

V!CAS

User's Guide

Hardware and Installation

NOTE

The information in this manual is subject to change without notice.

This manual provides a description of the BinTec V!CASteleworking router. The instructions included in this manual are compatible with software version 4.6.

While every effort has been made to ensure the accuracy of all information in this document, BinTec Communications GmbH 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 and the BinTec logo are registered trademarks of BinTec Communications GmbH.

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

Warning

As a multi-protocol ISDN router this product is known to establish ISDN connections as needed depending upon the system's configuration. To avoid unwanted charges the user is advised to continually monitor the product to ensure it operates within the bounds of the user's expectations.

BinTec Communications is not responsible for incidental or consequential loss of data, incurrence of connection costs, or other damages resulting from the unsupervised use of the product.

All rights 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 an information retrieval systems, without the prior written permission of the copyright owner.

- am, lb

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 GmbH could void the authority to operate the equipment.

CE Notice

The  symbol means that the V!CAS 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 V!CAS also adheres to ISDN requirements in France and may be connected to Euro-Numeris.

GS

The GS (Geprüfte Sicherheit) symbol means that the V!CAS adheres to the standards defined by the German safety regulations.

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

V!CAS 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.

- 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.
- 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.
-

V!CAS

User's Guide
Version 1.2

Contents

1. Introduction

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

2. Installing the V!CAS

Connecting the V!CAS to the LAN	8
Connecting the V!CAS to the ISDN	10
Connecting analog devices to the V!CAS	10
Connecting the V!CAS to a PC or terminal	11
The BOOT sequence	11
Logging in for the first time	12

3. Working with the V!CAS

SNMP, MIBs, and V!CAS System Tables	16
Configuration Files, Flash, and the TFTP	18
Physical and Software Interfaces	19

Setup Tool vs. SNMP Shell 20

Using Setup Tool 21

 Menu Layout..... 21

 Menu Structure 22

 Special Menu Commands 23

 Menu Navigation 24

4. Setup Tool Menus

Setup Tool Main Menu 26

Basic System Configuration 28

Hardware Interfaces 32

 LAN Interface :

 WAN Interface :

Partner Management 40

Configuring Protocols 53

System Administration 87

5. How do I Configure ...

Hardware Interfaces 100

 How do I configure an ISDN interface in general? 100

 How do I configure a leased line connection? 102

 How do I configure an Ethernet interface? 103

IP Features 104

 How do I configure dialup TCP/IP access for an ISDN partner?.... 104

 How do I configure Dialup Access to
 CompuServe Online Services..... 106

 How do I configure the V!CAS to accept
 its IP address dynamically? 107

 How do I configure the V!CAS as a dynamic IP address server?.. 108

 How do I configure Internet access for my LAN using NAT?..... 109

 How do I configure access lists to protect my network? 111

 How do I configure the V!CAS as a RADIUS client? 113

 How do I configure the V!CAS as a BOOTP relay agent? 115

IPX Features 116

 How do I connect my local and remote
 IPX networks over ISDN? 116

X.25 Features	118
How do I configure an X.31 link (X.25 in the D-channel)?	119
How do I configure X.31 in the B-channel (Case A/Case B)?	121
How do I configure X.25 access for a host on my LAN?	123
How do I configure ISDN dialup access for an X.25 partner?	125
How do I route IP traffic over X.25 with MPX25?	126
How do I use the VICAS as a TCP-X.25 bridge?	128
POTS Features	131
How can I configure my POTS ports if I only have one MSN?	131
How can I configure my POTS ports using more than one MSN? ..	132
General	134
How can I retrieve accounting information (ISDN and TCP/IP)? ..	134
How do I use the VICAS as a Bridge to link two LANs over ISDN? ..	136
How can I improve security?	138
How can remote users access the VICAS' status page?	142

6. Troubleshooting

General Troubleshooting	147
Debugging Tools	147
debug	147
isdnlogin	148
bricktrace	148
System Errors	148
Software Problems	150
IPX Routing	150
ISDN Connections	152
POTS Connections	156

7. Command Reference

The SNMP shell commands	157
BRICKtools for UNIX Commands	163

8. Hardware/Firmware Configuration

Hardware	166
Front Panel Indicators	166
The Back Plane	167

The Power Socket..... 168
The Network Ports..... 168
Telephony Ports 168
Serial Port..... 168
The Main Board 168
Firmware 169
 Upgrading System Software 169
 BOOTmonitor 169
 Automatic booting over TFTP 172
General System Specifications 173

A. Technical Data

Pin Assignments 174
 ISDN S₀ interface 174
 POTS Port for analog equipment..... 175
 Serial Port..... 176
 Ethernet Ports..... 177

B. Index

1

INTRODUCTION

What's covered

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

How to contact BinTec Communications

Ways to contact BinTec	Telephone number or address
Telephone	+49 911 96 73 0
FAX	+49 911 688 07 25
Mail	BinTec Communications GmbH Willstätterstraße 30 D-90449 Nürnberg GERMANY
e-Mail	Sales: sales@BinTec.de Service: support@BinTec.de
WWW	http://www.BinTec.de

How to get the latest software and documentation

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

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

About your User Documentation

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

This document includes information for users that are familiar with networking and telecommunications and describes the V!CAS hardware and includes all the basic information you need to setup, configure, and administer your V!CAS.

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

Note:



Your V!CAS belongs to BinTec's successful family of BIANCA/BRICK ISDN routers.

Whenever the term "BRICK" is used throughout the user documentation, please be assured that these sections also apply to your V!CAS.

Features

“Now that I've got this new V!CAS—what can I do with it?”

Your V!CAS can serve a number of different purposes—most of them at the same time. These include (but are not limited to) the following:

- *Small PBX*—connect up to two analog devices, such as telephones, fax machines, or modems, to your V!CAS. This setup is especially useful in small office environments.

You can make internal calls between the two connected telephones free of charge, make two independent ISDN calls at the same time, use one ISDN B channel for a phone call while transferring data on the other, or even use both B channels for data transfer and still be able to accept incoming calls via the *Priority Voice Technology*.

- *Keypad Facilities*—when you dial additional digits during an established connection (Suffix Dialling / Nachwahl) from an analog telephone connected to a POTS port, these digits are not only sent as DTMF tones, but also as keypad data packets.

You can access special functions on some external PBXs by using Suffix Dialling (*Nachwahl*). Please refer to the manual of your PBX for a description of its special functions.

- *Remote TAPI server*—you can use computer telephony applications on your Windows 95 or Windows NT PC to dial for you, to open up database entries of customers depending on their telephone number, or as an intelligent answering machine.

For instructions on installing the Remote TAPI please refer to the *BRICKware for Windows* online documentation.

Please note that the Remote TAPI is available for both Windows 95 and Windows NT, but not for Windows 3.x.

- *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 for the power of CAPI applications.
- *Router*—use your V!CAS for routing IP or IPX packets received via ethernet from your PC to your company LAN over the ISDN, and vice versa.
- *Bridge*—use your V!CAS to connect two LANs.
- *Remote configuration*—configure your V!CAS from a remote site using the *isdnlogin* program (please refer to the *Getting Started* or *Los Geht's* manuals).
- *Priority Voice Technology*—incoming and outgoing voice calls take precedence over existing 2-B-channel data connections (e.g. Multi-LinkPPP).

This means that the data connection temporarily gives up one of its B channels for the duration of the voice call.

Note: Your ISDN access has to support the »Call waiting« feature (»Anklopfen« in Germany) for the incoming voice call to be signalled to your V!CAS.

Without this feature, the Priority Voice Technology only works for outgoing voice calls.

- *STAC compression*—V!CAS supports the STAC compression according to RFC 1974 and 1962 standards (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 V!CAS is also compatible with Cisco's proprietary STAC implementation which is automatically detected at connection time.

These are but a few instances. You will find many more in examples throughout this guide and the other manuals of your user documentation.

What's covered in this guide

Chapter 1 Introduction is this chapter.

Chapter 2 Installing the V!CAS describes physically installing the V!CAS on your LAN.

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

Chapter 4 Setup Tool Menus describes all the menus and variables you'll see when configuring the V!CAS' 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 V!CAS. 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 V!CAS.





Chapter 7 Command Reference describes the shell commands available from the V!CAS' SNMP shell.


Chapter 8 Hardware/Firmware Configuration describes the V!CAS hardware, and important tasks, such as upgrading the system software.

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

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 V!CAS feature.
	References to information in other sections or documents that may be helpful.
	Points out important information such as safety precautions and common pitfalls.

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	 represents a submenu or menu command found in Setup Tool.

2

INSTALLING THE V!CAS

What's covered

- Connecting the V!CAS to the LAN8
- Connecting the V!CAS to the ISDN10
- Connecting the V!CAS to a PC or terminal11
- The BOOT sequence11
- Logging in for the first time12

You may have already installed and setup your V!CAS 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 V!CAS on your LAN and attaching a serial console. Then we'll cover the brief BOOT sequence the V!CAS goes through when starting up, and describe the login procedures you should use when logging in for the first time.

Connecting the VICAS to the LAN

This section explains how to connect the VICAS to your LAN. You can connect your VICAS to an ethernet using either the 10Base2 or 10BaseT port on the back plane.

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

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.

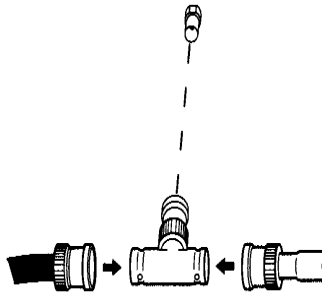



Figure 1: BNC Connector

-  1. Attach the BNC T-connector to the BNC port on the back plane 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 VICAS 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
10BaseT

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 V!CAS to your ethernet using the 10BaseT port.

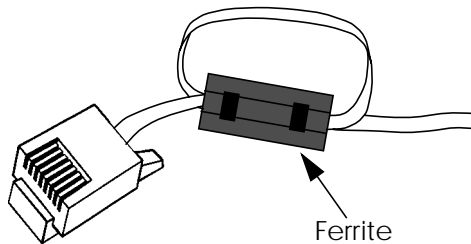


Figure 2: RJ-45 Western Plug with Ferrite



1. Attach a twisted pair cable to your V!CAS by inserting the 8 pin RJ-45 jack into the twisted pair port on the back plane marked 10BaseT.
2. Make a small loop into your twisted pair cable as close as possible to the V!CAS and attach a ferrite to it.

Note: You must use a ferrite with your twisted pair ethernet cable. Otherwise the V!CAS may produce a higher amount of electromagnetic radiation and therefore possibly cause interference with other devices.



3. Attach the other end of the twisted pair cable to an input port of your concentrator

Connecting the VICAS to the ISDN

The VICAS 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 VICAS.

Connecting analog devices to the VICAS

You can connect up to two analog devices, such as telephones, fax machines, or modems, to the POTS¹ ports A and B of your VICAS.

Note: Please note, however, that these devices must be configured to use tone dialling (*Mehrfrequenzwahl* in Germany), and *not* pulse selection (*Impulswahl* in Germany). Also make sure to use cables with the correct pinout (see Appendix A).



If you just connect VICAS to the ISDN and two analog telephones to ports A and B you can use the following functions without any further configuration.

- Free-of-charge internal calls between the two connected devices—the device at port A can be reached by dialling »*1«, the number for port B is »*2«. You can of course change these numbers if needed.
- You can call any external number by simply dialling it. If your VICAS is connected to the ISDN through an external PBX, you may have to dial a prefix code for external calls.

For instructions on how to configure the phone numbers for the POTS ports please refer to pages 84 ff.

1. »Plain old telephone service«

Note: Some PBXs and exchanges may, however, refuse to forward calls without an ISDN calling party number. In these cases you will have to further configure your V!CAS before you can make external calls.



Connecting the V!CAS to a PC or terminal

A PC or terminal can be connected directly to the V!CAS using the 9 pin serial port on the backplane marked serial console. Please use the included laplink 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 V!CAS can be set using the *BOOTmonitor* which is described in Chapter 8.

The BOOT sequence

Each time you power up the system, the V!CAS 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.

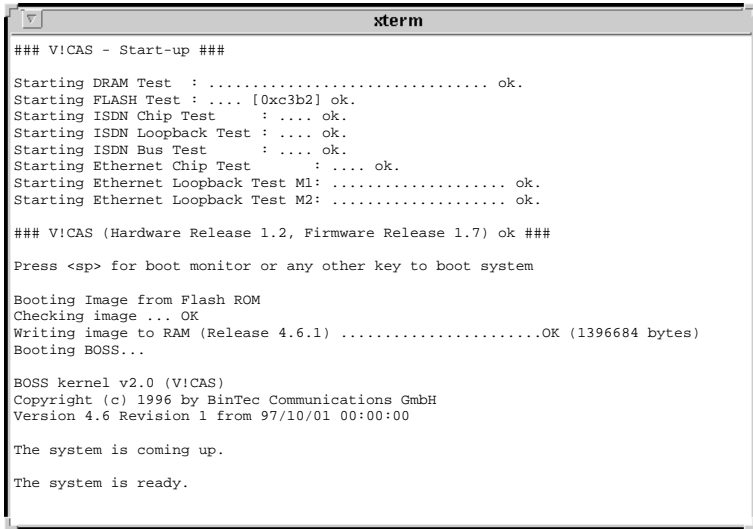
Power-up Mode
BOOTmonitor Mode
Normal Operation Mode

During Power-up Mode, the V!CAS 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 V!CAS waits 4 seconds for the user to press the spacebar which activates the BOOTmonitor. See BOOTmonitor, page 169, in Chapter 8 for information on using the BOOTmonitor.

Normal Operation Mode is entered once the V!CAS 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
### V!CAS - Start-up ###
Starting DRAM Test : ..... ok.
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.
Starting Ethernet Loopback Test M1: ..... ok.
Starting Ethernet Loopback Test M2: ..... ok.

### V!CAS (Hardware Release 1.2, Firmware Release 1.7) 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 4.6.1) .....OK (1396684 bytes)
Booting BOSS...

BOSS kernel v2.0 (V!CAS)
Copyright (c) 1996 by BinTec Communications GmbH
Version 4.6 Revision 1 from 97/10/01 00:00:00

The system is coming up.

