

BIANCA/BRICK-XS

User's Guide

Hardware and Installation

*Version 1.7
Document #71000D*

July 1999

Copyright © 1999 BinTec Communications AG
All rights reserved

Purpose:

This manual explains the installation and configuration of BIANCA/BRICK-XS and BRICK-XS Office with the Software Release 4.9.4. Before installing and configuring your router, please note the security instructions described in your BIANCA/BRICK-XS and BRICK-XS office 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-XS and BRICK-XS Office, can be retrieved at www.bintec.de.

As an ISDN multiprotocol router, BIANCA/BRICK-XS and BRICK-XS Office 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.

FCC Notice — Class B Computing Device

NOTE: *This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the FCC Rules and meets all requirements of the Canadian Interference-Causing Equipment Regulations. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to try to correct the interference by one or more of the following measures:*

- *Reorient or relocate the receiving antenna.*
- *Increase the separation between the equipment and receiver.*
- *Connect the equipment into an outlet on a circuit different from that to which the receiver is connected*
- *Consult the dealer or an experienced radio/T.V. technician for help.*

The use of a non-shielded interface cable with the referenced device is prohibited. Changes or modifications not expressly approved by BinTec Communications AG could void the authority to operate the equipment.

CE Notice

The **CE** symbol means that the BRICK-XS 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-XS adheres to ISDN requirements in France and may be connected to Euro-Numeris.

GS

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

ISDN Ordering Codes (IOC) for the U.S.A.

The BIANCA/BRICK-XS operates with the following IOCs:

Capability Package 'S' and

EZ-ISDN-1

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-XS and BRICK-XS Office 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:*
 - 100 - 240 VAC
 - 50 - 60 Hz
 - max. 0.2 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.*
- *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.*
- *Do not attempt to open this equipment. This equipment may only be repaired by an authorized technician. Unauthorized opening and repair of this equipment may expose the user to dangerous voltage, other hazards, and will nullify the guarantee and liability limitations of BinTec Communications.*
- *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.*

BIANCA/BRICK-XS

*User's Guide
Version 1.7*

Contents

1. Introduction

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

2. Installing the BRICK

| | |
|---|----|
| <i>Connecting the BRICK to the LAN</i> | 8 |
| <i>Connecting the BRICK to the ISDN</i> | 10 |
| <i>Connecting the BRICK to a PC or terminal</i> | 10 |
| <i>The BOOT sequence</i> | 11 |
| <i>Logging in for the first time</i> | 13 |

3. Working with the BRICK

| | |
|---|----|
| <i>SNMP, MIBs, and BRICK System Tables</i> | 15 |
| <i>Configuration Files, Flash, and the TFTP</i> | 18 |
| <i>Physical and Software Interfaces</i> | 19 |
| <i>Setup Tool vs. SNMP Shell</i> | 20 |
| <i>Using Setup Tool</i> | 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 47
Configuring Protocols 65
System Administration 104

5. How do I Configure ...

..... 122
Hardware Interfaces 123
 How do I configure an ISDN interface in general? 123
 How do I configure a leased line connection? 125
 How do I configure Dynamic Short Hold? 126
 How do I configure an Ethernet interface? 128
IP Features 129
 How do I configure dialup TCP/IP access for an ISDN partner?... 129
 How do I configure Dialup Access to CompuServe Online
 Services 132
 How do I configure the BRICK to accept its IP address
 dynamically? 134
 How do I configure the BRICK as a dynamic IP address server?... 135
 How do I configure Internet access for my LAN using NAT? 137
 How do I configure the BRICK as a RADIUS Client? 140
 How do I configure the BRICK as a BOOTP relay agent? 143
IPX Features 144
 How do I connect my local and remote IPX networks over
 ISDN? 144
Fax Features 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 |
| Serial Console | 171 |
| Software Problems | 172 |
| IPX Routing..... | 172 |
| OSPF Routing | 174 |
| ISDN Connections | 175 |

7. Command Reference

| | |
|------------------------------------|-----|
| The SNMP shell commands | 181 |
| BRICKtools for UNIX Commands | 192 |

8. Hardware/Firmware Configuration

| | |
|-------------------------------------|-----|
| Hardware | 196 |
| Front Panel Indicators | 196 |
| The Back Plane..... | 198 |
| The Main Board | 199 |
| Firmware | 200 |
| Upgrading System Software | 200 |
| BOOTmonitor | 200 |
| Automatic booting over TFTP | 203 |
| General System Specifications | 205 |

A. Technical Data

| | |
|---|-----|
| <i>Pin Assignments</i> | 206 |
| <i>ISDN S₀ Interface</i> | 206 |
| <i>Ethernet Port</i> | 207 |
| <i>Serial Port</i> | 208 |
| <i>Important Safety Information</i> | 208 |

B. Approvals

1

INTRODUCTION

What's covered

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

How to contact BinTec Communications

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

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 *Quick Install Guide* and *Kurzanleitung*, the *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 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

BRICK-XSThe BRICK-XS offers a low-cost, high-compatibility solution for today's SOHO (small Office Home Office) environments. The system offers both power and flexibility through features not limited to the following:

- *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 breaches 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.
- *Remote configuration*—configure your BRICK-XS from a remote site using the isdnlogin program (please refer to the *Getting Started* or *Los Gehr's* manuals).
- *STAC compression*—BRICK-XS 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-XS 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-XS 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.

- **Open Shortest Path First—OSPF** is an interior routing protocol that can be used as an alternative to RIP. Though generally more complex OSPF scales better to the requirements of larger network installations. OSPF also addresses some of the limitations of RIP including Faster Network Convergence, Routing Authentication, and Link-Cost Acknowledgement.
- **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, and important tasks, such as 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 LAN*8
- *Connecting the BRICK to the ISDN*.....10
- *Connecting the BRICK to a PC or terminal*.....10
- *The BOOT sequence*11
- *Logging in for the first time*13

You may have already installed and setup your BIANCA/BRICK using the Configuration Wizard or 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 your BRICK-XS to an ethernet using either the 10Base2 or 10BaseT port on the back plane.

At boot time, and during normal operation mode, the BRICK automatically detects which LAN port is currently in use (however, only one port per module may be used at a time).

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.



Thin Coax Cabling (10Base2)

If your network is setup using thin coaxial cabling, stations on your network are directly attached to the network cabling using a BNC connector as shown in figure 1 below. A transceiver is usually not required.

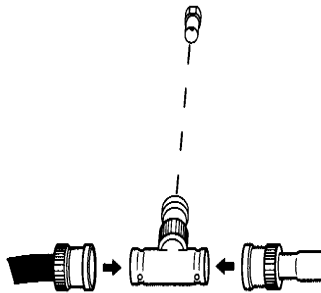


Figure 1: BNC Connector



1. Attach the BNC T-connector to the BNC port on the back plane of your BRICK-XS marked "10Base2".

2. Attach one end of the coaxial cable to an open end of the T-connector. Align the notches in the cable end with those on the T-connector and push the cable in, twisting about a quarter turn.
3. If the BRICK-XS is going to be the last station on your network you will also need to attach a 50Ω terminator to the other end of the T-connector.

Thin coaxial Cabling requirements. Though thin coaxial cabling is less expensive and easier to install, distance and attachment restrictions are more stringent than for thick coaxial cabling. Thin coaxial segments have a maximum distance of 185 meters and each segment can support up to 30 stations.

Twisted pair cabling (10Base)

If your network is setup using twisted pair (or telephone) wiring then individual stations are attached to the network through UTP (unshielded twisted pair) connectors. A UTP connector is a telephone type (RJ-45) connector also known as a western plug. A twisted pair cable connects the UTP port of each station on the network to a central 10BaseT concentrator. You can attach the BRICK-XS to your ethernet using the 10BaseT port with the included twisted pair cable and ferrite as shown in figure 2.

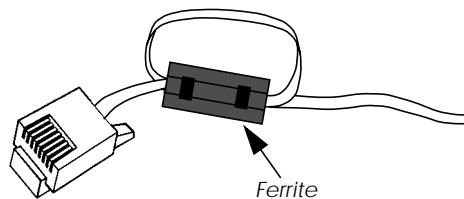


Figure 2: RJ-45 Western Plug with Ferrite

- ! 1. Attach a twisted pair cable to your BRICK-XS by inserting the 8 pin RJ-45 jack into the twisted pair port on the back plane marked 10BaseT.
2. Make a small loop in the twisted pair cable as close as possible to the BRICK and attach a ferrite to it as shown in figure 2 above.
3. Attach the other end of the twisted pair cable to an input port of your concentrator.

Connecting the BRICK to the ISDN

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 BRICK-XS ISDN BRI port 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 the port marked ISDN S₀ on the BRICK-XS.

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. 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 200, 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-XS - Start-up ###
Starting FLASH Test : ... [0xc3b2] ok.
Starting ISDN Chip Test : ... ok.
Starting ISDN Loopback Test : ... ok.
Starting ISDN Bus Test : ... ok.
Starting Ethernet Chip Test : ... ok.

### BIANCA/BRICK-XS (Hardware Release 1.2, Firmware Release 1.4) ok ###

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 (1660496 bytes)
Booting BOSS...

BOSS kernel v2.0 (BIANCA/BRICK-XS)
Copyright (c) 1996 by BinTec Communications AG
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 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 Tables* 15
- *Configuration Files, Flash, and the TFTP* 18
- *Physical and Software Interfaces* 19
- *Setup Tool vs. SNMP Shell* 20
- *Using Setup Tool* 21

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.

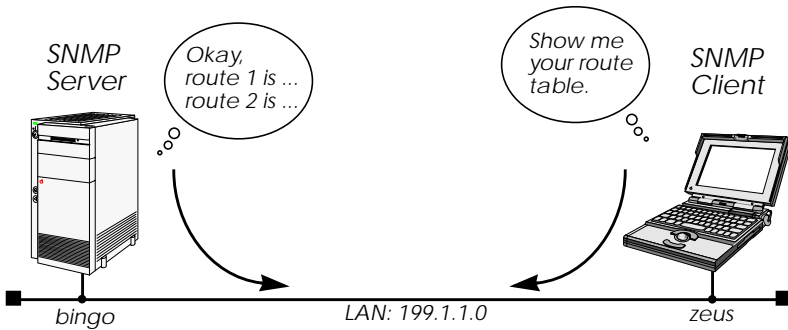
SNMP, MIBs, and BRICK System Tables

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.



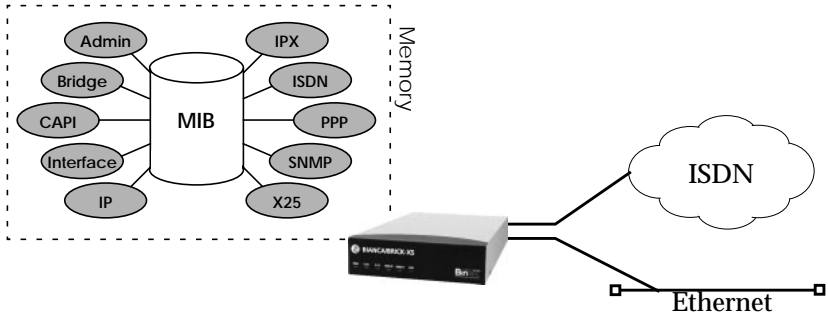
After booting, the BRICK starts a login shell. We sometimes refer to it as the SNMP shell because special commands can be entered from the shell which are given directly to the BRICK’s SNMP server-process. This means that the BRICK’s SNMP shell can be accessed from an SNMP client application, as well 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.

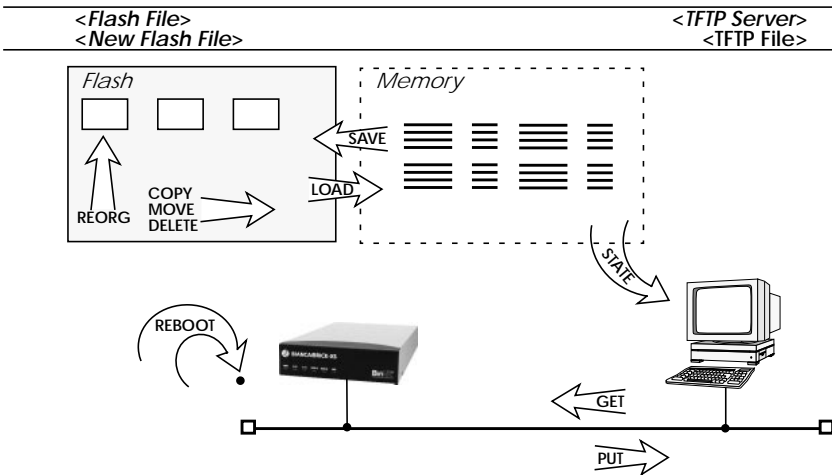
Note: As soon as a variable is changed in memory, the setting becomes effective immediately, the BRICK does not have to be rebooted nor do configuration files need to be reloaded. Any changes made to memory not saved in a configuration file, however, are lost once the system is shut down.



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.

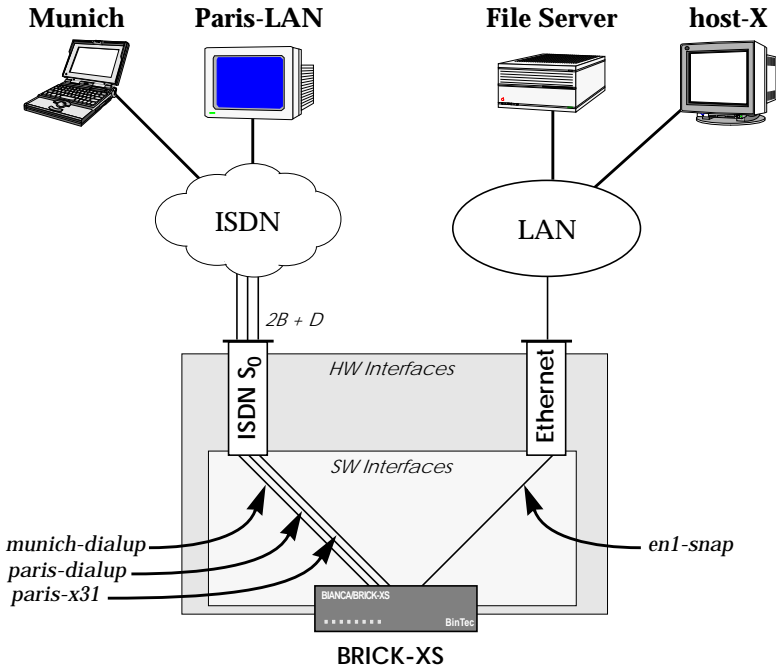
As a SOHO multiprotocol router the BRICK-XS was designed to link your local and remote networks (or hosts) using WAN links such as ISDN dialup, leased line, and X.25 connections. To establish connections to these sites, the BRICK uses the Software Interfaces that you configure. By “Software Interface”, 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 of 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-XS interconnects the LAN in Paris and a site in Munich with the file servers and other hosts on the local ethernet.

