802.5.

The token ring module offers both a 9 pin DB-9 port and a RJ-45 port for twisted pair cabling. See Appendix A (pages 241 and 236) for individual pin assignments for the DB-9 and RJ-45 ports. There are no jumper settings required.

By default the token ring module is configured for 16Mbit operation with early token release. These settings can be changed, see Chapter 4.

Note: When using the UTP port a ferrite must be attached as follows.

1. Make sure the system is powered off.
2. Make a small loop in your twisted pair cable as close as possible to the BRICK and attach a ferrite as shown.



3. Attach the cable to the CM-TR's UTP port.
4. Attach the other end of the cable to your MAU.

The WAN Modules

CM-1BRI S₀ BRI Adapter

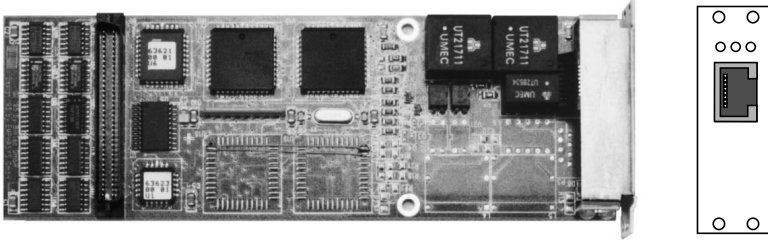


Figure 7: CM-1BRI Adapter

The CM-1BRI is a basic rate interface adapter specially designed for the BIANCA/BRICK. As a basic interface to the integrated services digital network, it has a single S₀ port on the back plane. CM-1BRI supports the standard D channel for signalling, and two B (bearer) channels for data transfers.

There are three status indicators located on the back plane. The LEDs indicate various status conditions, as follows.

CM-1BRI back plane LEDs:

Colour	State	Meaning
Red	On	One or more B channels are in use.
Amber	On	D channel currently in use, protocol stack is loaded.
Green	On	Layer 1 of ISDN connection is stable.

CM-1EBRI S₀ BRI Adapter

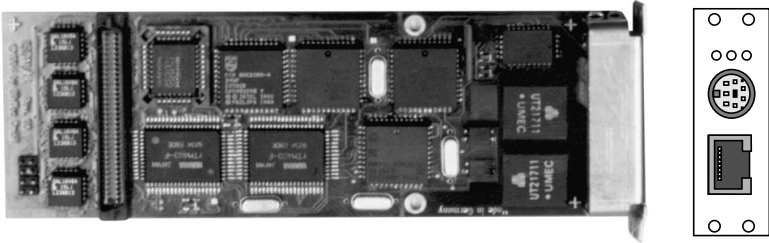


Figure 8: CM-1EBRI Adapter

The CM-1EBRI is a basic rate interface adapter designed for the BIANCA/BRICK. The CM-1EBRI has on-board hardware for group 3 FAX support, V.110, and support for analog modem communications. On the backplane, there is an S₀ port and a special audio interface. The audio interface is available for connecting a special headset for telephony applications. See Appendix A on page 242 for pin assignments for the audio interface. This adapter supports the standard D channel and two B channels.

There are three status indicators located on the back plane. The LEDs indicate various status conditions, as follows:

CM-1EBRI back plane LEDs:

Colour	State	Meaning
Red	On	One or more B channels are in use.
Amber	On	D channel currently in use, protocol stack is loaded.
Green	On	Layer 1 of ISDN connection is stable.

CM-2BRI 2xS₀ BRI Adapter

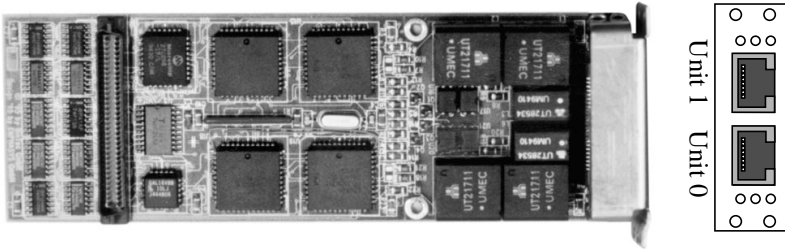


Figure 9: CM-2BRI Adapter

The CM-2BRI is a basic rate interface adapter designed for the BIANCA/BRICK. This adapter has two S₀ ports on the back plane (Unit 0 and Unit 1), which combined, support 4 B channels and 2 D channels for signalling.

There are six status indicators located on the back plane; each S₀ interface is assigned 3 LEDs. The LEDs correspond to various status conditions for their respective ports as follows:

CM-2BRI back plane LEDs:

Colour	State	Meaning
Red	On	One or more B channels are in use.
Amber	On	D channel currently in use, protocol stack is loaded.
Green	On	Layer 1 of ISDN connection is stable.

CM-2XBRI Enhanced 2xS₀ BRI Adapter

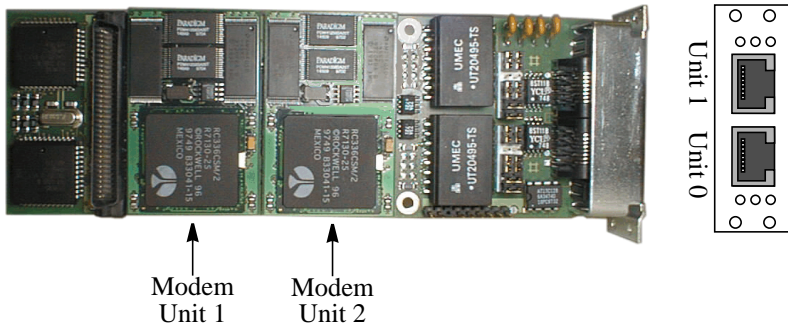


Figure 10: CM-2XBRI Adapter

The CM-2XBRI is a basic rate interface adapter that supports up to two daughter card modem boards. Each modem board includes two digital modems supporting V.34 data transmission (33.6Kbps) and V.17 FAX (14.4Kbps).

As a double BRI adapter, two S₀ ports are located on the back plane (Units 0 and 1 shown above), which combined, support 4 B channels and 2 D channels for signalling.

Six status indicators located on the back plane; each S₀ interface is assigned 3 LEDs. The LEDs correspond to various status conditions for their respective ISDN ports as follows:

CM-2XBRI back plane LEDs:

Colour	State	Meaning
Red	On	One or more B channels are in use.
Amber	On	D channel currently in use, protocol stack is loaded.
Green	On	Layer 1 of ISDN connection is stable.

TE / NT Mode Jumper Settings

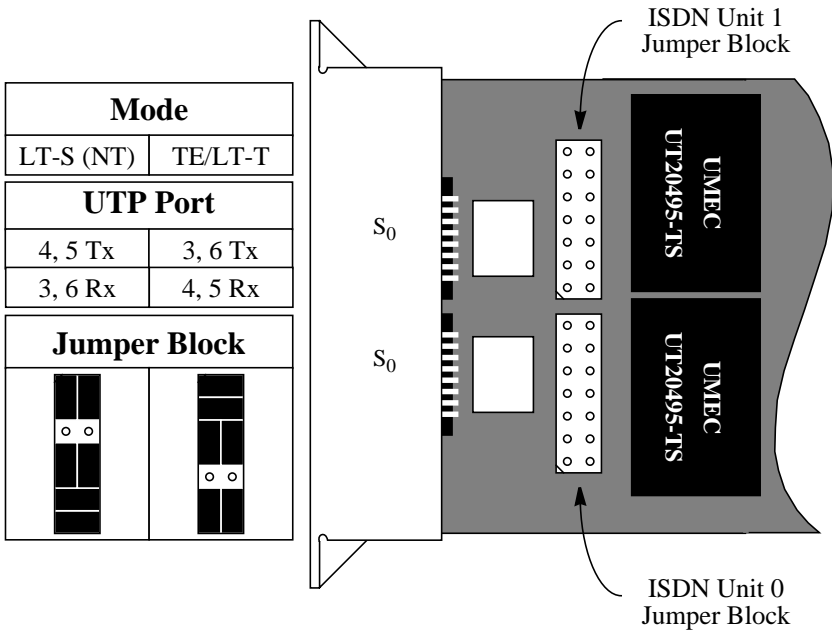
There are 14 jumper pairs (7 for each ISDN Unit) located on the CM-2XBRI which designate which mode (TE or NT) the respective ISDN port should operate in. By default TE mode is configured. NT mode means that your BRICK will supply a carrier signal to the bus, allowing you to connect other ISDN equipment (telephone, fax, etc.) to your BRICK.

Note: Currently, only TE mode may be used. Using NT mode could damage your CM-2XBRI. Support for NT mode is planned for a future software release.



Use the jumpers settings exactly as shown below for TE mode. The jumpers are installed correctly on delivery.

The jumper settings for TE and NT mode are shown below.



BIANCA/CM-PRI S_{2M} PRI Adapter

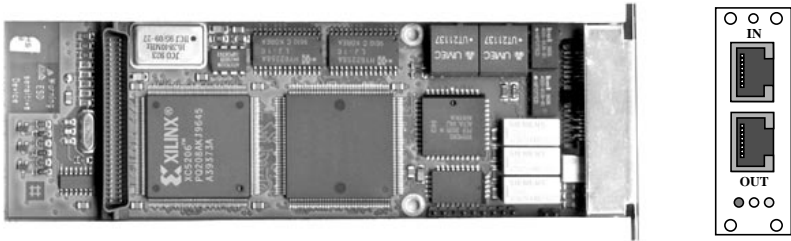


Figure 11: BIANCA/CM-PRI Adapter

Designed as a primary rate interface for the BRICK, the BIANCA/CM-PRI (hardware Rev. 2.1) has one S_{2M} interface (marked IN) on the back plane, and one OUT port which can be used with internal relays for PRI Circuit Switching. This allows a connected PRI line to be automatically switched over to a backup router if the BRICK is powered down.

BIANCA/CM-PRI supports one D channel for signalling and up to 30 B channels for data transfers. In addition, the BIANCA/CM-PRI is prepared to work with BinTec's modem modules.

There are also three status indicators located on the back plane. The LEDs indicate various status conditions, as follows:

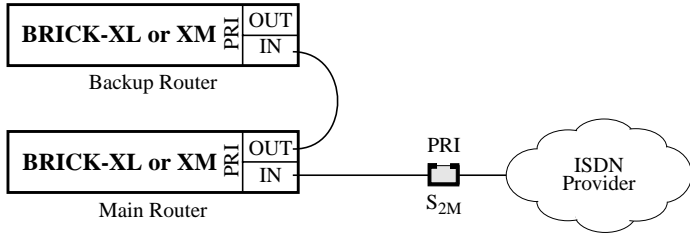
BIANCA/CM-PRI back plane LEDs:

Colour	State	Meaning
Red	On	One or more B channels are in use.
Amber	On	D channel currently in use, protocol stack is loaded.
Green	On	Layer 1 of ISDN connection is stable.

See Appendix A on page 237 for additional information on installing an NT for use with the BRICK-XL2 and BIANCA/CM-PRI module.

PRI Circuit Switching

As long as the BRICK is receiving power all traffic received from the IN port is processed locally. However, if power fails, the BRICK automatically redirects signals from pin 1, 2, 4 and 5 of the IN port to pins 1, 2, 4 and 5 of the OUT port using internal relays.



To setup a backup router for the PRI line, connect a standard RJ-45 cable between the BIANCA/CM-PRI's OUT port and the IN port of the backup router.

Note: Note that only devices that are approved for connection to the public ISDN network in your country may be connected to the BIANCA/CM-PRI's OUT port.



CM-X21 Adapter

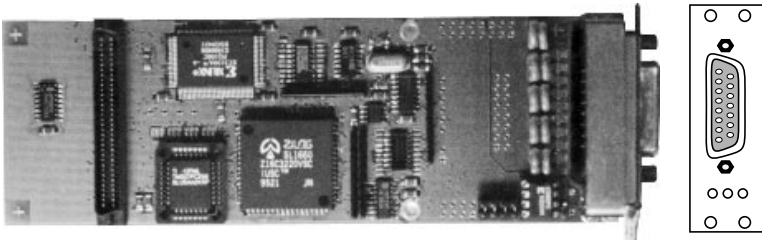


Figure 12: CM-X21 Adapter


The CM-X21 module provides a standard X.21 interface which complies with the V.11 recommendation. The X.21 interface provides a full-duplex

synchronous mode and can be configured to operate as either a DTE (passive mode) or DCE (active mode). When in active mode the X.21 interface can be set to operate at baud rates between 2400 and 2048k.

There are also three status indicators located on the back plane. The LEDs indicate various status conditions, as follows:

CM-X21 back plane LEDs:

Colour	State	Meaning
Red	On	Error transmitting a packet.
Amber	On	Frame being sent/received.
Green	On	Layer 1 is active (i.e., incoming and outgoing calls are possible).