The system is ready.
```

After the system comes up, the V!CAS starts various system daemons depending on which features are licensed on your V!CAS. 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 V!CAS for the first time;

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

Note that the V!CAS 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, please refer to Setup Tool’s **SYSTEM** menu on page 29.

3

WORKING WITH THE V!CAS

What's covered

- SNMP, MIBs, and V!CAS System Tables16
 - Configuration Files, Flash, and the TFTP18
 - Physical and Software Interfaces19
 - Setup Tool vs. SNMP Shell.....20
 - Using Setup Tool.....21
-

In the previous chapter we explained physically installing the V!CAS on your LAN. If you haven't already configured your V!CAS 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 V!CAS. First we'd like to explain a few basic concepts that make the V!CAS 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.

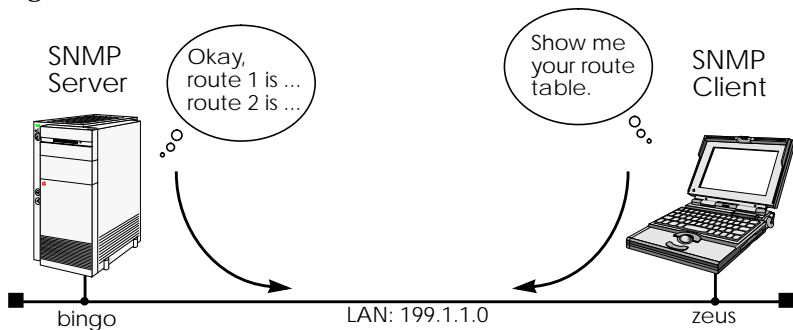
Then we'll cover using Setup Tool (i.e., menu structure, key commands, etc.) on the V!CAS. This section contains some important information including some of the finer points to using Setup Tool. You may decide to return to this section for future reference while using Setup Tool.

SNMP, MIBs, and VICAS System Tables

Remote access is one of the VICAS' most important features and means that as an administrator, you have just as much control of the VICAS from a telnet session as you do from an attached console. This section describes the underlying concepts such as SNMP, MIBs, and VICAS 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.

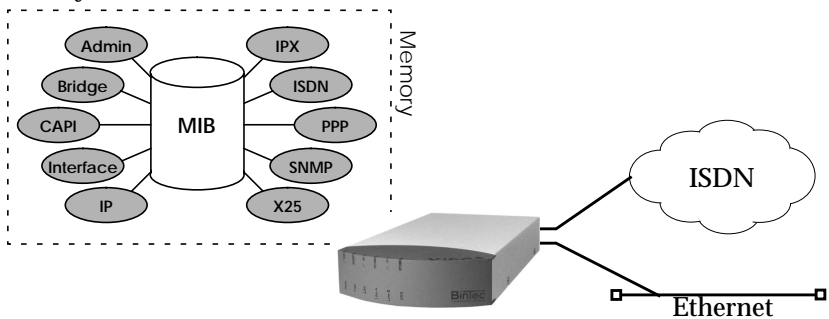


After booting, the VICAS starts a login shell. We sometimes refer to it as the SNMP shell because special commands can be entered from the shell which are given directly to the VICAS' SNMP server-process. This means that the VICAS' SNMP shell can be accessed from an SNMP client application, as well as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

Upon booting, the VICAS 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.



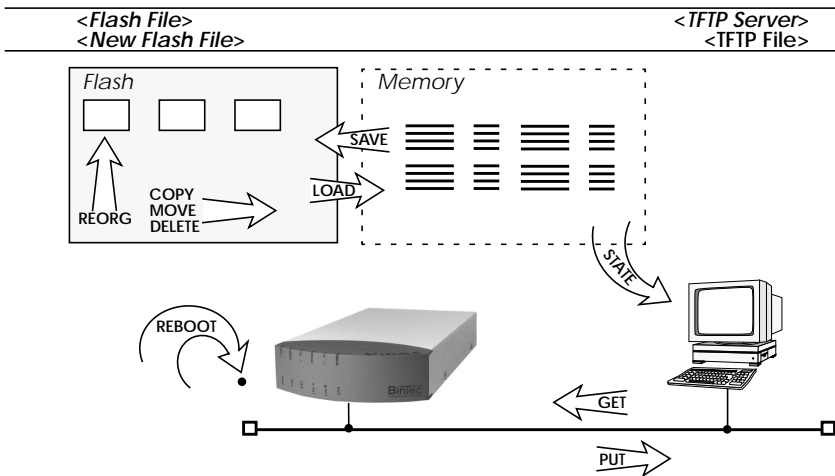
These variables can be changed by editing the system tables; the VICAS then updates the respective variables in memory instantly. As mentioned earlier, the VICAS can be managed from any of its ports.

Note:  As soon as a variable is changed in memory, the setting becomes effective immediately, the VICAS 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 VICAS 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 VICAS and remote hosts is made possible by the **TFTP**, or Trivial File Transfer Protocol. Using TFTP, it's also possible for the VICAS to retrieve its boot-image (or system software) from a TFTP host. See the section on the BOOTmonitor in Chapter 8.

Physical and Software Interfaces

One of the central concepts used on the V!CAS is the idea of interfaces. This section briefly explains the idea of interfaces used on the V!CAS.

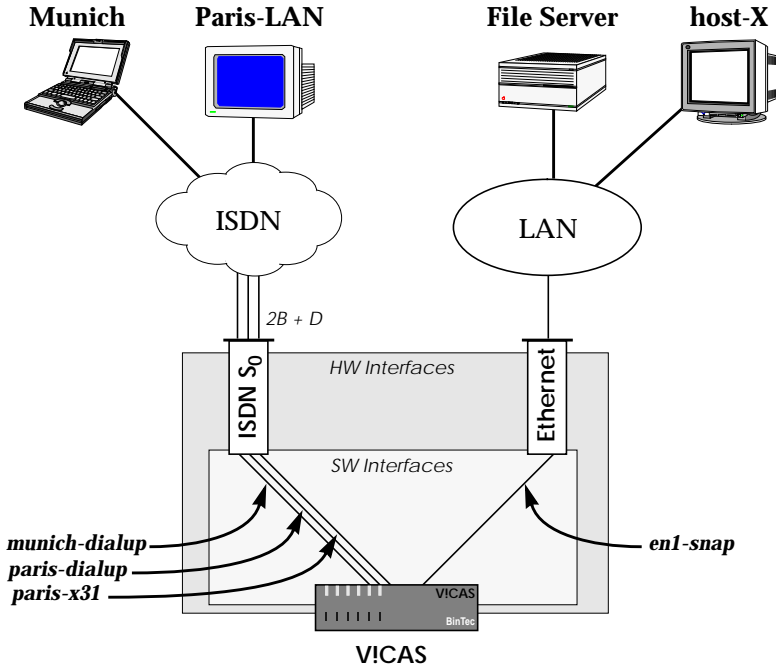
As a router the V!CAS was designed to link your local and remote networks (or hosts) using WAN links such as ISDN dialup, leased line, and X.25 connections. To establish connections to these sites, the V!CAS uses the Software Interfaces that you configure. By configuring a software interface, we simply mean that you create an interface by giving it a name and specify 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 V!CAS. Software interfaces are easily added or changed using the V!CAS' Setup Tool under the WAN Partners menu. You can create as many software interfaces as you need. When routing, the V!CAS maps software interfaces onto physical hardware interfaces.

Let's consider the example shown on the following page. The V!CAS 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 V!CAS' 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 dialup connections.



Setup Tool vs. SNMP Shell

As mentioned earlier, administering the V!CAS' features involves managing the various system variables (or tables of variables) defined in the V!CAS' 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 V!CAS' Setup Tool removes the complexity of administering the V!CAS 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 V!CAS and its features remotely from simple character based connections such as telnet, terminal emulation programs, isdnlogin, and minipad.

This document describes administering the V!CAS 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.

V!CAS' hostname:
Useful for sites with several BRICKS.

V!CAS Setup Tool BinTec Communications GmbH

[P][ROUTING]: IP Route Table vicas

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

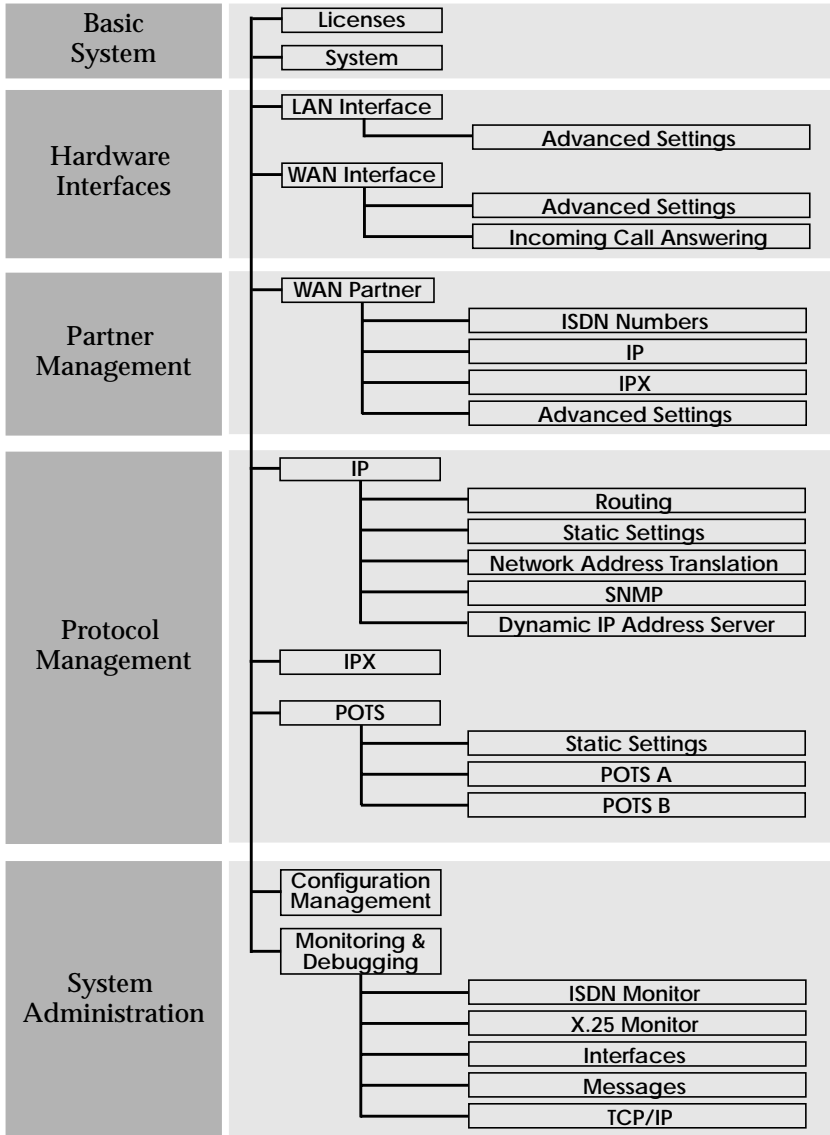
Destination	Gateway	Mask	Flags	Me	Inter/Partner	Pro
199.1.2.2	199.1.1.20	255.255.255.128	US	0	en1	loc
199.1.1.0	199.1.1.2	255.255.255.128	US	0	en1	loc

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



Special Menu Commands




















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



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

Menu Navigation

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

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

4

SETUP TOOL MENUS

What's covered

• Basic System Configuration.....	28
• Hardware Interfaces.....	32
• Partner Management.....	40
• Configuring Protocols.....	53
• System Administration.....	87

In the previous chapter we gave you a brief overview of working with the VICAS 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** .

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 V!CAS' 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 V!CAS.

V!CAS Setup Tool	BinTec Communications GmbH vicas
<div style="display: flex; justify-content: space-between;"> Licenses System </div> <p>LAN Interface: CM-BNC/TP, Ethernet</p> <p>WAN Interface: CM-1BRI, ISDN S0</p> <p>Feature Module: CM-POTS-MOD1-14</p> <p>WAN Partner</p> <p>IP IPX X.25 POTS MODEM</p> <p>Configuration Management</p> <p>Monitoring and Debugging</p> <p>Exit</p>	
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter	

- WAN Partner** Used for adding/deleting ISDN partners.
- IP** Based on the information you provided in the Licenses menu,
- IPX** this section lists the protocols that can be configured on your
- X.25** V!CAS. Initially, only the IP protocol is listed.

POTS Here you can edit the parameters necessary for the POTS ports.

CONFIGURATION MANAGEMENT

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

MONITORING AND DEBUGGING

These menus are useful in debugging problems on your network and allow you to monitor the V!CAS' ISDN and X.25 interfaces, TCP/IP traffic by interface or protocol, and syslog messages.

Basic System Configuration

LICENSES →

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

Available subsystems and possible statuses include:

Subsystem	BRIDGE	CAPI	TAPI	IP	IPX	OSPF	STAC	X25
Status	builtin		valid			not_valid		

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

VICAS Setup Tool [LICENSE]: Licenses	BinTec Communications GmbH vicas								
<p>Available Licenses:</p> <p>IP (builtin), TAPI (builtin), OSPF (valid), CAPI (valid), BRIDGE (valid), X25 (valid), IPX (valid), STAC (valid)</p> <table border="1"> <thead> <tr> <th>Serialnumber</th> <th>Mask</th> <th>Key</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>101546</td> <td>311</td> <td>88PNUPZ</td> <td>ok</td> </tr> </tbody> </table> <p>ADD DELETE EXIT</p>		Serialnumber	Mask	Key	State	101546	311	88PNUPZ	ok
Serialnumber	Mask	Key	State						
101546	311	88PNUPZ	ok						
<p>Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit</p>									

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 V!CAS' basic system settings. Some fields are required for the IP and PPP protocols, and others are optional variables that contain administrative information.

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

System Name = Defines the V!CAS' system name and is used by IP as the hostname. If the system name is not set, the V!CAS 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 V!CAS at connection time for IP partners configured for PAP or CHAP authentication.

Location = (optional) The physical location of your V!CAS.

Contact = (optional) Person responsible for this V!CAS. This text string must contain a valid email address if the system administrator is to be contacted from the V!CAS' 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.

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	✓ ²	—

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

Note: Since the admin user has complete access to the V!CAS' configuration information, the admin password should be protected.



RADIUS Password = Required for sites using RADIUS servers for user authentication.

HTTP Server Password = Required for viewing the HTTP status pages of your V!CAS. You should change this password from its default value *bintec*.

Syslog output on serial console = Specifies whether to display system messages to the console and may be useful when debugging.

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

Highest priority	debug	DebugEmergency
	emerg	Emergency Messages
	alert	Alert Messages
	crit	Critical Messages
	err	Error Messages
	warning	Warning Messages
	notice	Notice Messages
lowest priority	info	Info 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.

SYSTEM → **EXTERNAL SYSTEM LOGGING** →

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.

VICAS Setup Tool		BinTec Communications GmbH	
[SYSTEM][LOGGING]: External System Logging		vicas	
Log Host	Level	Facility	Type
ADD	DELETE	EXIT	

For each host the following parameters must be set.

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

Level = Defines the level of messages to send to this host. See “Message level for the syslog table” (p. 30) for info on message levels.

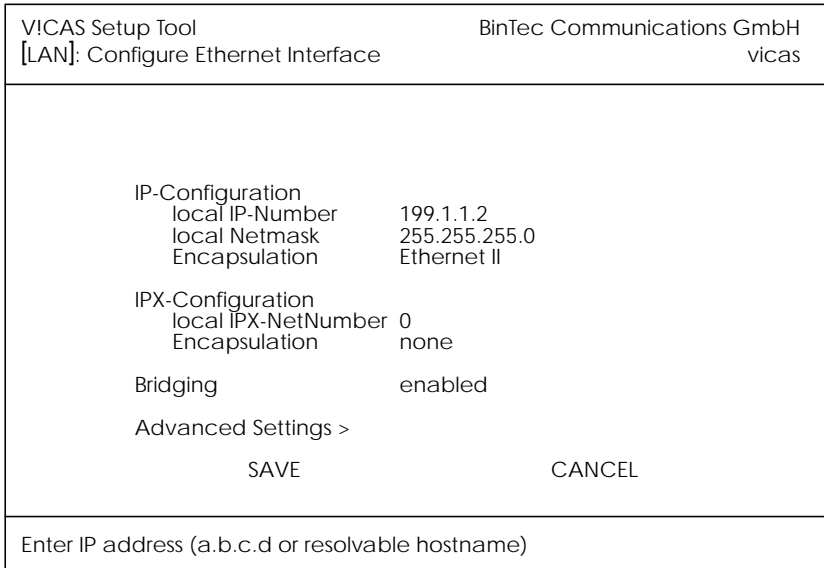
Facility = The facility on the log host, messages should be sent to. For UNIX hosts, this facility (level 0 – 7) must be configured appropriately. For PCs, you will need a separate application such as *DIME Syslog*.

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 ethernet interface of your V!CAS.



IP-Configuration

local IP-Number = The IP address of the LAN interface.

local Netmask = The netmask to use for this interface.

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

IPX-Configuration

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

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

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

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



V!CAS Setup Tool [LAN][ADVANCED]: Advanced Settings	BinTec Communications GmbH vicas				
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; text-align: center; vertical-align: top;"> RIP Send RIP Receive IP Accounting Proxy Arp </td> <td style="width: 50%; text-align: center; vertical-align: top;"> RIP V2 RIP V2 on off </td> </tr> <tr> <td style="text-align: center; padding-top: 20px;">SAVE</td> <td style="text-align: center; padding-top: 20px;">CANCEL</td> </tr> </table>		RIP Send RIP Receive IP Accounting Proxy Arp	RIP V2 RIP V2 on off	SAVE	CANCEL
RIP Send RIP Receive IP Accounting Proxy Arp	RIP V2 RIP V2 on 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 V!CAS also sends the netmask of propagated IP addresses. This allows the V!CAS 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



Proxy Arp = Turns proxy ARP for this interface to on or off. When turned on, the V!CAS answers all ARP requests received on this interface, with its own hardware address.

WAN Interface : CM-1BRI, ISDN S0 →

This menu contains settings for the ISDN interface.

VICAS Setup Tool [WAN]: WAN Interface	BinTec Communications GmbH vicas
<p>Result of autoconfiguration: Euro ISDN, point to multipoint</p> <p>ISDN Switch Type autodetect on bootup</p> <p>D-Channel dialup B-Channel 1 dialup B-Channel 2 dialup</p> <p>Incoming Call Answering > Advanced Settings></p> <p style="text-align: center;">SAVE CANCEL</p>	
Use <Space> to select	

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

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

The following protocols are supported for dialup and leased lines.

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

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 37.

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 V!CAS 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.

VICAS Setup Tool		BinTec Communications GmbH
[WAN][INCOMING]: Incoming Call Answering		vicas
Item	Number	Mode
ADD	DELETE	EXIT

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

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

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

Number = the telephone number to use for this item.

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

1. Called »Anlagenanschluß« in Germany

CM-1BRI, ISDN S0

ADVANCED SETTINGS

VICAS Setup Tool		BinTec Communications GmbH	
[WANI][Advanced]: Advanced Settings		vicas	
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).

VICAS Setup Tool		BinTec Communications GmbH	
[WAN]: WAN Partners		vicas	
Current WAN Partner Configuration			
Partnername	Protocol	State	
partnerbrick	ppp	dormant	
ADD	DELETE	EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit			

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

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

Select **DELETE** to remove a partner configuration 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.

VICAS Setup Tool		BinTec Communications GmbH	
[WAN][ADD]: Configure WAN Partner		vicas	
Partner Name		<X> IP	<> IPX <> BRIDGE <> X.25
Enabled Protocols		PPP	
Encapsulation		no	
Identify by Calling Number		CHAP and PAP	
PPP Authentication Protocol			
Partner PPP ID			
Local PPP ID		vicas	
PPP Password			
ISDN Numbers >			
IP >			
IPX >			
Advanced Settings >			
SAVE		CANCEL	
Enter string, max length = 25 chars			

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

Enabled Protocols = Depending on the type of traffic you will be routing with this partner, select the protocols the link to this partner will support.

Encapsulation = Defines the type of encapsulation to use over this link. Depending on which protocols you enabled for this partner, the available encapsulation methods will vary.

Also note that encapsulations using STAC compression are only available if STAC is licensed on your VICAS.

See the table below for encapsulation characteristics.

WAN Partner Link Encapsulation

Compression	Encapsulation	Protocol			
		IP	IPX	Bridge	X.25
—	PPP	IP	IPX	Bridge	
STAC	PPP + Compression				
—	Async PPP over X.75				
—	Async PPP over X.75/T.70/BTX				
—	Multi-Protocol LAPB Framing				
V.42 bis	Multi-Protocol LAPB Framing + Compression				
—	Multi-Protocol HDLC Framing				
—	HDLC Framing (only IP)				
—	LAPB Framing (only IP)				
V.42 bis	LAPB Framing (only IP) + Compression				
—	X.25_PPP	X.25			
STAC	X.25:PPP + Compression				
—	X.25				
—	X31 B-Channel				
—	X.25 No Signalling				

Identify by Calling Number = This determines whether this partner should be identified using the Calling Party’s Number in ISDN. Note, if turned off, the partner must be identified using either PAP or CHAP authentication protocols.

The following three settings only apply if PPP (or X.25_PPP) encapsulation is being used.

PPP Authentication Protocol = Specifies how this partner is authenticated at connection time. If calling line identification is not used, at least one authentication mechanism must be used.

Partner PPP ID = The PPP ID this caller must use at connection time.

Local PPP ID = The PPP ID your V!CAS should use for this partner. The Local PPP ID from the **SYSTEM** menu is displayed as a default setting.

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

ISDN Ports to use = This field defines which ISDN interfaces can be used to open connections with this partner. The list only displays the ISDN D-channel stacks that are currently available.



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

VICAS Setup Tool		BinTec Communications GmbH
[WAN][ADD][ISDN NUMBERS]: ISDN Numbers ()		vicas
ISDN Numbers for this partner:		
ISDN Number	Direction	
ADD	DELETE	EXIT

Select **ADD** to add a new ISDN number. In the subsequent dialogue, enter an ISDN telephone number this partner can be reached at.

Instead of just entering a single telephone number in the ISDN Number field, you can also use wildcards to make entries for groups of numbers. The table below lists the currently supported wildcards.

ISDN Number Wildcard Matching

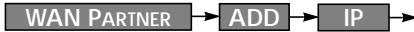
*	Match zero or more digits. 45* matches any number beginning with 45, i.e., 45, 4512, 4512345, 459, etc.
?	Match any single digit. 5? matches 50 through 59.
[]	Brackets denote a set of possible digits to match. A hyphen may be used for inclusive ranges. 21[45] only matches 214 or 215 (4 or 5) 21[6-8] matches 216, 217, 218 (6 through 8, inclusive) 21[^9] matches 210 through 218. (not 9)
{ }	Curly braces denote an optional string to match. {0911}2145 matches 09112145 and 2145 (optional)

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

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

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

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



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

V!CAS Setup Tool [WAN][ADD][IP]: IP Configuration ()	BinTec Communications GmbH vicas						
<table style="width: 100%; border: none;"> <tr> <td style="width: 60%;">IP Transit Network</td> <td style="width: 40%;">no</td> </tr> <tr> <td>Partner’s LAN IP Address</td> <td></td> </tr> <tr> <td>Partner’s LAN Netmask</td> <td></td> </tr> </table>		IP Transit Network	no	Partner’s LAN IP Address		Partner’s LAN Netmask	
IP Transit Network	no						
Partner’s LAN IP Address							
Partner’s LAN Netmask							
SAVE	CANCEL						
Use <Space> to select							

Transit Network = Specifies whether to use a transit network between the V!CAS 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.

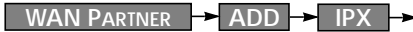
Assign “dynamic” if the V!CAS receives its IP address and the IP addresses for the primary and secondary domain name server from this partner at connection time.

local ISDN IP Address = The V!CAS’ IP address on the transit network.

Partner’s ISDN IP Address = The partner’s IP address on the transit network.

Partner’s LAN IP Address = The partner’s IP on the remote LAN.

Partner’s LAN Netmask = The netmask to use for the remote LAN. Only required for LANs using non-standard netmasks. If left blank, a standard netmask for the respective network class will be used.



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

VICAS Setup Tool		BinTec Communications GmbH	
[WAN][ADD][IPX]: IPX Configuration ()		vicas	
IPX NetNumber	0		
Send RIP/SAP Updates triggered + piggyback(on changes, per. if link active)			
Update Time	60		
Age Multiplier	4		
OK		CANCEL	
Enter integer value			

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

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

In IPX networks, RIP and SAP packets are broadcast to adjacent networks to inform them of current routes and services. The traffic generated by RIP and SAP is okay for LANs but for adjacent networks connected over WAN interfaces, consideration must be made.

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

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

Update Time = Determines how often periodic updates are sent.

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

Routes and services not updated within

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



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

VICAS Setup Tool		BinTec Communications GmbH
[WAN][ADD][ADVANCED]: Advanced Partner Settings ()		vicas
Callback		no
Static Short Hold		20
Delay after Connection Failure		300
Channel-Bundeling		dynamic
Total Number of Channels		2
RIP Send		RIP V1
RIP Receive		RIP V1 + V2
Van Jacobson Header Compression		off
IP Accounting		off
Dynamic IP-Address Server		off
Layer 1 Protocol		ISDN 64 kbps
Provider Configuration >		
	OK	CANCEL
Use <Space> to select		

Callback = If callback is “expected” the VICAS calls this partner, hangs up, and waits for the partner to call back. “yes” means: if this partner requests a connection (by calling the VICAS), terminate the call and initiate a new connection to this partner.

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.



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

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

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

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

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

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

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.

RIP Send = Which types of RIP packets to send to this partner. If RIPv2 packets are sent, the V!CAS also sends the netmask of the propagated IP address, which allows the V!CAS 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 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.

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  →  menu for information on the format of accounting messages.

Dynamic IP-Address Server = Set to “on” if you want the V!CAS to assign this partner a fresh IP address at connection time. The next free IP address is taken from the pool of addresses defined under **IP** → **DYNAMIC IP ADDRESSES**. This partner can also—on request—get its domain name server addresses from the V!CAS.

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 **INCOMING CALL ANSWERING** menu explained on page 37.

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	<u>d</u> ata <u>t</u> ransmission <u>o</u> ver <u>v</u> oice <u>b</u> earer; useful e.g. in the US where voice calls sometimes cost less than data connections
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



You can use this menu to configure dialup IP connections to CompuServe Online Services. The menu contains user access information (host machine, member ID, and password) which is used to generate *biboPPPLog-inString* used at connection time.

VICAS Setup Tool	BinTec Communications GmbH								
[WAN][EDIT][ADVANCED][PROVIDER]: Provider Configuration(cis)	vicas								
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">Provider</td> <td style="width: 50%;">Compuserve Network</td> </tr> <tr> <td>Host</td> <td>CIS</td> </tr> <tr> <td>User ID</td> <td>12345,6789</td> </tr> <tr> <td>Password</td> <td>secret</td> </tr> </table>	Provider	Compuserve Network	Host	CIS	User ID	12345,6789	Password	secret	
Provider	Compuserve Network								
Host	CIS								
User ID	12345,6789								
Password	secret								
OK	CANCEL								
Use <Space> to select									

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

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

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

Host = The CompuServe hostname to dial into.

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

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

Configuring Protocols



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.

VICAS Setup Tool [IP]: IP Configuration	BinTec Communications GmbH vicas
Routing Static Settings Network Address Translation Access Lists Dynamic IP Addresses (Server Mode) DHCP Server SNMP OSPF EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter	

ROUTING contains the IP routing table of your VICAS.

STATIC SETTINGS contains some required parameters such as the VICAS' 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 VICAS uses when operating as an IP address server.

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

SNMP contains basic settings required for the SNMP.

OSPF contains settings required for the OSPF routing protocol.



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:

V!CAS Setup Tool		BinTec Communications GmbH				
[IP][ROUTING]: IP Routing		vicas				
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 loc
199.1.1.0	199.1.1.2	255.255.255.0	US	0	en1	
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.



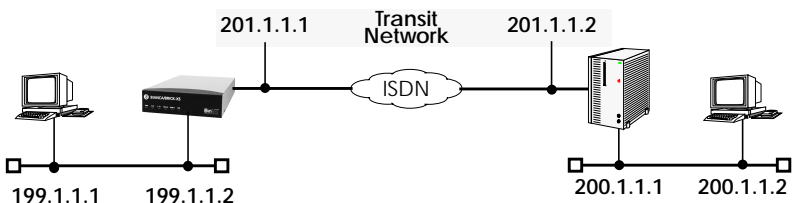
Use this menu to add (or make changes) to the IP routing table.

VICAS Setup Tool		BinTec Communications GmbH
[IP][ROUTING][ADD]: Add or Change IP Route		vicas
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 VICAS. For routes that use WAN interfaces, specify whether the route includes transfer network. If "discard" is used the VICAS 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 V!CAS 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.