Suppose host-X 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.



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-XS Setup Tool      BinTec Communications AG
[IP][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)

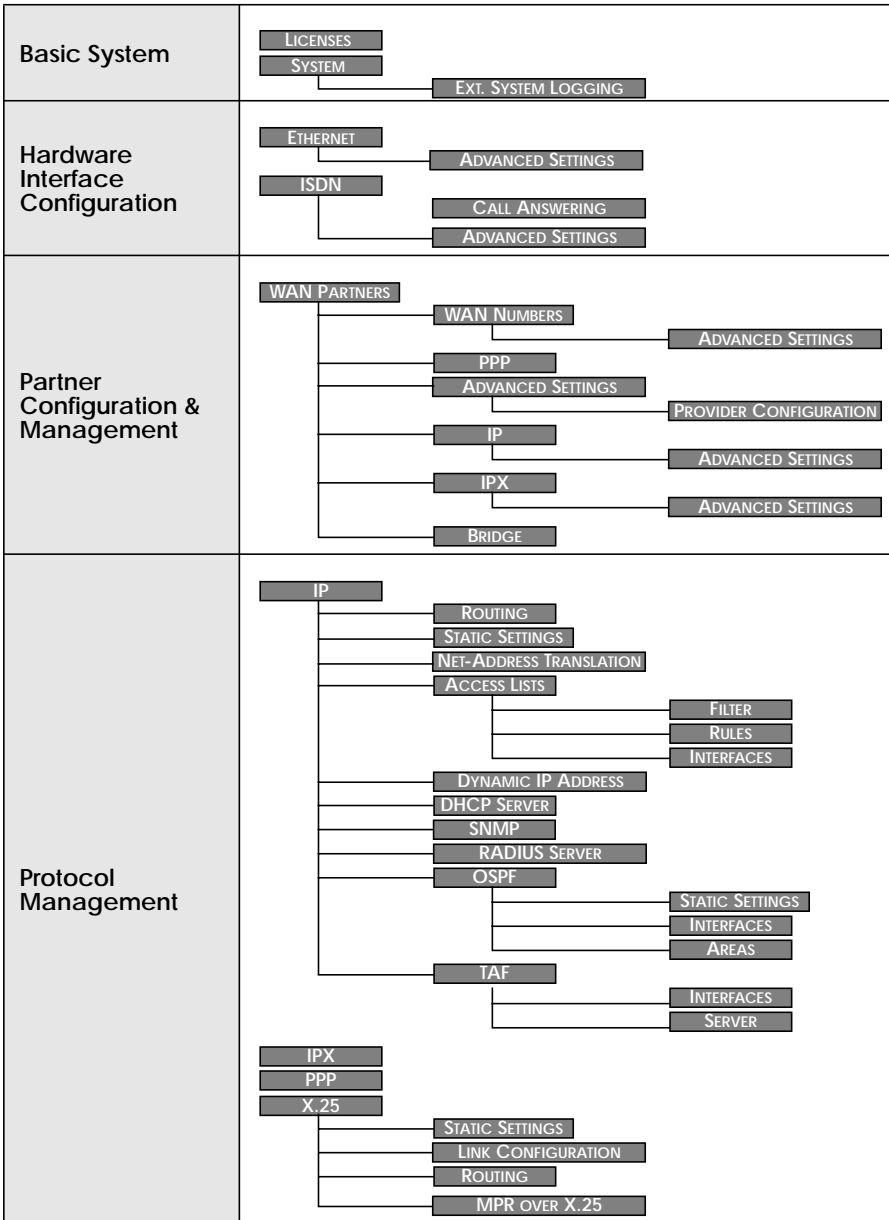
| Destination | Gateway | Mask | Flags | Me | Interf/Partner | Pro |
|-------------|------------|-----------------|-------|----|----------------|-----|
| 199.1.2.2 | 199.1.1.20 | 255.255.255.128 | US | 0 | en1 | loc |
| 199.1.1.0 | 199.1.1.2 | 255.255.255.128 | US | 0 | en1 | loc |

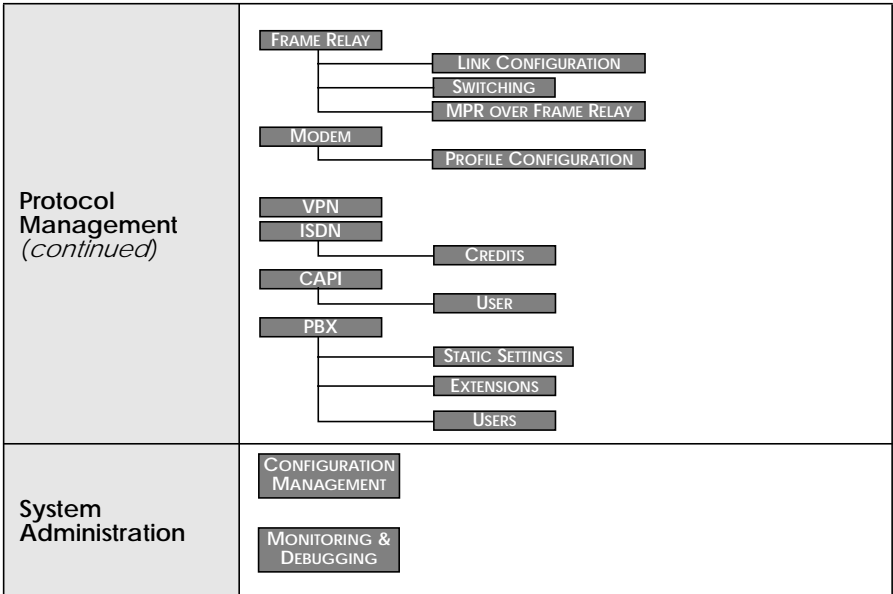
ADD DELETE EXIT

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.

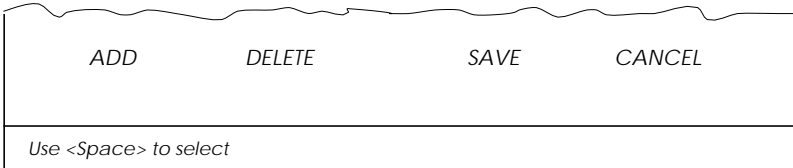


The menus available on your system will depend partly on Hardware (installed communications/feature modules) and Software (which features are licensed on your system).

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.



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

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-XS 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 | <i>Cursor jumps to the: test-account entry.</i> |
| a p o l o | <i>Cursor jumps to: apollo-11 entry first then to: apolonia after the last "o".</i> |

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 Interfaces*.....37
- *Partner Management*.....47
- *Configuring Protocols*.....65
- *System Administration*.....104

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-XS and BRICK-XS office establish 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 100, 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 176 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. |
| LAN Interface | Used for configuring the ethernet interface. |
| WAN Interface | Used for configuring the ISDN interface. |
| Feature Module | Displays the type of the feature module installed in your BRICK-XS office. |

```

BIANCA/BRICK-XS Setup Tool                               BinTec Communications AG
[LICENSE]: Licenses                                     brick

Licenses                System
LAN Interface:         CM-BNC/TP, Ethernet
WAN Interface:         CM-1BRI, ISDN S0
Feature Module:        CM-, MOD2-14

WAN Partner
IP      IPX      PPP      X.25  FR1    MODEM  VPN      ISDN   CAPI

Configuration Management
Monitoring and Debugging

Exit

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

```

1. Only on systems with 2-MB of flash.

| | |
|--------------------|--|
| 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 modem(On XS Office systems only)s.

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 ¹ | IP | IPX |
| | OSPF | STAC | VPN | X25 | |

1. only available on BRICK-XS with 2 MB Flash ROM

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

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

| | | | |
|---|--------|-----------------------------------|-------|
| BIANCA/BRICK-XS Setup Tool [LICENSE]: Licenses | | BinTec Communications AG brick | |
| Available Licenses: | | | |
| IP (builtin), OSPF (valid), CAPI (valid), BRIDGE (valid), X25 (valid), IPX (valid), STAC (valid) | | | |
| Serialnumber | Mask | Key | State |
| 101546 | 313 | 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.

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

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 | <i>emerg</i> | Emergency Messages |
| | <i>alert</i> | Alert Messages |
| | <i>crit</i> | Critical Messages |
| | <i>err</i> | Error Messages |
| | <i>warning</i> | Warning Messages |
| | <i>notice</i> | Notice Messages |
| | <i>info</i> | Info Messages |
| Lowest priority | <i>debug</i> | 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-XS Setup Tool | | BinTec Communications AG | |
| [SYSTEM][LOGGING]: External System Logging | | brick | |
| <i>Log Host</i> | <i>Level</i> | <i>Facility</i> | <i>Type</i> |
| <i>santorini</i> | <i>debug</i> | <i>local0</i> | <i>both</i> |
| <i>naxos-pc</i> | <i>info</i> | <i>local2</i> | <i>system</i> |
| <i>saxos-pc</i> | <i>err</i> | <i>local3</i> | <i>system</i> |
| <i>ADD</i> | <i>DELETE</i> | <i>EXIT</i> | |

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

LAN Interface : CM-BNCTP, ETHERNET →

This menu contains settings for the BRICK's ethernet interface.

| | | | | | | | | | | | | | | | | | | | | | |
|---|-----------------------------------|-------------------------|--|------------------------|-----------|----------------------|---------------|----------------------|-------------|------------------------------|--|----------------------------|---|----------------------|------|-----------------|---------|-------------------------------|--|------|--------|
| BIANCA/BRICK-XS Setup Tool [LAN]: Configure Ethernet Interface | BinTec Communications AG brick | | | | | | | | | | | | | | | | | | | | |
| <table style="width: 100%; border: none;"> <tr> <td colspan="2" style="padding-left: 20px;"><i>IP-Configuration</i></td> </tr> <tr> <td style="padding-left: 40px;"><i>local IP-Number</i></td> <td>199.1.1.2</td> </tr> <tr> <td style="padding-left: 40px;"><i>local Netmask</i></td> <td>255.255.255.0</td> </tr> <tr> <td style="padding-left: 40px;"><i>Encapsulation</i></td> <td>Ethernet II</td> </tr> <tr> <td colspan="2" style="padding-left: 20px;"> <i>IPX-Configuration</i></td> </tr> <tr> <td style="padding-left: 40px;"><i>local IPX-NetNumber</i></td> <td>0</td> </tr> <tr> <td style="padding-left: 40px;"><i>Encapsulation</i></td> <td>none</td> </tr> <tr> <td style="padding-left: 20px;"><i>Bridging</i></td> <td>enabled</td> </tr> <tr> <td colspan="2" style="padding-left: 20px;"><i>Advanced Settings ></i></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> | | <i>IP-Configuration</i> | | <i>local IP-Number</i> | 199.1.1.2 | <i>local Netmask</i> | 255.255.255.0 | <i>Encapsulation</i> | Ethernet II | <i>IPX-Configuration</i> | | <i>local IPX-NetNumber</i> | 0 | <i>Encapsulation</i> | none | <i>Bridging</i> | enabled | <i>Advanced Settings ></i> | | SAVE | CANCEL |
| <i>IP-Configuration</i> | | | | | | | | | | | | | | | | | | | | | |
| <i>local IP-Number</i> | 199.1.1.2 | | | | | | | | | | | | | | | | | | | | |
| <i>local Netmask</i> | 255.255.255.0 | | | | | | | | | | | | | | | | | | | | |
| <i>Encapsulation</i> | Ethernet II | | | | | | | | | | | | | | | | | | | | |
| <i>IPX-Configuration</i> | | | | | | | | | | | | | | | | | | | | | |
| <i>local IPX-NetNumber</i> | 0 | | | | | | | | | | | | | | | | | | | | |
| <i>Encapsulation</i> | none | | | | | | | | | | | | | | | | | | | | |
| <i>Bridging</i> | enabled | | | | | | | | | | | | | | | | | | | | |
| <i>Advanced Settings ></i> | | | | | | | | | | | | | | | | | | | | | |
| SAVE | CANCEL | | | | | | | | | | | | | | | | | | | | |
| Enter IP address (a.b.c.d or resolvable hostname) | | | | | | | | | | | | | | | | | | | | | |

IP-Configuration

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

local Netmask = The netmask to use for this interface.