Note:  The four jumper settings on the X.21 module are intended for future use. They should remain bridged (or jumpered), these are the default settings and should not be changed.

Function Modules

Function modules add new functions to your BRICK-XL2. The following function modules are currently available:

- FM-8MOD modem modules, which add 8 to 64 analog K56flex/V.90 compatible modems to your BRICK-XL2.
- FM-STAC, which can perform STAC compression on all B channels available on your BRICK-XL2.

FM-8MOD Modem Module

Hardware

The modem hardware consists of several components. The FM-MODI2 Modem Connection Kit which comes with: a modem shuttle frame which is installed below the main board, a special feature module which fits into any BRICK-XL2 SBus slot (5, 6, and 7 are preferred), two ribbon cables for connecting the feature module to the shuttle, and one or more FM-8MOD modem modules each containing eight K56flex/V.90 compatible modems. Each shuttle holds up to four FM-8MOD modem modules.

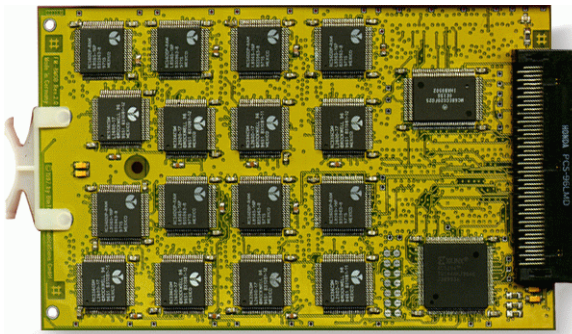


Figure 13: FM-8MOD modem module



Up to two FM-MODI2 shuttle frames can be installed on the BRICK-XL2 for a total of up to 64 modems. FM-MODI2 modem connection kits may be purchased directly from BinTec Communications or from your local BinTec distributor.

K56flex/V.90 Technology

The K56flex technology offers a new step up in modem speed. In conjunction with digital exchanges it is now possible to achieve data rates of up to 56kbps from central-site modems connected to the ISDN (e.g. internet service providers) to the client modem connected to the analogue telephone network (*downstream*). The other direction—from client to server (*upstream*)—still uses the V.34 standard with speeds of up to 33.6kbps.

This technology is especially useful for applications, where the data throughput is typically larger in the server→client direction (*downstream*), e.g. for internet providers.

Supported Standards

Each FM-8MOD function module offers eight modems capable of all current modem standards including K56flex and V.90, as well as the most commonly used fax standards. You can have up to eight FM-8MOD modules installed in your BRICK-XL2, thus offering up to 64 independent analog fax modems in connection with the FML-MODI2 modem connector module and a BIANCA/CM-PRI S_{2M} module.

Each modem on the FM-8MOD supports the following standards:

Standard	Description
K56flex/V.90	56,000, 54,000, 52,000, 50,000, 48,000, 46,000, 44,000, 42,000, 40,000, 38,000, 36,000, 34,000, or 32,000 bps <i>downstream</i> 33,600, 31,200, 28,800, 26,400, 24,000, 21,600, 19,200, 16,800, 14,400, 12,000, 9,600, 7,200, 4,800, or 2,400 bps <i>upstream</i>
V.34	33,600, 31,200, 28,800, 26,400, 24,000, 21,600, 19,200, 16,800, 14,400, 12,000, 9,600, 7,200, 4,800, or 2,400 bps
V.FC (»Fast Class«)	28,800, 26,400, 24,000, 21,600, 19,200, 16,800, 14,400, 12,000, 9,600, 7,200, 4,800, or 2,400 bps

Standard	Description
V.32bis	14,400, 12,000, 9,600, 7,200, or 4,800 bps
V.32	9,600, 7,200, or 4,800 bps
V.23	1,200 bps (1200/75, BTX)
V.22bis	2,400 or 1,200 bps
V.22	1,200 bps
Bell 212	1,200 bps
V.21	300 bps
Bell 103	300 bps
V.42 LAPM, MNP 2-4, 10	Error correction modes
V.42bis, MNP 5	Data compression
V.27	fax at 2400, 4800 bps
V.29	fax at 7200, 9600 bps ^a
V.17	fax at 7200, 9600, 12000, 14400 bps ^a

- a. When the CAPI (client) application requests a transmission speed, the BRICK always negotiates the best possible speed with the remote side. If the remote side is only capable of 7200 or 9600, V.29 modulation is used since this standard is most commonly supported.

The modems are not bound to a certain B channel, but are allocated to the next free channel as needed. This *dynamic resource allocation and distribution* technology (DRAD) provides for maximum flexibility.

You can easily update the system software for your modem modules by using the *modem* command (see p. 190).

FM-STAC Compression Module

The FM-STAC module fits in any BRICK-XL2 SBus slot. There are no connectors on its backplane. You do not need a special license to use the STAC compression.

Once you have installed the FM-STAC module in an empty slot of your BRICK-XL2 you can use STAC compression with all *PPP Encapsulations* (**ppp**, **x25_ppp**, **x75_ppp**, **x75btx_ppp**) by setting the *Compression* variable to **stac** from the SNMP shell, or by choosing the **PPP + Compression** or **X.25:PPP + Compression** encapsulations from the [WAN Partner][ADD] menu in the Setup Tool.

The FM-STAC module is able to compress data on all ISDN B channels available on your BRICK simultaneously. The compression ratio is typically 2-4.

Installing Communications Modules

If you ordered additional communication modules with your BRICK-XL2 or need to reconfigure the hardware setup, in the future you may need to install/exchange the communications modules. This section describes the procedures needed to do so. To install FM-8MOD modem modules see page (229) "Installing the Modem Connection Kit". If your BRICK has arrived with the communications modules already in place, you can skip this section and return to it when needed.

Note: Static electricity can cause severe damage to electronic equipment. To minimize the chance of damage to the BIANCA/BRICK or your communications modules, these safety precautions should be followed.



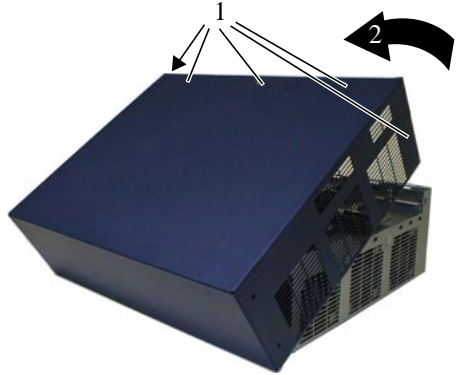
1. Always handle circuit boards by the edges only. Never touch the exposed circuitry.
2. Ground yourself before handling the communications modules. To discharge any static electricity from your body, touch the metal chassis of a computer that is plugged in but turned off.

To install or exchange communications modules:

Disconnecting the BIANCA/BRICK-XL2

1. Disconnect all cables to the BRICK-XL2. If the BRICK-XL2 is mounted in a 19" rack dismount it and remove the mounting brackets.
2. Position the BRICK- XL2 on a clean flat surface.

3. Remove the five screws (1) securing the external housing in place. (Three on top and one each on the sides.)
4. Holding the front of the housing in place tilt the rear of the housing up and away from the internal chassis (2) until it is at 90 degrees to the chassis.



Note: Before removing or installing modules.



If you previously saved configuration information, the modules must be reinstalled in the same slots. Otherwise, your configuration settings won't correspond to the board assignments and the BRICK will not function properly.

Removing Modules

5. Remove all screws securing the modules. These are located on the back plane along the left and right sides of each module. The back planes of the communication modules are formed to overlap, so that they fit snugly together once installed. Grasping the module at the edges, pull the module upward out it's socket.

Installing Modules

6. Remove dummy plates of the BRICK-XL2's back plane if required. Position the back plane of the module in an open window of the BRICK-XL2's back plane, so that the pins line up with the socket on the main board. Ensure that the back planes of the modules and the dummy plates overlap properly. Then push down lightly until the pins are seated in the sockets.

Reattaching the BIANCA/BRICK-XL2

7. Once you are finished inserting or removing the modules reattach dummy plates if required and lightly secure each module into place by replacing the screws on the back plane.
8. Align the external housing with the metal tabs located on the front side of the BRICK-XL2's chassis (as shown in Step 4 above).
9. Holding the front of the housing in place, tilt the rear of the housing to the rear and secure it to the chassis with the five screws you removed earlier (and the mounting brackets if applicable). Reattach the network cables and then the power cord to power up the BRICK.

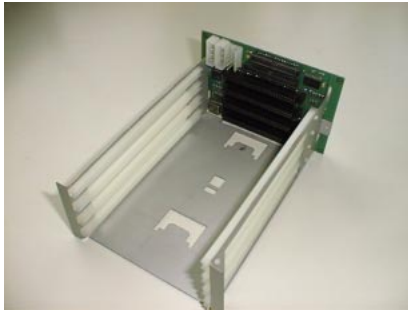
Installing the Modem Connection Kit

This section describes installing the FM-MODI2 Modem Connection Kit.

Requirements:

With your FM-MODI2 kit you will have received:

- One FM-MODI2 internal modem shuttle:



- One FM-MODI2 SBus function module:



- One 34-pin ribbon cable.
- One 40-pin ribbon cable.

To install the modem kit you will also need a cross-tip screwdriver.



Safety Precautions:

Note: Static electricity can cause severe damage to electronic equipment. To minimize the chance of damage to the BRICK-XL2 or your FM-MODI2 Modem Connection Kit, these safety precautions must be followed.

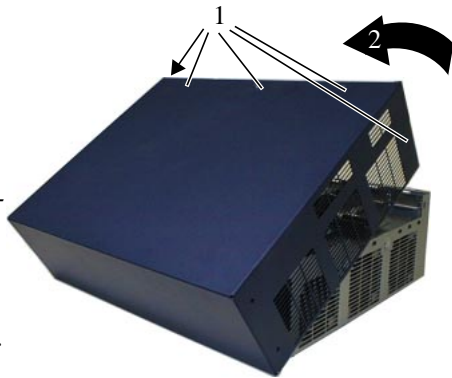
- Always handle circuit boards by the edges only. Never touch the exposed circuitry.
- Ground yourself before handling the FM-8MOD modem modules. To discharge any static electricity from your body, touch the metal chassis of a computer that is plugged in but turned off.

1. Disconnect all cables to the BRICK-XL2. If the BRICK-XL2 is mounted in a 19" rack, dismount it and remove the mounting brackets.

2. Position the BRICK-XL2 on a clean, flat surface.

3. With a cross-tip screwdriver remove the five screws (1) securing the external housing in place. (Three on top and one each on the sides.)

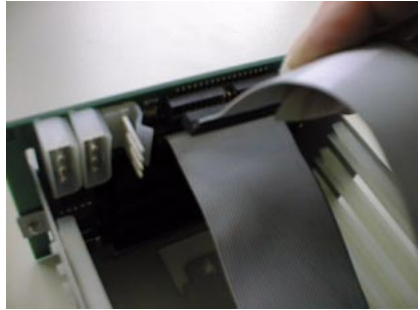
4. Holding the front of the housing in place, tilt the rear of the housing up and away from the internal chassis (2) until it is at 90 degrees to the chassis.



5. Connect both ribbon cables to the modem shuttle's backplane.

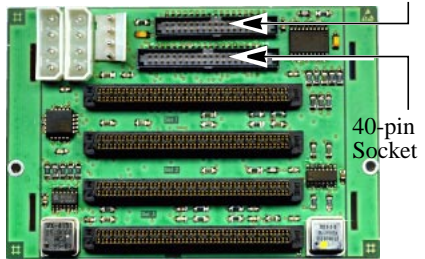
On the 34-pin and 40-pin ribbon cables locate the end of the cable with the notch pointing to the inside (towards the cable side).

Connect these ends of the cable to the shuttle's backplane (34-pin and 40-pin sockets) making sure to align the notches on the cable-ends with the cut-outs on the socket.



Modem Shuttle Backplane

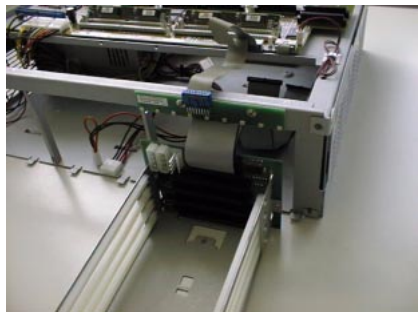
34-pin Socket



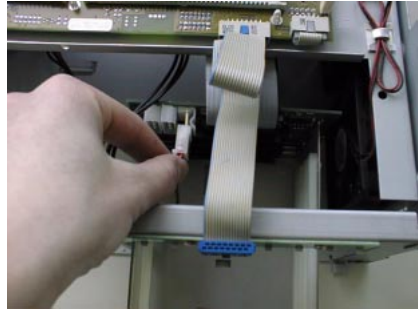
6. Locate a free slot. Only use slot 4 through 6, do not use the slot in which the power supply is mounted. In our example we use slot 6.