This **Static Settings** menu contains some of the basic settings for your V!CAS.

VICAS Setup Tool [IP][STATIC]: IP Static Settings	BinTec Communications GmbH vicas
Domain Name Primary Domain Name Server Secondary Domain Name Server Time Protocol Time Offset (seconds) Time Update Interval (seconds) Time Server Remote CAPI Server TCP port Remote TRACE Server TCP port RIP UDP port BOOTP Relay Server Unique Source IP Address RADIUS Server HTTP TCP port	bricks.com 199.1.1.99 TIME/UDP 0 86400 199.1.1.99 6000 7000 520 80
SAVE	CANCEL
Enter string, max length = 35 chars	

Domain Name = Sets the V!CAS' IP domain name.

Primary Domain Name Server = The IP address of the V!CAS' domain name server.

Secondary Domain Name Server = An alternate name server.

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

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

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

Time Update Interval (seconds) = The interval in seconds at which current time should be updated/retrieved. Similar to Time Offset values between 1 and 24 are assumed to be hours and converted to seconds. For Protocol=time_udp, time_tcp, or time_snmp 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 V!CAS' timeserver.

Remote CAPI Server TCP port = The port number to use for CAPI connections. Default value: 6000

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

RIP UDP port = The port number used on the V!CAS 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 V!CAS 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 V!CAS' IP address. When routing to partners over a transit network, the V!CAS 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 to use instead.

RADIUS Server = The RADIUS server's IP address.

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

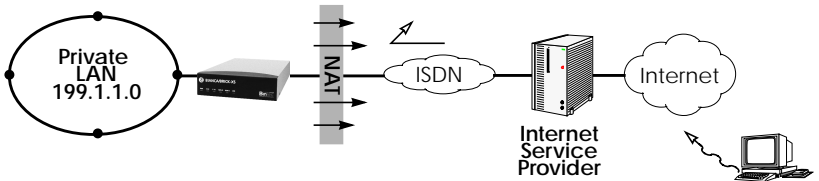
IP → **Network Address Translation** →

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

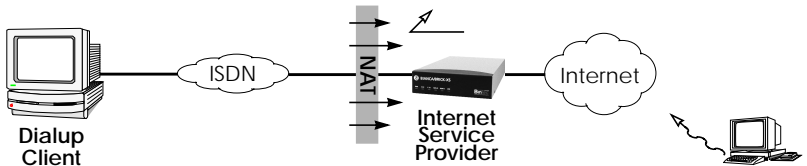
VICAS Setup Tool [IP][NAT]: NAT Configuration	BinTec Communications GmbH vicas
Select IP Interface to be configured for NAT en1 en1-snap partnerbrick EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select	

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

Forward NAT means, allow all traffic destined (moving-forward) for 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 session are allowed over this NAT interface. From this menu you can add, change, or delete session profiles.

VICAS Setup Tool		BinTec Communications GmbH	
[IP][NAT][CONFIG]: NAT Configuration (en1)		vicas	
<p>Network Address Translation off</p> <p>Configuration for sessions requested from outside</p> <p>Service Destination Source Dep. Dest. Dep. Port Remap</p>			
<p>ADD DELETE SAVE CANCEL</p>			
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.

VICAS Setup Tool		BinTec Communications GmbH	
[IP][NAT][CONFIG][ADD]: Edit NAT Configuration (en1)		vicas	
Service		user defined	
Protocol		icmp	
Port (-1 for any)		-1	
Destination			
SAVE		CANCEL	
Use <Space> to select			

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

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

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

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

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

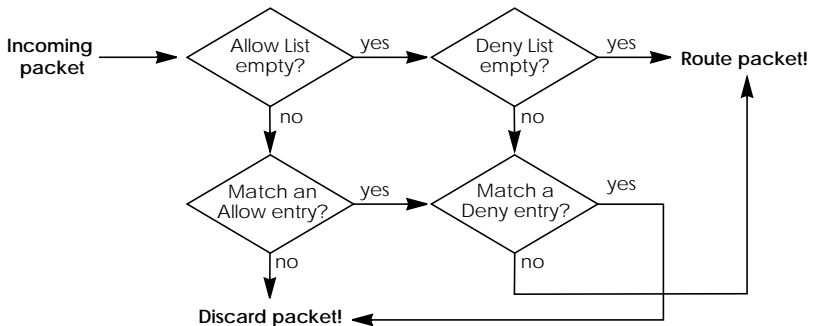
Select **CANCEL** to abort the entries made so far and return to the previous menu.



This menu displays the IP Access Lists. The V!CAS has an Allow list and a Deny list based on the mode of the entries configured here. Each entry specifies an interface to monitor incoming traffic on and defines a set of IP packets.

V!CAS Setup Tool		BinTec Communications GmbH				
[IP][ACCESS]: IP Access Lists		vicas				
M (Mode) values are: a (Allow), d (Deny)						
Access Lists configured:						
M	Prt	Int./Partner	Src Address	Src Port	Dst Address	Dst Port
a	tcp	dialup1	any	any	any	any
d	tcp	dialup1	any	any	any	21
d	tcp	dialup1	210.1.2.3/24	any	any	23
d	tcp	dialup1	any	25-103	any	clients
ADD		DELETE		EXIT		

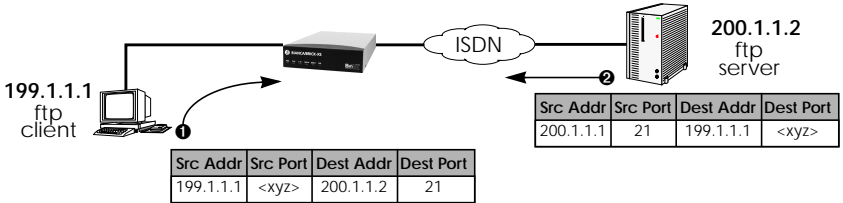
IP packets are tested to see if they match deny/allow entries. The decision whether to route the packet is based on the following algorithm



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.



Use this menu to create an Allow or Deny access entry. Depending on the Mode set for the entry, the packet will be routed or dropped.

VICAS Setup Tool		BinTec Communications GmbH	
[IP][ACCESS][ADD]: Add or Change Access List Entry		vicas	
Mode	deny		
Protocol	any		
Source Interface/Partner	dialup1		
Source Address			
Source Mask			
Source Port	specify range		
Specify Port	5	to Port	100
Destination Address			
Destination Mask			
Destination Port	specify		
Specify Port	23		
	SAVE		CANCEL
Use <Space> to select			

Mode = Allow or deny the following packets to be routed.

Protocol = Set the protocol to match, or “any” to match all protocols.

Source Interface/Partner = Select the interface (or partner) to monitor incoming IP frames on. Set to “any” to monitor all interfaces.

Source Address = (optional) Set the IP address to match frames from.

Source Mask = (optional) Apply an optional mask.

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

Source Port Ranges

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

Destination Address = (optional) The IP address of the destination host to match.

Destination Mask = (optional) Apply an optional mask.

Destination Port = A range of ports to apply (see Source Port, above).

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

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



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

VICAS Setup Tool		BinTec Communications GmbH
[IP][DYNAMIC]: Dynamic IP Addresses (Server)		vicas
IP Address	Number of consecutive addresses	
ADD	DELETE	EXIT

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 there are two required fields.

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 V!CAS 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.

V!CAS Setup Tool		BinTec Communications GmbH	
[IP][DHCP]: DHCP Server		vicas	
Interface	IPAddress	Number	Lease Time (Minutes)
en1	199.1.1.70	15	30
en1	199.1.1.85	5	120
tr6-snap	200.1.2.50	4	120
ADD	DELETE	EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select			

The V!CAS 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 V!CAS interface with a set of IP addresses. The V!CAS will assign an available IP address from the appropriate

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

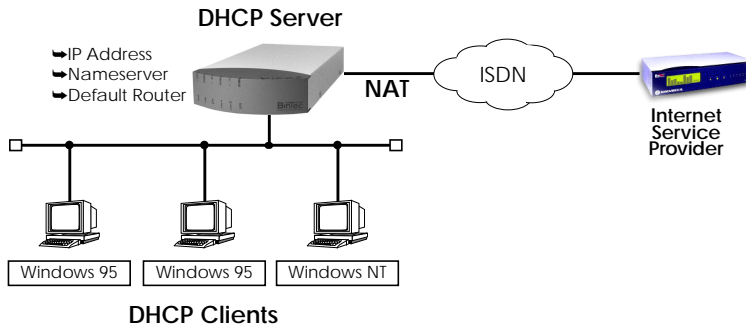
IP Address = Defines the first IP address in the set.

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

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

Internet Access for the LAN using DHCP and NAT

DHCP can be used in combination with NAT (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 V!CAS (only one official IP Address is required).
2. Configure V!CAS as DHCP Server.



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

V!CAS Setup Tool	BinTec Communications GmbH
[IP][SNMP]: SNMP Configuration	vicas
SNMP listen UDP port	161
SNMP trap UDP port	162
SNMP trap broadcasting	off
SNMP trap community	snmp-Trap
SAVE	CANCEL
Enter integer range 0..65535	

SNMP listen UDP port = Defines the UDP port the V!CAS uses for receiving SNMP requests.

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

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

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

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

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

IPX →

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

VICAS Setup Tool [IPX]: IPX Configuration	BinTec Communications GmbH vicas
Local System Name	BRICK
Internal Network Number	f9000e91
enable IPX spoofing	yes
enable SPX spoofing	yes
NetBIOS Broadcast replication	yes
SAVE	CANCEL
Enter string, max length = 35 chars	

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

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

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

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

NetBIOS Broadcast replication = Defines how NetBIOS packets are used.

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

“on LAN only” only NetBIOS hosts attached to the V!CAS 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.

X.25 →

The X.25 menu contains several submenus used to configure the X.25 protocol on the V!CAS.

V!CAS Setup Tool [X.25]: X.25 Configuration	BinTec Communications GmbH vicas
Static Settings Link Configuration Routing Multiprotocol over X.25 EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter	

STATIC SETTINGS contains the V!CAS' X.25 address.

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

ROUTING contains the V!CAS' 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.

X.25 → STATIC SETTINGS →

The X.25 Static Settings menu contains the local X.25 address.

V!CAS Setup Tool	BinTec Communications GmbH
[X.25][STATIC]: X.25 Static Settings	vicas
Local X.25 Address	
SAVE	CANCEL
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter	

Local X.25 Address = The official X.25 address of your V!CAS. Setting this variable is only required if the V!CAS is not directly connected to an official X.25 data network. When connected directly, the V!CAS ascertains its X.25 address automatically.

The X.25 address must be set here for sites implementing private X.25 networks, or when X.25 in the B-channel is used.

X.25 → **LINK CONFIGURATION** →

This menu displays a list of all interfaces that support the X.25 protocol. The number of available interfaces listed here is a combination of hardware (which modules are installed) and software interfaces (configured WAN partners).

- **Dialup interfaces** Entries for each X.25-compatible WAN partner configured on the system.
- **X.31 interfaces** If you're receiving X.31 services from your ISDN provider an X.31 link is also present. X.31 links have the format:
x31d-<slot number>-<unit number>-<TEI>

VICAS Setup Tool	BinTec Communications GmbH
[X.25][LINK]: X.25 Link Configuration	vicas
<p>Select link to configure</p> <p>x13 en1-llc (create new configuration)</p> <p>DELETE CONFIGURATION EXIT</p>	
<p>Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit</p>	

Before an X.25-compatible interface can be used, its link characteristics must first be set.

To edit an X.25 link highlight the entry and then enter <Return>.

To remove an X.25 link, tag the entry for deletion (spacebar) and select

DELETE CONFIGURATION .



This menu is used to configure the basic characteristics of the X.25 link.

VICAS Setup Tool		BinTec Communications GmbH	
[X.25][LINK][EDIT]: Change X.25 Link Configuration		vicas	
Link		en1-llc	
L3 Mode		dte	
L3 Window Size		128 bytes	
L3 Packet Size		2	
Lowest Two-Way-Channel (LTC)	1		
Highest Two-Way-Channel (HTC)	2		
Partner MAC Address (LLC)			
Layer 2 Behaviour		disconnect after timeout	
Disconnect Timeout		1000	
SAVE		CANCEL	
Use <Space> to select			

Link = This is the name of the link your are editing and cannot be changed here.

L3Mode = This defines the mode the VICAS operates in at Layer 3 of the X.25 protocol stack. Set to DCE if the VICAS must provide clocking information or DTE if provided by the remote side of link.

Lowest Two-Way-Channel (LTC) = LTC and HTC must be set to reflect the number of Virtual Channel(s) you have arranged for from your X.25 network provider.

Highest Two-Way-Channel (HTC) = Defines the highest number that can be assigned to a Virtual Channel.

Partner MAC Address (LLC) = Used when configuring a link for a partner on the LAN and specifies the host's MAC or hardware address.

Layer 2 Behaviour = Defines whether (and if so, when) the link should be disconnected when no virtual channels are active.

Disconnect Timeout = Time in seconds to wait before closing the link once the line becomes inactive.

X.25 → **ROUTING** →

This menu displays the X.25 routing table. X.25 routes are used for routing traffic over X.25 interfaces. Routes can be added, removed, or changed here.

VICAS Setup Tool		BinTec Communications GmbH	
[X.25][ROUTING]: X.25 Route Table		vicas	
Source Link	Dest. Link	Dest. Link Addr.	Dest. X.25 Addr.
ADD	DELETE	EXIT	

Note that the order of routes listed here have precedence. When the VICAS routes X.25 packets, the first matching route is always used.

To edit an X.25 route, highlight the entry and then enter <Return>.

Select **ADD** to create a new X.25 route.

Select **DELETE** to remove an X.25 route entry that has been tagged (using the spacebar) for deletion.

Select **EXIT** to accept the list of X.25 routes and return to the previous menu.



X.25 routes configured with Setup Tool are based on two factors.

- Source link Link X.25 call_packet first arrived on.
- Dest. X.25 Address The address the packet is addressed to.

You must define the destination link where the X.25 packets will be routed by specifying these two parameters. Standard wildcard characters can also be used in the Destination Address parameter.

{123}45	Either 12345 or 45	[68]*	Any # starting with 6 or 8
[^5]*	Any # not starting with 5	624*	All #s starting with 624

The order of routes is also important. An incoming call may match more than one route. The first matching route is always used.

Also note that there are different X.25 addressing standards, and depending on where the X.25 partner is calling from, the actual X.25 address received by the VICAS may differ.


VICAS Setup Tool		BinTec Communications GmbH	
[X.25][ROUTING][EDIT]: Add or Change X.25 Routes		vicas	
Source Link	any		
Destination Link	local		
Destination X.25 Address	45*		
SAVE		CANCEL	
Use <Space> to select			

SAVE immediately saves route to memory and returns to the previous menu.

CANCEL discards entries made here and returns to previous menu.

X.25 → MULTIPROTOCOL OVER X.25 →

This menu lists the Multiprotocol Routing over X.25, or MPX25, interfaces configured on the system. MPX25 allows the V!CAS to route IP, IPX, and Bridge, traffic over X.25 links. Each MPX25 interface defines an X.25 link to route one or more protocols over.

Note:  The underlying X.25 subsystem must first be configured before any MPX25 interface can be configured here. See the menus:

X.25 → STATIC SETTINGS →
 X.25 → LINK CONFIGURATION →
 X.25 → ROUTING →

VICAS Setup Tool		BinTec Communications GmbH	
[X.25][MPR]: Multiprotocol over X.25		vicas	
Interface Name	Destination X.25 Address	Encapsulation	
ADD	DELETE	EXIT	

Select **ADD** to create a new MPX25 link.

Select **DELETE** to remove an MPX25 link tagged for deletion.

Select **EXIT** to accept the list of MPX25 links and return to the previous menu.



Use this menu to add or change MPX25 interfaces.

VICAS Setup Tool		BinTec Communications GmbH
[X.25][MPR][ADD]: Add or change X.25 MPR		vicas
Partner Name Enabled Protocols Encapsulation X.25 Destination Address	mpxpartner1 <X> IP <> IPX <> BRIDGE ip_rfc877 49911555	
IP > IPX > Advanced Settings >		
SAVE		CANCEL
Enter string, max length = 25 chars		

Partner Name = Enter a unique name to identify this MPX25 partner.

Enabled Protocols = “X” selects the protocols that can be routed (received/transmitted) with this partner.

Encapsulation = Depending on which protocol(s) are enabled for this partner, select the type of encapsulation to use. Note that the remote MPX25 partner must be configured to use the same encapsulation.

Encapsulation	Protocol		
ip_rfc877	IP		
ip			
mpr	IPX	Bridge	
ipx			

X.25 Destination Address =The X.25 address for this partner. There must be an appropriate X.25 route for this address in the X.25 routing

table. The special "{" and "}" characters can be used to define an optional string of digits to use when matching incoming X.25 calls. For outgoing calls to this partner, the digits between these characters are used. {00}4991155 matches both 004991155 and 4991155 for incoming calls, outgoing calls are placed using 004991155.



This is where you configure the IP settings for this remote MPX25 partner and is only available if the IP protocol has been enabled.

Note: The settings used in this menu are the same as those used in the WAN PARTNER -> ADD -> IP menu described on page 46 but only apply to this MPX25 partner.



This is where you configure the IPX settings for the remote MPX25 partner. This menu is only available if IPX has been enabled.

Note: The settings used in this menu are the same as those used in the WAN PARTNER -> ADD -> IPX menu described on page 47 but only apply to this MPX25 partner.



This menu can be used to configure several advanced features, such as RIP support, IP Accounting, and the Short Hold mechanism.

Note: The settings used in this menu are a subset of those used in the WAN PARTNER -> ADD -> ADVANCED SETTINGS menu described on page 49 but only apply to this MPX25 partner.

POTS →

This menu contains three submenus. Use these submenus to configure phone numbers etc. for the two POTS ports of your V!CAS.

V!CAS Setup Tool	BinTec Communications GmbH
[POTS]: POTS Configuration	vicas
Static Settings POTS A POTS B EXIT	
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter	

STATIC SETTINGS contains the TAPI server port.

POTS A and **POTS B** are used to configure the type of device connected to the POTS ports as well as the ports' internal and external numbers.

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

POTS

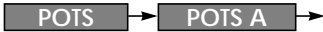


STATIC SETTINGS

The POTS Static Settings menu contains the TAPI server port.

VICAS Setup Tool [POTS] [STATIC]: POTS Static Settings	BinTec Communications GmbH vicas
Remote TAPI Server Port	6001
SAVE	CANCEL
Enter integer range 0..65535	

Remote TAPI Server Port = The TCP port number to use for TAPI connections. Default value: 6001.



In the POTS A and POTS B menus you can specify the internal and external phone numbers and type or device to use for POTS port A or B respectively.

VICAS Setup Tool		BinTec Communications GmbH	
[POTS] [POTS A]: POTS A Configuration		vicas	
Type		any	
Internal Number		*1	
External Numbers >			
SAVE		CANCEL	
Use <Space> to select			

Type = Specifies the type of device connected to this POTS port.

Type	Accept calls for...
any	all voice services
fax	fax machines
telephony	telephones
modem	modems
disable	no calls possible at all

Internal Number = The POTS port can be reached under this number from the other POTS port for internal (i.e. toll-free) calls.

Note: The internal numbers should always start with either an asterisk »*« or a hash mark »#«. If internal numbers start with a digit (0-9) you will not be able to make external calls starting with that same digit any more.






This menu displays a list of all external numbers (MSNs) configured for the POTS port. You can add new numbers, or change or delete existing ones.

VICAS Setup Tool		BinTec Communications GmbH
[POTS]	[POTS A]	[EXTERNAL NUMBERS]
		vicas
External Numbers	Direction	
1	both	
ADD	DELETE	EXIT
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit		

Note that there are two fields, External Numbers and Direction. In the External Numbers field you can enter an MSN, in the Direction field you can specify whether this External Number should be used for *incoming* calls only, for *outgoing* calls, or for *both* incoming and outgoing calls.

Note: You can have an arbitrary number of *incoming* entries, but you should configure only **one** *outgoing* or *both* entry for each POTS port.

 This is to ensure you have a specific number for outgoing calls.

To edit an existing number, highlight the entry and press <Return>.

To add a new number select **ADD**.

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

To accept the entries and return to the **POTS** → **POTS A** menu select **EXIT**. Note that the changed numbers become effective immediately.

MODEM →

At the moment this menu only contains the **PROFILE CONFIGURATION** sub-menu, where you can configure up to eight different modem profiles.

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 VICAS. The settings are shown below should be fine for 14400 modems.

VICAS Setup Tool		BinTec Communications GmbH
[MODEM][PROFILE][EDIT]: Configure Profile		vicas
Name	Profile 1	
Description		
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/V.32bis or below for 14400 modems.

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

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

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

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

Max Receive Bps = the maximum baudrate you want to use with this profile. You can set any speed supported by the current modula-

tion (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.

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.

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

Operation = Select the operation to perform.

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

Operation	Meaning/Effect
put	If successful ¹ , overwrites/creates <TFTP File Name> on host at <TFTP Server> with contents of <Name in Flash>.
get	If successful ¹ , overwrites/creates <Name in Flash> in Flash with contents of <TFTP File Name> retrieved from host at <TFTP Server>.
state	If successful ¹ , overwrites/creates <TFTP File Name> on host at <TFTP Server > with contents of memory.
reboot	Reboot the VICAS; settings not previously saved are lost.

1. Host must support TFTP, file must exist and be writeable.

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

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

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

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

New Name in Flash = Filename in Flash to create.

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

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

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

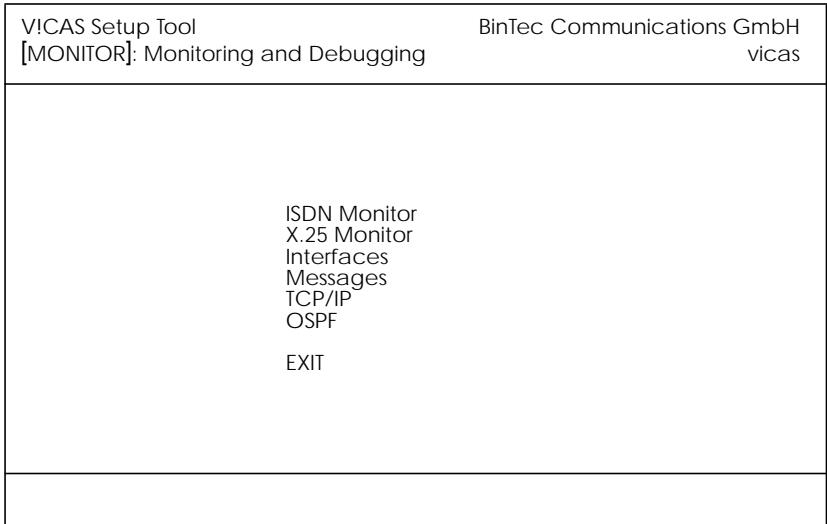
Note: If the “error” state is reported, it may help to refer to the menu **MONITORING AND DEBUGGING** → **MESSAGES** for cause.

To perform the selected operation, select **START OPERATION** and enter <Return>.

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

MONITORING AND DEBUGGING →

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



ISDN MONITOR lets you track incoming and outgoing ISDN calls.

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 V!CAS' system logging and accounting mechanisms.

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

OSPF menu lets you monitor OSPF related information.

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



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

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.

V!CAS Setup Tool	BinTec Communications GmbH				
[MONITOR][ISDN CALLS]: ISDN Monitor - Calls	vicas				
Dir Remote Number	Charge	Duration	Stack	Channel	State
EXIT					
(c)alls	(h)istory	(d)etails	(s)tatics		

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

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

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

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

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

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

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

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

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

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

MONITORING AND DEBUGGING → 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.

As when using the ISDN Monitor described on page 90, the menu commands (c, h, d, and s) listed at the bottom of the screen list different statistics relating to X.25 calls.

VICAS Setup Tool		BinTec Communications GmbH		
[MONITOR][X.25 CALLS]: X.25 Monitor		vicas		
From	To	Calling Addr	Called Addr	Duration
xi3	local	1 0	0	591
EXIT				
(c)alls	(h)istory	(d)etails	(s)tatics	

The (c)alls listing shows currently established X.25 connections.

From	To	Calling Addr	Called Addr	Duration
xi1	local	1	0	591
mpr-1	london2	3	2	139

The (h)istory listing shows a list of completed X.25 connections (both incoming and outgoing) since the last system reboot.

From	To	Starttime	Duration	Cause
xi1	central	19:33:52	0	(0x01) number busy
local	london2	19:34:01	2	(0x03) network congestion

For completed calls, you can display additional information about the call. Select a call from the list, then enter "d" to see a detailed listing.

The **(d)etails** listing shows specific information about completed calls.