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 |
| <i>Ethernet II</i> | ● | ● | | |
| <i>Ethernet SNAP</i> | ● | ● | | |
| <i>Ethernet 802.2 LLC</i> | | ● | ● | ● |
| <i>Novell 802.3</i> | | ● | | |

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

CM-BNCTP, ETHERNET → ADVANCED SETTINGS →

| | | |
|--|------------------|-----------------------------------|
| BIANCA/BRICK-XS Setup Tool [LAN][ADVANCED]: Advanced Settings | | BinTec Communications AG brick |
| RIP Send RIP Receive | RIP V2 RIP V2 | |
| IP Accounting Proxy Arp Back Route Verify | on off 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 <iface> prot <prot>
<source IP address> -> <dest. IP address>*

WAN Interface : CM-1BRI, ISDN S0 →

This menu contains settings for the BRICK-XS's ISDN interface.

| | | | | | | | | | | | | | | | | | |
|---|---------------------------------------|-------------------------------------|---------------------------------------|-------------------------|-----------------------------|------------------|---------------|--------------------|---------------|--------------------|---------------|-------------------------------------|--|------------------------------|--|-------------|---------------|
| BIANCA/BRICK-XS Setup Tool [WAN]: WAN Interface | BinTec Communications AG brick | | | | | | | | | | | | | | | | |
| <table style="width: 100%; border: none;"> <tr> <td style="width: 45%;"><i>Result of autoconfiguration:</i></td> <td><i>Euro ISDN, point to multipoint</i></td> </tr> <tr> <td><i>ISDN Switch Type</i></td> <td><i>autodetect on bootup</i></td> </tr> <tr> <td><i>D-Channel</i></td> <td><i>dialup</i></td> </tr> <tr> <td><i>B-Channel 1</i></td> <td><i>dialup</i></td> </tr> <tr> <td><i>B-Channel 2</i></td> <td><i>dialup</i></td> </tr> <tr> <td colspan="2" style="padding-top: 10px;"><i>Incoming Call Answering ></i></td> </tr> <tr> <td colspan="2" style="padding-top: 5px;"><i>Advanced Settings></i></td> </tr> <tr> <td style="text-align: center; padding-top: 20px;"><i>SAVE</i></td> <td style="text-align: right; padding-top: 20px;"><i>CANCEL</i></td> </tr> </table> | | <i>Result of autoconfiguration:</i> | <i>Euro ISDN, point to multipoint</i> | <i>ISDN Switch Type</i> | <i>autodetect on bootup</i> | <i>D-Channel</i> | <i>dialup</i> | <i>B-Channel 1</i> | <i>dialup</i> | <i>B-Channel 2</i> | <i>dialup</i> | <i>Incoming Call Answering ></i> | | <i>Advanced Settings></i> | | <i>SAVE</i> | <i>CANCEL</i> |
| <i>Result of autoconfiguration:</i> | <i>Euro ISDN, point to multipoint</i> | | | | | | | | | | | | | | | | |
| <i>ISDN Switch Type</i> | <i>autodetect on bootup</i> | | | | | | | | | | | | | | | | |
| <i>D-Channel</i> | <i>dialup</i> | | | | | | | | | | | | | | | | |
| <i>B-Channel 1</i> | <i>dialup</i> | | | | | | | | | | | | | | | | |
| <i>B-Channel 2</i> | <i>dialup</i> | | | | | | | | | | | | | | | | |
| <i>Incoming Call Answering ></i> | | | | | | | | | | | | | | | | | |
| <i>Advanced Settings></i> | | | | | | | | | | | | | | | | | |
| <i>SAVE</i> | <i>CANCEL</i> | | | | | | | | | | | | | | | | |
| <i>Use <Space> to select</i> | | | | | | | | | | | | | | | | | |

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.

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

1. This type of leased line is called »Digital 64S mit Doppelschaltung« 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.

| <i>Item</i> | | <i>Number</i> | <i>Mode</i> | <i>Username</i> |
|----------------------|--|---------------|----------------------|-----------------|
| <i>ISDN Login</i> | | 993031 | <i>right to left</i> | |
| <i>PPP (routing)</i> | | 993030 | <i>right to left</i> | |
| <i>ADD</i> | | <i>DELETE</i> | <i>EXIT</i> | |

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) | <i>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).</i> |
| ISDN Login | <i>login service</i> |
| PPP 64k | <i>64kbps PPP data connection</i> |
| PPP 56k | <i>56kbps PPP data connection (not supported by the feature module)</i> |
| PPP Modem | <i>selects Modem Profile 1 as configured in the [MODEM] menu</i> |
| PPP DOVB | <i>data transmission over voice bearer; useful e.g. in the US where voice calls sometimes cost less than data connections</i> |
| PPP V.110 (1200 - 38400) | <i>bit-rate adaption according to V.110 (1200 bps, 2400 bps, ..., 38400 bps)</i> |
| PPP Modem Profile 1 ... 8 | <i>selects Modem Profile 1 ... 8 as configured in the [MODEM] menu</i> |
| CAPI 1.1 EAZ0 ... 9 Mapping | <i>EAZ mapping for CAPI 1.1 applications</i> |

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.

1. Called »Anlagenanschluß« in Germany

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

CM-1BRI, ISDN S0 → ADVANCED SETTINGS →

| | | | |
|------------------------------------|---------------|--------------------------|--|
| BIANCA/BRICK-XS Setup Tool | | BinTec Communications AG | |
| [WAN][Advanced]: Advanced Settings | | brick | |
| X.31 TEI Value | specify | | |
| Specify TEI Value | 0 | | |
| X.31 TEI Service | Packet Switch | | |
| SAVE | | CANCEL | |
| Use <Space> to select | | | |

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”.

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).

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

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.

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

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.

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.


| | | | |
|---|--------|---------------------------------|----------|
| <i>BIANCA/BRICK-XS Setup Tool</i> | | <i>BinTec Communications AG</i> | |
| [WAN][ADD][WAN NUMBERS]: WAN Numbers () | | <i>brick</i> | |
| WAN Numbers for this partner: | | | |
| WAN Number | 9302 | Direction | 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 |
| [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 |

| Wildcard | Example | Outgoing Calls | Incoming Calls |
|----------|----------|---|--|
| {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.

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

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.

| | | | | | | | | | | | | | | | | | |
|---|--|-----------------------|-------------------|-----------------------|-------------|---------------------|--------------|---------------------|-------------|------|------|-------------------|------------|--------------------------------|------------|----|--------|
| <i>BIANCA/BRICK-XS Setup Tool</i> [WAN][ADD][PPP]: PPP settings () | <i>BinTec Communications AG</i> brick | | | | | | | | | | | | | | | | |
| <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; padding: 5px;"> <i>Authentication</i> </td> <td style="width: 50%; padding: 5px;"> <i>CHAP + PAP</i> </td> </tr> <tr> <td style="padding: 5px;"> <i>Partner PPP ID</i> </td> <td style="padding: 5px;"> <i>none</i> </td> </tr> <tr> <td style="padding: 5px;"> <i>Local PPP ID</i> </td> <td style="padding: 5px;"> <i>brick</i> </td> </tr> <tr> <td style="padding: 5px;"> <i>PPP Password</i> </td> <td style="padding: 5px;"> <i>none</i> </td> </tr> <tr> <td style="padding: 5px;"> </td> <td style="padding: 5px;"> </td> </tr> <tr> <td style="padding: 5px;"> <i>Keepalives</i> </td> <td style="padding: 5px;"> <i>off</i> </td> </tr> <tr> <td style="padding: 5px;"> <i>Link Quality Monitoring</i> </td> <td style="padding: 5px;"> <i>off</i> </td> </tr> <tr> <td style="padding: 20px 5px 5px 5px;"> OK </td> <td style="padding: 20px 5px 5px 5px;"> CANCEL </td> </tr> </table> | | <i>Authentication</i> | <i>CHAP + PAP</i> | <i>Partner PPP ID</i> | <i>none</i> | <i>Local PPP ID</i> | <i>brick</i> | <i>PPP Password</i> | <i>none</i> | | | <i>Keepalives</i> | <i>off</i> | <i>Link Quality Monitoring</i> | <i>off</i> | OK | CANCEL |
| <i>Authentication</i> | <i>CHAP + PAP</i> | | | | | | | | | | | | | | | | |
| <i>Partner PPP ID</i> | <i>none</i> | | | | | | | | | | | | | | | | |
| <i>Local PPP ID</i> | <i>brick</i> | | | | | | | | | | | | | | | | |
| <i>PPP Password</i> | <i>none</i> | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| <i>Keepalives</i> | <i>off</i> | | | | | | | | | | | | | | | | |
| <i>Link Quality Monitoring</i> | <i>off</i> | | | | | | | | | | | | | | | | |
| 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 | <i>CHAP</i> |
| | <i>PAP</i> |
| | <i>CHAP + PAP</i> |
| | <i>CHAP + PAP + MS-CHAP</i> |
| | <i>MS-CHAP</i> |
| | <i>none</i> |
| | <i>LAPB Framing (only IP)</i> |
| | <i>LAPB Framing (only IP) + Compression</i> |

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.

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

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

| Setup Tool | SNMP Shell | Explanation |
|-------------------------------------|--------------------|--|
| <i>no</i> | <i>disabled</i> | <i>no Callback possible</i> |
| <i>expected (awaiting callback)</i> | <i>expected</i> | <i>wait for a call back from a partner</i> |
| <i>yes</i> | <i>enabled</i> | <i>accept callback requests and call back immediately</i> |
| <i>yes (delayed)</i> | <i>delayed</i> | <i>accept callback requests and call back after <i>RetryTime</i> seconds¹</i> |
| <i>yes (PPP negotiation)</i> | <i>ppp_offered</i> | <i>accept callback requests and negotiate the callback number inband</i> |

1. 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 126).



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 |
|----------------|---|----------------------------|-------------------|
| <i>static</i> | <i>No</i> | <i>N</i> | <i>N</i> |
| <i>dynamic</i> | <i>Yes</i> | <i>1</i> | <i>N</i> |
| <i>no</i> | <i>No</i> | <i>1</i> | <i>1</i> |

“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 page 43.