For easy attachment of the power connector, position the FM-MODI2 internal modem shuttle as shown here.

Feed the ribbon cables under the mainboard and align the shuttle housing with the metal cut-outs on the bottom.

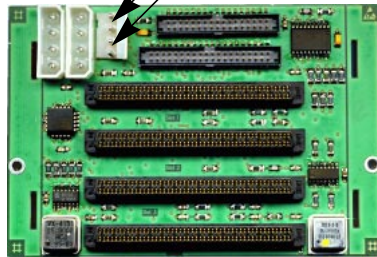


7. Locate an available internal power connector in the BRICK-XL2 and connect it to the power socket on the modem shuttle. The red wires should be at the top. The nose of the internal power connector should snap into place.



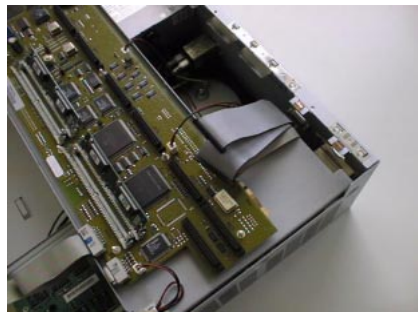
Power Socket

Red
Black

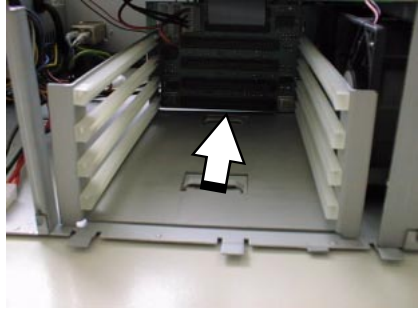


Modem Shuttle Backplane

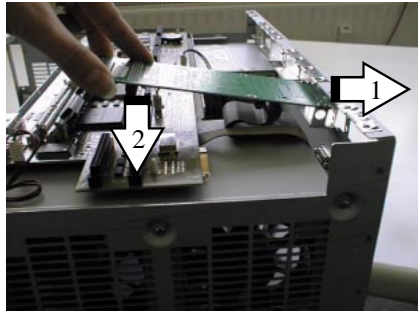
8. Feed the ribbon cables under the mainboard and pull them out at the rear side of the mainboard as shown beneath. Ensure that the ribbon cables and the power cable do not cross or are parallel. In rare cases this can lead to a failing data transmission.



9. Pressing the shuttle down, slide the shuttle forward until it snaps into place.



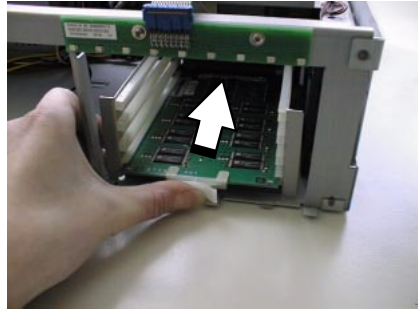
10. Connect the ribbon cables to the included SBus module and install the module into an SBus slot (slots 5 - 7 are preferred) as described below:



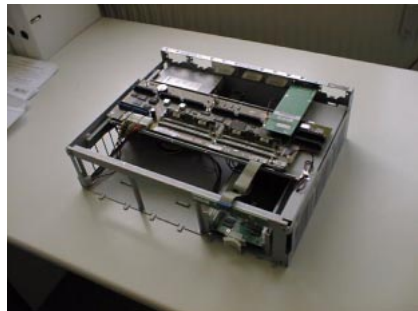
NOTE: Although the FM-MODI2 SBus module may be installed in any slot, try to avoid rearranging existing modules. If existing modules are not reinstalled in the same slots, your configuration settings won't match to the new arrangement and the BRICK won't work properly.

- Connect the ribbon cables to the SBus module.
- Remove dummy plates of the BRICK-XL2's back plane if required.
- Arrange the ribbon cable as shown above.
- Position the back plane of the SBus module in an open window of the BRICK-XL2's back plane (1) so that the pins line up with socket on the mainboard. Ensure that the back planes of the SBus module and the dummy plates overlap properly.
- Then push down lightly (2) until the pins are seated in the socket.
- Secure the SBus module into place by replacing screws on the back plane. Reattach dummy plates if required.

11. To install your FM-8MOD modem board(s), align the modem module with a free slot in the shuttle frame. Note that you must begin with Slot 1 on the bottom of the shuttle, then continue with Slot 2, Slot 3 etc. Slowly slide the module into place until it contacts with the 96-pin port on the shuttle's backplane. Then gently push the module forward until the pins are seated in the sockets.



12. Once you have installed your modem modules, align the housing with the metal tabs located on the front side of the BRICK-XL2's chassis. Holding the front of the housing in place, tilt the housing to the rear and secure it to the chassis with the five screws you removed in step 3 (and the mounting brackets if applicable). Reattach the network and power cabling to power up the BRICK.



13. After rebooting the BRICK, you can verify the installed modems have been detected by either:

- Checking the contents of the *biboAdmBoardTable* from the SNMP shell. You should find an entry with a *PartNo* field of FM-MOD-56K/X X denotes the number of installed modems.
- Viewing Setup Tool's main menu. The FM-MOD-56K string mentioned above should also appear in the main menu under the slot number where the FM-MODI SBus module is installed.

To verify the operational state of each installed modem refer to Setup Tool's **MONITORING AND DEBUGGING** → **MODEM** menu.

A

TECHNICAL DATA

What's covered

- General System Specifications
- Pin Assignments
 - ISDN Interfaces
 - Ethernet
 - Serial Port
 - Other Modules
- Important Safety Information in:
 - Danish, Dutch, Finnish, French,
 - German, Greek Safety Instructions, Italian,
 - Norwegian, Portugese,
 - Swedish, Spanish

General System Specifications

- Processor: MC68EC040, 33 MHz
- Memory: 2 x 8 MB/32 bit EDO SIMM,
2 MB/8 bit flash-ROM
- Interfaces: 7 miniSBus slots
(for communications modules)
- Serial: 1 x RS 232 C, Sub9 Male (PC), 1,200 - 115k Bd.
- LEDs: 9 (1 Power, 7 Function, 1 Error)
- Power: 115/230 VAC, 60/50 Hz, max. 6.0/3.0 A, universal power supply¹ with internal fan.
- Dimensions: 440 mm x 132 mm x 360 mm (WHD)
- Weight: 7.5 Kg.

1. The universal power supply senses the incoming voltage and adjusts accordingly. However, using a voltage other than 230V will require a separate power cord (not included).

Pin Assignments

ISDN S₀ Interface(s) for CM-1BRI, CM-2BRI

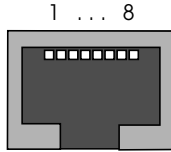


Figure 14: ISDN S₀ BRI Interface

Pin assignments for S₀ ports are is as follows:

Pin	Function
1	Not used
2	Not used
3	Transmit (+)
4	Receive (+)
5	Receive (-)
6	Transmit (-)
7	Not used
8	Not Used

UTP Port for the BIANCA/CM-PRI

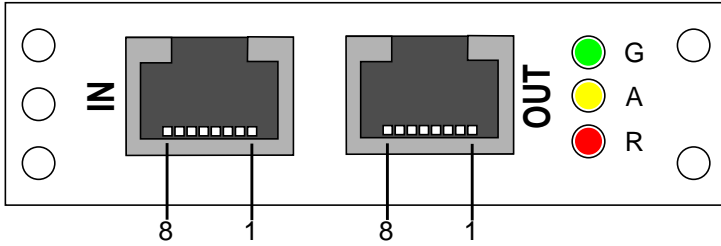


Figure 15: ISDN S_{2M} PRI Interface

Pin assignments for the IN and OUT ports of the CM-PRI S_{2M} module:

Pin	Function	Normal marking on NT
1	Receive, NT to TE (+)	S2Mab/a
2	Receive, NT to TE (-)	S2Mab/b
3	Not used	
4	Transmit, TE to NT (+)	S2Man/a
5	Transmit, TE to NT (-)	S2Man/b
6-8	Not used	

Note: Installing an NT (Network Terminator)



For the installation of an NT for the PMX, it is advisable to install an appropriate main-socket with the above mentioned pin assignments for send and receive lines.

This will allow for easy connection of the BRICK's PRI interface using the included cable. Additionally, note that for the NT, a separate voltage supply (60V) needs to be installed. The company that installs your NT should be informed that this voltage supply needs to be installed separately and is not being provided for by the connected end devices (usually a PBX for S_{2M} interfaces).

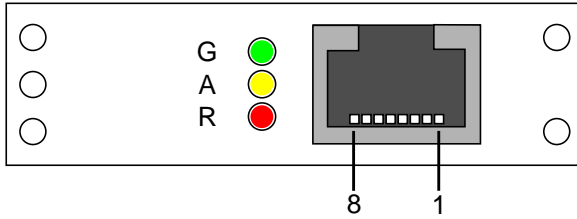
Special Note for NTs in Germany

In Germany, the send lines (NT->TE) on the connector block are often marked with S2Mab (a and b), and the receive lines (TE->NT) with S2Man (a and b).

On the NT itself, there are usually several LEDs provided for displaying various status conditions. The following indicators and their meanings seem to be somewhat standardized. In doubt, please refer to the operators manual for your NT.

- LED1 Color: green
 Marked: "NT"
 Meaning: LED-on normally means that the proper voltage is being supplied.
- LED2 Color: red
 Marked: "UK2"
 Meaning: LED-on (or blinking) normally means that the S_{2M} interface has not been activated at the switching station. In such cases, you will have to contact you local telephone company to have the interface activated.
- LED3 Color: red
 Marked: "S2M"
 Meaning: LED-on normally means that signals are not being received from the end device.

TP Port for the CM-100BT



The backplane of the CM-100BT communications module consists of an RJ-45 port for the connection of a category 5 TP cable (with external shielding) and three LEDs for status indications.

Pin Assignments		Status Indicators		
Pin	Function	Colour	State	Meaning
1	Transmit (+)	Red	On	Receiving packets.
2	Transmit (-)	Amber	On	Transmitting packets.
3	Receive (+)	Green	On	10Mbps mode operation.
6	Receive (-)		Blink	100Mbps mode operation.
4,5,7,8	Not used		Off	Network interface down.

Pinout/colours for straight-through and crossover cables.

Note that pairs: 1-2, 3-6, 4-5, and 7-8 **must** be twisted.

Straight-Through Cable		Crossover Cable	
Pin	Colour (both ends)	End One	End Two
1	Orange-White	Orange-White	Green-White
2	Orange	Orange	Green
3	Green-White	Green-White	Orange-White
4	Blue	Blue	Brown-White
5	Blue-White	Blue-White	Brown
6	Green	Green	Orange
7	Brown-White	Brown-White	Blue
8	Brown	Brown	Blue-White

Serial Port

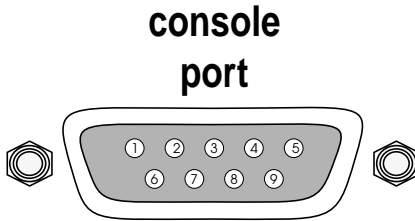


Figure 16: 9 Pin Serial Port

Pin assignments for the 9 pin serial port are as follows:

Pin	Function
1	DCD (not connected)
2	Receive
3	Transmit
4	DTR - DSR (redirected to pin 6)
5	Ground
6	DSR - DTR (redirected to pin 4)
7	RTS - CTS (redirected to pin 8)
8	CTS - RTS (redirected to pin 7)
9	(not connected)

DB9 Port for the CM-TR

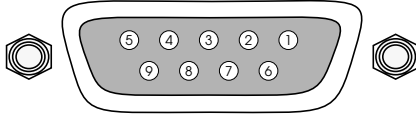


Figure 17: 9 Pin Port for Token Ring Interface

Pin assignments for the DB9 port are as follows:

Pin	Function
1	Receive (-)
2	Not Connected
3	Not Connected
4	Not Connected
5	Transmit (-)
6	Transmit (+)
7	Not Connected
8	Not Connected
9	Receive (+)

For the pin assignments for the RJ-45 port on this module, see page 236.