```

Clear Cause          Clear Diag
Proro ID    1          State      dataxfer

Source:
Interface    paris-dialup
VC Number    1
X.25 Address
Link Address

Destination:
Interface    local
VC Number    1
X.25 Address 555
Link Address

Packet Size (In/Out) 128/128   Window Size (In/Out) 2/2
EXIT

```

The **(s)tatistics** listing shows transfer activity for established X.25 calls.

```

Duration 971

Send:
Packets    1555
Bytes      10032

Receive:
Packets    1552
Bytes      20999

Packets/s    0
Bytes/s      0

Packets/s    0
Bytes/s      0

```



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.

VICAS Setup Tool		BinTec Communications GmbH		
[MONITOR][INTERFACE]: Interface Monitoring		vicas		
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.

MONITORING AND DEBUGGING →

INTERFACES →

EXTENDED →

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

VICAS Setup Tool				BinTec Communications GmbH		
[MONITOR][INTERFACE][EXTENDED]: Extended Interface Monitoring				vicas		
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>.



The Syslog Messages menu actively displays system messages generated on the VICAS. 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 31.

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

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

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

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




MONITORING AND DEBUGGING

TCP/IP

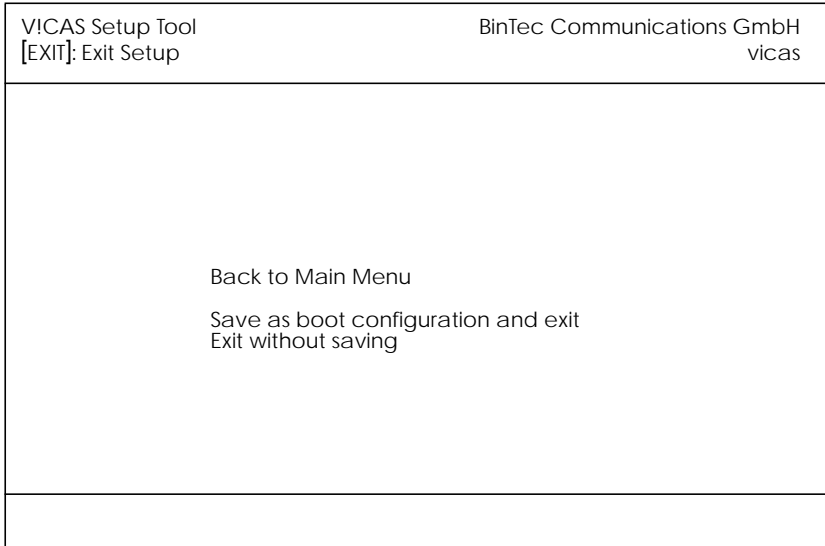
The IP Statistics Menu can be used to monitor different statistics relating to the ICMP, IP, UDP, and TCP protocols routed by the V!CAS. Initially, the menu displays information relating to the IP. Use the menu commands (c, i, u, and t) shown at the bottom of the screen, to see other information relating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

VICAS Setup Tool		BinTec Communications GmbH	
[MONITOR][IP]: IP Statistics		vicas	
InReceives	3912	OutNoRoutes	0
InHdrErrors	0	ReasmTimeout	500
InAddrErrors	0	ReasmReqds	0
ForwDatagrams	0	ReasmOKs	0
InUnknownProtos	0	ReasmFails	0
InDiscards	0	FragOKs	0
InDelivers	3321	FragFails	0
OutRequests	9	FragCreates	0
OutDiscards	0	RoutingDiscards	0
EXIT			
I(C)MP		(I)P	
		(U)DP	
		(T)CP	

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

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 VICAS' features
 - Hardware Interfaces 100
 - IP Features 104
 - IPX Features 116
 - X.25 Features 118
 - POTS Features 131
 - General 134
-

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

Now we'll explain, 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 VICAS' features.



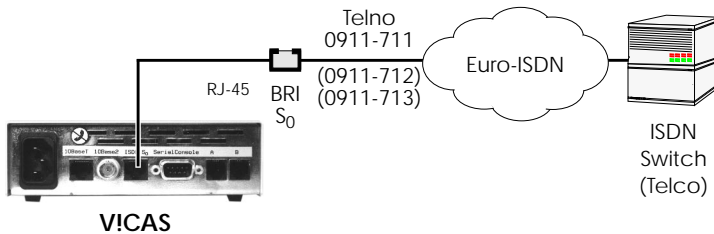
This section contains references to other information you may find helpful when configuring a particular feature (i.e., tips on testing features, troubleshooting, or general background information).

(p. 41) 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.

Hardware Interfaces

How do I configure an ISDN interface in general?

Configuring an ISDN interface on the VICAS involves telling the VICAS 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 VICAS knows the basic information about this interface, you can begin to configure different ISDN partners the VICAS can establish connections with.



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

WAN Interface: → Here's where we tell the VICAS what type of ISDN service we're receiving over this line.

Result of autoconfiguration: In most cases, the VICAS 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 autodetection. Only if autodetection 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 Interface: → → Here's where we tell the VICAS how to answer incoming calls on this line. This allows you take advantage of the different telephone numbers provided by your carrier. The VICAS 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 V!CAS 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 V!CAS to dispatch calls received for 0911-713 to the Login service and have other calls be given to Routing service.

WAN Interface:  →

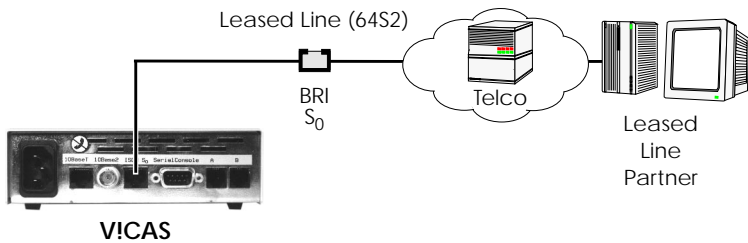
These settings aren't normally required since the V!CAS detects this information automatically.

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 V!CAS is similar to the basic procedure mentioned on page 100, for ISDN interfaces in general.

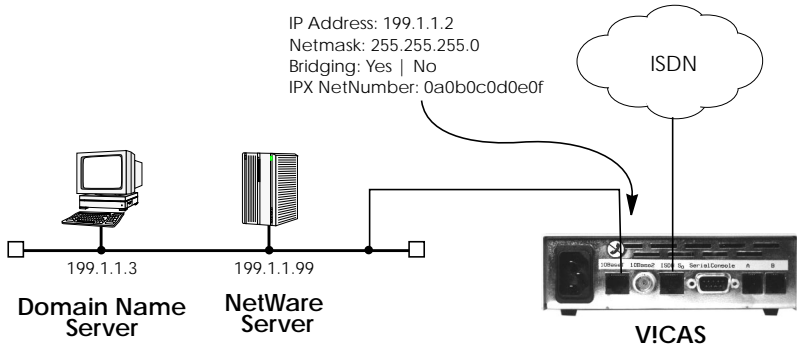
After setting the basic information about the physical interface you need to configure the WAN partner attached to the other end of the line. The V!CAS automatically creates a temporary WAN partner interface named according to the slot and unit the leased line was configured for. For our leased line 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 104.

How do I configure an Ethernet interface?

Configuring an ethernet interface on the V!CAS involves telling the V!CAS 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.

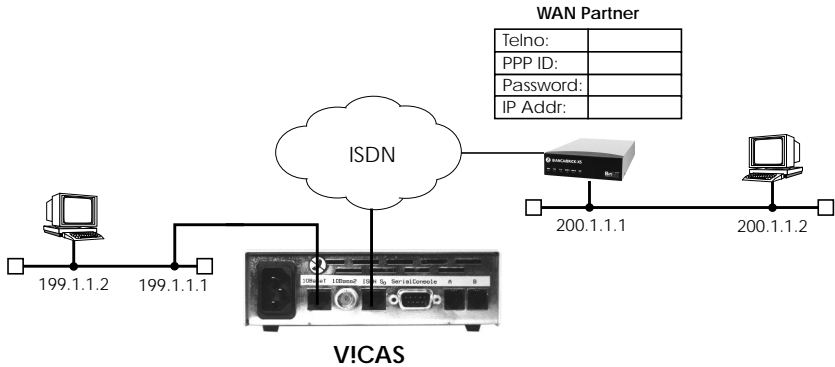
Under the **ADVANCED SETTINGS** → menu the following advanced features can optionally be enabled:

- 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 V!CAS will use for authentication.
- IP Address and Netmask (if non-standard mask is used)



Configure it

(p. 41) **WAN PARTNER** → **ADD** →

Create Partner Interface

Here you'll need to set:

Partner Name	<i><Unique Partner Name></i>
Enabled Protocols	IP
Encapsulation	<i><select an IP compatible method></i>
Identify by Calling Number	<i><yes or no></i>
PPP Authentication Protocol	PAP and CHAP
Partner PPP ID	<i><WAN partner's PPP ID></i>

PPP Password <PPP password for V!CAS>
 ISDN Ports to use <ports to use for calls to this partner>

Then, under **ISDN NUMBERS** → set

ISDN Number <partner's ISDN telephone number>
 Direction both

And, under **IP** → configure the partner's IP address.

If this partner is a stand-alone host or is a router connected to a LAN that uses a standard netmask you can leave the Netmask field empty.

IP Transit Network no
 Partner's LAN IP Address <your partner's IP Address>
 Partner's LAN Netmask <optional>

For sites that need to use a transfer network, please see page 55 for more information.

More Info

There are several partner-specific features that can be configured under the **ADVANCED SETTINGS** → menu such as Proxy ARP, RIP settings, Channel Bundling, IP Accounting and Callback support. Using these features is optional and fairly straight forward. See the menu description on page 49 in Chapter 4 for more 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 *biboPPPEncapsulation* variable:

<code>x75_ppp</code>	async PPP over X.75
<code>x75btx_ppp</code>	async PPP over X.75/T.70/BTX (T-Online)

These settings can be used to enable the VICAS 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

In **WAN PARTNER** → **ADD** → you'll need to set:

Partner Name	cis
Enabled Protocols	IP
Encapsulation	Async PPP over X.75
Identify by Calling Number	yes
PPP Authentication Protocol	none

Then, under **ISDN NUMBERS** → set:

ISDN Number	<CIS's telephone number>
Direction	outgoing

Under **IP** → assign dynamic to transit network field.

IP Transit Network	dynamic
--------------------	---------

Under **ADVANCED SETTINGS** → **PROVIDER CONFIGURATION** →

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

This information is used to automatically generate the required *biboPPPLoginString* variable.

TIP: 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.

Also, you may want to set *ShortHold* to 100 since the CIS login may take up to 20 seconds or more.

How do I configure the V!CAS to accept its IP address dynamically?

The V!CAS 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. 46) **WAN PARTNER** → **ADD** → **IP** → **Configure WAN partner (server)**

The WAN partner that assigns the V!CAS' IP address is configured just like any other WAN partner with one exception. The following field must be set to "dynamic".

IP Transit Network	dynamic
--------------------	---------

All other settings for this partner are configured as described on page 104.

(p. 55) **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>



More Info

In most cases configuring the V!CAS 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 109.

How do I configure the V!CAS as a dynamic IP address server?

The V!CAS 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 from a client, the V!CAS 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 the address pool.



Configure it

(p. 65) **IP** → **DYNAMIC IP ADDRESSES** → **ADD** → Address pool

Define the set of IP addresses the V!CAS should use for dialup clients.

IP Address <1st address in the block>
 Number of consecutive addresses <total # of addresses>

If you don't have a complete block of addresses you'll have to assign each address individually.

(p. 41) **WAN PARTNER** → **ADD** → Dialup Clients

Here you'll need to set:

Partner Name <Unique Partner Name>
 Enabled Protocols IP
 Encapsulation <select an IP compatible method>
 Identify by Calling Number <yes or no>
 PPP Authentication Protocol PAP and CHAP
 Partner PPP ID <WAN partner's PPP ID>
 PPP Password <PPP password for V!CAS>
 ISDN Ports to use <ports to use for calls to this partner>

Then, under **ISDN NUMBERS** → set

ISDN Number <partner's ISDN telephone number>
 Direction both

Under **ADVANCED SETTINGS** → tell the V!CAS to operate as the address server for this client with.

Dynamic IP-Address Server on

How do I configure Internet access for my LAN using NAT?

Using NAT, or Network Address Translation, the V!CAS 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 V!CAS will dial into.
- The V!CAS' PPP Password.
- An IP address (not needed if assigned dynamically).



Configure it

(p. 41)

WAN PARTNER → **ADD** →

Configure ISP interface

Configure a new ISDN interface for your ISP. Here you'll need to set:

Partner Name	<ISP Name>
Encapsulation	PPP
Identify by Calling Number	<yes or no>
PPP Authentication Protocol	PAP and CHAP
Partner PPP ID	<PPP ID of ISP's system>
PPP Password	<PPP password assigned by ISP>

Under **ISDN NUMBERS** → set

ISDN Number	<your ISP's ISDN telephone number>
Direction	outgoing

Under **IP** → configure your IP address.

If your address is assigned dynamically all you need to do here is set IP Transit Network to "dynamic". Otherwise set the fields as follows:

IP Transit Network	yes
Local ISDN IP Address	<V!CAS' static IP Address>
Partner ISDN IP Address	<V!CAS' static IP Address>

(p. 59) **IP** → **Network Address Translation** → **Enable NAT**

From this list, select the ISP interface you just configured.

Network Address Translation on

Now configure the types of incoming connections you want to allow. Under **ADD** specify the internal host, and services to allow. You might want to allow access to an FTP server on the LAN.

Service	ftp
Destination	<IP address of your FTP server>

(p. 55) **IP** → **ROUTING** → **ADD** → **Setup IP Routing**

All that's left to do now is to add a default route to your ISP.

Route Type	Default route
Network	WAN without transit network
Partner / Interface	<ISP interface name>

? More Info

Additional Routing Settings: Note that routing settings on some workstations on your LAN may need to be modified to include a default route that specifies the LAN address of your V!CAS. Check your operating system's instructions to see what changes need to be made.

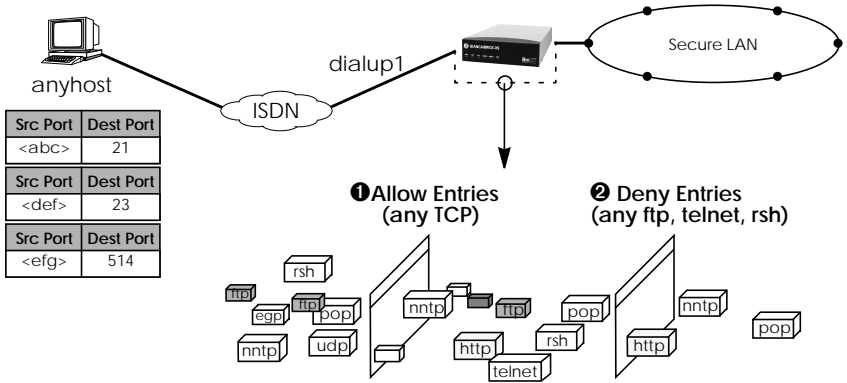
- On most UNIX workstations, you can add the route with:
`route add default <V!CAS' LAN Address> 1`
 This may not be needed if the workstation understands RIP. It will learn about new routes from the V!CAS every 30 seconds.
- On Windows 95 systems with Microsoft TCP/IP change "Properties-Systemcontrol-Network-TCP/IP-Properties-Gateway" and add the V!CAS as the primary gateway.

Another option is to use Proxy ARP on the LAN. This can be configured under: **CM-BNCTP, ETHERNET** → **ADVANCED SETTINGS**

How do I configure access lists to protect my network?

Access Lists provide a filtering mechanism that allows you to limit the types of traffic you want the V!CAS to route. For example, you might want to control access to the telnet service on a specific host to one or two remote ISDN hosts. This is done using Allow and Deny lists.

Below is a brief example of how the Allow and Deny Lists are used.



Before you begin

First decide what types of IP traffic you want to limit. You'll want to take the following things into consideration.

- What interface do you want to monitor incoming traffic on.
- What services and/or hosts do you want to allow/deny access to.
- What services do you absolutely need (DNS, FTP, HTTP).



Configure it



Configure Allow Entries

First, configure the Allow entries for the interface you want to monitor IP traffic on. The Source/Destination Address/Mask/Port fields should be set appropriately depending on what you are filtering.