| Value | Meaning |
|-----------------------|--|
| ISDN 64kbps | 64kbps ISDN data connection |
| ISDN 56kbps | 56kbps ISDN data connection |
| Modem | selects Modem Profile 1 as configured in the [MODEM] menu |
| DOVB | <i>data transmission over voice bearer</i> ; useful e.g. in the US where voice calls sometimes cost less than data connections |
| 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 *biboPPPLoginString* used at connection time.

```

BIANCA/BRICK-XS 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:

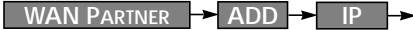
| Online Provider | Encapsulation in WAN Partner menu |
|-------------------------------------|--|
| <i>not defined</i> | <i>(default value, i.e. do not use this option)</i> |
| <i>CompuServe via T-Online</i> | <i>async PPP over X.75/T.70NL/T-Online²</i> |
| <i>CompuServe Corporate Network</i> | <i>async PPP over X.75¹</i> |
| | <i>async PPP over X.75/T.70NL/T-Online²</i> |
| <i>CompuServe Network</i> | <i>async PPP over X.75¹</i> |

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-XS 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.

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

RIP Send = Which types of RIP packets to send to this partner. If IPv2 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>



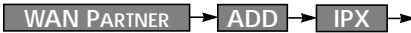
Please note that in cases where packets should take an asymmetric path—i.e. be received via one interface, but transmitted via a different interface—you have to switch *Back Route Verify* **off**, otherwise these packets are also discarded.

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.

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

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 |
|------------------------------|-------------------------|---------------|------------------------|---|
| <i>timed update</i> | <i>always</i> | <i>yes</i> | <i>yes</i> | <i>May lead to higher ISDN costs.</i> |
| <i>piggyback</i> | <i>never</i> | <i>yes</i> | <i>yes</i> | <i>At least 1 static route/service must be configured for partner</i> |
| <i>triggered + piggyback</i> | <i>only for changes</i> | <i>yes</i> | <i>yes</i> | <i>default setting (sufficient in most cases)</i> |
| <i>triggered</i> | <i>only for changes</i> | <i>yes</i> | <i>no</i> | <i>Less traffic but is less reliable than triggered + piggyback.</i> |
| <i>passive triggered</i> | <i>never</i> | <i>yes</i> | <i>no</i> | <i>At least 1 static route/service must be configured for partner</i> |
| <i>off</i> | <i>never</i> | <i>no</i> | <i>no</i> | <i>All routes/services must be configured statically.</i> |

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.

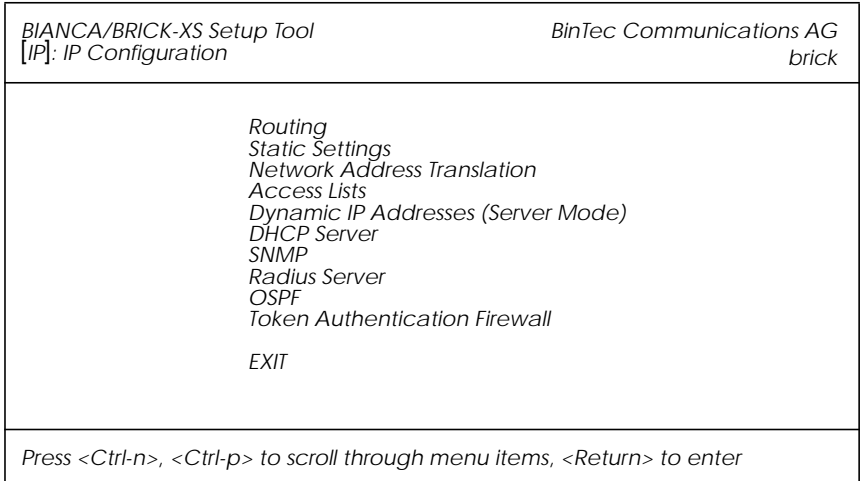


Enable Bridging = To enable bridging with this PPP partner set this field to “yes”.

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.



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-XS Setup Tool | | BinTec Communications AG | | | |
| [IP][ROUTING]: IP Routing | | 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 | Met. | Interf./Partner Pro |
| 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.



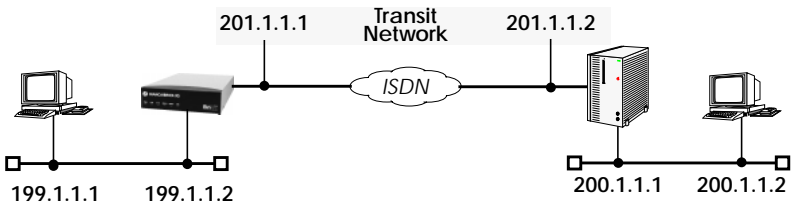
Use this menu to add (or make changes) to the IP routing table.

| | | | |
|--|-----------------------------|--------------------------|--|
| BIANCA/BRICK-XS 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 manufacturers). 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.

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

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 61 for information on automatic WINS/DNS address negotiation.

Time Protocol = The protocol to use to retrieve current time. The following protocols are possible.

| Protocol | Explanation |
|------------------|--|
| <i>time_udp</i> | <i>Time Service (RFC 868) via UDP</i> |
| <i>time_tcp</i> | <i>Time Service (RFC 868) via TCP</i> |
| <i>time_sntp</i> | <i>SNTP (Simple Network Time Protocol, RFC 1769) via UDP</i> |
| <i>isdn</i> | <i>ISDN D-Channel</i> |
| <i>none</i> | <i>Disable time retrieval altogether</i> |

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 over its 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 its 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.

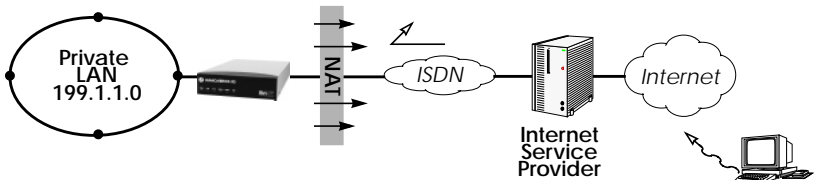
IP → Network Address Translation →

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

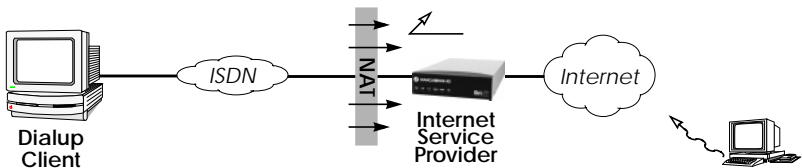
| | |
|--|-----------------------------------|
| BIANCA/BRICK-XS Setup Tool [IP][NAT]: NAT Configuration | BinTec Communications AG brick |
| <p>Select IP Interface to be configured for NAT</p> <pre> en1 partnerbrick1 partnerbrick2 partnerbrick3 partnerbrick4 EXIT </pre> | |
| <p>Press <Ctrl-n>, <Ctrl-p>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

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-XS 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.

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

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-XS Setup Tool                               BinTec Communications AG
[IP][ACCESS]: IP Access Lists                             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:

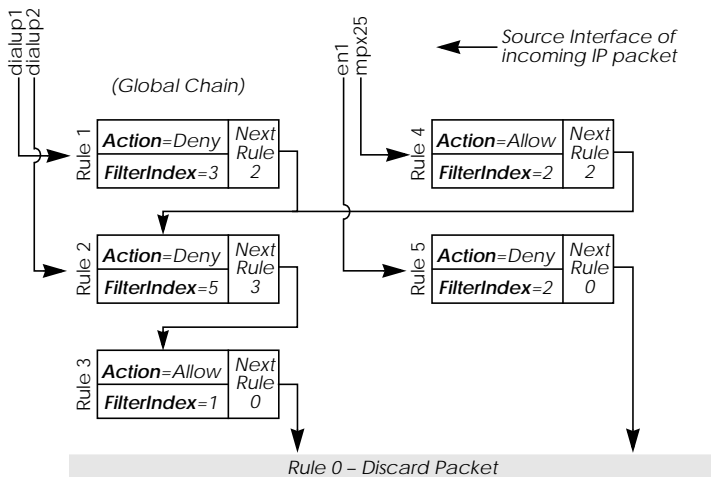
1. Access Filter to compare the packet to.
2. Action to take if a packet matches/doesn't-match a filter.
3. Index of the next rule to use if no action was taken.

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.

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

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.

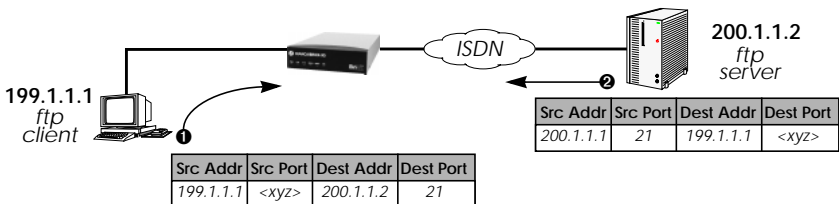
Source Port Ranges

| | | | |
|--------------------------------|---------------------|----------------|-----------------|
| 0 ... 1023 | 1024 ... 4999 | 5000 ... 32767 | 32768 ... 65535 |
| <i>privileged</i> | <i>unprivileged</i> | | |
| <i>server</i> | <i>clients</i> | <i>server</i> | <i>clients</i> |
| <i>specify / specify range</i> | | | |

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.

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

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.

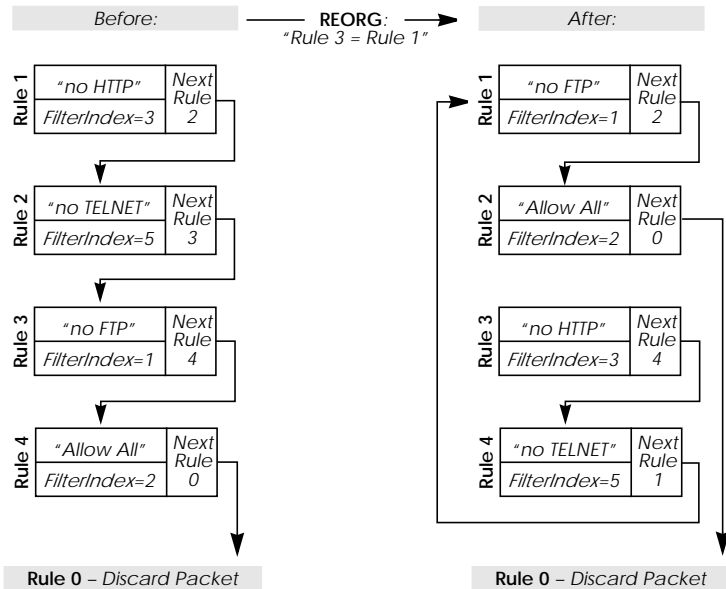
Action = The action field defines whether to allow or discard the packet based on whether or not the packet matches the filter (defined in the following field) or not.

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.

| | | |
|--|----------------------------|---------------------------------|
| <i>BIANCA/BRICK-XS Setup Tool</i> | | <i>BinTec Communications AG</i> |
| <i>[IP][ACCESS][INTERFACES]: Configure First Rules</i> | | <i>brick</i> |
| <i>Configure first rules for interfaces</i> | | |
| <i>Interface</i> | <i>First Rule</i> | <i>First Filter</i> |
| <i>en1</i> | <i>0 (no access rules)</i> | |
| <i>sales1</i> | <i>2</i> | <i>3 (all else)</i> |
| <i>sales2</i> | <i>2</i> | <i>3 (all else)</i> |
| <i>sales2</i> | <i>2</i> | <i>3 (all else)</i> |
| <i>EXIT</i> | | |
| <i>Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select</i> | | |

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.

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

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.

| <i>BIANCA/BRICK-XS Setup Tool</i> | | <i>BinTec Communications AG</i> | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|------------------------|---------------------------------|--------------------------|---------------------|------------------|--------------|--------------------------|--------------------|------------|---------------------|----------|-----------|--|------------|---------------------|----------|------------|--|------------|------------------------|----------|------------|---------------------|-----------------|-------------------|----------|------------|--|
| [IP][DHCP]: DHCP Server | | <i>brick</i> | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;"><i>Interface</i></th> <th style="text-align: left;"><i>IPAddress</i></th> <th style="text-align: left;"><i>Count</i></th> <th style="text-align: left;"><i>Lease Time (Min.)</i></th> <th style="text-align: left;"><i>MAC Address</i></th> </tr> </thead> <tbody> <tr> <td><i>en1</i></td> <td><i>192.168.1.70</i></td> <td><i>9</i></td> <td><i>30</i></td> <td></td> </tr> <tr> <td><i>en1</i></td> <td><i>199.168.1.85</i></td> <td><i>5</i></td> <td><i>120</i></td> <td></td> </tr> <tr> <td><i>en1</i></td> <td><i>192.120.130.144</i></td> <td><i>1</i></td> <td><i>480</i></td> <td><i>00a0f90046e7</i></td> </tr> <tr> <td><i>tr6-snap</i></td> <td><i>200.1.2.50</i></td> <td><i>4</i></td> <td><i>120</i></td> <td></td> </tr> </tbody> </table> <div style="display: flex; justify-content: space-around; width: 100%;"> <i>ADD</i> <i>DELETE</i> <i>EXIT</i> </div> | | | | <i>Interface</i> | <i>IPAddress</i> | <i>Count</i> | <i>Lease Time (Min.)</i> | <i>MAC Address</i> | <i>en1</i> | <i>192.168.1.70</i> | <i>9</i> | <i>30</i> | | <i>en1</i> | <i>199.168.1.85</i> | <i>5</i> | <i>120</i> | | <i>en1</i> | <i>192.120.130.144</i> | <i>1</i> | <i>480</i> | <i>00a0f90046e7</i> | <i>tr6-snap</i> | <i>200.1.2.50</i> | <i>4</i> | <i>120</i> | |
| <i>Interface</i> | <i>IPAddress</i> | <i>Count</i> | <i>Lease Time (Min.)</i> | <i>MAC Address</i> | | | | | | | | | | | | | | | | | | | | | | | | |
| <i>en1</i> | <i>192.168.1.70</i> | <i>9</i> | <i>30</i> | | | | | | | | | | | | | | | | | | | | | | | | | |
| <i>en1</i> | <i>199.168.1.85</i> | <i>5</i> | <i>120</i> | | | | | | | | | | | | | | | | | | | | | | | | | |
| <i>en1</i> | <i>192.120.130.144</i> | <i>1</i> | <i>480</i> | <i>00a0f90046e7</i> | | | | | | | | | | | | | | | | | | | | | | | | |
| <i>tr6-snap</i> | <i>200.1.2.50</i> | <i>4</i> | <i>120</i> | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p style="text-align: center;"><i>Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select</i></p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

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.

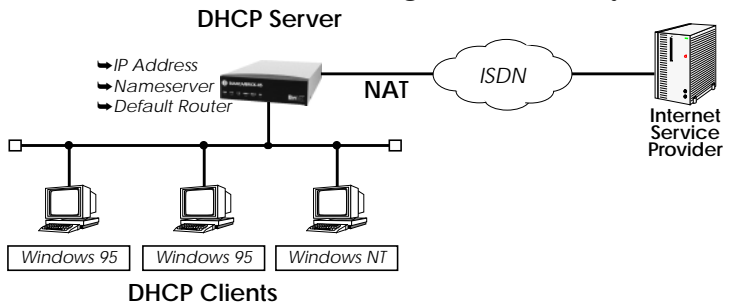
This only works, if *Number of consecutive addresses* is set to 1.

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.



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:

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

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.

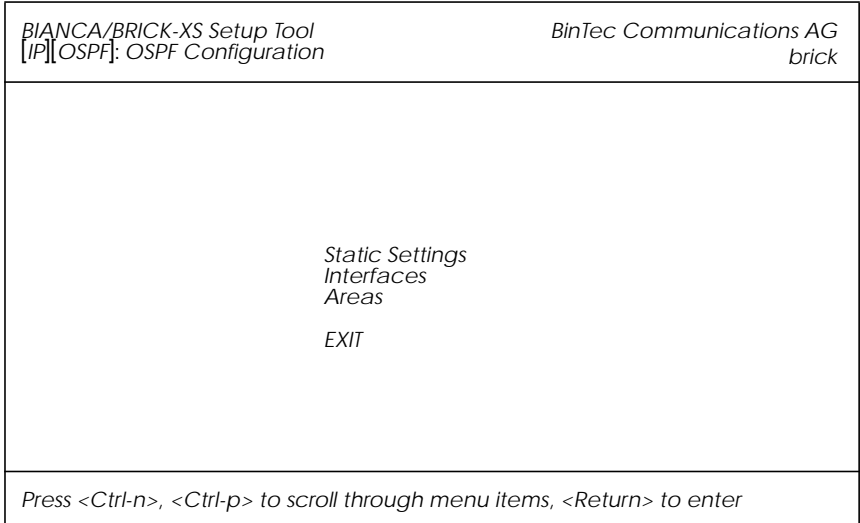
Default value: 1

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 *BIANCA/BRICK Extended Feature Reference* (contained on the Companion CD).

“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 accepts the entries and returns to the main menu.

Selecting 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.

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

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

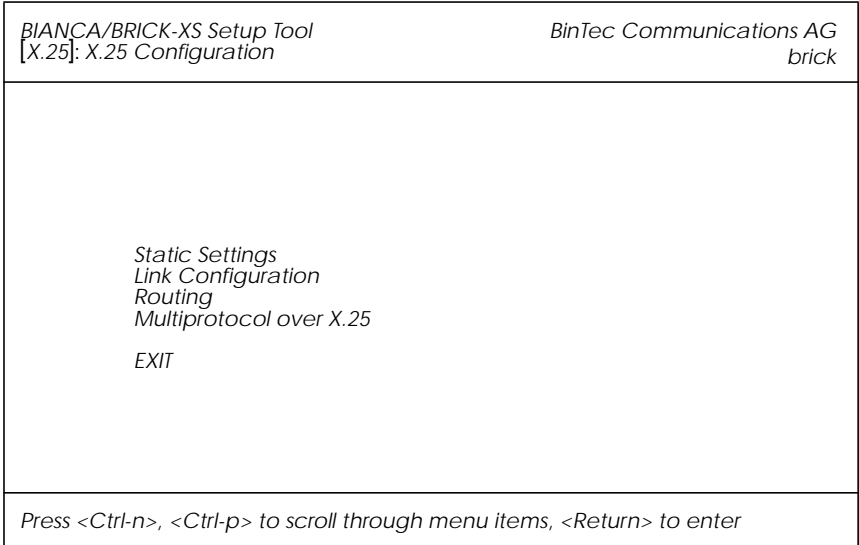
Authentication Protocol = Defines the type of PPP authentication protocol to offer the caller first. Possible values include: none, PAP, CHAP, CHAP + PAP, MS-CHAP, and CHAP + PAP + MS-CHAP.