Audio interface for the CM-1EBRI

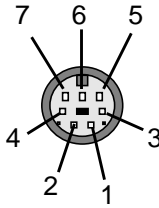


Figure 18: CM-1EBRI Audio Interface

The pin assignments for the CM-1EBRI audio interface are as follows:

Pin	Function
1	Loudspeaker (-)
2	Loudspeaker (+)
3	Earpiece (-)
4	Earpiece (+)
5	Hook switch
6	Ground
7	Microphone

The audio interface can be used for connecting special handsets. These audio devices consist of a microphone, earpiece, and a loudspeaker. Both dynamic and electret microphones are supported.

Note: The loudspeaker and earpiece receptacles for audio interfaces must be ground-free. To connect an external amplifier to a receptacle, signals must be decoupled using a capacitor.



15 Pin Port for the CM-X21

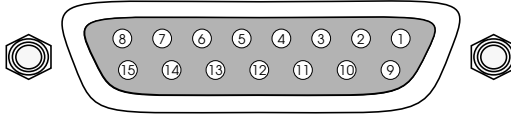


Figure 19: 15 Pin X.21 Port

The pin assignments for the CM-X21 module conform to the V.11 recommendations and are as follows:

Pin	Function	Mnemonic
1	Protection Ground	PG
2	Transmit (A)	T
3	Control (A)	I
4	Receive (A)	R
5	Indicate (A)	I
6	Signal Timing Element (A)	S
7	Not Connected	
8	Signal Ground	SG
9	Transmit (B)	T
10	Control (B)	I
11	Receive (B)	R
12	Indicate (B)	I
13	Signal Timing Element (B)	S
14	Not Connected	
15	Not Connected	

Important Safety Information

Danish: Sikkerhedshenvisninger

Apparatet opfylder de pågældende sikkerhedsbestemmelser for informationsteknisk udstyr til brug i kontoromgivelser.

I dette afsnit finder De sikkerhedshenvisninger, som De absolut skal overholde, når De håndterer Deres system.

Hvis De har spørgsmål med hensyn til opsætning og drift i den beregnede omgivelse, bedes De venligst at henvende Dem til vores service.

- BRICK er beregnet til at blive brugt på kontorer. BRICK opbygger som ISDN-multi-protokol-routere ISDN-forbindelser afhængigt af systemkonfigurationen. De bør overvåge produktet for at undgå uønskede gebyrer.
- Apparatet skal kun transporteres i originalemballagen eller anden egnet forpakning, som beskytter mod stød og slag.
- Venligst læg mærke til henvisningerne for omgivelelsesbetingelserne før apparatet opstilles eller tages i drift.
- Når apparatet flyttes fra kolde omgivelser ind i driftsrummet, er det muligt, at bedugging opstår både på apparatets ydre og indre. Vent indtil en temperaturudligning har fundet sted og apparatet er helt tørt før det tages i drift.
- Kontroller om apparatets nominelle spænding, som angives på typeskiltet, stemmer overens med den lokale netspænding. Apparatet må anvendes under følgende betingelserne:
115 / 230 VAC
60 / 50 Hz
maks. 6,0 / 3,0 A
- Tilslut apparatet kun til en stikdåse med beskyttelsesleder, som er jordforbundet efter forskrifterne (apparatet er udrustet med en sikkerhedskontrolleret netledning).
- Vær sikker på, at husinstallationens stikdåse med beskyttelsesleder er frit tilgængelig. For en fuldstændig adskillelse fra nettet skal netstikket trækkes.
- Læg ledningerne således, at de ikke danner en farekilde (snublefare) og ikke beskadiges. Ved tilslutning af apparatet læg venligst mærke til de pågældende henvisninger i driftsvejledningen.
- Dataoverføringsledningerne skal under tordenvejr hverken tilsluttes eller frakobles.
- Ved systemets ledningsinstallation læg venligst mærke til rækkefølgen, som beskrevet.
- Pas på, at ingen objekter (f. eks. smykkekedler, clips osv.) eller vædske kan nå ind i apparatets indre (elektrisk stød, kortslutning).
- OBS: Ved u hensigtsmæssig udskiftning af batteriet består eksplosionsfare. Må kun udskiftes med samme eller ækvivalent type. De brugte batterier skal bortskaffes i hehold til producentens oplysninger.
- I nødstilfælde (f.eks. beskadiget kasse eller betjeningslemme, indtrængning af vædske eller fremmedlegemer) skal netstikket trækkes med det samme og servicen skal underrettes.
- Venligst læg mærke til, at den bestemmelsesmæssige drift af systemet (iht. IEC 950 / EN 60950) kun er sikret, når kabinetlåget er monteret (køling, brandbeskyttelse, afskærmning).
- Apparatet må kun åbnes af fagpersonale. Reparaturer skal derfor kun udføres af autoriseret fagpersonale. Ved uvedkommende åbning og u hensigtsmæssige reparaturer er det muligt, at brugeren udsættes for en betydelig fare.
- Anvend kun de vedlagte kabler. Hvis der anvendes andre kabler, tager BinTec Communications AG ingen ansvar for opståede skader.
- CE-tegnet betyder, at „BRICK“ svarer til følgende EF-retningslinjer: elektromagnetisk kompatibilitet (89/336/EWG) og lavspænding (73/23/EWG).
- Elektrostatisk opladning kan medføre skader i apparatet. De skulle derfor have en antistatisk manchette på håndledet eller berøre en jordet flade, før De berører det åbnede apparat.
- Apparatet må under ingen omstændigheder renses vådt. Pga. indtrængende vand kan der opstå alvorlige farer for anvenderen (f.eks. stød).
- Anvend aldrig skurepulver, alkaliske rengøringsmidler, korroderende eller skurende hjælpemidler. Overfladen af apparatet kan ellers beska diges.

Dutch: Veiligheidsadviezen

Het apparaat voldoet aan de desbetreffende veiligheidseisen voor installaties van informatietechniek voor kantoorgebruik.

De in dit hoofdstuk vermelde veiligheidsvoorschriften dienen beslist in acht te worden genomen.

Als u vragen heeft over het installeren en ingebruikneming van de apparatuur in de daarvoor bestemde ruimte, dient u contact op te nemen met onze service.

- BRICK is bestemd voor toepassing in een kantooromgeving. Als ISDN-Multi-Protocol-Router maakt BRICK afhankelijk van de systeemconfiguratie ISDN-verbindingen. Om ongewenste kosten te vermijden, dient u het product absoluut te bewaken.
- Vervoer dit apparaat alleen in de originele verpakking. Indien dit niet mogelijk is dient u van een andere geschikte schokvrije verpakking gebruik te maken.
- Voor installatie en ingebruikneming van de apparatuur dient u de veiligheidsvoorschriften van apparaat en bedrijfsruimte in acht te nemen.
- Wanneer het apparaat vanuit een koude omgeving in de bedrijfsruimte wordt gebracht, kan er condensvorming zowel aan de buiten- als ook aan de binnenkant ontstaan. Wacht tot het apparaat aan de temperatuur is aangepast en volkomen droog is voordat u het in gebruik neemt.
- Controleer of de op het typeplaatje van het apparaat aangegeven netspanning met de plaatselijke netspanning overeenkomt. Het apparaat mag alleen uitsluitend onder naleving van volgende voorschriften in bedrijf worden genomen:
115 / 230 VAC
60 / 50 Hz
maks. 6,0 / 3,0 A
- Sluit het apparaat alleen op een volgens voorschrift geaard veiligheidsstopcontact aan (het apparaat is van een op veiligheid gecontroleerde stroomkabel voorzien).
- Zorg er voor, dat het veiligheidsstopcontact van de huisinstallatie vrij toegankelijk is. Haal de stekker uit het stopcontact als u de stroomtoevoer wilt onderbreken.
- Breng de aansluitingen zodanig aan, dat deze geen gevaar vormen (struikelen) en niet beschadigd kunnen worden. Let bij het installeren op de betreffende voorschriften voor ingebruikneming.
- De leidingen voor de gegevenstransmissie niet bij onweer aansluiten of loskoppelen.
- Let op de juiste kabelaansluitingen in de aangegeven volgorde.
- Attentie: Bij onjuist verwisselen van de batterij bestaat ontploffingsgevaar. Alleen omwisselen voor hetzelfde of een gelijkwaardig type. De gebruikte batterijen moeten volgens de aanwijzingen van de fabriek bij het afval gedaan worden.
- Zorg dat er geen voorwerpen (zoals sierketting, paperclip enz.) in het apparaat kunnen komen en stel het apparaat niet bloot aan vocht om kortsluiting of een gevaarlijke elektrische schok te voorkomen.
- Trek in noodgevallen (b.v. bij beschadiging van het frame of bedieningseenheid, bij indringen van vocht of voorwerpen) onmiddellijk de stekker uit het stopcontact en raadpleeg de service.
- Zorg er voor, dat de bediening van het apparaat alleen met een gesloten beschermkap geschiedt (koeling, brandbescherming, radio-ontstoring) en onder inachtneming van de bedrijfsvoorschriften (volgens IEC 950/EN 60 950) van het systeem.
- Open in geen geval zelf het apparaat. Voor uw eigen veiligheid gelieve u alle onderhoud uitsluitend door gekwalificeerd personeel te laten uitvoeren. Door onbevoegd openen en ondeskundige reparaties kunnen aanzienlijke gevaren voor de gebruiker ontstaan.
- Gebruik uitsluitend de meegeleverde kabels. Indien u andere kabels gebruikt, kan de firma BinTec Communications AG op geen enkele wijze verantwoordelijk worden gesteld voor enige vorm van schade.
- Electrostatische (op)ladingen kunnen tot schade aan het apparaat voeren. Draag daartoe een antistatische manschet om de pols of raak een geaard vlak aan, voordat u het geopende apparaat aanraakt.
- Het apparaat mag in geen geval nat worden gereinigd. Door indringend water kunnen aanzienlijke gevaren voor de gebruiker ontstaan (b.v. elektrische schok).
- Nooit een schuurmiddel, alkalische reinigingsmiddelen, scherpe of schurende hulpmiddelen gebruiken. De oppervlakte van het apparaat kan daardoor worden beschadigd.

Finnish: Turvallisuusohjeita

Laite vastaa toimistotiloissa käytettäviin tietotekniikan laitteisiin päteviä asianmukaisia turvallisuusohjeita.

Tästä jaksosta löytyvät ne turvallisuusohjeet, joiden noudattaminen on ehdottomasti välttämätöntä järjestelmän kanssa työskennellessä. Mikäli tarvitset lisätietoja laitteen pystyttämisen tai käytön suhteen suunnitellussa ympäristössä, käänny asiakaspalvelumme puoleen.

- BRICK on suunniteltu käytettäväksi toimistotiloissa. BRICK toimii ISDN-monikäytäntö-reittiohjaimena ja luo järjestelmän konfiguraation mukaisesti ISDN-yhteyksiä. Epätoivottujen maksujen välttämiseksi on tuotteen toimintaa välttämättä valvottava.
- Kuljeta laitetta vain alkuperäispakkauksessa tai muussa asianmukaisessa pakkauksessa, jossa laite on törmäys- ja iskusuojattu.
- Ota ympäristöolosuhteita koskevat ohjeet huomioon ennen laitteen pystyttämistä ja käyttöä.
- Kun laite tuodaan kylmästä tilasta käyttötilaan, voi sekä laitteen ulko- että sisäpuolella ilmetä kosteutta. Odota, kunnes laite on sopeutunut lämpötilaan ja ehdottomasti kuiva, ennenkuin otat sen käyttöön.
- Tarkasta, vastaako laitteen tyyppikilven nimellisyännite paikallista verkkoyännitettä. Laitetta saa käyttää seuraavien olosuhteiden vallitessa:
115 / 230 VAC
60 / 50 Hz
maks. 6,0 / 3,0 A
- Kytke laite vain sääntöjenmukaisesti maadoitettuun suojakosketinpistorasiaan (laite on varustettu turvallisuustarkastetulla verkkojohdolla).
- Varmista, että sisäasennuksen suojakosketinpistorasia on esteettömästi saavutettavissa. Täydellisen erottaminen verkosta on tehtävä vetämällä verkkopistoke.
- Sijoita johdot niin, että niistä ei aiheudu vaaraa (kompastumisvaara) ja että niitä ei vahingoiteta. Tee laitteen liitännät käyttöohjeen vastaavia kohtia noudattaen.
- Älä liitä tiedonvälitysjohtoja äläkä vedä niitä pois ukonilman aikana.
- Noudata järjestelmän kaapeloinnissa kuvauksen mukaista järjestystä.
- Varmista, että pieniä osia (esim. koruketjuja, paperipinteitä) tai nesteitä ei pääse tunkeutumaan laitteen sisäosaan (sähköisku, oikosulku).
- Huomio: Räjähdysvaara, jos paristot vaihdetaan epäasianmukaisesti. Vaihto vain samanlaiseen tai samanarvoiseen malliin. Käytettyjen paristojen jätteenpoisto on tehtävä valmistajan ohjeiden mukaisesti.
- Vedä hätätilanteessa (esim. vioittunut kotelo tai ohjausosa, nesteiden tai vieraiden osien sisään-tunkeutuminen) verkkopistoke heti ulos ja ota yhteys asiakaspalveluun.
- Huomaa, että järjestelmän käytön tarkoituksenmukaisuus (IEC 950/EN 60 950 muk.) on taattu vain kotolon kannen ollessa asennettuna (jäähdytys, palontorjunta, häiriönpisto).
- Vain ammattihenkilökunta saa avata laitteen. Tästä syystä kehotamme teettämään kaikki korjaukset valtuutetuilla ammatti henkilöillä. Asianton avaaminen ja asiantuntemattomat korjaustyöt voivat aiheuttaa käyttäjälle huomattavia vaaroja.
- Käytä vain mukana seuraavia kaapeleita. Mikäli käytetään muita kaapeleita, BinTec Communications AG ei vastaa tällöin syntyvistä vahingoista.
- CE-merkki tarkoittaa, että „BRICK“ vastaa seuraavia EY-direktiivejä: EMV (89/336/EWG) ja pienyännite (73/23/EWG).
- Laitteen „Euro-NUMERIS“ (Ranska) liitäntä on myös mahdollista, sillä laite täyttää Euroopan yhteisössä vaadittavien määräysten lisäksi myös ranskalaiset ISDN vaatimukset.
- Sähköstaattiset lataukset voivat johtaa laitteen rikkoutumiseen. Käytä tästä syystä antistaattista mansettia ranteen ympärillä tai koske maa doitetuun pintaan ennen kuin kosketat avattuun laitteeseen.
- Laitetta ei saa missään tapauksessa puhdistaa märillä välineillä. Sisääntunkeutuva vesi voi vaarantaa käyttäjän turvallisuutta (esim. sähköiskun vaara).
- Koskaan ei saa käyttää hankausaineita, emäksisiä puhdistusaineita, teräviä tai hankaavia apuvälineitä. Nämä voivat vaurioittaa laitteen pintaa.