```
Mode                allow
Source Interface/Partner  <name of interface to monitor>
```



(p. 63) **IP** → **ACCESS LISTS** → **ADD** → **Configure Deny Entries**
Next, configure the Deny entries for the same interface.

Mode	deny
Source Interface/Partner	<name of interface to monitor>

More Info

Information about different port numbers can be found in RFC 1700. On UNIX workstations refer to the `/etc/services` file or the man page for “services”.

Separate Access Lists for IP, IPX, and Bridging traffic are supported; however currently, only IP access lists may be configured with Setup Tool. IPX and Bridging filters must be configured via the SNMP shell.

Another useful feature for controlling access to your networks is Network Address Translation. Configuring NAT is explained on page 109.

How do I configure the VICAS as a RADIUS client?

RADIUS (Remote Authentication Dial In User Service) is a client/server security system often used by ISPs (Internet Service Providers) to control access to a network. The server maintains a database of user authentication data. If a RADIUS server is being used on the LAN, the VICAS can be configured as a RADIUS client.



Before you begin

You'll need the following information

- The IP address of your RADIUS server.
- The RADIUS Client Key
(as defined in the Key field of */etc/radb/clients*).



Configure it

(p. 57)



Set Server's IP Address

Set the IP address of the host operating as the RADIUS server.

RADIUS Server <IP Address>

(p. 29)



Set the RADIUS Client Key

Set the key the VICAS will use when polling the RADIUS server.

RADIUS Server Password <Client Key>

The VICAS is now configured as a RADIUS client.

Before refusing connections for incoming callers that can't be authenticated using PAP or CHAP, the RADIUS server is polled. If the server authenticates the caller, a new interface is created on demand. The characteristics of the new interface must be configured on the server in */etc/radb/users*.

The VICAS also adds a static route for the partner. Once the connection is closed, the interface and route are deleted, and any accounting data are sent to the server.



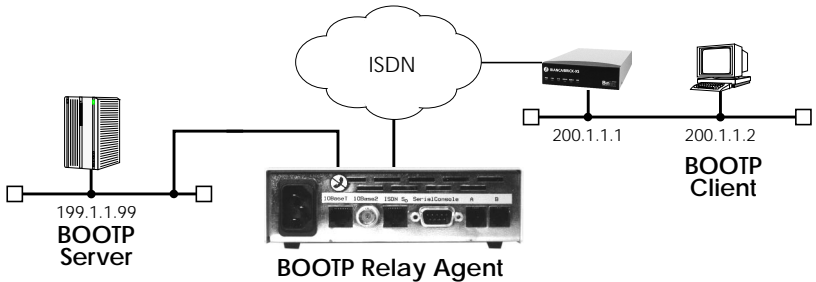
More Info

The characteristics of partner interfaces which are authenticated via the RADIUS server are defined in `/etc/radb/users`. The VICAS supports the following RADIUS attributes which correspond as follows:

RADIUS Attributes	Direction	Setup Tool setting on VICAS
User-Name	REQ	[WAN][ADD] Partner PPP ID
User-Password	REQ	[WAN][ADD] PPP Password
CHAP-Password	REQ	[WAN][ADD] PPP Password
NAS-Identifier	REQ	[System] System Name
Service-Type	ANS	fixed value: framed
Framed-Protocol	ANS	fixed value: ppp
Framed-IP-Address	ANS	[WAN][ADD][IP]: Partner's IP Address
Framed-IP-Netmask	ANS	[WAN][ADD][IP]: Partner's IP Netmask
Framed-Routing	ANS	N/A (RIP-listen/send/both)
Framed-Compression	ANS	N/A (vanj)
Framed-Route	ANS	N/A
Framed-IPX-Network	ANS	N/A
Session-Timeout	ANS	N/A
Idle-Timeout	ANS	[WAN][ADD][ADVANCED] ShortHold
CHAP-Challenge	REQ	[WAN][ADD] PPP Password
Port-Limit	ANS	[WAN][ADD][ADVANCED] Total Number of Channels

How do I configure the VICAS 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. 57) **IP** → **STATIC SETTINGS** → **Set BOOTP Server Address**
 BOOTP Server Address <server's IP Address>

The VICAS will now forward all BOOTP requests received over any of its interfaces (WAN or LAN) to the server.

(p. 41) **WAN PARTNER** → **ADD** → **(optional) WAN Partner**
 If the server or client is accessible via a dialup link, the appropriate WAN partner must also be configured before the VICAS 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 V!CAS.
- 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.
- The remote router's PPP ID and Password if authentication is used.
- An Internal IPX Network Number for the V!CAS if the default value is already in use.



Configure it

- (p. 28) **LICENSES** → Verify License
 Verify the IPX subsystem is valid.
- (p. 32) **CM-BNCTP, ETHERNET** → Configure LAN interface
 Enter the IPX Network Number of the LAN attached to this interface.
- (p. 41) **WAN PARTNER** → Create new WAN Partner
 Create a new WAN partner for the remote IPX router the V!CAS should call.
 Make sure the IPX protocol is enabled and select an appropriate encapsulation method; in most cases "PPP" will be fine.
- (p. 47) **WAN PARTNER** → **ADD** → **IPX** → Partner specific IPX settings

Set the IPX specific settings for this interface.

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. 69) **IPX** →

Global IPX protocol Settings

Set the V!CAS' Local System Name. Note this name is only used for IPX and may be different than the hostname of your V!CAS.

If the default Internal Network Number used by the V!CAS is already in use by another router, change its value here.

(see the 'ipx internal net' command on your NetWare server).

To save on ISDN charges it is recommended that you enable IPX and SPX spoofing and set NetBIOS Broadcast replication to "on LAN only".



More Info

The `ipxping` command is available from the SNMP shell and can be used to test routing connections between the V!CAS 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.

X.25 Features

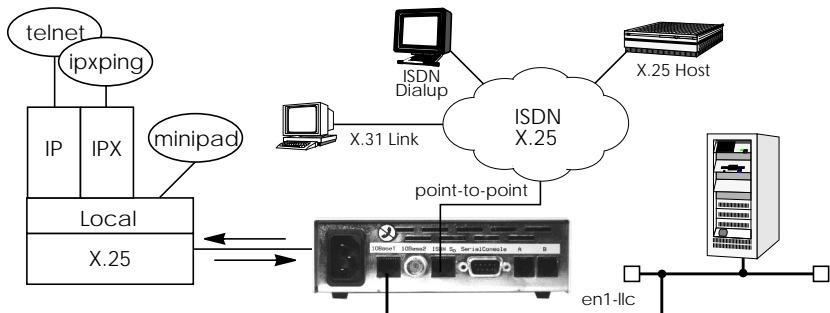
The following pages describe configuring some of the most common X.25 features on the V!CAS such as:

- How do I configure an X.31 link (X.25 in the D-channel)?
- How do I route IP traffic over X.25 with MPX25?
- How do I configure X.31 in the B-channel (Case A/Case B)?
- How do I configure X.25 access for a host on my LAN?
- How do I configure ISDN dialup access for an X.25 partner?
- How do I use the V!CAS as a TCP-X.25 bridge?

Special Note: The X.25 Local Interface

In X.25 routing the V!CAS decides where to forward X.25 calls based on the configured X.25 routes. An X.25 route can lead to a point-to-multipoint interface such as an ethernet, or a point-to-point interface such as a dialup ISDN or X.25 network partner. Another option is the V!CAS' special "local" interface.

This local interface is an internal *virtual* interface. Here, the X.25 packet is given to one of the V!CAS' software processes depending on contents (user data field) of the X.25 packet. The respective software process may need to reroute the call in which case the packet is passed back to the lower level routing instance. For example, when routing IP traffic over X.25 links (see Multiprotocol routing configuration on page 126).



How do I configure an X.31 link (X.25 in the D-channel)?

X.31 is a supplementary service offered by your ISDN provider which allows X.25 packets to be transmitted over an ISDN D-channel. This section describes configuring the X.31 data link that can be used by hosts on the LAN to connect to stations on the public X.25 network.



Before you begin

Before you start verify the following information from your ISDN carrier.

- The TEI value assigned to this interface.
- The Window and Packet size to use for Layer 3.
- The X.25 address of your V!CAS.
- The ISDN telephone number for this subscriber outlet.



Configure it

(p. 28) **LICENSES** →

Verify License

Verify your X.25 license is valid. You should find "X25 (valid)".

(p. 73) **X.25** → **LINK CONFIGURATION** →

Configure the X.31 Link

If the V!CAS is connected to the ISDN subscriber outlet you're receiving the X.31 service on, you should see an X.31 link in this menu, otherwise connect the cabling and reboot the system. When autodetected properly this link has the form:

```
x31d<Module Slot>-<ISDN Unit>-<TEI Value>
```

Verify the detected TEI value is correct then highlight the link and press <Return> to define the characteristics of this data link.

L3 Mode	dte
L3 Window Size	128 bytes
L3 Packet Size	2
Lowest Two-Way-Channel	1
Highest Two-Way-Channel	2
Layer 2 Behaviour	always active


(p. 76) **X.25** → **ROUTING** →

Create Route for Incoming Calls

Next, create a route for incoming calls. This will allow calls arriving on the X.31 link that are addressed to the V!CAS' X.25 address to be

given to the local¹ interface. The result: PAD calls are given to the PAD subsystem, calls containing IP data go to the IP subsystem, etc.

Source Link	x31d<slot>-<unit>-<TEI>
Destination Link	local
Destination X.25 Address	<V!CAS' ISDN telno>

Note:  The ISDN telephone number used here should be in the format: <country code><area code><local number>

(p. 76)  **Create Route for Outgoing Calls**

Create an X.25 route for outgoing calls. This route says that all calls from the local¹ interface are routed to the X.31 link.

Source Link	local
Destination Link	x31d<slot>-<unit>-<TEI>
Destination X.25 Address	<leave empty>

 **More Info**

Testing the X.31 Link

You can test the X.31 link from a remote X.25 host using a PAD (Packet Assembler Disassembler) by calling the V!CAS at it's X.25 address.

In Germany, a special "Echo Port" provided by the Deutsche Telekom can be used to verify your V!CAS is accessible over X.31. Using minipad from the SNMP shell call the echo port with:

minipad 026245911029002

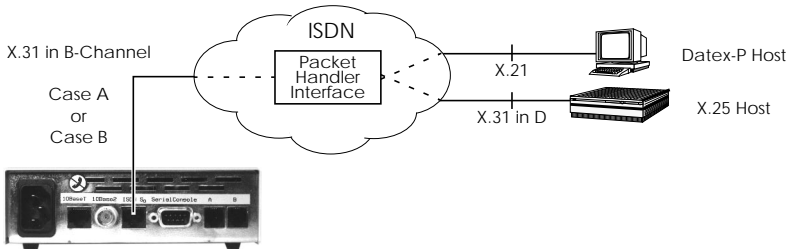
You should see a login prompt. Close the X.25 call with Control-P. You can also connect to the Deutsche Telekom's Traffic Generator service to verify data transfers are possible over the X.31 link. This can be done with:

minipad 026245911029003

1. See page 118 for information on the V!CAS' special local interface.

How do I configure X.31 in the B-channel (Case A/Case B)?

The V!CAS supports X.31 in the B-channel according to Case A and B. Case A and B are alternative procedures that can be used to access the public X.25 network from an S₀ interface. In both scenarios the V!CAS accesses X.25 hosts through the Packet Handler Interface (PHI) provided by the ISDN carrier.



When using the X.31 in the B-channel on the V!CAS, a WAN Partner interface can be configured for this PHI that can be used as a *virtual* router for all X.25 hosts. Individual X.25 Partner interfaces are not required.



Before you begin

You will need the following information.

- The V!CAS' ISDN telephone number.
- (Case A only) The telephone number of your local PHI. Contact your local carrier for this information.



Configure it

(p. 41) **WAN PARTNER** → **ADD** →

Configure WAN Partner

First, configure the PHI as a new WAN partner.

Partner Name	phi
Enabled protocols	<X> X.25
Encapsulation	X31-B-channel

Under **ISDN NUMBERS** → set your PHI's ISDN number if your carrier supports Case A. For Case B you don't need to configure the number.

ISDN Number	<PHI's telephone number>
Direction	both

(p. 73) **X.25** → **LINK CONFIGURATION** → **Configure the Link**

Next, set the link characteristics for the partner you just created in the previous step. In most cases the following can be used. If connections can't be established, verify with you carrier.

L3 Mode	dte
L3 Window Size	128 bytes
L3 Packet Size	2
Lowest Two-Way-Channel	1
Highest Two-Way-Channel	2
Layer 2 Behaviour	disconnect when idle

(p. 76) **X.25** → **ROUTING** → **ADD** → **Route for Incoming Calls**

Create a route for incoming calls. This will allow calls coming from our PHI interface that are addressed to the V!CAS' X.25 telephone number to be given to the local¹ interface.

Source Link	<interface name for PHI>
Destination Link	local
Destination X.25 Address	<V!CAS' ISDN telephone number>

(p. 76) **X.25** → **ROUTING** → **ADD** → **Route for Outgoing Calls**

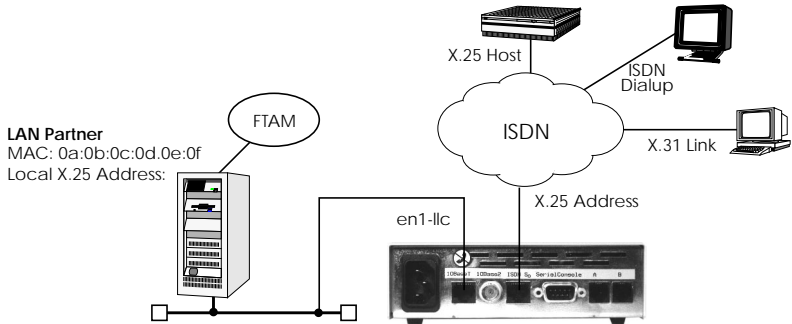
Create another route for outgoing calls. This route says that all calls from the local¹ interface are routed to the PHI.

Source Link	local
Destination Link	<interface name for your PHI>
Destination X.25 Address	<leave empty>

1. See page 118 for information on the V!CAS' special local interface.

How do I configure X.25 access for a host on my LAN?

LAN hosts can utilize X.25 WAN links provided by the V!CAS to connect to remote X.25 hosts. The appropriate WAN links should already be configured. This section describes how to configure the LLC link (X.25 over ethernet), the local portion of the end-to-end communication link. An LLC link is specific to a particular LAN host.



Before you begin

Before you start you're going to need the following information.

- The V!CAS' X.25 address.
- The LAN partner's MAC address.
- A locally assigned X.25 address for the LAN partner.



Configure it

(p. 72) **X.25** → **STATIC SETTINGS** → **Configure X.25 Local Address**

First, verify the V!CAS' local X.25 address is configured.

X.25 Local Address <V!CAS' X.25 Address>

(p. 73) **X.25** → **LINK CONFIGURATION** → **Create LAN Host Link**

We need to create a new link for the host on the V!CAS' LAN. Select the appropriate link template from the list depending on which LAN this host is on. Ethernet templates have the format:

en<slot>-llc (create new configuration)

Highlight the entry and enter <Return> to configure the link. For ethernet links the following settings should be acceptable.

L3 Mode	dce
L3 Packet Size	1024 bytes
L3 Window Size	5
Lowest Two-Way-Channel	1
Highest Two-Way-Channel	4095
Partner MAC address (LLC)	<LAN Partner's MAC address>
Layer 2 Behaviour	disconnect when idle

An X.25 (LLC) link now exists for our LAN host. You may need to verify the Packet and Window sizes and the number of Virtual Channels for this link are compatible with the settings used on the LAN host.

(p. 76) **X.25** → **ROUTING** → **ADD** →

Edit X.25 Routing Table

Here we create an X.25 route that says: give incoming calls from this LAN Partner that are addressed to the V!CAS' X.25 address to the special local¹ interface.

Source Link	en1<slot>-llc
Destination Link	local
Destination X.25 Address	<V!CAS' X.25 address>

(p. 76) **X.25** → **ROUTING** → **ADD** →

Edit X.25 Routing Table

Now we'll create another route so that X.25 calls addressed to our LAN host find the correct link. This route says: all X.25 calls received from the local interface that are addressed to our LAN host should be routed to the host at <MAC address> over the ethernet link.

Source Link	local
Destination Link	en<slot>-llc
Destination Link Address	<LAN Partner's MAC address>
Destination X.25 Address	<LAN Partner's X.25 address>



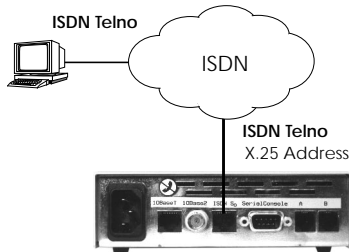
More Info

Depending on how you've set up X.25 routing, you can test your X.25 configurations using minipad. See minipad on page 160.

1. See page 118 for information on the V!CAS' special local interface.

How do I configure ISDN dialup access for an X.25 partner?

This section describes how to configure an ISDN dialup access for an X.25 partner. Here an available ISDN B-channel will be used to transfer X.25 user data with this remote host.



Before you begin

Before you start you're going to need the following information.

- The V!CAS' ISDN telephone number and X.25 address.
- The remote X.25 partner's ISDN telephone number.



Configure it

(p. 72) **X.25** → **STATIC SETTINGS** → **Configure X.25 Local Address**

Verify the V!CAS' X.25 address is set here.

(p. 41) **WAN PARTNER** → **ADD** → **Edit WAN Partner**

Create a new WAN partner interface and enable only X.25 traffic.

Enabled Protocols <X> X.25

Encapsulation X.25

Under **ISDN NUMBERS** → set the partner's ISDN number.

ISDN Number <the X.25 partner's ISDN telephone number>

Direction both

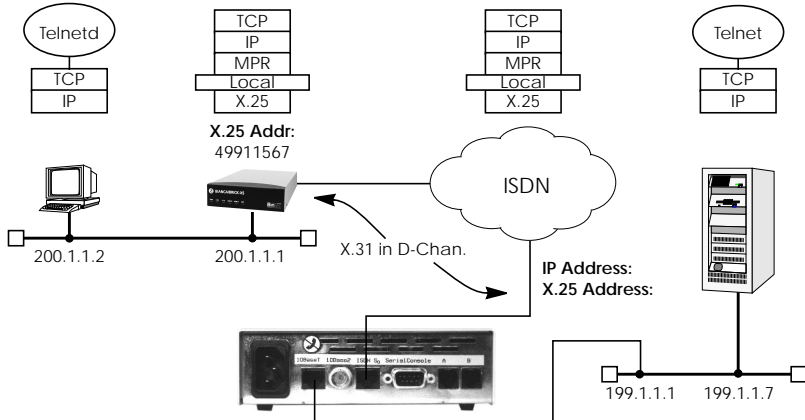
Note: If the remote site is another BRICK verify the Incoming Call Answering settings configured there to ensure this number will be dispatched to the routing service.



Return to the previous menu and select **SAVE**.

How do I route IP traffic over X.25 with MPX25?

The V!CAS can be configured to route multiple protocols (IP, IPX, and Bridging) over X.25. This mechanism allows you to use existing X.25 links as the transport medium for routing other protocols. We call these interfaces MPX25 for short. We'll assume that the X.31 link has already been configured and that the appropriate routes are set. (Configuring different X.25 links are described beginning on page 119.)



Before you begin

Before you start you're going to need the following information.

- The V!CAS' X.25 address.
- The remote partner's X.25 address.
- The remote partner's IP address.




Configure it

(p. 78) X.25 → MULTIPROTOCOL OVER X.25 → ADD → New MPX25 Partner

Create a new MPX25 interface for the remote X.25 partner. Here's where we define the types of traffic (IP, IPX, and Bridge) to transport over this link. For our example above, we're only routing IP.

Enabled Protocols	<X>IP
Encapsulation	<one of: ip_rfc877 ip mpr>
X.25 Destination Address	<MPX25 partner's X.25 address>

Note:  Only if an X.31 in D-channel link is being used as the transport medium, the X.25 address entered here should be preceded by {00}. This will allow outgoing calls to be placed correctly (using: 00<country code><area code><local number>) and incoming calls to be identified (the X.25 network delivers calls without the preceding 00).

Next, edit the protocol-relevant settings for this partner. In our example, we're routing IP over X.25 so we need to set the remote partner's IP address here.

So under  set.

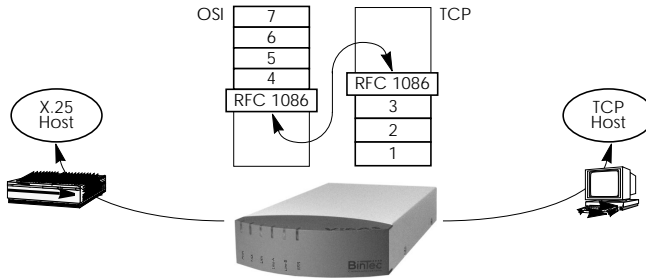
IP Transit Network	yes
Local ISDN IP Address	<V/CAS' IP address>
Partner's ISDN IP Address	<MPX25 partner's IP address>
Partner's LAN IP Address	<optional>
Partner's LAN Netmask	<optional>

More Info

Depending on how you've set up X.25 routing, you can test your X.25 configurations using minipad. See minipad on page 160.

How do I use the V!CAS as a TCP-X.25 bridge?

The V!CAS can be used as a TCP-X.25 bridge as described in RFC 1086. Using this mechanism, the V!CAS can be used to allow X.25 and TCP hosts to communicate by providing an end-to-end ISO-TP0 connection.



Depending on which side initiates the connection (see the examples under *More Info* shown on page 129) the V!CAS performs the appropriate protocol mappings as shown above.



Before you begin

No special information is required to configure the V!CAS as an ISO-TP0 bridge. Please note however that TCP clients must support RFC 1006 which describes how to transmit TP0 packets over TCP.



Configure it

(p. 28) **LICENSES** →

Verify License

Verify your X.25 license. You should see “X.25(ok)” in this menu.

(p. 76) **X.25** → **ROUTING** → **ADD** →

Route for outgoing calls

X.25 routing must be configured so that incoming and outgoing calls can be established. Using the special *local* interface (see page 118) a minimal X.25 routing setup could be used as follows.

Source Link	local
Destination Link	<X.25 interface name ¹ >

1. Use an available X.25 compatible interface name here.

(p. 76) **X.25** → **ROUTING** → **ADD** →

Route for incoming calls

Create another route for incoming calls. The interface name used in the Source Link field should be the same interface used in the previous step.

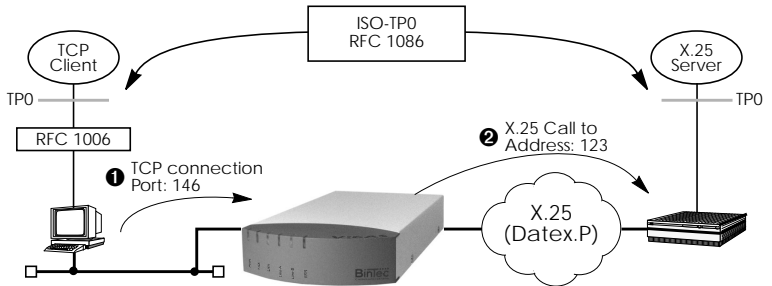
Source Link	<X.25 interface name>
Destination Link	local

? More Info

Two common uses for this mechanism are as follows. For more detailed reference please refer to RFCs 1006 and 1086 respectively.

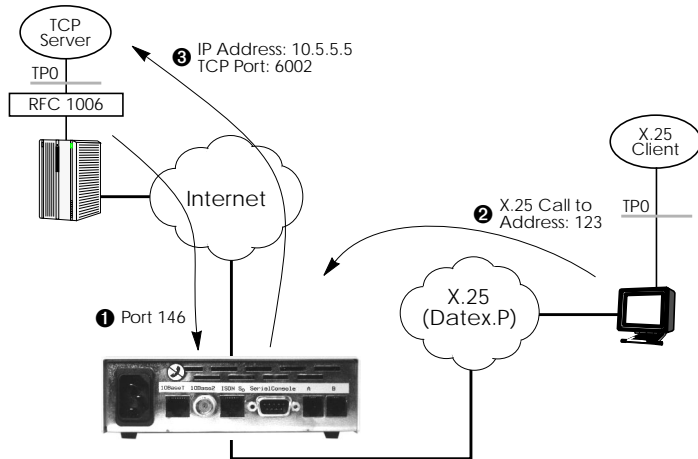
TCP Client requests connection to X.25 Server

Here the TCP-Client initiates a connection (as defined in RFC 1086) with the VICAS using TCP port 146. The VICAS then contacts the remote X.25-Server and transparent TP0 packets can begin to be exchanged between the two endpoints.



X.25 Client requests connection to TCP Server

Here the TCP-Server must first initiate a connection with the V!CAS at TCP port 146 where it registers its IP address and port number. It instructs the V!CAS to accept incoming calls addressed to an X.25 address (123) and route the connection to the registered TCP port number (6002) and IP address (10.5.5.5).



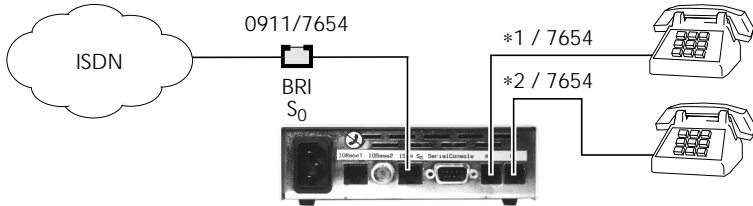
Note: The V!CAS will listen for incoming calls to the registered address only as long as the TCP (port 146) connection between the registering host and the V!CAS exists.



POTS Features

How can I configure my POTS ports if I only have one MSN?

You can connect—and use—two analog telephones to the POTS ports of your VICAS even if you only have received one MSN with your ISDN access.



Let's assume you want both telephones to ring if someone calls your ISDN telephone number, 7654. If you talk on one phone, the other should still ring if a call comes in, which is useful for small office applications.



Before you begin

All you need to know is your ISDN telephone number (MSN).



Configure it

Take the following steps for both POTS port A and B.

(p. 82) **POTS** → **POTS A** →

POTS A Type

Select the type of device connected to port A using the spacebar. In our example this would be *telephony*.

(p. 83) **POTS** → **POTS A** → **EXTERNAL NUMBERS** → **ADD** Ext. Number

Add a new external number entry. Use your ISDN telephone number as External Number, 7654 in our example, and set the Direction field to *both* with the spacebar. This means that this number will be used for both incoming and outgoing calls.

Repeat the steps given above for POTS port B.

Both telephones will now behave as described above.

How can I configure my POTS ports using more than one MSN?

If you have received more than one MSN with your ISDN access you can use the different numbers to route calls to the appropriate port.

The configuration uses the same Setup Tool menus as the POTS configuration with only one MSN.

Let's assume you received the three MSNs 7654, 7655 and 7656 with your ISDN access, and you want to connect analog telephones to POTS port A and B.

The telephone at port A should accept all calls for MSN 7654, the telephone at port B should accept calls for MSN 7655, and both telephones should accept calls for MSN 7656.



Before you begin

You need to know your ISDN telephone numbers, which of these numbers to use for which POTS port, and which device is connected to which POTS port.



Configure it

(p. 82) **POTS** → **POTS A** →

POTS A Type

Select the type of device connected to port A using the spacebar. In our example this would be *telephony*.

(p. 83) **POTS** → **POTS A** → **EXTERNAL NUMBERS** → **ADD** **Ext. Number**

Add a new external number entry. Use the ISDN telephone number you want to use for this telephone as External Number, *7654* in our example, and set the Direction field to *both* with the spacebar. This means that this number will be used for both incoming and outgoing calls.

Now add another external number, using the common ISDN number, *7656* in our example, and set the direction to *incoming*. This handles the calls for both telephones.

Note: You can have an arbitrary number of *incoming* entries, but you should configure only **one** *outgoing* or *both* entry for each POTS port.



Now you can configure port B.

(p. 82) **POTS** → **POTS B** →

POTS B Type

Select the type of device connected to port B using the spacebar. In our example this would be *telephony*.

(p. 83) **POTS** → **POTS B** → **EXTERNAL NUMBERS** → **ADD** Ext. Number

Add a new external number entry. Use the ISDN telephone number you want to use for this telephone as External Number, *7655* in our example, and set the Direction field to *both* with the spacebar.

Now add one more external number, using the common ISDN number, *7656* in our example, and set the direction to *incoming*.



More Info

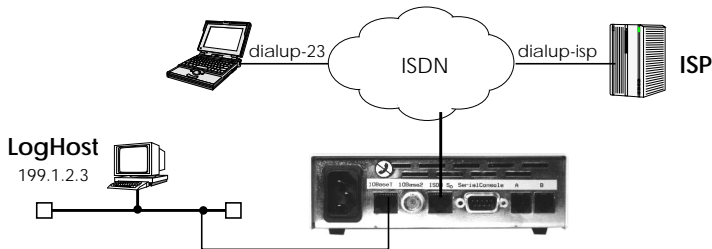
For more information on the POTS menus please refer to pages 84 ff.

General

How can I retrieve accounting information (ISDN and TCP/IP)?

Various system messages are generated on the VICAS based on different events. Accounting messages are a subset of these messages. The VICAS 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. 34) **CM-BNCTP, ETHERNET** → **ADVANCED SETTINGS** → **LAN Interfaces**

Turn on IP accounting for each LAN interface you want the VICAS to generate IP accounting messages for.

IP accounting on

- (p. 49) **WAN PARTNER** → **ADD** → **ADVANCED SETTINGS** → **WAN Interfaces**
 Turn on IP accounting for each IP-capable WAN interface you want the VICAS to generate IP accounting messages for.

IP Accounting on

- (p. 31) **SYSTEM** → **EXTERNAL SYSTEM LOGGING** → **Add Log Host**
 Here's where you add (or change) remote hosts the VICAS 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.

Note: 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.

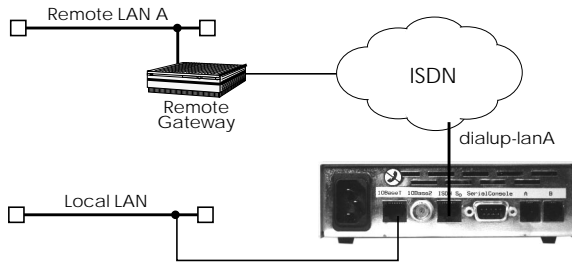


More Info

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 do I use the V!CAS as a Bridge to link two LANs over ISDN?

The V!CAS 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.



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 V!CAS' PPP Password (only if PAP or CHAP is used).



Configure it

(p. 41) **WAN PARTNER** → **ADD** →

Configure Gateway

Configure the remote gateway as a new WAN partner.

Partner Name	<unique interface name>
Enabled protocols	<X> BRIDGE
Identify by Calling Number	<yes or no>
Encapsulation	PPP
PPP Authentication Protocol	<PAP, CHAP, or both>
Partner PPP ID	<gateway's PPP ID>
PPP Password	<V!CAS' PPP password>

Under **ISDN NUMBERS** → **set**

ISDN Number	<gateway's ISDN number>
Direction	both

(p. 32) **CM-BNCTP, ETHERNET** →

Enable LAN interfaces

Next, enable the LAN interface you want the VICAS to forward packets from.

Bridging `enabled`

Once the local interface is enabled the VICAS can begin to learn MAC addresses from remote LANs and begins to fill its forwarding table. This is particularly important when bridging over ISDN links so that unnecessary ISDN charges can be avoided.



More Info

Additional control of bridged traffic is available using special bridge filters which are similar to the Access List mechanism described on page 111. Currently, this must be configured from the SNMP shell using the *dot1dStaticAllowTable* and *dot1dStaticDenyTable*.

How can I improve security?

The VICAS 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 VICAS 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 30). 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 you have the option of using the **Calling Line ID** feature of ISDN. This option should always be used by setting

Identify by Calling Number yes

In addition to CLID the CHAP and PAP authentication protocols are available by setting

PPP Authentication Protocol <PAP, CHAP, or both>

Login access via isdnlogin

The isdnlogin program can be used to login to the VICAS 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 *isdnLoginOnPPPDispatch* 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 V!CAS is possible using PAD applications such as minipad. To disable login access via PAD calls enter the following from the shell:

```
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 **SysLog Messages**.