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.



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.

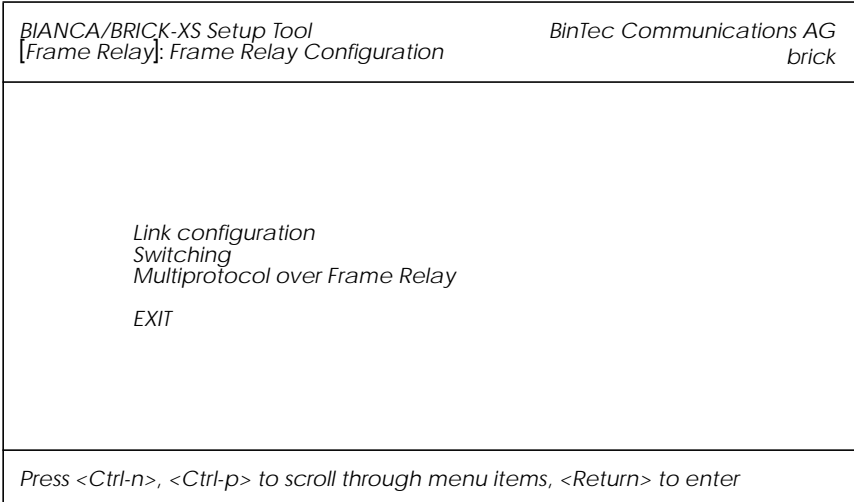
MULTIPROTOCOL OVER X.25 is used to configure the Multiprotocol Routing over X.25 (MPX25) feature.

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.

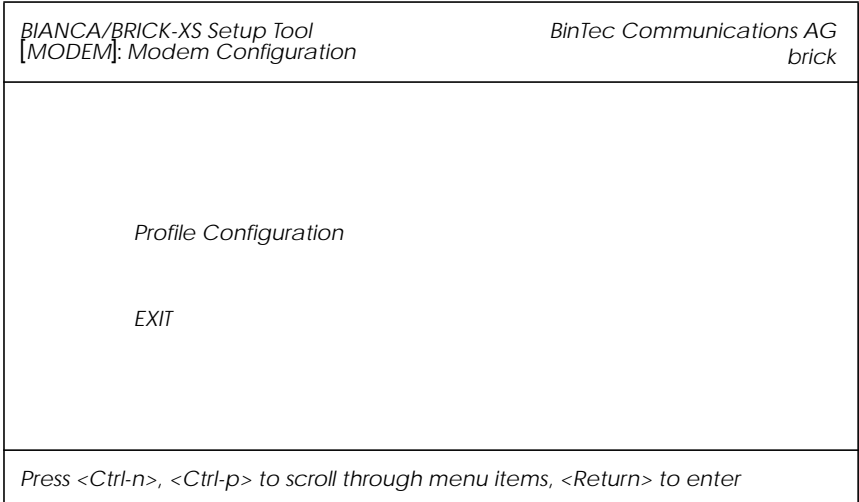
SWITCHING contains settings for each Frame Relay Virtual Circuit.

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 →

Note that this menu is only available on BRICK-XS Office systems.



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 14400 modems.

| | | | |
|---|--------------|--------------------------|--------|
| BIANCA/BRICK-XS Setup Tool | | BinTec Communications AG | |
| [MODEM][PROFILE][EDIT]: Configure Profile | | brick | |
| Name | Profile 1 | | |
| Description | Default User | | |
| Modulation | V.32bis | | |
| Error Correction | LAPM | | |
| Automode | on | | |
| Min Bps | 300 | | |
| Max Receive Bps | 14400 | | |
| Max Transmit Bps | 14400 | | |
| 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; 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 |
|-----------------|--|
| <i>none</i> | <i>Do not use any error correction.</i> |
| <i>required</i> | <i>First tries LAPM and then MNP5 error correction. If both fail, the modem will hang up.</i> |
| <i>auto</i> | <i>First tries LAPM and then MNP5 error correction. If both fail, the modem will not use error correction.</i> |
| <i>LAPM</i> | <i>Selects LAPM error correction. If this fails, the modem will hang up.</i> |
| <i>MNP</i> | <i>Selects MNP4 error correction. If this fails, the modem will hang up.</i> |

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.

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

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 BIANCA/BRICK Extended Feature 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.

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

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-XS 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  →  menu as shown on page 109.

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-XS 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.

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

Operation = Select the operation to perform.

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

| Operation | Meaning/Effect |
|---------------|---|
| <i>put</i> | If successful ¹ , overwrites/creates <TFTP File Name> on host at <TFTP Server> with contents of <Name in Flash>. |
| <i>get</i> | 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. |
| <i>state</i> | If successful ¹ , overwrites/creates <TFTP File Name> on host at <TFTP Server> with contents of memory ² . |
| <i>reboot</i> | 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 |
|----------------|---------------------------------------|
| <i>todo</i> | The operation has not been started. |
| <i>running</i> | The command is currently running. |
| <i>done</i> | The operation is done. |
| <i>error</i> | The operation could not be completed. |

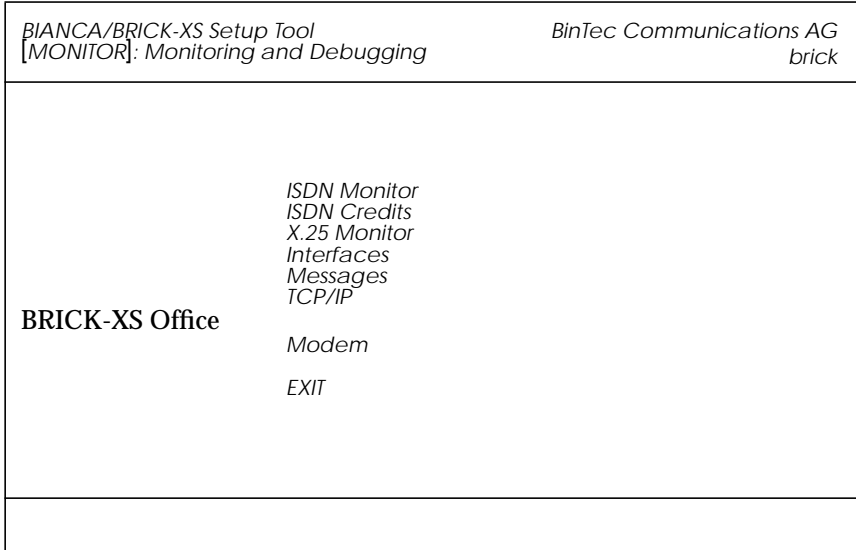
If the "error" state is reported Setup Tool's message monitoring menu, **MONITORING AND DEBUGGING** → **MESSAGES** may contain a possible cause

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.

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

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

| <i>Dir</i> | <i>Remote Number</i> | <i>Charge</i> | <i>Duration</i> | <i>Stack</i> | <i>Channel</i> | <i>State</i> |
|------------|----------------------|---------------|-----------------|--------------|----------------|-----------------|
| <i>in</i> | <i>2</i> | | <i>2910</i> | <i>0</i> | <i>B1</i> | <i>active</i> |
| <i>out</i> | <i>3</i> | | <i>106</i> | <i>0</i> | <i>B2</i> | <i>disc_req</i> |

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.

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

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.

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

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.

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

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-XS 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 | |
| Transmit Packets | 9 | 0 | 0 | 0 |
| Transmit Octets | 1193 | 0 | 0 | 0 |
| Transmit Errors | 0 | | 0 | |
| Active Connections | N/A | | 0 | |
| Duration | N/A | | 0 | |
| EXIT | EXTENDED | | EXTENDED | |

Use <Space> to select

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.



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-XS 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  Dspltem  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>.

MONITORING AND DEBUGGING →

MESSAGES →

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-XS 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.





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.

| | | | |
|-------------------------------------|-------------|---------------------------------|--------------|
| <i>BIANCA/BRICK-XS Setup Tool</i> | | <i>BinTec Communications AG</i> | |
| <i>[MONITOR][IP]: IP Statistics</i> | | <i>brick</i> | |
| <i>InReceives</i> | <i>3912</i> | <i>OutNoRoutes</i> | <i>0</i> |
| <i>InHdrErrors</i> | <i>0</i> | <i>ReasmTimeout</i> | <i>500</i> |
| <i>InAddrErrors</i> | <i>0</i> | <i>ReasmReqds</i> | <i>0</i> |
| <i>ForwDatagrams</i> | <i>0</i> | <i>ReasmOKs</i> | <i>0</i> |
| <i>InUnknownProtos</i> | <i>0</i> | <i>ReasmFails</i> | <i>0</i> |
| <i>InDiscards</i> | <i>0</i> | <i>FragOKs</i> | <i>0</i> |
| <i>InDelivers</i> | <i>3321</i> | <i>FragFails</i> | <i>0</i> |
| <i>OutRequests</i> | <i>9</i> | <i>FragCreates</i> | <i>0</i> |
| <i>OutDiscards</i> | <i>0</i> | <i>RoutingDiscards</i> | <i>0</i> |
| <i>EXIT</i> | | | |
| <i>I(C)MP</i> | <i>(I)P</i> | <i>(U)DP</i> | <i>(T)CP</i> |

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-XS Setup Tool | | | BinTec Communications AG | | |
|------------------------------------|------------------|----------------------|--------------------------|-----------------|------------|
| [MONITOR][OSPF]: OSPF Monitor | | | brick | | |
| <i>Interface</i> | <i>DR</i> | <i>BDR</i> | <i>Admin Status</i> | <i>State</i> | |
| en1 | 192.168.30.1 | 192.168.30.0 | active | BDR | |
| brickxs | 0.0.0.0 | 0.0.0.0 | active | PTP | |
| <i>Neighbor</i> | <i>Router ID</i> | <i>Interface</i> | <i>Retx Queue</i> | <i>State</i> | |
| 192.168.30.1 | 10.0.1.1 | en1 | 0 | full | |
| 12.0.0.2 | 11.0.0.2 | brickxs | 0 | full | |
| <i>Area</i> | <i>Type</i> | <i>Link State ID</i> | <i>Router ID</i> | <i>Sequence</i> | <i>Age</i> |
| 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).



This menu allows your to monitor the status of each modem installed on your BRICK. On BRICK-XS Office systems, there will always be exactly two entries in this menu. The individual fields shown below correspond to the SNMP table entries in the *mdmTable*.

| BIANCA/BRICK-XS Setup Tool | | | | | | BinTec Communications AG | | | |
|------------------------------------|---------|--------|-----------|------|------------|--------------------------|---------|----------|---------------|
| [MONITOR] [MODEM]: Modem Calls | | | | | | brick | | | |
| Index | Action | Type | State | Mode | Modulation | Err Corr | ComprTX | RX Speed | ifindex/BChan |
| 2000 | enabled | mdm144 | connected | ppp | v32bis | none | none | 14K 14K | 2000/1 |
| 2001 | enabled | mdm144 | 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-XS Office the index numbers for the two internal modems will be always be 2000 and 2001.

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.

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.

| <i>BRICK/BinGO! Product:</i> | <i>Modem Types</i> | | | |
|-------------------------------|--------------------|---------------|----------------|----------------|
| | <i>mdm144</i> | <i>mdm336</i> | <i>csm336</i> | <i>csm56K</i> |
| <i>BinGO! Plus</i> | - | - | - | - |
| <i>BinGO! Professional</i> | ✓ | | - | - |
| <i>BIANCA/BRICK-XS Office</i> | ✓ | - | - | - |
| <i>BIANCA/BRICK-XM</i> | - | - | ✓ ¹ | - |
| <i>BIANCA/BRICK-XMP</i> | - | - | - | ✓ |
| <i>BIANCA/BRICK-XL2</i> | - | - | ✓ 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:

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

Mode = The mode the modem is currently in.

| | |
|--------------|---|
| <i>modem</i> | <i>Modulation mode.</i> |
| <i>ppp</i> | <i>Modulation mode + asynchronous HDLC framing.</i> |
| <i>fax</i> | <i>A FAX is being sent or received.</i> |
| <i>dtmf</i> | <i>Sending or receiving DTMF touchtones.</i> |
| <i>none</i> | <i>The modem is currently not in use.</i> |

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 .

| | | | | |
|----------------|----------------|----------------|------------|----------------|
| <i>bell103</i> | <i>bell212</i> | <i>v21</i> | <i>v22</i> | <i>v22bis</i> |
| <i>v23</i> | <i>v32</i> | <i>v32bis</i> | <i>v34</i> | <i>k56flex</i> |
| <i>vfc</i> | <i>v90</i> | <i>unknown</i> | | |

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

| | |
|-------------|---|
| <i>none</i> | <i>Error correction is not being performed.</i> |
| <i>alt</i> | <i>MNP error correction.</i> |
| <i>lapm</i> | <i>LAPM error correction.</i> |

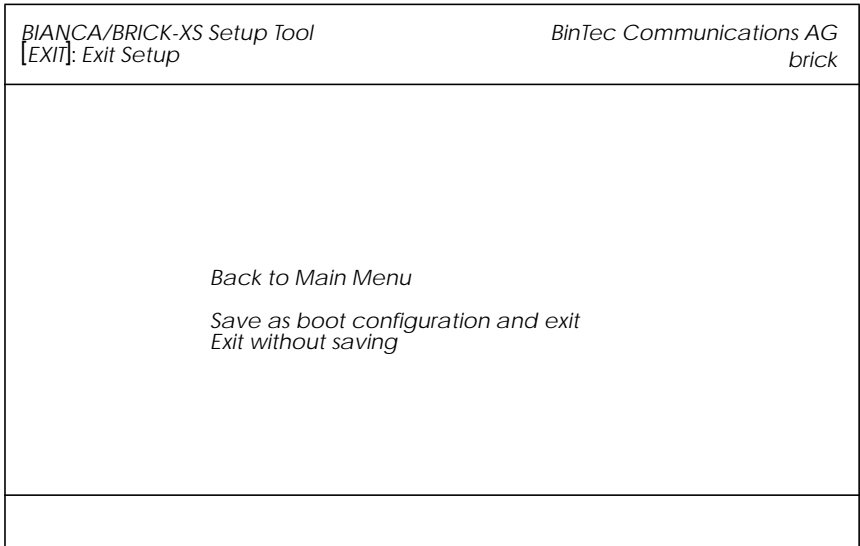
TX Speed = The transmit speed negotiated by the modems. This will always be the same as the RX Speed.

RX Speed = The receive speed negotiated by the modems. As stated above, this is always the same as the TX Speed.

Ifindex/BChannel = If a connection has been established, this field identifies the ifindex 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* 123
 - *IP Features* 129
 - *IPX Features* 144
 - *Fax Features* 146
 - *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. 48) 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



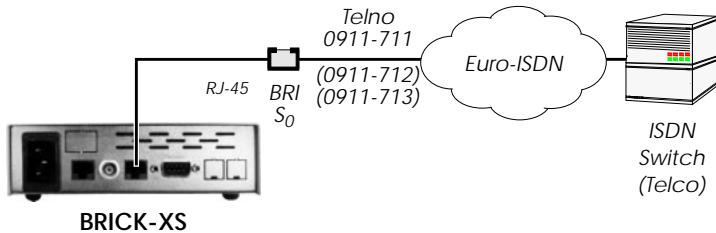
As an ISDN multiprotocol router, BIANCA/BRICK-XS and BRICK-XS office establish ISDN connections in accordance with the system's configuration. Incorrect or incomplete configuration of your product may cause unwanted charges. The conditions that lead to establishing connections are largely dependent on 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 109, 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 176 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.



The settings for our ISDN interface shown above would be configured in Setup Tool as follows:

WAN Interface: `CM-1BRI, ISDN S0` → Here's where we tell the BRICK what type of ISDN service we're receiving over this line.

Result 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.

WAN InterfacePABX: 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 ISDN interface 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.