French: Conseils de Sécurité

Cet appareil doit respecter certaines consignes de sécurité pour l'installation des techniques d'information et la mise en oeuvre dans son environnement de travail.

Dans ce document vous trouverez des conseils de sécurité à prendre en compte pour l'utilisation de votre système.

En cas de questions sur l'installation et le fonctionnement dans l'environnement prévu, n'hésitez pas à contacter notre service technique.

- BRICK est prévu pour être employé dans les bureaux. BRICK établit des connexions ISDN qui dépendent de la configuration du système en tant que routeur ISDN Multi à procès-verbal. Pour éviter de payer des taxes inconsidérément, vous devriez absolument surveiller ce produit.
- Le transport de l'appareil doit se faire dans l'emballage d'origine ou dans un autre protégeant des secousses et mauvais coups.
- Avant l'installation et l'utilisation de l'appareil, faire attention à bien respecter les conditions d'environnement.
- Si avant son utilisation l'appareil est mis en réserve dans un environnement froid, celui-ci peut-être humide non seulement extérieurement mais aussi intérieurement.
- Attendre donc que l'appareil soit à une température ambiante et totalement sec avant de le mettre en marche.
- Vérifier sur la plaque du constructeur que le voltage de l'appareil coïncide avec le voltage de l'environnement. Le matériel doit respecter les conditions suivantes :
115 / 230 VAC
60 / 50 Hz
maks. 6,0 / 3,0 A
- Ne relier l'appareil qu'à une prise de terre conforme aux instructions. (Le matériel est équipé d'une ligne de secteur conforme aux normes de sécurité.)
- Être certain que la prise de terre du bâtiment soit libre d'accès. Elle doit être séparée des autres prises du secteur.
- Poser les lignes électriques de façon à ce qu'elles n'entraînent aucun danger (risque de trébuchement) et qu'elles ne se détériorent pas.
- Prendre en considération les instructions du manuel d'utilisation pour le branchement électrique de l'appareil.
- Pendant un orage, ne pas connecter ou déconnecter les câbles de transmission de données ni ne débrancher l'appareil.
- Lors du câblage du système, respecter à l'ordre de priorité décrit dans le manuel.
- Attention: Il peut y avoir danger d'explosion, lors du changement inadéquat des piles. Remplacer seulement par le même modèle ou un équivalent. Les piles usées sont à jeter au rebut d'après les données du fabricant.
- Faire attention à ce qu'aucun objet (par ex. bijoux, trombones,...) ou qu'aucun liquide ne tombe dans l'appareil (décharge électrique, coupure de courant...)
- En cas d'urgence (introduction de capsules, ustensiles de bureau, liquides et autres corps étrangers dans l'appareil) débrancher immédiatement la prise et informer le service.
- Bien noter que du bon assemblage du boîtier dépend le bon fonctionnement du système (refroidissement, pare-feu, interférence magnétique).
- L'appareil ne doit être ouvert que par le personnel qualifié. Avant son ouverture, débrancher l'appareil. Par conséquent, ne laisser que le personnel autorisé faire les réparations.
- Une erreur dans l'ouverture du boîtier ou une erreur dans la réparation peuvent entraîner des conséquences extrêmement dangereuses pour l'utilisateur.
- N'utiliser que les câbles joints au matériel. En cas d'utilisation d'autres câbles, BinTec Communications ne se porte pas garant des incidents.
- Le signe CE signifie, que „BRICK“ correspond aux directives suivantes de la CEE: EMV (89/336/CEE) et basse tension (73/23/CEE).
- L'appareil peut être raccordé au système „Euro-NUMERIS“ (France), car il remplit en plus des réglementations nécessaires de la CEE, les caractéristiques de ISDN français.
- Des charges électrostatiques peuvent endommager les appareils. C'est pourquoi, il est recommandé de porter un manchon antistatique au poignet ou de toucher une surface mise à terre, avant d'ouvrir l'appareil.
- L'appareil ne doit en aucun cas être nettoyé au mouillé. D'importants dangers peuvent survenir pour l'utilisateur (par ex.: décharge électrique), si de l'eau pénètre dans l'appareil.

- N'employez jamais de produits abrasifs, de nettoyants alcalins ou autres produits tranchants ou grattants. La surface de l'appareil pourrait être de cette façon endommagée.

German: Sicherheitshinweise

Das Gerät entspricht den einschlägigen Sicherheitsbestimmungen für Einrichtungen der Informationstechnik für den Einsatz in einer Büroumgebung.

In diesem Abschnitt finden Sie Sicherheitshinweise, die Sie beim Umgang mit Ihrem System unbedingt beachten müssen.

Falls Sie Fragen zum Aufstellen und Betrieb in der vorgesehenen Umgebung haben, wenden Sie sich bitte an unseren Service.

- BRICK ist für den Einsatz in einer Büroumgebung bestimmt. Als ISDN-Multi-Protokoll-Router baut BRICK in Abhängigkeit von der Systemkonfiguration ISDN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen.
- Transportieren Sie das Gerät nur in der Originalverpackung oder einer anderen geeigneten Verpackung, die Schutz gegen Stoß und Schlag gewährt.
- Beachten Sie vor dem Aufstellen und Betrieb des Gerätes die Hinweise für die Umgebungsbedingungen.
- Wenn das Gerät aus kalter Umgebung in den Betriebsraum gebracht wird, kann Betauung - sowohl am Geräteäußeren als auch im Geräteinneren auftreten. Warten Sie, bis das Gerät temperaturangeglichen und absolut trocken ist, bevor Sie es in Betrieb nehmen.
- Überprüfen Sie, ob die auf dem Typenschild angegebene Nennspannung des Geräts mit der örtlichen Netzspannung übereinstimmt. Das Gerät darf unter den folgenden Bedingungen betrieben werden:
115 / 230 VAC
60 / 50 Hz
maks. 6,0 / 3,0 A
- Schließen Sie das Gerät nur an eine vorschriftsmäßig geerdete Schutzkontakt-Steckdose an (das Gerät ist mit einer sicherheitsgeprüften Netzleitung ausgerüstet).
- Stellen Sie sicher, daß die Schutzkontakt-Steckdose der Hausinstallation frei zugänglich ist. Zur vollständigen Netztrennung muß der Netzstecker gezogen werden.
- Verlegen Sie die Leitungen so, daß sie keine Gefahrenquelle (Stolpergefahr) bilden und nicht beschädigt werden. Beachten Sie beim Anschluß des Gerätes die entsprechenden Hinweise in der Betriebsanleitung.
- Schließen Sie Datenübertragungsleitungen während eines Gewitters weder an noch ziehen Sie sie ab.
- Beachten Sie beim Verkabeln des Systems die Reihenfolge, wie beschrieben.
- Achtung: Bei unsachgemäßem Austausch der Batterie besteht Explosionsgefahr. Ersatz nur durch denselben oder einem gleichwertigen Typ. Die gebrauchten Batterien sind nach Angaben des Herstellers zu entsorgen.
- Achten Sie darauf, daß keine Gegenstände (z. B. Schmuckketten, Büroklammern etc.) oder Flüssigkeiten in das Innere des Geräts gelangen (elektrischer Schlag, Kurzschluß).
- Ziehen Sie in Notfällen (z.B. geschädigtes Gehäuse oder Bedienelement, Eindringen von Flüssigkeit oder Fremdkörpern) sofort den Netzstecker und verständigen Sie den Service.
- Beachten Sie, daß der bestimmungsgemäße Betrieb (gem. IEC 950/ EN 60 950) des Systems nur bei montiertem Gehäusedeckel gewährleistet ist. (Kühlung, Brandschutz, Funkentstörung)
- Das Gerät darf nur von Fachpersonal geöffnet werden. Vor Öffnen des Gerätes Netzstecker ziehen. Lassen Sie deshalb Reparaturen am Gerät nur von autorisiertem Fachpersonal durchführen. Durch unbefugtes Öffnen und unsachgemäße Reparaturen können erhebliche Gefahren für den Benutzer entstehen.
- Verwenden Sie nur die beigelegten Kabel. Falls Sie andere Kabel verwenden, übernimmt BinTec Communications AG für auftretende Schäden keine Haftung.
- Das CE-Zeichen bedeutet, daß die BRICK den folgenden Richtlinien der EG entspricht: EMV (89/336/EWG) und Netzspannung (73/23/EWG).
- 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 berühren.
- Das Gerät darf auf keinen Fall naß gereinigt werden. Durch eindringendes Wasser können erhebliche Gefahren für den Anwender (z. B. Stromschlag) und das Gerät entstehen.
- Niemals Scheuermittel, alkalische Reinigungsmittel, scharfe oder scheuernde Hilfsmittel benutzen.

Greek Safety Instructions:

Πληροφορίες ασφάλειας

Η συσκευή ανταποκρίνεται στις συνήθεις διατάξεις ασφάλειας για εγκαταστάσεις της τεχνικής πληροφοριών για χρήση σε περιβάλλον γραφείου.

Σ' αυτό το κεφάλαιο θα βρείτε πληροφορίες ασφάλειας που πρέπει οπωσδήποτε να τις τηρήσετε κατά τη χρησιμοποίηση του συστήματός σας.

Αν έχετε ερωτήσεις σχετικά με την τοποθέτηση και λειτουργία στον προβλεπόμενο χώρο, παρακαλούμε να απευθυνθείτε στο σέρβις μας.