The V!CAS stores a limited number of messages. The best way is to setup an external Log Host and have the V!CAS forward all messages to it. A LogHost can be a UNIX host (using Syslogd) or a PC (using BRICKware). Configuring the V!CAS to forward messages to a LogHost is described on page 134.

Examine your SysLog Messages from time to time to see what's happening on your system (access list violations, problems, charging information, etc).

While the V!CAS 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** → menu. See Chapter 4 beginning on page 89.

CAPI Port

You can also control access to the V!CAS' CAPI port by changing the TCP port number (default 6000) 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 111 for configuring Access Lists.

Trace Port

Information transmitted over the 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 V!CAS' trace port.

From the SNMP shell enter: `biboAdmTracetcPort=0`

Under Setup Tool see the  →  → menu.

SNMP Port

Access to the V!CAS' SNMP port number can also be changed (default = 161) or disabled by setting to 0. To disable the SNMP port:

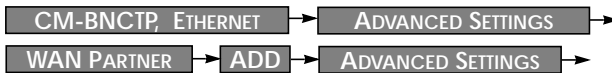
From the SNMP shell enter: `biboAdmSNMPPort=0`

Under Setup Tool see the  →  → 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 V!CAS learns about new IP routes using the **RIP Receive** field for both Ethernet and WAN Partner interfaces using the following menus.



Even though small, outgoing RIP packets contain information about your internal networks. You can restrict the interfaces the V!CAS broadcasts RIP information on using the **RIP Send** fields on the above mentioned menus.

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 111 for information on using IP access lists.

RADIUS

Many sites use a separate RADIUS server for more advanced authentication procedures. The V!CAS can be configured as a RADIUS client that polls the RADIUS server at connection time. See page 113.

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 V!CAS' status page?

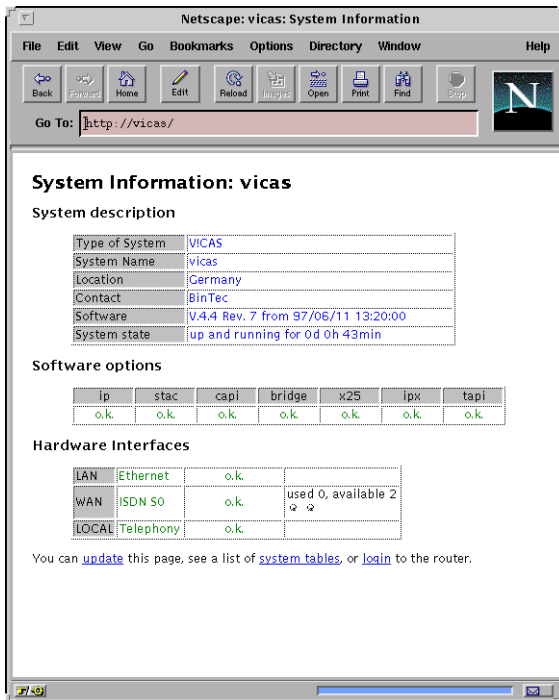
The V!CAS provides status information about its operational state (installed licenses, available ISDN channels) in HTML. The status page is primarily intended for end users on the V!CAS' LAN that are having problems connecting to remote sites. From this page users can then inform the system administrator via email if a problem exists.

To access the status-page point a WWW browser (Netscape Navigator or Microsoft's Internet Explorer) at the V!CAS 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 V!CAS' 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.



The status page consists of three tables.

System Description

This information is retrieved from the *admin* table. If a valid email address is detected in the SysContact field the V!CAS 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 *biboAdmLicInfoTable* and displays the status of the V!CAS subsystems.

Hardware Interfaces

This table displays the current state of the V!CAS' hardware interfaces. Possible reasons for the different states (column three) are as follows:

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

Note: Access to the V!CAS' status page can be disabled by setting the HTTP port to 0.
 See the HTTP port field in the   menu.

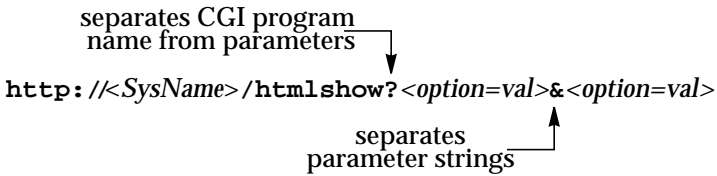
SNMP-Table Browsing

The contents of the V!CAS SNMP tables can be browsed via HTTP browsers using the "SNMP Tables" link from the V!CAS main Status-Page. Initially this link displays a list of all system tables found on the V!CAS. From there, individual system tables can be selected; the V!CAS creates the appropriate HTML pages on-the-fly.

CGI Program: `htmlshow`

The contents of V!CAS SNMP tables and variables can also be selectively displayed to any WWW browser using the internal `htmlshow` program. The V!CAS authenticates `htmlshow` queries using the SNMP community passwords (admin, read, write) once per browser session.

The syntax for using `htmlshow` adheres to the CGI (Common Gateway Interface) standard and can be referenced as follows:



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`

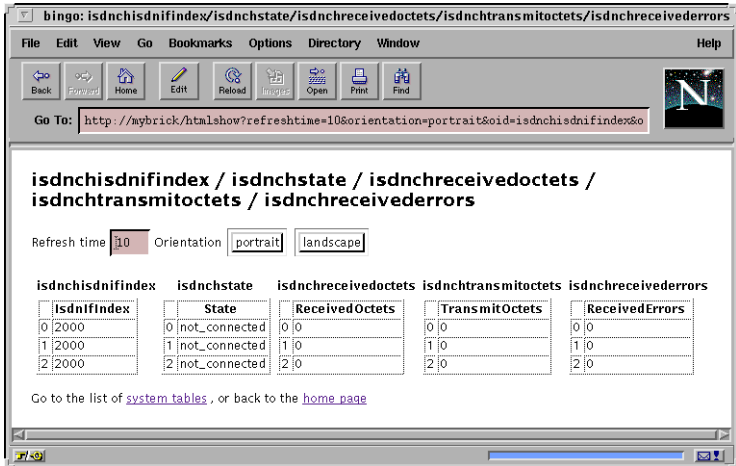
If `interval` is specified the display is updated every `interval` seconds. Entering 0 in the resulting text field disables automatic refresh updates.

`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
```



TIP: References to HTML pages generated by the V!CAS 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 V!CAS 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 V!CAS.

6

TROUBLESHOOTING

What's covered

- General Troubleshooting147
- Debugging Tools.....147
- System Errors.....148
- Software Problems.....150
- ISDN Connections152

General Troubleshooting

In general, if you are having problems, it may be helpful to have the VICAS temporarily save All System Logging Messages. Then you can view the system messages as the events occur.

In Setup Tool under **SYSTEM** → set:

Maximum Number of Syslog Entries 30

Message level for the syslog table debug

Alternatively, from the same menu you can set

Syslog output on serial console yes

then exit Setup Tool and let the messages scroll to the screen.

Debugging Tools

debug

The debug command can be used from the SNMP shell to debug one or more VICAS 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.

bricktrace

You can use the **bricktrace** utility 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, please see chapter 7.

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 V!CAS to its initial configuration state as it arrived. This can be done from the `BOOTmonitor` at startup.

I can't reach the V!CAS via the network.

- If the V!CAS 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 on 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.

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 48. These settings must be compatible with the settings used by the servers on the VICAS' LAN.
- The Network Number for the VICAS' LAN interface is either not set (in *ipxCircNetNum*) or could not be obtained from the server. If this is the case, the VICAS 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 V!CAS of the change since it doesn't know the server exists yet. The V!CAS 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 V!CAS.

- 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 V!CAS 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 f. 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 VICAS 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 VICAS 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.

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

The VICAS refuses to close an existing ISDN connection.

- Is the bricktrace program running over an ISDN-PPP connection? The tracer continually sends packets over ISDN which results in a permanent connection (i.e. the connection can't be closed).

Unwanted ISDN Connections

Verify the **biboAdmLogHostTable**.

- Are syslog events being sent to an ISDN-PPP partner? Each time PPP closes an ISDN connection (after 23 seconds) a new syslog message is created. If these messages are being sent over ISDN-IP, this will force a new connection to be opened.

RIP packets are continually routed over ISDN.

- Is there 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
```

POTS Connections

Internal calls do not connect

- Verify that neither of the two POTS ports is disabled. The *Type* field in both the **POTS** → **POTS A** → and **POTS** → **POTS B** → menu must be set to *any, telephony, fax, or modem*.
- Verify in the **POTS** → **POTS A** → and **POTS** → **POTS B** → menus that you dial the configured *Internal Numbers*.

Internal calls do not appear in the ISDN History

- That's right. They're not supposed to show up there, because they are not—strictly speaking—ISDN connections, but internal connections, free of charge.

My analog phone does not ring even if I dial the correct number

- Verify that the correct *External Number* has been configured in the appropriate **POTS** → **POTS x** → **EXTERNAL NUMBERS** menu.
- Make sure that the *Direction* field is set to either *both* or *incoming*.

7

COMMAND REFERENCE

What's covered

- SNMP Shell Commands
 - telnet..... 157
 - ping..... 157
 - ipxping..... 158
 - traceroute..... 158
 - lstat..... 158
 - netstat..... 159
 - isdnlogin..... 159
 - minipad..... 160
 - date..... 160
 - update..... 160
 - setup..... 161
 - debug..... 161
 - p..... 161
 - ifconfig..... 162
 - halt..... 162
- BRICKtools for UNIX Commands
 - bricktrace..... 163
 - capitrace..... 163

The SNMP shell commands

The VICAS 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 *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.

ping

ping [**-c** *<count>*] *host* [*size*]

The ping program 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.



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 VICAS and an IPX server. Ipyping 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)

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
```

The ifstat command displays status information for each of the system's interfaces, based on the contents of the *ifTable*. Ifstat takes no parameters, as it simply displays an overview of the status of each interface since the last system boot. The information is displayed in eleven columns.

netstat

```
netstat [-i | -r] | -p]
```

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.

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 VICAS 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 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	dovb	56k

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 disable X.25 connections to the minipad, *x25LocalPadCall* must be set to "dont_accept".

date

date [YYMMDDHHMMSS]

The VICAS 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 <ipaddress> <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.

setup

setup

The setup command is used from the SNMP shell to start the V!CAS Setup Tool. Setup Tool provides a menu oriented interface to configuring the V!CAS 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 [-t] [show | all | [<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 V!CAS' various subsystems. Command line parameters are used as follows:

- t** Print a timestamp before each debugging message.
- show** Show all possible subsystems that can be debugged.
- all** Display debugging information for all subsystems.
- <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 V!CAS' 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.

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> VICAS' 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 powering the system off/on.

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][-l]
```

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 VICAS. The environment variable CAPI_HOST must be set to the IP address of the VICAS to trace CAPI messages on.

Command line parameters 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.milliseconds” 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))

8

HARDWARE/FIRMWARE CONFIGURATION

What's covered

- Hardware
 - Front Panel Indicators..... 166
 - The Back Plane..... 167
 - The Main Board 168
- Firmware
 - Upgrading System Software .. 169



The VICAS belongs to BinTec's highly successful family of BIANCA/BRICK ISDN routers. It is specially designed to allow teleworkers to connect their computer to their company's LAN and at the same time serve as a small PBX with two POTS ports for analog end-devices (telephones, faxes, etc.).

In this chapter we'll cover the VICAS 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 VICAS. The various LEDs have different meanings depending on which mode the VICAS is in. As the VICAS 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.
FAX	Blinking	DRAM test is being performed
LAN	Off	Not used.
Line A	Blinking	Flash ROM test is being performed.
Line B	Blinking	CHIP test is being performed.
ERR	Off	Not used.

BOOTmonitor Mode

LED(s)	State	Meaning
PWR	On	Power is being supplied.
FAX	Off	Not used.
LAN	Blinking	Performing a TFTP transfer.

LED(s)	State	Meaning
Line A Line 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.
FAX	-	Reserved for future updates.
LAN	On	Packet being sent over the LAN interface.
Line A, Line B	On	Data transmission on B-Channel 1 (Line A) or B-Channel 2 (Line B)
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 V!CAS. For information on the individual pin assignments of each port, see *Appendix A*.

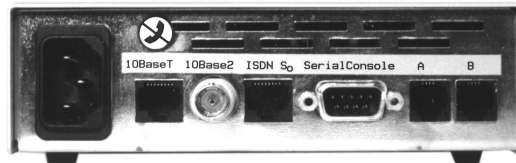


Figure 3: Back Plane

The Power Socket

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

Before supplying power to the V!CAS, please verify the power rating identified on the marking label complies with your local power source

The Network Ports

The V!CAS has a 10base2 (BNC) and 10baseT (TP) port for connecting to the LAN and an ISDN S₀ port (marked ISDN-S/T) for connecting to your ISDN subscriber outlet.

Telephony Ports

The V!CAS also has two telephony ports (POTS¹ ports, marked A/B on the back plane) for the connection of analogue devices (e.g. telephones, fax machines, etc.).

Serial Port

The V!CAS 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 V!CAS*, explains connecting a terminal.

The Main Board

Your V!CAS 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 3.

1. Plain old telephone service

Firmware

Upgrading System Software

You may decide to upgrade your VICAS' 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 releases.

After obtaining the newest software you can perform the upgrade in any of the methods described as follows:

- **BOOTmonitor** (press the spacebar during bootup)
- **update** command (while the system is running)
- **TFTP** (retrieve the BOOT image via TFTP)

BOOTmonitor

After the internal self test has been successfully completed, the VICAS 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.

The commands from the BOOTmonitor menu are self guiding, informing/prompting you for confirmation along the way.

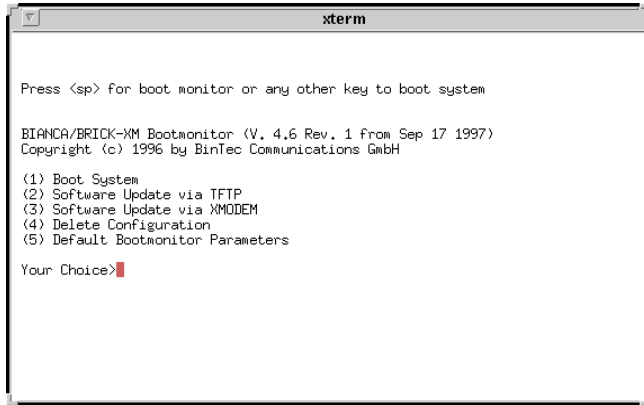


Figure 4: BOOTmonitor

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 V!CAS when powered up.

Software Updates

To upgrade the V!CAS firmware, first select either option (2) or (3) to specify how the new image should be transferred to the V!CAS. 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 V!CAS is turned off, your old software release will be used upon a subsequent reboot.



Delete Configuration

You can select option (4) to return the V!CAS 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.
- Which LAN interface to use for TFTP file transfers (when more than 1 are present).
- The IP address for the V!CAS
- 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 V!CAS.

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 V!CAS. The default setting is set at 9600 baud, which is supported by practically all terminals.



Automatic booting over TFTP

The V!CAS 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 V!CAS 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
 - POTS Port
 - Serial Port
- Important Safety Information in:
Danish, Dutch, Finnish, French,
German, Greek, Italian,
Norwegian, Portugese,
Swedish, and Spanish

General System Specifications

Processor:	MC68EC020, 20 MHz
Memory:	4 MB/32 bit DRAM SIMM, 1 MB/8 bit flash-ROM
Interfaces:	ISDN WAN S ₀ IEEE 802.3 LAN (10BaseT and 10Base2) 2 POTS ports for analog end-devices (telephone, fax, etc.)
Serial:	RS 232 C, Sub9 Male (PC), 1,200 - 115k Bd.
Display:	LEDs: 1 Power, 4 Function, 1 Error
Power:	100-240 VAC, 60/50 Hz, max. 0.2 A, universal power supply ¹ with internal fan.
Dimensions:	151 mm 45 mm x 305 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

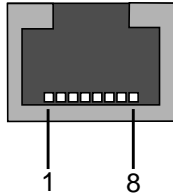


Figure 5: ISDN S₀ BRI Interface (RJ45 socket)

The pin assignment for the S₀ port is as follows:

Pin	Function
1 & 2	Not used
3	Transmit (+)
4	Receive (+)
5	Receive (-)
6	Transmit (-)
7 & 8	Not used

POTS Port for analog equipment

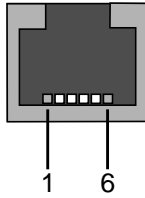


Figure 6: POTS port (RJ11 socket)

The pin assignment for the POTS ports is as follows:

Pin	Function
1	Not used
2	Not connected
3	A
4	B
5	Not connected
6	Not used

A and B are the two lines necessary to connect analog telecommunications equipment (telephone, fax, modem, etc.).

Note: Please note that some manufacturers use RJ11 plugs with different pin assignments for A and B with their analog telephones, so you will need an adapter cable to connect them to your V!CAS.



Serial Port

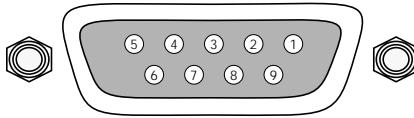


Figure 7: 9 Pin Serial Port

Pin assignment for the 9 pin serial port is as follows:

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

Ethernet Ports

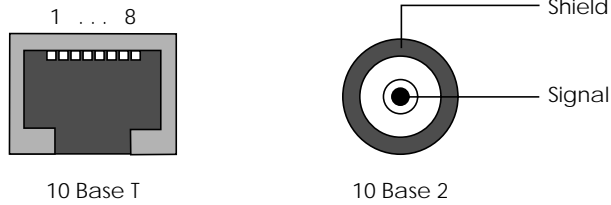


Figure 8: Twisted pair port (10 Base T) and BNC port (10 Base 2)

Pin assignments for Twisted pair RJ45 port are as follows:

Pin	Function
1	TD +
2	TD -
3	RD +
4	Not used by 10BaseT
5	Not used by 10BaseT
6	RD -
7	Not used by 10BaseT
8	Not used by 10BaseT

If you want to connect your V!CAS to your PC via Twisted Pair ethernet directly (i.e. without using an external hub) you have to use a crossover cable, where the pins are connected as follows:

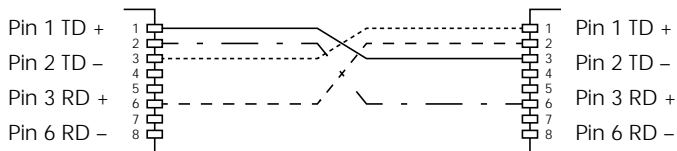


Figure 9: Twisted Pair ethernet Crossover cable

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.