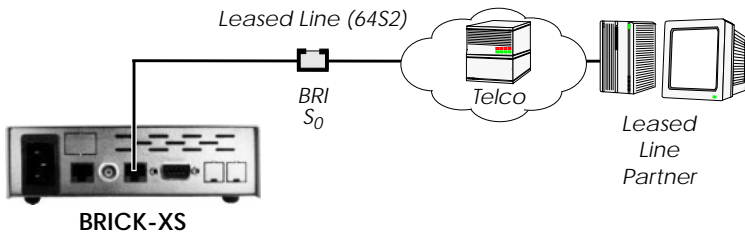
BIANCA/BRICK-XS These settings aren't normally required since the BRICK detects this information automatically.

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 123, 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” 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 129.

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. 56) 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.

Info: 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.

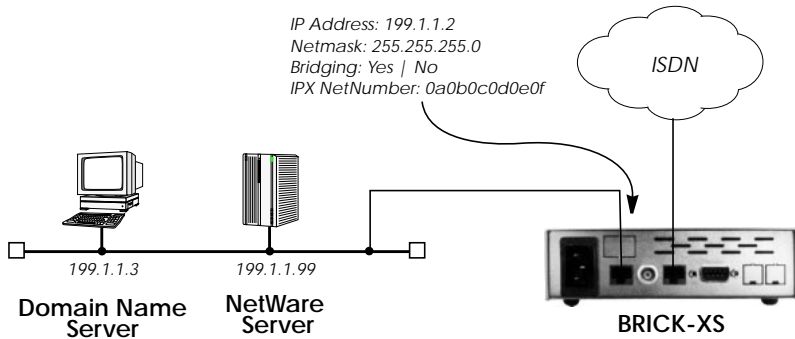
For example, in Germany there are different maximum charging unit lengths for different tariff zones (City = 4 minutes, long distance calls = 2 minutes), so you can set the *Static Short Hold* to 245 (>4 minutes) for City connections, and to 125 (>2 minutes) for long distance calls, to avoid nullifying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

Configuring an ethernet interface on the BRICK involves telling the BRICK a few things about the LAN attached to this interface such as the IP address and netmask to use and the type of header information to apply to frames sent over this interface.



This information is configured in the **CM-BNCTP, ETHERNET** → menu.

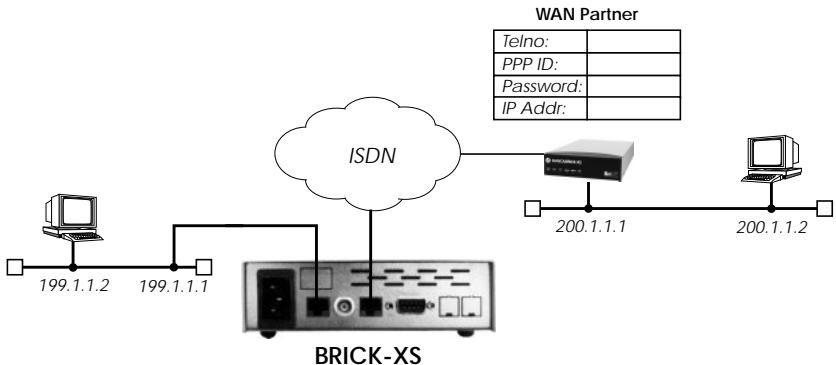
Under the **ADVANCED SETTINGS** → menu the following advanced features can optionally be enabled:

- RIP (versions 1 and 2)
- IP Accounting
- Proxy ARP

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. 48) **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. 51) **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 > | |

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

(p. 54) **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. 60) **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 56 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. 48) **WAN PARTNER** → **ADD** → **Create Partner Interface**

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

(p. 51) **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. 59) **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. 60) 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. 59) 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. 60) **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. 60) **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 137.

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. 48) **WAN PARTNER** → **ADD** → **Dialup Clients**

Here you'll need to set:

| | |
|---------------|----------------------------------|
| Partner Name | <Unique Partner Name> |
| Encapsulation | <select an IP compatible method> |

(p. 51) **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. 54) **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. [60](#)) **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. [61](#)) **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. 48) **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. 51) **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. 54) **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. 60) **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)  →  → **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  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)  →  →  → **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> |

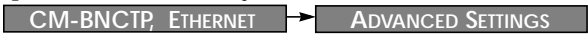
More Info

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: 

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

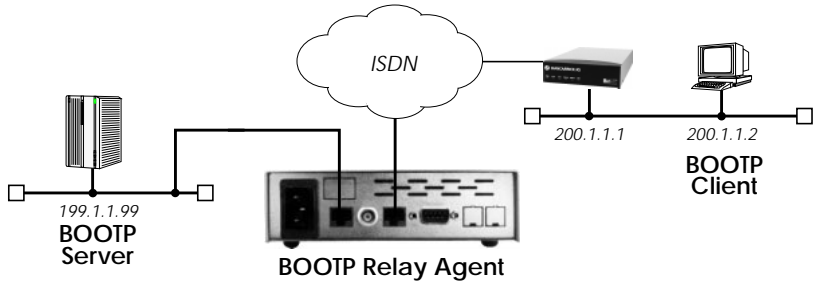
Additional information regarding RADIUS is contained in the *Extended Feature Reference* on the Companion CD. As a quick reference the BRICK supports the following RADIUS attributes which can be used in the RADIUS server’s user database. For configuration information relating to your RADIUS server refer to your local documentation.

| RADIUS Attribute | Type | R / A | Remark |
|---------------------------|----------------|-------|---|
| <i>User-Name</i> | <i>string</i> | REQ | <i>User name, mandatory inband: PPP partner name outband: PPP partner telephone number</i> |
| <i>User-Password</i> | <i>string</i> | REQ | <i>Password for PAP authentication</i> |
| <i>CHAP-Password</i> | <i>string</i> | REQ | <i>Password for CHAP authentication</i> |
| <i>NAS-Identifier</i> | <i>string</i> | REQ | <i>sysName of the BRICK</i> |
| <i>Service-Type</i> | <i>integer</i> | ANS | <i>Framed (for PPP) Callback-Framed (for PPP with Callback)</i> |
| <i>Framed-Protocol</i> | <i>integer</i> | ANS | <i>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</i> |
| <i>Framed-IP-Address</i> | <i>ipaddr</i> | ANS | <i>Partner IP address</i> |
| <i>Framed-IP-Netmask</i> | <i>ipaddr</i> | ANS | <i>Partner IP netmask</i> |
| <i>Framed-Routing</i> | <i>integer</i> | ANS | <i>None, RIPv1-Broadcast, RIPv1-Listen, RIPv1-Broadcast-Listen</i> |
| <i>Framed-Compression</i> | <i>integer</i> | ANS | <i>None, Van-Jacobson-TCP-IP</i> |
| <i>Framed-Route</i> | <i>string</i> | ANS | <i>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</i> |

| RADIUS Attribute | Type | R / A | Remark |
|-------------------------|----------------|--------------|---|
| <i>Idle-Timeout</i> | <i>integer</i> | <i>ANS</i> | <i>Shorthold</i> |
| <i>Port-Limit</i> | <i>integer</i> | <i>ANS</i> | <i>Number of B channels (== MaxConn)</i> |
| <i>Reply-Message</i> | <i>string</i> | <i>ANS</i> | <i>outband: ifDescr is set to this name (instead of using the telephone number)</i> |
| <i>Callback-Number</i> | <i>string</i> | <i>ANS</i> | <i>telephone number for Callback</i> |

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)



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. 48)



(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-BNCTP, ETHERNET** →

Configure LAN interface

Enter the IPX Network Number of the LAN attached to this interface.

Local IPX-NetNumber

<IPX Network Number>

(p. 48) **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. 63) **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.



Fax Features

How do I configure fax service from RVS-COM

Note:  With your router you have received just one license for RVS-COM Lite. If you want to install RVS-COM Lite on more PCs, contact RVS Datentechnik GmbH. You can retrieve the address from RVS-COM Lite's online help.

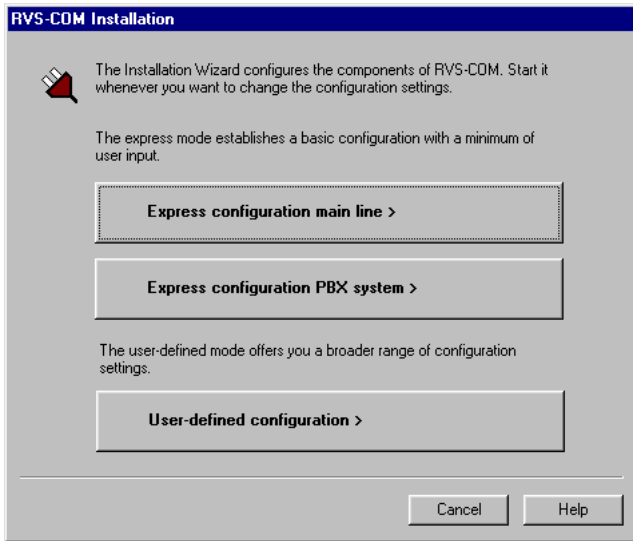
Info:  If you work with the softfax solution when faxing with your router and RVS-COM Lite, the fax software must always be started when you want to receive faxes. On installing RVS-COM Lite, RVS-COM is stored in the Windows Taskbar – as long as you do not close the program, RVS-COM is available at all times.
On BRICK-XS Office systems you may disable the Softmodem option in the RVS CommCenter and use hardware fax.

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 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.

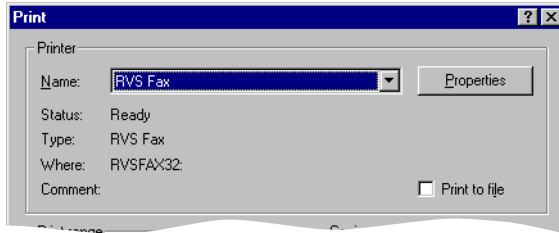
Click Next>. The ISDN Phone Numbers component is configured.

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.

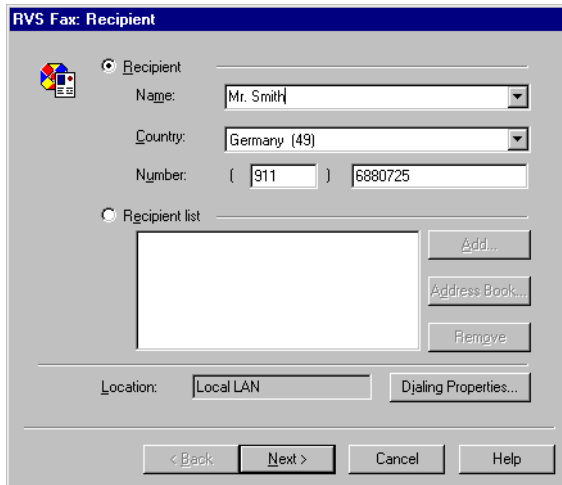
Faxing from MS Applications via RVS Fax

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.

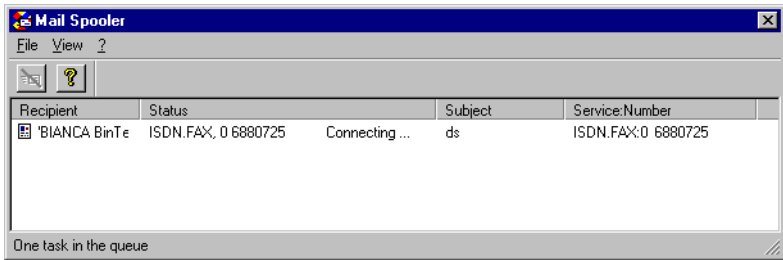
1. From the application menu select the File option then Print...
2. In the Printer section of the print setup dialog, select the printer name **RVS Fax**.



3. The RVS Fax Assistant is then started. The parameters for this fax can be defined here.



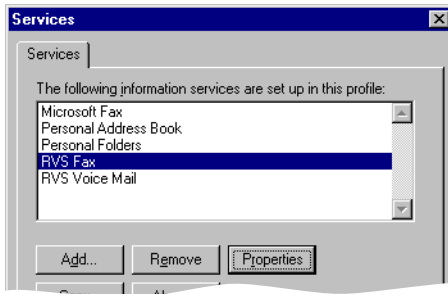
4. The new fax is then spooled to the Mail Spooler which shows the status of the fax transmission.



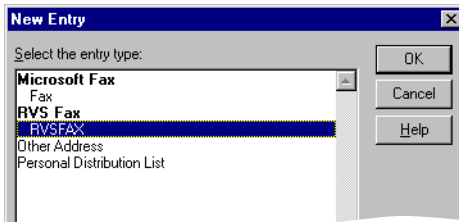
Faxing from Microsoft Exchange

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.

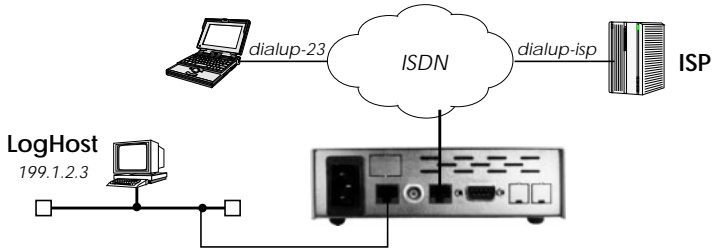
The image shows a Windows-style dialog box titled "New RVSFAX Properties". It has four tabs: "Business", "Phone Numbers", "Notes", and "RVSFAX - Fax", with the last one selected. The dialog is divided into two main sections. The "Name" section contains two text input fields: "Vorname:" with the value "BIANCA" and "Nachname:" with the value "BinTec". The "Faxnummer" section contains a "Land:" dropdown menu set to "Germany (49)" and a "Nummer:" field with a country code dropdown set to "911" and a main number field containing "6880725". At the bottom of the dialog 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-BNCTP, 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. 56) **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.

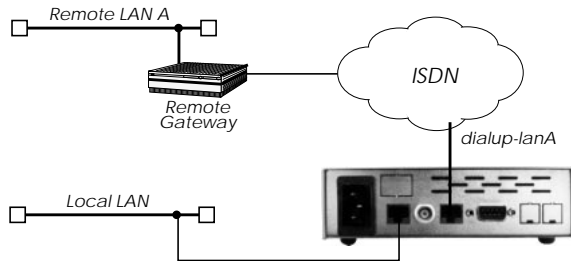
Info: Do NOT turn IP accounting on for the LAN interface if you are using an external Log Host. Since the sending of a message requires a UDP connection this must be heeded to avoid an endless cycle of connections.

? 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 must be accessible over ISDN/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. 48) **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) |

(p. 54) 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> |

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 106.

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.

`CM-BNCTP, ETHERNET` → `ADVANCED SETTINGS` →

`WAN PARTNER` → `IP` → `ADVANCED SETTINGS` →

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 it's 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 163, 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:

| Interface | Displayed State | Possible Causes |
|-----------|-----------------|-----------------------------|
| LAN | <i>o.k.</i> | <i>Normal operation.</i> |
| | <i>inactive</i> | <i>Cable not connected.</i> |

| Interface | Displayed State | Possible Causes |
|-----------|---------------------|---|
| WAN | <i>o.k.</i> | <i>Normal operation.</i> |
| | <i>inactive</i> | <i>No B-channels currently in use.</i> |
| | <i>unconfigured</i> | <i>Cable not connected or incorrect D-channel protocol is being used.</i> |

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   menu.

Column four of the Hardware Interfaces table displays the current state of the ISDN B-Channels and analog 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).

System Information: BIANCA

System description

| | |
|----------------|-------------------------------------|
| Type of System | BIANCA/BRICK-XS |
| 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 | TUNNELING | CAPI | BRIDGE | X25 | FRAME_RELAY | IPX |
|------|------|------------|------|--------|------|-------------|------|
| o.k. | o.k. | no license | o.k. | o.k. | o.k. | no license | o.k. |

Hardware Interfaces

| Interface | Protocol | Status | Usage |
|-----------|----------|--------|---------------------|
| LAN | Ethernet | o.k. | |
| WAN | ISDN S0 | o.k. | used 2, available 0 |
| LOCAL | | | |

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>

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
```