- Μεταφέρετε τη συσκευή μόνο στη γνήσια συσκευασία ή σε μια άλλη κατάλληλη συσκευασία που να προσφέρει προστασία από ωθήσεις και χτυπήματα.
- Πριν την τοποθέτηση και λειτουργία της συσκευής προσέξτε τις πληροφορίες για τις συνθήκες του χώρου.
- Εάν η συσκευή μεταφέρεται από κρύο περιβάλλον στον χώρο παραγωγής, μπορεί να παρουσιασθεί υγραποίηση - και στο εξωτερικό μέρος και στο εσωτερικό μέρος της συσκευής. Γι' αυτό το λόγο απαιτείται ένα χρονικό διάστημα εγκαταστάσεως τουλάχιστο 12 ωρών.
Περιμένετε μέχρι να προσαρμοσθεί η συσκευή στη θερμοκρασία και να είναι απόλυτα στεγνή, πριν τη θέσετε σε λειτουργία.
- Ελέγξτε εάν η ονομαστική (κανονική) τάση που αναφέρεται στην πινακίδα τύπου της συσκευής συμφωνεί με την τοπική ονομαστική (κανονική) τάση. Η συσκευή επιτρέπεται να τεθεί σε λειτουργία υπό τις ακόλουθες προϋποθέσεις:

100 - 240 VAC
60 / 50 Hz
max. 0,2 A

- Συνδέστε τη συσκευή μόνο σε έναν κανονικά γειωμένο ρευματολήπτη με επαφή προστασίας (η συσκευή είναι εξοπλισμένη με έναν ελεγμένο για ασφάλεια αγωγό δικτύου). Σε περίπτωση σύνδεσης σε έναν μη γειωμένο ρευματολήπτη με επαφή προστασίας υπάρχουν κίνδυνοι για τον χρήστη, π.χ. ηλεκτροπληξία.
- Εξασφαλίστε το να είναι ελεύθερα προσιτός ο ρευματολήπτης με την επαφή προστασίας στην εγκατάσταση του οικήματος. Για την πλήρη διακοπή του δικτύου ο ρευματολήπτης πρέπει να τραβηχθεί έξω.
- Τοποθετήστε τους αγωγούς έτσι ώστε να μην δημιουργούν καμιά πηγή κινδύνου και να μην φθειρόνται. Αλλάξτε αμέσως έναν φθαρμένο αγωγό. Κατά τη σύνδεση της συσκευής προσέξτε τις σχετικές πληροφορίες στο εγχειρίδιο λειτουργίας.
- Μην συνδέετε αγωγούς μεταφοράς δεδομένων κατά τη διάρκεια μιας καταιγίδας ούτε να τους αποσυνδέετε.
- Κατά την τοποθέτηση των καλωδίων του συστήματος προσέξτε τη σειρά, όπως περιγράφεται.

- Προσέξτε να μην πέσουν αντικείμενα (π.χ. χρυσαφικά, αλυσίδες, συνδετήρες κλπ.) ή υγρά στο εσωτερικό της συσκευής (ηλεκτροπληξία, βραχυκύκλωμα).
 - Σε περίπτωση έκτακτης ανάγκης (π.χ. φθαρμένο περίβλημα ή εξάρτημα χρησιμοποίησης, εισροή υγρού ή εισδοχή ξένων αντικειμένων) αποσυνδέστε αμέσως τον ηλεκτρολήπτη και ενημερώστε το σέρβις.
 - Προσέξτε ότι η κανονική λειτουργία (σύμφωνα με τα IEC 950 / EN 60 950) του συστήματος εξασφαλίζεται μόνο με το συναρμολογημένο καπάκι του περικαλύμματος (Ψύξη, πυροπροστασία, άρση των παρασίτων).
 - Η συσκευή επιτρέπεται να ανοιχθεί μόνο από ειδικευμένο προσωπικό. Π' αυτό φροντίστε ώστε οι επισκευές της συσκευής να γίνονται μόνο από εξουσιοδοτημένο ειδικευμένο προσωπικό.
Με ανεπίτρεπτο άνοιγμα και ακατάλληλες επισκευές μπορεί να προκύψουν σημαντικοί κίνδυνοι για τον χρήστη. Ανεπίτρεπτο άνοιγμα των συσκευών έχει σα συνέπεια τον αποκλεισμό της εγγύησης και ευθύνης της **BinTec Communications** ΕΠΕ.
 - Χρησιμοποιείτε μόνο τα επισυναπτόμενα καλώδια. Σε περίπτωση που χρησιμοποιήσετε άλλα καλώδια, η εταιρεία **BinTec Communications** ΕΠΕ δεν αναλαμβάνει καμιά ευθύνη για εμφανιζόμενες ζημιές. Ελέγξτε εάν οι αγωγοί είναι άψογοι και αβλαβείς. Αλλάξτε αμέσως έναν φθαρμένο αγωγό.
 - Ηλεκτροστατικές φορτώσεις μπορεί να οδηγήσουν σε βλάβες της συσκευής. Π' αυτό να φοράτε μια αντιστατική περιχειρίδα στο χέρι σας ή να ακουμπάτε σε μια γειωμένη επιφάνεια, πριν πιάσετε την ανοιγμένη συσκευή.
 - Η συσκευή δεν επιτρέπεται να καθαρισθεί με υγρά σε καμιά περίπτωση. Με την εισροή νερού μπορεί να προκύψουν σημαντικοί κίνδυνοι για τον χρήστη (π.χ. ηλεκτροπληξία).
 - Μη χρησιμοποιείτε ποτέ αφρώδη μέσα, αλκαλικά απορρυπαντικά, ισχυρά ή αφρώδη βοηθητικά υλικά. Με αυτά τα μέσα μπορεί να φθαρεί η επιφάνεια του περικαλύμματος.
- Σημαντική πληροφορία για το ειδικευμένο προσωπικό:
- Πριν ανοίξετε το σύστημα βγάλτε τον ρευματολήπτη.

Προσοχή: Σε περίπτωση ακατάλληλης αντικατάστασης της μπαταρίας υπάρχει κίνδυνος έκρηξης. Αντικατάσταση μόνο με τον ίδιο ή με ισάξιο τύπο. Οι μεταχειρισμένες μπαταρίες πρέπει να εξουδετερώνονται σύμφωνα με τις οδηγίες του κατασκευαστή.

Το σήμα CE σημαίνει ότι το BRICK... ανταποκρίνεται στις κατευθυντήριες γραμμές της Ε.Ε.: EMV (89/336/ΕΟΚ) και χαμηλή τάση (73/23/ΕΟΚ).

Η συσκευή μπορεί να συνδεθεί και στο Ευρω-NUMERIS (Γαλλία), γιατί εκτός από τις απαιτούμενες στην Ε.Ε. διατάξεις εκπληρώνει επιπρόσθετα και τις απαιτήσεις του γαλλικού ISDN.

Italian: Avvisi di sicurezza

L'apparecchio è conforme alle normative di sicurezza del settore per arredamenti tecnico-informatici, per l'utilizzo in ambienti di lavoro (uffici).

In questa sezione trovate avvisi di sicurezza che dovrete assolutamente osservare nell'uso del vostro sistema. Se avete delle domande sull'installazione ed il funzionamento nell'ambiente previsto, rivolgetevi per cortesia al nostro service.

- BRICK è destinato ad essere impiegato in ambiente d'ufficio. Quale ISDN-Multi-Protokoll-Router istituisce BRICK collegamenti ISDN in dipendenza della configurazione di sistema. Onde evitare conteggi indesiderati dovrebbe assolutamente sorvegliare il prodotto.
- portate l'apparecchio solo nella confezione originale od in un'altra confezione adatta, che assicuri protezione da urti di ogni genere.
- Prima dell'installazione e dell'avvio dell'apparecchio abbiate cura di osservare le indicazioni relative alle "condizioni ambientali".
- Se l'apparecchio viene portato nell'ambiente di lavoro da un ambiente freddo, è possibile che si produca acqua di condensa sia all'esterno che all'interno dell'apparecchio. Attendete pertanto che l'apparecchio si sia adattato alla temperatura e che sia assolutamente asciutto, prima di farlo funzionare.
- Verificate che la tensione normale riportata sulla targhetta del modello sia la stessa della rete locale. L'apparecchio può essere messo in funzione alle seguenti condizioni:
115 / 230 VAC
60 / 50 Hz
maks. 6,0 / 3,0 A
- Allacciate l'apparecchio solo ad una presa a terra protetta a norma di legge (l'apparecchio è provvisto di conduttore di corrente a norma di sicurezza).
- Assicuratevi che la presa a terra protetta dell'impianto locale sia liberamente accessibile. Per interrompere del tutto la corrente, è necessario staccare la spina.
- Posate i cavi conduttori in modo tale che non costituiscano fonte di pericolo (pericolo di inciampare) e che non vengano danneggiati. Nell'allacciare l'apparecchio attenetevi alle rispettive indicazioni nelle istruzioni di funzionamento.
- Non allacciate né staccate le linee di trasmissione dati durante un temporale.
- Cablando il sistema attenetevi all'ordine, come descritto.
- **Attenzione:** Nel caso la batteria venga impropriamente sostituita, sussiste pericolo di esplosione. Sostituire la batteria esclusivamente con il medesimo tipo ovvero con una batteria che abbia le caratteristiche identiche. Le batterie vanno smaltite e trattate secondo le indicazioni del produttore
- Assicuratevi che nessun oggetto (quali ad es.: catenine, graffette, ecc.) né alcun liquido penetrino all'interno dell'apparecchio (pericolo di scossa elettrica, corto circuito).
- In casi di emergenza (ad es.: danni all'involucro o ai comandi, penetrazione di liquidi o di oggetti estranei) staccate subito la spina ed avvisate il service.
- Tenete presente che il funzionamento del sistema secondo le norme (IEC 950/EN 60950) può venir garantito soltanto se il coperchio dell'involucro è montato (raffreddamento, protezione anti-incendio, schermatura contro radio-disturbi).
- L'apparecchio può venir aperto soltanto da personale specializzato. Fate pertanto eseguire eventuali riparazioni all'apparecchio soltanto da personale specializzato ed autorizzato. L'apertura da parte di persone non autorizzate o riparazioni effettuate in modo improprio possono dare origine a notevoli pericoli per l'utilizzatore.
- Utilizzate soltanto i cavi allegati. Se utilizzate altri cavi, la ditta BinTec Communications AG non assume alcuna responsabilità per eventuali danni verificatisi.
- Cariche elettrostatiche possono causare danni agli apparecchi. Indossare quindi un polsino antistatico o toccare una superficie collegata con la terra durante le operazioni all'apparecchio aperto.
- L'apparecchio durante le operazioni di pulizia non deve in nessun caso venir bagnato. L'infiltrazione di acqua può causare notevole pericolo per l'utente (ad es.: scossa elettrica).
- Non utilizzare in nessun caso sostanze detergenti abrasive, né detergenti alcalini, né materiali taglienti o abrasivi, perché potrebbero danneggiare la superficie.

Norwegian: Sikkerhetsveiledning

Dette apparatet imøtekommer de krav som stilles til sikkerhet når det gjelder informasjonstekniske innretninger til kontorbruk.

Dette avsnitt inneholder sikkerhetsveiledninger som de absolutt bør lese gjennom innen forsøk på å håndtere systemet.

Hvis det oppstår problemer eller spørsmål i forbindelse med oppstillingen eller drift av systemet, bør de henvende dem til vår serviceavdeling.

- BRICK er beregnet for innsats på kontoromgivelser. Som ISDN-Multi-Protokoll-Router bygger BRICK opp ISDN-forbindelser i avhengighet av systemkonfigurasjonen. For å unngå uønskede gebyrer, bør produktet absolutt overvåkes.
- Når apparatet skal transporteres, bruk alltid originalemballasjen eller annen egnet emballasje som gir beskyttelse mot slag eller støt.
- Før oppstilling og igangsettelse av apparatet, følg veiledningen hva angår de respektive omgivelsesbetingelser.
- Både utenfor og inne i apparatet kan det oppstå dugg når apparatet kommer fra kalde omgivelser og inn i bedriftsrommet.
Vent inntil apparatets temperatur tilsvarende romtemperaturen. Apparatet må absolutt være helt tørt før igangsettelsen.
- Kontroller om apparatets nominelle spenning angitt på typeskiltet overensstemmer med den strømkildens spenning. Apparatet må kun drives under følgende forutsetninger:
115 / 230 VAC
60 / 50 Hz
maks. 6,0 / 3,0 A
- Påse at husinstallasjonens sikkerhetsstikkontakt er fritt tilgjengelig. Til fullstendig atskillelse fra nettet må støpslet trekkes ut.
- Legg ut ledningene på en måte at de ikke utgjør en farekilde (snublefare) og ikke kan skades. Vær oppmerksom på detaljene i driftsveiledningen når de tilkople apparatet.
- Ved tordenvær skal dataledningene hverken tilkoples eller trekkes ut.
- Se opp for den riktige rekkefølgen når de tilslutter systemets kabelforbindelser.
- Vær oppmerksom på at hverken gjenstander (for eks. smykkekedjer, binders, osv.) eller vesker kommer inn i apparatet (elektrisk støt, kortslutningsfare).
- I en nødsituasjon (for eks. når kabinettet eller et betjeningselement har fått en skade, veske eller fremmedlegeme har kommet inn i apparatet) trekk ut støpslet og kontakt vår kundeservice.
- Vær oppmerksom på at det kun består garanti for systemets bestemmelsesmessige drift (ifølge IEC 950/EN 60 950) hvis apparatlokket er montert (kjøling, brandsikring, radiostøybeskyttelse).
- Pass på: Ved usakkyndig utskifting av batteriet kan det oppstå eksplosjonsfare. Utskifting må kun foretas med et batteri av samme eller likeverdig type. Brukte batterier må bortskaffes i henhold til angivelser fra produsenten.
- Apparatet må kun åpnes av fagfolk. La derfor apparatet kun repareres gjennom autorisert fagpersonale. Inngrep eller reparasjoner utført av personer som ikke er autoriserte reparatører av vedkommende produkt kan medføre alvorlige farer for brukeren.
- Bruk kun de vedpakkede kabler. Dersom de bruker andre kabler, fraskriver BinTec Communications AG seg ethvert ansvar hvis det oppstår skader.
- CE-tegnet betyr at „BRICK“ tilsvarende følgende direktiver fra EG: EMV (89/336/EWG) og lavspenning (73/23/EWG).
- Apparatet kan også tilkoples til „Euro-NUMERIS“ (Frankrike), da det i tillegg til EG forskriftene også tilfredsstiller det franske ISDN.
- Elektrostatiske oppladninger kan føre til skade på apparatene. Ha derfor på deg en antistatisk masjett rundt hendededde eller ta på en jordet flate før du berører det åpnede apparatet.
- Apparatet må under ingen omstendighet rengjøres med vann. Dersom det trenger inn vann, kan dette føre til alvorlige skader for brukeren (f.eks. strømstøt).
- Bruk aldri skuremidler, alkalisk rengjøringsmiddel eller skarpe, skurende hjelpemidler. Overflaten på kassen kan derved bli skadet.