- 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 bedugning 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.
- Dataoverførselsledningerne skal under tordenvejr hverken tilsluttes eller frakobles.
- Ved systemets ledningsinstallation læg venligst mærke til rækkefølgen, som beskrevet.
- Pas på, at ingen objekter (f. eks. smykkekedler, clips osv.) eller vædsker 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 u hensigtsmæssige reparaturer er det muligt, at brugeren udsættes for en betydelig fare. En ikke tilladt åbning af apparaterne har til følge, at BinTec Communications GmbH fralægger sig enhver form for garanti og ansvar.
- Anvend kun de vedlagte kabler. Hvis der anvendes andre kabler, tager BinTec Communications GmbH ingen ansvar for opståede skader.
- Vigtig henvisning til fagpersonalet: Netstikket skal trækkes før systemenheden åbnes.
- CE-tegnet betyder, at „VICAS“ 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 manchette på håndledet eller berøre en jordet flade, før De berører det åbnede apparat.
- Apparatet må under ingen omstændigheder renses vådt. Pga. indtrængende vand kan der opstå alvorlige farer for anvenderen (f.eks. stød).
- Anvend aldrig skurepulver, alkaliske rengøringsmidler, korroderende eller skurende hjælpemidler. Overfladen af apparatet kan ellers beskadiges.

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.

- 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
 - max. 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 GmbH uit.
- Gebruik uitsluitend de meegeleverde kabels. Indien u andere kabels gebruikt, kan de firma BinTec Communications GmbH op geen enkele wijze verantwoordelijk worden gesteld voor enige vorm van schade.
- Electrostatische (op)ladingen kunnen tot schade aan het apparaat voeren. Draag daartoe een antistatische manschet om de pols of raak een geaard vlak aan, voordat u het geopende apparaat aanraakt.
- Het apparaat mag in geen geval nat worden gereinigd. Door indringend water kunnen aanzienlijke gevaren voor de gebruiker ontstaan (b.v. elektrische schok).
- Nooit een schuurmiddel, alkalische reinigingsmiddelen, scherpe of schurende hulpmiddelen gebruiken. De oppervlakte van het apparaat kan daardoor worden beschadigd.

Finnish: Turvallisuusohjeita

Laite vastaa toimistotiloissa käytettäviin tietotekniikan laitteisiin päteviä asianmukaisia turvallisuusohjeita.

Tästä jaksosta löytyvät ne turvallisuusohjeet, joiden noudattaminen on ehdottomasti välttämätöntä järjestelmän kanssa työskennellessä. Mikäli tarvitset lisätietoja laitteen pystyttämisen tai käytön suhteen suunnitellussa ympäristössä, käänny asiakaspalvelumme puoleen.

- 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 nimellisarvot 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 verkkojohdolla).
- 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 liittäminen käyttöohjeen vastaavia kohtia noudattaen.
- Älä liitä tiedonvälitysohjoja äläkä vedä niitä pois ukonilman aikana.
- Noudata järjestelmän kaapeloinnissa kuvauksen mukaista järjestystä.
- Varmista, että pieniä osia (esim. koruketjuja, paperipinteitä) tai nesteitä ei pääse tunkeutumaan laitteen sisäosaan (sähköisku, oikosulku).
- 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, palantorjunta, häiriöpoisto).
- Vain ammattihenkilökunta saa avata laitteen. Tästä syystä kehoitamme teettämään kaikki korjaukset valtuutetuilla ammatti henkilöillä. Asiantuntemattomat korjaukset voivat aiheuttaa käyttäjälle huomattavia vaaroja. Laitteiden luvaton avaaminen sulkee BinTec Communications GmbH:n pois takuusta ja vastuusta.
- Käytä vain mukana seuraavia kaapeleita. Mikäli käytetään muita kaapeleita, BinTec Communications GmbH ei vastaa tällöin syntyvistä vahingoista.
- Tärkeä vihje ammattihenkilökunnalle: Vedä verkkopistoke ennen järjestelmäyksikön avaamista.
- CE-merkki tarkoittaa, että „VICAS“ 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.

- 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 - 240VAC
 - 60 / 50 Hz
 - max. 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. 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 GmbH 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 „VICAS“ correspond aux directives suivantes de la CEE: EMV (89/336/CEE) et basse tension (73/23/CEE).
- L'appareil peut être raccordé au système „Euro-NUMERIS“ (France), car il remplit en plus des réglementations nécessaires de la CEE, les caractéristiques de ISDN français.
- Des charges électrostatiques peuvent endommager les appareils. C'est pourquoi, il est recommandé de porter un manchon antistatique au poignet ou de toucher une surface mise à terre, avant d'ouvrir l'appareil.
- L'appareil ne doit en aucun cas être nettoyé au mouillé. D'importants dangers peuvent survenir pour l'utilisateur (par ex.: décharge électrique), si de l'eau pénètre dans l'appareil.
- N'employez jamais de produits abrasifs, de nettoyants alcalins ou autres produits tranchants ou grattants. La surface de l'appareil pourrait être de cette façon endommagée.

German: Sicherheitshinweise

Das Gerät entspricht den einschlägigen Sicherheitsbestimmungen für Einrichtungen der Informationstechnik für den Einsatz in einer Büroumgebung.

In diesem Abschnitt finden Sie Sicherheitshinweise, die Sie beim Umgang mit Ihrem System unbedingt beachten müssen.

Falls Sie Fragen zum Aufstellen und Betrieb in der vorgesehenen Umgebung haben, wenden Sie sich bitte an unseren Service.

- Transportieren Sie das Gerät nur in der Originalverpackung oder einer anderen geeigneten Verpackung, die Schutz gegen Stoß und Schlag gewährt.
- Beachten Sie vor dem Aufstellen und Betrieb des Gerätes die Hinweise für die Umgebungsbedingungen.
- Wenn das Gerät aus kalter Umgebung in den Betriebsraum gebracht wird, kann Betauung - sowohl am Geräteäußeren als auch im Geräteinneren auftreten. Warten Sie, bis das Gerät temperaturangeglichen und absolut trocken ist, bevor Sie es in Betrieb nehmen.
- Überprüfen Sie, ob die auf dem Typenschild angegebene Nennspannung des Geräts mit der örtlichen Netzspannung übereinstimmt. Das Gerät darf unter den folgenden Bedingungen betrieben werden:
 - 100 - 240 VAC
 - 60 / 50 Hz
 - max. 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. Schmuckketten, Büroklammern etc.) oder Flüssigkeiten in das Innere des Geräts gelangen (elektrischer Schlag, Kurzschluß).
- Ziehen Sie in Notfällen (z.B. geschädigtes Gehäuse oder Bedienelement, Eindringen von Flüssigkeit oder Fremdkörpern) sofort den Netzstecker und verständigen Sie den Service.
- Beachten Sie, daß der bestimmungsgemäße Betrieb (gem. IEC 950/ EN 60 950) des Systems nur bei montiertem Gehäusedeckel gewährleistet ist. (Kühlung, Brandschutz, Funkenstörung)
- Das Gerät darf nur von Fachpersonal geöffnet werden. 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 GmbH zur Folge.
- Verwenden Sie nur die beigelegten Kabel. Falls Sie andere Kabel verwenden, übernimmt BinTec Communications GmbH 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 V!CAS 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. Die Oberfläche des Gehäuses kann dadurch beschädigt werden.

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
60 / 50 Hz
max. 0,2 A

- Συνδέστε τη συσκευή μόνο σε έναν κανονικά γειωμένο ρευματολήπτη με επαφή προστασίας (η συσκευή είναι εξοπλισμένη με έναν ελεγχόμενο 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. Πα την πλήρη διακοπή του δικτύου ο ρευματολήπτης πρέπει να τραβηχθεί έξω.
- Τοποθετείστε τους αγωγούς έτσι ώστε να μην δημιουργούν καμιά πηγή κινδύνου και να μην φθείρονται. Αλλάξτε αμέσως έναν φθαρμένο αγωγό. Κατά τη σύνδεση της συσκευής προσέξτε τις σχετικές πληροφορίες στο χειρίδιο λειτουργίας.
- Μην συνδέετε αγωγούς μεταφοράς δεδομένων κατά τη διάρκεια μιας καταιγίδας ούτε να τους αποσυνεδέετε.
- Κατά την τοποθέτηση των καλωδίων του συστήματος προσέξτε τη σειρά, όπως περιγράφεται.

- Προσέξτε να μην πέσουν αντικείμενα (π.χ. χρυσαφικά, αλυσίδες, συνδετήρες κλπ.) ή υγρά στο εσωτερικό της συσκευής (ηλεκτροπληξία, βραχυκύκλωμα).
 - Σε περίπτωση έκτακτης ανάγκης (π.χ. φθαμένο περίβλημα ή εξάρτημα χρησιμοποίησης, εισροή υγρού ή εισδοχή ξένων αντικειμένων) αποσυνδέστε αμέσως τον ηλεκτρολήπτη και ενημερώστε το σέρβις.
 - Προσέξτε ότι η κανονική λειτουργία (σύμφωνα με τα IEC 950 / EN 60 950) του συστήματος εξασφαλίζεται μόνο με το συναρμολογημένο καπάκι του περικαλύμματος (Ψύξη, πυροπροστασία, άρση των παρασίτων).
 - Η συσκευή επιτρέπεται να ανοιχθεί μόνο από ειδικευμένο προσωπικό. 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 φθαμένο 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 καθαριστεί με υγρά σε καμιά περίπτωση. Με την εισροή νερού μπορεί να προκύψουν σημαντικοί κίνδυνοι για τον χρήστη (π.χ. ηλεκτροπληξία).
 - Μη χρησιμοποιείτε ποτέ αφρώδη μέσα, αλκαλικά απορρυπαντικά, ισχυρά ή αφρώδη βοηθητικά υλικά. Με αυτά τα μέσα μπορεί να φθαρεί η επιφάνεια του περικαλύμματος.
- Σημαντική πληροφορία για το ειδικευμένο προσωπικό:
- Πριν ανοίξετε το σύστημα βγάλτε τον ρευματολήπτη.

Προσοχή: Σε περίπτωση ακατάλληλης αντικατάστασης της μπαταρίας υπάρχει κίνδυνος έκρηξης. Αντικατάσταση μόνο με τον ίδιο ή με ισάξιο τύπο. Οι μεταχειρισμένες μπαταρίες πρέπει να εξουδετερώνονται σύμφωνα με τις οδηγίες του κατασκευαστή.

Το σήμα CE σημαίνει ότι το **BRICK** ανταποκρίνεται στις κατευθυντήριες γραμμές της Ε.Ε.: EMV (89/336/ΕΟΚ) και χαμηλή τάση (73/23/ΕΟΚ).

Η συσκευή μπορεί να συνδεθεί και στο Ευρω-**Numeris** (Γαλλία), γιατί εκτός από τις απαιτούμενες στην Ε.Ε. διατάξεις εκπληρώνει επιπρόσθετα και τις απαιτήσεις του γαλλικού ISDN.

Italian: Avvisi di sicurezza

L'apparecchio è conforme alle normative di sicurezza del settore per arredamenti tecnico-informatici, per l'utilizzo in ambienti di lavoro (uffici).

In questa sezione trovate avvisi di sicurezza che dovrete assolutamente osservare nell'uso del vostro sistema. Se avete delle domande sull'installazione ed il funzionamento nell'ambiente previsto, rivolgetevi per cortesia al nostro service.

- 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
 - max. 0,2 mA
- 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 GmbH.
- Utilizzate soltanto i cavi allegati. Se utilizzate altri cavi, la ditta BinTec Communications GmbH 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 detersive abrasive, né detersivi alcalini, né materiali taglienti o abrasivi, perché potrebbero danneggiare la superficie.

Norwegian: Sikkerhetsveiledning

Dette apparatet møtekommer 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.

- 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 tilkople apparatet.
- Ved tordenvær skal dataledningene hverken tilkoples eller trekkes ut.
- Se opp for den riktige rekkefølgen når de tilslutter systemets kabelforbindelser.
- Vær oppmerksom på at hverken gjenstander (for eks. smykkekedjer, binders, osv.) eller vesker kommer inn i apparatet (elektrisk støt, kortslutningsfare).
- I en nødsituasjon (for eks. når kabinettet eller et betjeningselement har fått en skade, veske eller fremmedlegeme har kommet inn i apparatet) trekk ut støpslet og kontakt vår kundeservice.
- Vær oppmerksom på at det kun består garanti for systemets bestemmelsesmessige drift (ifølge IEC 950/EN 60 950) hvis apparatlokket er montert (kjøling, brandsikring, radiostøybeskyttelse).
- 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 GmbH fraskriver seg hvert garantiansvar.
- Bruk kun de vedpakkede kabler . Dersom de bruker andre kabler, fraskriver BinTec Communications GmbH seg ethvert ansvar hvis det oppstår skader.
- Viktig instruks til fagpersonale:
Koble fra nettverkstøpslet før systemenheten åpnes.
- CE-tegnet betyr at „VICAS“ 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 håndleddet eller ta på en jordnet 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.

- 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
 - máx. 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 GmbH da garantia e da assunção de responsabilidade.
- Utilize apenas os cabos fornecidos juntos. No caso da utilização de outros cabos, a BinTec Communications GmbH 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.

- 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
max. 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 dataöverföringskablar vid åskväder.
- Beakta den beskrivna ordningsföljden vid anslutning av systemets kablar.
- Se noga till att inga föremål (smycken, gem o dyl) eller vätskor kommer in i maskinen. Då finns risk för elektriska stötar och kortslutning.
- Vid nödfall (t ex maskinhölje eller -delar går sönder, vätska eller främmande föremål kommer in i maskinens inre), drag omedelbart ut nätkontakten och underrätta serviceavdelningen.
- Observera att reglementsenlig systemdrift (enl. IEC 950/EN 60950) endast garanteras 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 GmbH:s garanti- och ansvarsåtagande ur kraft.
- Använd endast bifogade kablar. Om andra kablar används, ansvarar BinTec Communications GmbH ej för uppkomna skador.
- Viktig upplysning till fackpersonal: Drag ut nätverkskontakten innan systemenheten öppnas.
- CE-beteckningen innebär att „VICAS“ motsvarar följande EU-riktlinjer: EMV (89/336/EWG) och lågspänning (73/23/EWG).
- Maskinen kan även anslutas till „Euro-NUMERIS“ (Frankrike) eftersom den, utöver de erforderliga föreskrifterna inom EU, även uppfyller de franska ISDN-kraven.
- Statisk elektricitet kan medföra skada på maskinen. Använd därför en antistatisk manschett runt handleden, eller vidrör först en jordad yta, innan ni rör vid den öppnade maskinen.
- Maskinen får under inga omständigheter vätrenöras. 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.

- 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
 - max. 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.
- 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 GmbH.
- Utilice sólo los cables suministrados de fábrica. De utilizarse cables diferentes BinTec Communications GmbH 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.

INDEX

A

- access
 - CAPI port 139
 - isdnlogin 138
 - SNMP port 140
 - trace port 140
 - X.25 139
- access lists 62, 111, 141
- accounting 134
 - IP 34, 50
- autoconfiguration 35, 100

B

- Basic rate interface 10, 155, 174
- biboAdmSyslogTable 152
- biboPPPTable 153
- BNC
 - Port 8
- BNC port 177
- BOOTmonitor 169
- BOOTP 58, 115
- bricktrace 148, 153, 154, 155, 163
- Bridging 136, 153
- Btx 159
- bundelling 49

C

- callback 49
- CAPI 3, 28
 - port 139
 - Remote 3
- capitrac 163
- channel
 - virtual 74
- CLID 42
- Compression
 - STAC 4, 41
 - V.42 bis 42
- CompuServe 106
- CTS 176

D

- date 160
- DDI 38
- debug 161
- debugging 89
- DHCP Server 53, 66
- Direct Dial In 38
- DTR 176

E

Encapsulation 153
 for IPX packets 33
encapsulation
 for IPX packets 33
Error messages 148

F

Facsimile support 159

G

Gateway 136

H

halt 162
HTML status page 142
HTTP port number 142

I

ifconfig 162
ifstat 158
intruders 139
IP 53
 accounting 34, 50, 134
IP address
 address pool 65
 dynamic client 107
 server mode 108
IPX 69, 116
 network number 47
ipxping 158
ISDN
 accounting 134
 call answering 37
 switch type 35
ISDN monitor 90
isdnCallHistoryTable 148, 152, 153
isdnDispatchTable 153
isdnlogin 148, 152, 159
isdnlogind 159
isdnStkTable 153

L

leased line 102
licenses 28

M

message levels 30
messages 96
minipad 160
MODEM 84
monitor
 interfaces 94
 ISDN 90
 messages 96
 TCP/IP 97
 X.25 92
MPX25 126

N

NAT 59, 109, 140
NetBIOS 70
netstat 159

P

p 161
passwords 30, 148
ping 157
Port
 BNC 8, 177
 POTS 175
 Serial 149, 168, 176
 Telephony 168
 Twisted pair 177
 UTP 9
port
 SNMP 68
POTS 10, 80, 131
 port 10, 80, 175
PPP
 local PPP ID 29
Priority 161
Priority Voice Technology 3, 4

Protocols

- IP 148, 153, 154
- TCP 148

R

- RADIUS 58, 113, 141
- Remote CAPI 3
- Remote configuration 4
- Remote TAPI 3
- RIP/SAP 47, 140
- Router 4
- Routing 153
- routing 153
 - IP 54
 - multiprotocol 126
 - X.25 76
- RTS 176
- RVS-COM 4

S

- security 138
 - access lists 62
 - NAT 140
 - RIP 140
- Serial port 149, 168, 176
- server
 - CAPI 58
 - DNS 57
 - timeserver 58
 - trace 58
- SNMP port 68
- SNMP Shell
 - priority 161
- STAC compression 4, 41
- sysName 29
- system administration 87
- system messages 96

T

- TAPI 28
 - Remote 3
 - server port 80
- TCP/IP
 - dialup connection 104
 - statistics 97
- Telephony Ports 168
- telnet 155, 157
- TFTP 88, 172
- Time Server 58
- traceroute 158
- Twisted pair port 177

U

- update 160
- Utilities
 - bricktrace 148, 153, 154, 155, 163
 - capitrac 163
 - date 160
 - debug 161
 - halt 162
 - ifconfig 162
 - ifstat 158
 - ipxping 158
 - isdnlogin 159
 - minipad 160
 - p 161
 - ping 157
 - telnet 157
 - traceroute 158
 - update 160
- UTP port 9

V

- V.42 bis 42

X

X.25

 local X.25 address 72

 routing 76

X.25 monitor 92

X.25 over ISDN 125

X.31 119

 CaseA/B 121

XMODEM 170