isdnchisdnifindex / isdnchstate / isdnchreceivedoctets / isdnchtransmitoctets / isdnchreceivederrors

Refresh time Orientation

| isdnchisdnifindex | isdnchstate | isdnchreceivedoctets | isdnchtransmitoctets | isdnchreceivederrors |
|-------------------|-------------------|----------------------|----------------------|----------------------|
| isdnifindex | State | Received Octets | Transmit Octets | Received Errors |
| 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*..... 172
 - *ISDN Connections* 175
-

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 *175* 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.

Hardware Problems

Serial Console

On the BRICK-X 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 64. 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 front plane LEDs. Refer to Chapter 8 for meanings of the front panel indicators.
- 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 *biboPPPTable* (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 front panel indicators. Refer to Chapter 8 for the meanings of individual LEDs.

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 100. 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 56 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*

| | | | |
|------------------------|-----|-----------------------|-----|
| <i>telnet</i> | 181 | <i>date</i> | 188 |
| <i>ping</i> | 181 | <i>update</i> | 188 |
| <i>ipxping</i> | 182 | <i>setup</i> | 188 |
| <i>trace</i> | 182 | <i>debug</i> | 189 |
| <i>rtlookup</i> | 184 | <i>p</i> | 189 |
| <i>tracert</i> | 185 | <i>t</i> | 189 |
| <i>lfstat</i> | 185 | <i>ifconfig</i> | 190 |
| <i>netstat</i> | 186 | <i>halt</i> | 191 |
| <i>isdnlogin</i> | 186 | <i>ospfmon</i> | 191 |
| <i>minipad</i> | 187 | | |

- *BRICKtools for UNIX Commands*

| | | | |
|-------------------------|-----|------------------------|-----|
| <i>bricktrace</i> | 192 | <i>capitrace</i> | 192 |
|-------------------------|-----|------------------------|-----|

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 [-h23iNxx1] [-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 <tei> | set TEI filter (D-Channel only) |
| next | only display info for the next B-channel that is opened (B-Channel only) |
| -c <cref> | set callref filter (D-Channel only) |
| -d <MAC filter> | set destination MAC address filter (LAN only) |
| -s <MAC filter> | 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 [YYMMDDHHMMSS]

The BRICK has a software clock. Entering **date** by itself from the SNMP shell reads and displays the current time. Using **date** followed by a date string (YYMMDDHHMMSS) sets the clock 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.