Portuguese: Indicações de segurança

O aparelho corresponde às especificações de segurança para equipamentos da técnica de informação destinados ao uso num ambiente de escritório.

Neste ponto irá encontrar indicações de segurança que terá sempre de ter em atenção, aquando dos trabalhos com o seu sistema. Caso tenha quaisquer perguntas relativas à montagem e ao funcionamento no local previsto, pedimos-lhe que recorra ao nosso serviço de assistência técnica.

- O BRICK destina-se à utilização em escritórios. Enquanto Router multi-protocolo RDIS, o BRICK estabelece as ligações RDIS em função da configuração do sistema. Para evitar taxas adicionais deve vigiar sempre o produto..
- Transporte o aparelho apenas na embalagem original ou noutra embalagem adequada, com protecção contra pancadas e colisões.
- Antes da montagem e do funcionamento do aparelho, atenda às indicações relativas às condições do local.
- Caso se transporte o aparelho de um ambiente frio para o local de funcionamento, é possível a ocorrência de condensação, tanto no exterior como no interior do aparelho, pelo que é necessário aguardar durante um período de aclimatização de, no mínimo, 12 horas. Aguarde até o aparelho estar aclimatizado e completamente seco, antes da sua colocação em funcionamento.
- Verifique se a tensão nominal do aparelho, indicada na placa de tipo, corresponde á tensão local da rede. A colocação do aparelho em funcionamento é possível nas seguintes condições:
115 / 230 VAC
60 / 50 Hz
maks. 6,0 / 3,0 A
- Ligue o aparelho apenas a uma tomada de contacto de segurança com ligação á terra de acordo com os regulamentos (o aparelho encontra-se equipado com uma linha de rede com segurança controlada). No caso de ligação a uma tomada de contacto de segurança sem ligação à terra, existem perigos para o utilizador, como por exemplo o de choque eléctrico.
- Assegure-se de que está livre o acesso à tomada de contacto de segurança da instalação da casa. Para a completa separação da rede, deverá desligar-se a ficha de rede.
- Coloque as linhas de forma a que estas não constituam qualquer fonte de perigo (perigo de tropeçar) nem possam sofrer quaisquer danificações, procedendo à imediata substituição de uma linha danificada. Aquando da ligação do aparelho, atenda às indicações respectivas, constantes do manual de instruções.
- Assegure-se de que nenhum objecto (p.ex. pulseiras, clips, entre outros) ou líquido penetra no interior do aparelho (choque eléctrico, curto-circuito).
- Em caso de emergência (p.ex.: caixa ou elemento de comando danificada/o, entrada de líquido ou de corpos estranhos), desligue de imediato a ficha de rede e informe o serviço de assistência técnica.
- O aparelho deverá ser aberto apenas por pessoal técnico, pelo que quaisquer reparações deverão ser executadas somente por pessoal técnico autorizado. A abertura não autorizada e reparações inadequadas poderão causar enormes perigos para o utilizador.
- Utilize apenas os cabos fornecidos juntos. No caso da utilização de outros cabos, a BinTec Communications AG não assumirá qualquer responsabilidade por eventuais danos. Verifique se as linhas estão perfeitas e sem danificações, procedendo à imediata substituição de uma linha danificada.
- As cargas electrostáticas poderão originar danos no aparelho, pelo que deverá utilizar uma guarnição antiestática nos pulsos ou tocar numa superfície ligada à terra, antes de entrar em contacto com o aparelho aberto.
- A limpeza do aparelho não poderá, em caso algum, ser feita com um líquido. A entrada de água poderá originar enormes perigos para o utilizador (p.ex. o choque eléctrico).
- Nunca utilizar quaisquer substâncias abrasivas, produtos de limpeza alcalinos ou auxiliares pontiagudos ou abrasivos, dado que poderão danificar a superfície da caixa.

Swedish: Säkerhetsföreskrifter

Maskinen motsvarar de säkerhetsbestämmelser som är tillämpliga för informationsteknisk utrustning installerad i kontorsmiljö.

I detta avsnitt finner Du säkerhetsföreskrifter, vilka absolut måste iakttas vid användandet av systemet.

Om Du har frågor angående installation och användande av maskinen i den tänkta miljön, vänligen kontakta vår serviceavdelning.

- BRICK är avsedd för att användas i kontorsmiljö. I egenskap av ISDN-multi-protokoll-router bygger BRICK upp ISDN-linjer beroende på systemuppbyggnaden. För att undvika ofrivilliga avgifter bör du absolut övervaka produkten.
- Maskinen får endast transporteras i originalförpackningen eller i annan lämplig förpackning, som skyddar mot slag och stötar.
- Innan maskinen installeras och används, bör upplysningarna om förutsättningar beträffande den omgivande miljön beaktas.
- Om maskinen tas från en kall omgivning in i arbetsrummet, kan imma uppstå såväl utanpå som inuti maskinen. Vänta därför tills maskinen har samma temperatur som omgivningen och är absolut torr, innan Du tar den i bruk.
- Kontrollera att den på typskylten angivna märkspänningen för maskinen överensstämmer med den lokala nätspänningen. Maskinen får användas under följande förutsättningar:
 - 115 / 230 VAC
 - 60 / 50 Hz
 - maks. 6,0 / 3,0 A
- Maskinen får endast anslutas till godkänd jordad väggkontakt (maskinen är utrustad med en jordad nätkabel).
- Försäkra Dig om att den jordade väggkontakten är fritt tillgänglig. För att strömmen skall brytas helt, måste nätkontakten dras ut.
- Ordna sladdar och kablar på ett sådant sätt, att de inte utgör någon snubbelrisk för passerande, och så att kablarna inte riskerar att skadas. Följ bruksanvisningens råd vid anslutningen av maskinen.
- Undvik att ansluta eller dra ur dataöverföringskablar vid åskväder.
- Beakta den beskrivna ordningsföljden vid anslutning av systemets kablar.
- Se noga till att inga föremål (smycken, gem o dyl) eller vätskor kommer in i maskinen. Då finns risk för elektriska stötar och kortslutning.
- Vid nödfall (t ex maskinhölje eller -delar går sönder, vätska eller främmande föremål kommer in i maskinens inre), drag omedelbart ut nätkontakten och underrätta serviceavdelningen.
- Observera att reglementsenlig systemdrift (enl. IEC 950/EN 60950) endast garanteras vid monterat maskinhölje (kylning, brandskydd, gnistavstörning).
- Observera: Icke fackmässigt byte av batteri medför risk för explosion. Batteriet får endast bytas ut mot annat av samma eller likvärdig typ. Uttjänta batterier skall kasseras i enlighet med tillverkarens anvisningar.
- Maskinen får endast öppnas av fackpersonal. Låt därför endast auktoriserad fackman reparera maskinen. Obefogat öppnande och icke sakkunnig reparation kan medföra avsevärd fara för användaren.
- Använd endast bifogade kablar. Om andra kablar används, ansvarar BinTec Communications AG ej för uppkomna skador.
- CE-beteckningen innebär att „BRICK“ motsvarar följande EU-riktlinjer: EMV (89/336/EWG) och lågspänning (73/23/EWG).
- Maskinen kan även anslutas till „Euro-NUMERIS“ (Frankrike) eftersom den, utöver de erforderliga föreskrifterna inom EU, även uppfyller de franska ISDN-kraven.
- Statisk elektricitet kan medföra skada på maskinen. Använd därför en antistatisk manschett runt handleden, eller vidrör först en jordad yta, innan ni rör vid den öppnade maskinen.
- Maskinen får under inga omständigheter våt rengöras. Om vatten tränger in kan avsevärd fara uppstå för användaren (t ex elektrisk stöt).
- Använd aldrig skurpulver, alkaliska rengöring medel eller andra starka hjälpmedel vid rengöring. Maskinhöljet kan då ta skada.

Spanish: Instrucciones de seguridad

El aparato corresponde a las normas de seguridad vigentes para equipos de la técnica informativa destinados para el uso en oficinas.

En este apartado encuentra Vd las instrucciones de seguridad cuya observación es indispensable al usar su sistema.

Si tiene preguntas sobre la instalación y el funcionamiento en los locales provistos, diríjase a nuestro servicio.

- BRICK está previsto para su utilización en oficinas y despachos. Como router RSDI multiprotocolo, BRICK crea conexiones RSDI en función a la configuración del sistema. Para evitar gastos telefónicos no deseados es imprescindible controlar el aparato.
- Transporte el aparato sólo en el embalaje original u otro embalaje adecuado que le proteja contra choques o golpes.
- Tenga presente las advertencias sobre las condiciones ambientales antes de instalar y poner en funcionamiento el sistema.
- Cuando se lleve el aparato al lugar de trabajo de un ambiente frío, puede producirse agua de condensación tanto en la parte exterior como en la parte interior del mismo.
- Espere hasta que el aparato se haya adaptado a la temperatura ambiental y hasta que esté completamente seco antes de ponerlo en funcionamiento.
- Compruebe que la tensión nominal indicada en la placa indicadora de tipo corresponda con la tensión de la red local. El sistema puede ser accionado bajo las condiciones siguientes:
115 / 230 VAC
60 / 50 Hz
maks. 6,0 / 3,0 A
- Conecte el equipo sólo a una caja de enchufe con toma de tierra reglamentaria (el equipo está provisto de un cable de seguridad comprobado).
- Asegúrese de que sea accesible libremente la caja de enchufe con tomatierra de la instalación interior. Hay que sacar la clavija para la desconexión completa de la red.
- Coloque los cables de tal forma que no representen un peligro (peligro de tropezar) y que no se deterioren los mismos. Al conectar el equipo tenga presente las indicaciones correspondientes en las instrucciones de servicio.
- No conecte ni desconecte los cables de transmisión de datos durante una tormenta.
- Al instalar los cables del equipo observe la secuencia de operaciones conforme a las instrucciones.
- Observe que no caigan ningunos objetos (p.ej. colares, sujetapapeles, etc.) o se derrame ningún líquido al interior del aparato (peligro de sacudida eléctrica, cortocircuito).
- En casos de emergencia (p.ej. si se ha deteriorado la caja o algún elemento operativo, o bien ha penetrado algún líquido o cuerpo extraño) desenchúfe el equipo inmediatamente y póngase en contacto con el servicio al cliente.
- ¡Cuidado! En el caso del cambio no adecuado de la batería existe el peligro de explosión. Se debe sustituirla sólo por el mismo tipo u otro equivalente. Eliminar las baterías agotadas según las indicaciones del fabricante.
- Tenga presente que el funcionamiento correcto del sistema (según IEC 950/NE 6095) sólo se garantiza en el caso de estar colocada la tapa de la caja (refrigeración, protección contra incendios, supresión de interferencias).
- El aparato sólo debe ser abierto por personal especializado. Los trabajos de reparación por lo tanto deben ser realizados sólo por personal especializado y autorizado.
- Desenchufe el aparato antes de abrirlo.
- Caso de que el aparato sea abierto por personas no autorizadas y se realicen reparaciones inadecuadas pueden surgir peligros considerables para el usuario.
- Utilice sólo los cables suministrados de fábrica. De utilizarse cables diferentes BinTec Communications AG no asumirá ninguna responsabilidad por daños originados.
- Cargas electrostáticas pueden dañar los aparatos. Por ello, llevar una pulsera antiestática o tocar una superficie puesta a tierra antes de tocar el aparato abierto.
- En ningún caso se debe limpiar el aparato con líquidos. El agua que penetra entraña graves riesgos para el utilizador (por ejemplo electrocución).
- Nunca utilizar arena para fregar, agentes limpiadores alcalinos, cáusticos o ásperos, ya que ellos podrían dañar la superficie de la carcasa.

B

APPROVALS

The following BIANCA/BRICK ISDN communications modules have been approved for use within the European Community and Norway:

- BIANCA/CM-1BRI and BIANCA/CM-2BRI



- BIANCA/CM-PRI



- BIANCA/CM-1EBRI



BUNDESAMT FÜR ZULASSUNGEN IN DER TELEKOMMUNIKATION



ZULASSUNGSURKUNDE

Zulassungsnummer: A121073F

Objektbezeichnung: ISDN-Einsteck-Modul "BIANCA/CM-1BRI" u. "BIANCA/CM-2BRI"

Zulassungsinhaber: BinTec Computersysteme GmbH
Willstätter Str. 30
D-90449 Nürnberg

Zulassungsart: Allgemeinzulassung

Objektart: Telekommunikationseinrichtung mit digitaler Schnittstelle
für Netzzugang gemäß Anlage 1

Techn. Vorschrift: siehe Anlage(n) (Objektmerkmale)

Saarbrücken, den 26.10.1995

Im Auftrag

Hans-Peter Rosar



1 Anlage(n)

BUNDESAMT FÜR ZULASSUNGEN IN DER TELEKOMMUNIKATION

Federal Approvals Office For Telecommunications Of The Federal Republic Of Germany



ZULASSUNGSURKUNDE
Certificate of Type Approval

Urkundenummer : Z121444F Anzahl der Anlagen: -
Certificate No.:
Zulassungsart : EG-Zulassung (Annex II)
Category of approval:
Zulassungsinhaber : BinTec Computersysteme GmbH
Certificate Holder: Willstätter Str. 30
D-90449 Nürnberg

Produktbezeichnung : ISDN-Einsteckmodule "BIANCA/CM-1BRI" und
Designation of product: "BIANCA/CM-2BRI"

ProduktHersteller : BinTec Computersysteme GmbH
Manufacturer of product: Willstätter Str. 30
D-90449 Nürnberg

Konformität mit dem Baumuster:
Conformity with the examined type:

Der Zulassungsinhaber hat erklärt, daß das oben genannte Produkt dem in der
- EG-Baumusterprüfbescheinigung, Registriernummer B121072F vom 10.11.95
beschriebenen Baumuster entspricht.

Produktkontrolle :
Product inspection:

Das Bundesamt für Zulassungen in der Telekommunikation
Talstraße 34-42
D-66119 Saarbrücken

als benannte Stelle mit der Kenn-Nummer 0188

ist mit der Durchführung der Produktkontrolle gemäß Anhang II der Richtlinie
91/263/EWG des Rates vom 29. April 1991 beauftragt.

Hinweis: Diese Urkunde gilt nur in Verbindung mit den oben genannten Anlagen.
Comments: This certificate can only be used in conjunction with the above mentioned annex(es).

Saarbrücken, den 10.11.1995
Ort, Ausstellungsdatum:
Place, issue date:

gezeichnet: *Hans-Peter Rosar*

Hans-Peter Rosar



BUNDESAMT FÜR ZULASSUNGEN IN DER TELEKOMMUNIKATION



ZULASSUNGSURKUNDE

Zulassungsnummer: A119749F

Objektbezeichnung: ISDN Schnittstellenmodul "PRIME/two"

Zulassungsinhaber: BINTEC Computersysteme GmbH
Willstätter Str. 30
D-90449 Nürnberg

Zulassungsart: Allgemeinzulassung

Objektart: Telekommunikationseinrichtung mit digitaler Schnittstelle
für Netzzugang gemäß Anlage 1

Techn. Vorschrift: siehe Anlage(n) (Objektmerkmale)

Saarbrücken, den 20.07.1995



Im Auftrag

Hans Peter Rosar
Hans Peter Rosar

1 Anlage(n)

BUNDESAMT FÜR ZULASSUNGEN IN DER TELEKOMMUNIKATION

Federal Approvals Office For Telecommunications Of The Federal Republic Of Germany

**BAUMUSTERPRÜFBESCHEINIGUNG
TYPE-EXAMINATION CERTIFICATE**

Registriernummer : B122987H **Anzahl der Anlagen:** 1
Registration no.: Number of annexes:

Benannte Stelle : Bundesamt für Zulassungen in der Telekommunikation
Notified body:

Bescheinigungsinhaber: BinTec Computersysteme GmbH
Certificate holder: Willstätter Str. 30
 D-90449 Nürnberg

Produktbezeichnung : BIANCA/CM-1EBRI
Designation of product:

Produktbeschreibung : Die Einrichtung ist ein ISDN Einsteckmodul mit interner "Mini-Sbus" Schnittstelle und kommt z.B. in den Multiprotokoll Routern BIANCA/BRICK M zum Einsatz. Das Modul verfügt über eine ISDN S0 Schnittstelle und eine spezielle Audio Schnittstelle.
Product description:

ProduktHersteller : BinTec Computersysteme GmbH
Product manufacturer: Willstätter Str. 30
 D-90449 Nürnberg

Deutsche Vorschriften: BAPT 223 ZV 25
German Specifications: I-CTR 3 (94/797/EG)

Prüfergebnis : Das geprüfte Baumuster erfüllt die Anforderungen der oben genannten Vorschriften.
Statement: The examined type meets the requirements of the above mentioned specifications

Hinweis: Dieses Zertifikat gilt nur in Verbindung mit den o.g. Anlagen
Note: This certificate is only applicable in conjunction with the above mentioned annex(es).

Diese Bescheinigung ist erstellt in Übereinstimmung mit der TKZulV 1995
This certificate is issued in accordance with the TKZulV 1995

Saarbrücken, den 28.02.1996
Ort, Ausstellungsdatum:
Place, issue date:



gezeichnet: *Reiner Gassenburger*
Signed: Reiner Gassenburger

(Verantwortlicher der benannten Stelle)
(Manager of notified body)

Bundesamt für Zulassungen in der Telekommunikation, Talstraße 34-42, D-66119 Saarbrücken, Tel.: +49 8 61 5 98-0, Fax: +49 8 61 5 98-18 00

BUNDESAMT FÜR ZULASSUNGEN IN DER TELEKOMMUNIKATION

Federal Approvals Office For Telecommunications Of The Federal Republic Of Germany



EG-BAUMUSTERPRÜFBESCHEINIGUNG
EC TYPE-EXAMINATION CERTIFICATE

Registriernummer : B122988H **Anzahl der Anlagen:** 1
Registration no.: **Number of annexes:**

Benannte Stelle : Bundesamt für Zulassungen in der Telekommunikation
Notified body:

Bescheinigungsinhaber: BinTec Computersysteme GmbH
Certificate holder: Willstätter Str. 30
D-90449 Nürnberg

Produktbezeichnung : BIANCA/CM-1EBRI
Designation of product:

Produktbeschreibung : This equipemnt is an ISDN plug in modul with "Mini-
Product description: Sbus" bus system connection for use e.g. in Multi-
protocol Router family BIANCA/BRICK-M. There is an
ISDN basic rate interface and a special audio inter-
face on the backplane.

ProduktHersteller : BinTec Computersysteme GmbH
Product manufacturer: Willstätter Str. 30
D-90449 Nürnberg

EG-Vorschriften: I-CTR 3 (94/797/EEC)
EC specifications:

Prüfergebnis : Das geprüfte Baumuster erfüllt die Anforderungen der oben
genannten EG-Vorschriften.
statement: The examined type meets the requirements of the above mentioned EC specifications

Hinweis: Diese Bescheinigung gilt nur in Verbindung mit den o.g. Anlagen.
Note: This certificate is only applicable in conjunction with the above mentioned annex(es).

Diese Bescheinigung ist erstellt in Übereinstimmung mit der Richtlinie 91/269/EWG des Rates
This certificate is issued in accordance with the Council Directive 91/269/EEC

Saarbrücken, den 28.02.1996
Ort, Ausstellungsdatum:
Place, issue Date:



gezeichnet: *Reiner Gusenburger*
Signed: Reiner Gusenburger
[Verantwortlicher der benannten Stelle]
[Manager of notified body]

Bundesamt für Zulassungen in der Telekommunikation, Talstraße 34-42, D-66119 Saarbrücken, Tel.: +49 6 81 5 98-0, Fax: +49 6 81 5 98-16 00

INDEX

Symbols

+50395 202

A

access

 CAPI port 158

 isdnlogin 157

 SNMP port 159

 trace port 158

 X.25 158

access lists 76, 159

accounting 153

 IP 39, 63

autoconfiguration 41, 121

B

Back Route Verify 63

Basic rate interface 10, 181, 214, 215,
 216, 217, 236

BIANCA/CM-PRI 219

biboAdmSyslogTable 177

biboPPPTTable 177, 178

BOOTmonitor 205

BOOTP 71, 140

BRI

 modules 214, 216, 217, 236

bricktrace 169, 178, 180, 181, 196

Bridge 209

Bridging 155, 178

Btx 189

bundelling 58

C

callback 57

CAPI 3, 33

 port 158

 Remote 3

capitrace 196

CLID 52

Compression

 STAC 4, 50

CompuServe 130

CTS 240

D

date 190

DDI 44

debug 192

debugging 105

Denial-of-service attack 40, 63

DHCP Server 66, 84

Direct Dial In 44

DRAD 224

DTR 240

dynamic resource allocation and distri-
 bution 224

- E**
 - Encapsulation 177, 178
 - for IPX packets 38
 - encapsulation
 - for IPX packets 38
 - for token ring 40
 - Error messages 169, 170
- F**
 - Facsimile support 189, 215
 - FML-8MOD 222
- G**
 - Gateway 155
- H**
 - halt 194
 - HTML status page 161
 - HTTP port number 161
- I**
 - ifconfig 194
 - ifstat 187
 - intruders 158
 - IP 66
 - accounting 39, 63, 153
 - Back Route Verify 63
 - IP address
 - address pool 83
 - dynamic client 132
 - server mode 133
 - IPX 90, 141
 - network number 64
 - ipxping 184
 - ISDN
 - accounting 153
 - call answering 43
 - switch type 41
 - ISDN monitor 106
 - isdnCallHistoryTable 168, 177, 178
 - isdnDispatchTable 178
 - isdnlogin 168, 177, 188
 - isdnlogind 188
 - isdnStkTable 178
- K**
 - K56flex 223
- L**
 - leased line 122
 - licenses 33
- M**
 - message levels 35
 - messages 112
 - minipad 189
 - MODEM 95
 - modem 190
 - Modem Module 222
 - monitor
 - interfaces 110
 - ISDN 106
 - messages 112
 - TCP/IP 113
 - X.25 109
- N**
 - NAT 73, 134, 159
 - Negotiation
 - DNS 62
 - WINS 62
 - NetBIOS 91
 - netstat 188
 - Network Terminator 237, 238
 - NT 237, 238
- P**
 - p 193
 - Passwords 170
 - passwords 35, 169
 - ping 183
 - Port
 - Serial 170, 202, 240, 243
 - UTP 236, 237
 - port
 - SNMP 86
 - PPP
 - local PPP ID 34
 - PRI
 - module 11, 219, 220, 237
 - Primary rate interface 11, 219, 237
 - primary rate interface 127
 - Priority 193
 - Protocols

IP 169, 178, 180
TCP 169

R

RADIUS 160
 Accounting 87
 Multiple Servers 87
 Server 66, 67
Remote CAPI 3
Remote configuration 4
RIP/SAP 64, 159
Router 209
Routing 178
routing 177
 IP 67
rtlookup 186
RTS 240
RVS-COM 3

S

security 157
 access lists 76
 NAT 159
 RIP 159
Serial port 170, 202, 240, 243
server
 CAPI 71
 DNS 70
 timeserver 71
 trace 71
 WINS 70
Setup Tool
 List Navigation 26
 Menu Navigation 25
Short 123
Short Hold
 Dynamic 57, 123
 Static 57
SNMP port 86
SNMP Shell
 priority 193
STAC compression 4, 50
sysName 34
system administration 103
system messages 112

T

t 193
TCP/IP
 dialup connection 128
 statistics 113
telnet 181, 183
TFTP 104, 208
Time Server 71
token ring 40
trace 184
traceroute 187

U

update 190
Utilities
 bricktrace 169, 178, 180, 181, 196
 capitrace 196
 date 190
 debug 192
 halt 194
 ifconfig 194
 ifstat 187
 ipxping 184
 isdnlogin 188
 minipad 189
 modem 190
 netstat 188
 p 193
 ping 183
 rtlookup 186
 t 193
 telnet 183
 trace 184
 traceroute 187
 update 190
UTP port 236, 237

V

Van Jacobson Header Compression 62

X

X.21 48
X.25 monitor 109
XMODEM 207
XM-X21 48