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>.
```

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

| | | | |
|--|-----|--|-----|
| <i>Hardware</i> | 196 | <i>BOOTmonitor</i> | 200 |
| <i>Front Panel Indicators</i> | 196 | <i>Automatic booting over TFTP</i> | 203 |
| <i>The Back Plane</i> | 198 | | |
| <i>The Main Board</i> | 199 | | |
| <i>Firmware</i> | 200 | | |
| <i>Upgrading System Software</i> | 200 | | |



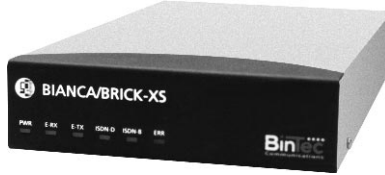
As a member of BinTec's BIANCA/BRICK family of multiprotocol routers, the BRICK-XS offers a low-cost high-capability solution for today's growing SOHO (Small Office Home Office) environments.

In this chapter we'll cover the BRICK hardware and some important tasks you may need to perform in future such as upgrading system software.



Hardware

Front Panel Indicators



There are six front panel indicators (LEDs) that display status information about your BRICK-XSBRICK. The various LEDs have different meanings depending on which mode the BRICK-XSBRICK is in. As the BRICK-XSBRICK is powered up, it switches between several operational modes.

- Power Up Mode
- BOOTmonitor Mode
- Normal Operation Mode

These meanings are described in the following tables.

Power Up Mode

| LED | State | Meaning |
|--------|----------|------------------------------------|
| PWR | On | Power is being supplied. |
| E-RX | Blinking | DRAM test is being performed |
| E-TX | Off | Not used. |
| ISDN-D | Blinking | Flash ROM test is being performed. |
| ISDN-B | Blinking | CHIP test is being performed. |
| ERR | Off | Not used. |

BOOTmonitor Mode

| LED(s) | State | Meaning |
|-------------------------|----------|---|
| PWR | On | Power is being supplied. |
| E-RX | Off | Not used. |
| E-T | Blinking | Performing a TFTP transfer. |
| ISDN-D ISDN-B ERR | On | BOOTmonitor is in use (or awaiting keyboard input). |
| | Blinking | BOOTmonitor decompressing boot image. |

Normal Operation Mode

| LED | State | Meaning |
|--------|----------------------|---|
| PWR | On | Power is being supplied. |
| E-RX | <i>Slow Blinking</i> | <i>Receiving a packet from the LAN interface.</i> |
| | <i>Fast Blinking</i> | <i>Receiving all packets on LAN (i.e., when the is bridging in promiscuous mode).</i> |
| E-TX | On | Packet being sent over the LAN interface. |
| ISDN-D | <i>Off</i> | <i>ISDN cable not connected. (error)</i> |
| | <i>On</i> | <i>D-Channel protocol found. (o.k.)</i> |
| | <i>Slow Blinking</i> | <i>D-Channel protocol found and Layer 1 is activated. (o.k.)</i> |
| | <i>Fast Blinking</i> | <i>Layer 1 is activated but no D-channel protocol was found. (error)</i> |
| ISDN-B | <i>Off</i> | <i>No connection.</i> |
| | <i>On</i> | <i>1 B-Channel in use.</i> |
| | <i>Blinking</i> | <i>2 B-Channels in use.</i> |
| ERR | On (intermitent) | Collision detected on the LAN. (each on state denotes a collision). |
| | On (constant) | The LAN cabling is not connected (no 10BaseT cable found) |

The Back Plane

As shown in figure 3, the back plane contains all the accessible ports for the BRICK-XSBRICK. For information on the individual pin assignments of each port, see *Appendix A*.



Figure 3: Back Plane BRICK-XS

The Power Socket

The BRICK-XS is capable of operating within 100 - 240 VAC, 50 - 60 Hz, max. 0.2 A. The BRICK-XS has a universal power supply that senses the incoming voltage and adjusts accordingly. Depending on the country you purchased your BRICK-XS in, you should be able to use the included power cord.

Before supplying power to the BRICK-XSBRICK, please verify the power rating identified on the marking label complies with your local power source.

The Network Ports

The BRICK-XSBRICK has a 10base2 (BNC) and 10baseT (TP) port for connecting to the LAN and an ISDN S₀ port (marked ISDN-S₀) for connecting to your ISDN subscriber outlet.

Serial Port

The BRICK-XSBRICK has a 9 pin serial port on the back plane for connecting a console and supports baud rates between 1200 and 115,200 baud. To

allow for compatibility with a wider variety of terminals, the pin assignments for the serial port have been modified. See *Appendix A* for individual pin assignments for the serial port. Chapter 2, *Installing the BRICK*, explains connecting a terminal.

The Main Board

The BRICK main board contains built-in LAN and ISDN interfaces. These interfaces are accessible via the ports on the back plane which are labelled as shown in figure 3above. There is also an internal slot for the addition of an optional feature board.

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 4 below. As long as the

BOOTmonitor is active (or awaiting keyboard input), all LEDs will remain on.

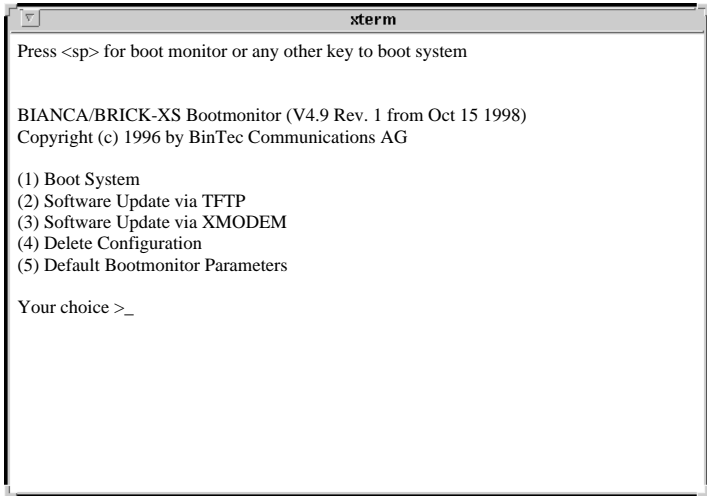


Figure 4: *BOOTmonitor*

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 IP address for the BRICK
- The IP address for the TFTP server
- 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.



A

TECHNICAL DATA

What's covered

- *General System Specifications*
- *Pin Assignments*
 - *ISDN Interface*
 - *Ethernet*
 - *Serial Port*
- *Important Safety Information in:*
 - *Danish, Dutch, Finnish, French,*
 - *German, Greek, Italian,*
 - *Norwegian, Portugese,*
 - *Swedish, Spanish*

General System Specifications

- Processor:** MC68EC020, 20 MHz
- Memory:** 4 MB/32 bit DRAM SIMM,
1 MB/8 bit flash-ROM
- Interfaces:** ISDN WAN S₀
Ethernet: IEEE 802.3 LAN (10BaseT and 10Base2)
internal slot for feature module (optional)
- Serial:** 1 x RS 232 C, Sub9 Male (PC), 1,200 - 115k Bd.
- LEDs:** 6 (1 Power, 4 Function, 1 Error)
- Power:** 100-240 VAC, 60/50 Hz, max. 0.2 A, universal
power supply¹ with internal fan.
- Dimensions:** 151 mm x 45 mm x 273 mm (WHD)

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

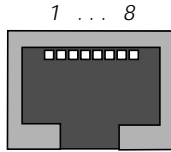


Figure 5: ISDN S₀ BRI Interface

Pin assignments for the S₀ port 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 |

Ethernet Port

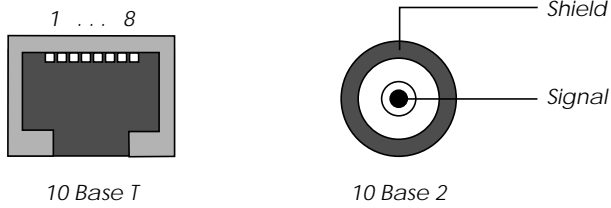


Figure 6: Twisted pair port (10 Base T) and BNC port (10 Base 2)

Pin assignments for the twisted pair (RJ45) port on the BRICK-XS are as follows:

| Pin | Function |
|-----|----------------------------|
| 1 | <i>TD +</i> |
| 2 | <i>TD -</i> |
| 3 | <i>RD +</i> |
| 4 | <i>Not used by 10BaseT</i> |
| 5 | <i>Not used by 10BaseT</i> |
| 6 | <i>RD -</i> |
| 7 | <i>Not used by 10BaseT</i> |
| 8 | <i>Not used by 10BaseT</i> |

Serial Port

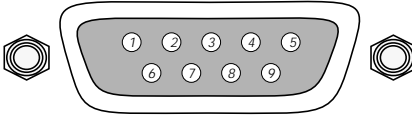


Figure 7: 9 Pin Serial Port

Pin assignments for the 9 pin serial port are as follows:

| Pin | Function |
|-----|--|
| 1 | <i>DCD (not connected)</i> |
| 2 | <i>Receive</i> |
| 3 | <i>Transmit</i> |
| 4 | <i>DTR - DSR (redirected to pin 6)</i> |
| 5 | <i>Ground</i> |
| 6 | <i>DSR - DTR (redirected to pin 4)</i> |
| 7 | <i>RTS - CTS (redirected to pin 8)</i> |
| 8 | <i>CTS - RTS (redirected to pin 7)</i> |
| 9 | <i>(not connected)</i> |

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 omgivelsesbetingelserne 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:
100 - 240 VAC
60 / 50 Hz
maks. 0,2 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. smykke kæder, clips osv.) eller vædske kan nå ind i apparatets indre (elektrisk stød, kortslutning).
- I nødstilfælde (f.eks. beskadiget kasse eller betjeningselement, 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 uhenigtsmæssige reparaturer er det muligt, at brugeren udsættes for en betydelig fare. En ikke tilladt åbning af apparaterne har til følge, at BinTec Communications AG fralægger sig enhver form for garanti og ansvar.
- Anvend kun de vedlagte kabler. Hvis der anvendes andre kabler, tager BinTec Communications AG ingen ansvar for opståede skader.
- Vigtig henvisning til fagpersonalet: Netstikket skal trækkes før systemenheden åbnes.
- CE-tegnet betyder, at „BRICK“ svarer til følgende EF-retningslinjer: elektromagnetisk kompatibilitet (89/336/EWG) og lavspænding (73/23/EWG).
- Elektrostatiske opladninger kan medføre skader i apparatet. De skulle derfor have en antistatisk manchet 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:
 - 100 - 240 VAC
 - 60 / 50 Hz
 - maks. 0,2 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.
- 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. Onbevoegd openen van de apparaten sluit elke vorm van aansprakelijkheid en garantie van de firma BinTec Communications AG uit.
- 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

Laitte vastaa toimistotiloissa käytettäviin tietotekniikan laitteisiin päteviä asianmukaisia turvallisuusohjeita.

Tästä jaksosta löytyvät ne turvallisuusohjeet, joiden noudattaminen on ehdottomasti välttämätöntä järjestelmän kanssa työskenneltäessä. 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 nimelliskäyttöjännite paikallista verkkojännitettä. Laitetta saa käyttää seuraavien olosuhteiden vallitessa:
100 - 240 VAC
60 / 50 Hz
maks. 0,2 A
- Kytke laite vain sääntöjenmukaisesti maadoitettuun suojakosketinpistorasiaan (laite on varustettu turvallisuustarkastetulla verkkojohtolla).
- Varmista, että sisäasennuksen suojakosketinpistorasia on esteettömästi saavutettavissa. Täydellinen 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 tiedonvälitysjohdoja äläkä vedä niitä pois ukonilman aikana.
- Noudata järjestelmän kaapeloinnissa kuvauksen mukaista järjestystä.
- Varmista, että pieniä osia (esim. koruketjuja, pa-peripinteitä) tai nesteitä ei pääse tunkeutumaan laitteen sisäosaan (sähköisku, oikosulku).
- 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 kotelon kannen ollessa asennettuna (jäähdytys, palontorjunta, häiriönpöisto).
- Vain ammattihenkilökunta saa avata laitteen. Tästä syystä kehotamme teettämään kaikki korjaukset valtuutetuilla ammatti henkilöillä. Asian avaaminen ja asiantuntemattomat korjaukset voivat aiheuttaa käyttäjälle huomattavia vaaroja. Laitteiden luvaton avaaminen sulkee BinTec Communications AG:n pois takuusta ja vastuusta.
- Käytä vain mukana seuraavia kaapeleita. Mikäli käytetään muita kaapeleita, BinTec Communications AG ei vastaa tällöin syntyvistä vahingoista.
- Tärkeä vihje ammattihenkilökunnalle: Vedä verkkopistoke ennen järjestelmäyksikön avaamista.
- CE-merkki tarkoittaa, että „BRICK“ vastaa seuraavia EY-direktiivejä: EMV (89/336/EWG) ja pienjännite (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 :
 - 100 - 240 VAC
 - 60 / 50 Hz
 - maks. 0,2 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.
- 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. Une personne non autorisée ouvrant l'appareil se porte donc garante des conséquences. BinTec Communications AG n'en prend aucune responsabilité.
- N'utiliser que les câbles joints au matériel. En cas d'utilisation d'autres câbles, BinTec Communications ne se porte pas garant des incidents.
- Conseil important pour le personnel qualifié: Avant l'ouverture de l'appareil, débrancher la prise.
- 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 nettoyeurs alcalins ou autres produits tranchants ou gratants. 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 temperaturangemessen 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:
 - 100 - 240 VAC
 - 60 / 50 Hz
 - maks. 0,2 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.
- Achten Sie darauf, daß keine Gegenstände (z. B. Schmuckkettchen, 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. Unerlaubtes Öffnen der Geräte hat den Garantie- und Haftungsausschluß der BinTec Communications AG zur Folge.
- Verwenden Sie nur die beigelegten Kabel. Falls Sie andere Kabel verwenden, übernimmt BinTec Communications AG für auftretende Schäden keine Haftung.
- Wichtiger Hinweis für das Fachpersonal: Ziehen Sie vor dem öffnen der Systemeinheit den Netzwerkstecker.
- 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 εγκλιματισμού 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
50-60 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.
- Η συσκευή επιτρέπεται να λειτουργήσει μόνο με το γνήσιο φως δικτύου **BinTec Communications**.

- 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) απουσνδέστε 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. Γι' 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 άσφογοι και αβλαβείς. Αλλάξτε αμέσως έναν φθαρμένο αγωγό.
- Ηλεκτροστατικές φορτώσεις μπορεί να οδηγήσουν σε βλάβες της συσκευής. Γι' 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 tecnici-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:
 - 100 - 240 VAC
 - 60 / 50 Hz
 - maks. 0,2 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.
- 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. L'apertura non autorizzata dell'apparecchio ha come conseguenza l'esclusione della garanzia e della responsabilità della ditta BinTec Communications AG.
- 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 tilsvarer 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:
 - 100 - 240 VAC
 - 60 / 50 Hz
 - maks. 0,2 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 tilkoples 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 betjeningslement 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).
- 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. Uautorisert åpning har til følge at BinTec Communications AG fraskriver seg hvert garantiansvar.
- Bruk kun de vedpakkede kabler . Dersom de bruker andre kabler, fraskriver BinTec Communications AG seg ethvert ansvar hvis det oppstår skader.
- Viktig instruks til fagpersonale: Koble fra nettverkstøpslet før systemenheten åpnes.
- CE-tegnet betyr at „BRICK“ tilsvarer følgende direktiver fra EG: EMV (89/336/EWG) og lavspenning (73/23/EWG).
- Apparatet kan også tilkoples til „Euro-NUMER-IS“ (Frankrike), da det i tillegg til EG forskriftene også tilfredsstiller det franske ISDN.
- Elektrostatisk oppladninger kan føre til skade på apparatene. Ha derfor på deg en antistatisk masjett rundt händleddet 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 à tensão local da rede. A colocação do aparelho em funcionamento é possível nas seguintes condições:
 - 100 - 240 VAC
 - 60 / 50 Hz
 - maks. 0,2 A
- Ligue o aparelho apenas a uma tomada de contacto de segurança com ligação à 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. A abertura não permitida dos aparelhos conduz à exclusão da BinTec Communications AG da garantia e da assunção de responsabilidade.
- 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 systemuppbbyggnaden. 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:
 - 100 - 240 VAC
 - 60 / 50 Hz
 - maks. 0,2 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 dataöverföringskabler 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 vidmonterat maskinhölje (kylning, brandskydd, gni-stavstörning).
- 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. Vid otillåtet öppnande av maskinen träder BinTec Communications AG:s garanti- och ansvarsåtagande ur kraft.
- Använd endast bifogade kablar. Om andra kablar används, ansvarar BinTec Communications AG ej för uppkomna skador.
- Viktig upplysning till fackpersonal: Drag ut nätverkskontakten innan systemenheten öppnas.
- CE-beteckningen innebär att „BRICK“ motsvarar följande EU-riktlinjer: EMV (89/336/EWG) och lågspänning (73/23/EWG).
- Maskinen kan även anslutas till „Euro-NUMER-IS“ (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 våtrengöras. 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:
100 - 240 VAC
60 / 50 Hz
maks. 0,2 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. collares, 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.
- 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. Si el aparato es abierto por una persona no autorizada esto tiene por consecuencia la exclusión de la garantía y responsabilidad asumidas por BinTec Communications AG.
- 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 BIANCA/BRICK-XS has been approved for use within the European Community and Norway:

- BIANCA/BRICK-XS



BUNDESAMT FÜR ZULASSUNGEN IN DER TELEKOMMUNIKATION

Federal Approvals Office For Telecommunications Of The Federal Republic Of Germany



EG-BAUMUSTERPRÜFBESCHEINIGUNG
EC TYPE-EXAMINATION CERTIFICATE

Registriernummer : B127047H Anzahl der Anlagen: 1
Registration no.: Number of annexes:
Benannte Stelle : Bundesamt für Zulassungen in der Telekommunikation
Notified body:
Bescheinigungsinhaber: BinTec Communications GmbH
Certificate holder: Willstätter Str. 30
D-90449 Nürnberg

Produktbezeichnung : BIANCA/BRICK-XS
Designation of product:
Produktbeschreibung : This equipment is a Remote Access Router with an ISDN
Product description: basic rate interface.

ProduktHersteller : BinTec Communications GmbH
Product manufacturer: Willstätter Str. 30
D-90449 Nürnberg

EG-Vorschriften: Commission Decision of 18. November 1994 on a Common Technical
EC specifications: Regulation for the pan-European Integrated Services Digital
Network ISDN (94/797/EC)
Basic access

Prüfergebnis : Das geprüfte Baumuster erfüllt die Anforderungen der oben
Statement: genannten EG-Vorschriften.
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 91/263/EWG des Rates
This certificate is issued in accordance with the Council Directive 91/263/EEC

Saarbrücken, den 10.05.1996
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, Telestraße 34-42, D-66119 Saarbrücken, Tel.: +49 6 81 6 98-0, Fax: +49 6 81 6 98-10 00

BUNDESAMT FÜR ZULASSUNGEN IN DER TELEKOMMUNIKATION

Federal Approvals Office For Telecommunications Of The Federal Republic Of Germany



BAUMUSTERPRÜFBESCHEINIGUNG TYPE-EXAMINATION CERTIFICATE

Registriernummer : B127049H **Anzahl der Anlagen:** 1
Registration no.: Number of annexes:
Benannte Stelle : Bundesamt für Zulassungen in der Telekommunikation
Notified body:
Bescheinigungsinhaber: BinTec Communications GmbH
Certificate holder: Willstätter Str. 30
 D-90449 Nürnberg

Produktbezeichnung : BIANCA/BRICK-XS
Designation of product:
Produktbeschreibung : Die Einrichtung ist ein Remote Access Router mit einer
Product description: ISDN S0 Schnittstelle.

Produkthersteller : BinTec Communications GmbH
Product manufacturer: Willstätter Str. 30
 D-90449 Nürnberg

Deutsche Vorschriften: I-CTR 3, BAPT 223 ZV 25, BAPT 224 ZV 9
German Specifications:

Prüfergebnis : Das geprüfte Baumuster erfüllt die Anforderungen der oben
Statement: genannten Vorschriften.
 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 1996
This certificate is issued in accordance with the TKZulV 1996

Saarbrücken, den 10.05.1996
City, Date of issue:



gezeichnet: *Reiner Gugenburger*
Signed: Reiner Gugenburger
 (Verantwortlicher der benannten Stelle)
 (Manager of notified body)

Bundesamt für Zulassungen in der Telekommunikation, Talstraße 34-42, D-86119 Saarbrücken, Tel.: +49 6 81 6 98-0, Fax: +49 6 81 6 98-18 00

INDEX

Symbols

+50395 199

A

access

CAPI port 158

isdnlogin 157

SNMP port 159

trace port 158

X.25 158

access lists 76, 159

accounting 153

IP 39, 62

autoconfiguration 41, 123

B

Back Route Verify 62

Basic rate interface 10, 179, 206

biboAdmSyslogTable 175

biboPPPTTable 175, 176

BNC

Port 8

BNC port 207

BOOTmonitor 200

BOOTP 71, 143

bricktrace 169, 176, 178, 179, 192

Bridging 155, 176

Btx 187

bundelling 57

C

callback 56

CAPI 3, 33

port 158

Remote 3

capitrace 192

CLID 50

Compression

STAC 3, 48

CompuServe 132

CTS 208

D

date 188

DDI 44

debug 189

debugging 106

Denial-of-service attack 40, 62

DHCP Server 65, 84

Direct Dial In 44

DTR 208

E

Encapsulation 175, 176

for IPX packets 38

encapsulation

for IPX packets 38

Error messages 169

F

Facsimile support 187

G

Gateway 155

H

halt 191

HTML status page 161

HTTP port number 161

I

ifconfig 190

ifstat 185

intruders 158

IP 65

- accounting 39, 62, 153
- Back Route Verify 62

IP address

- address pool 83
- dynamic client 134
- server mode 135

IPX 90, 144

- network number 63

ipxping 182

ISDN

- accounting 153
- call answering 43
- switch type 41

ISDN monitor 107

isdnCallHistoryTable 168, 175, 176

isdnDispatchTable 176

isdnlogin 168, 175, 186

isdnlogind 186

isdnStkTable 176

L

leased line 125

licenses 33

M

message levels 35

messages 113

minipad 187

MODEM 95, 96

monitor

interfaces 111

ISDN 107

messages 113

TCP/IP 114

X.25 110

N

NAT 73, 137, 159

Negotiation

- DNS 61

- WINS 61

NetBIOS 91

netstat 186

P

p 189

passwords 35, 169

ping 181

Port

- BNC 8, 207

- Serial 170, 198, 199, 208

- Twisted pair 207

- UTP 9

port

- SNMP 86

PPP

- local PPP ID 34

Priority 189

Protocols

- IP 169, 176, 178

- TCP 169

R

RADIUS 160

- Accounting 87

- Multiple Servers 87

- Server 65, 66

Remote CAPI 3

Remote configuration 3

RIP/SAP 63, 159

Routing 176

routing 175

- IP 66

rtlookup 184

RTS 208

RVS-COM 3

S

- security 157
 - access lists 76
 - NAT 159
 - RIP 159
- Serial port 170, 198, 199, 208
- server
 - CAPI 71
 - DNS 70
 - timeserver 71
 - trace 71
 - WINS 70
- Setup Tool
 - List Navigation 26
 - Menu Navigation 25
- Short 126
- Short Hold
 - Dynamic 56, 126
 - Static 56
- SNMP port 86
- SNMP Shell
 - priority 189
- STAC compression 3, 48
- sysName 34
- system administration 104
- system messages 113

T

- t 189
- TCP/IP
 - dialup connection 129
 - statistics 114
- telnet 179, 181
- TFTP 105, 203
- Time Server 71
- trace 182
- traceroute 185
- Twisted pair port 207

U

- update 188
- Utilities
 - bricktrace 169, 176, 178, 179, 192
 - capitrace 192
 - date 188

- debug 189
- halt 191
- ifconfig 190
- ifstat 185
- ipxping 182
- isdnlogin 186
- minipad 187
- netstat 186
- p 189
- ping 181
- rtlookup 184
- t 189
- telnet 181
- trace 182
- traceroute 185
- update 188

UTP port 9

V

- Van Jacobson Header Compression 61

X

- X.25 monitor 110
- XMODEM 202
- XM-X21 47

