BinGO!

User´s Guide

Installation and Configuration

Purpose This manual explains the installation and initial configuration of **BinGO!** with the Software Release 4.9.3. It is highly recommended that you read our Release Note containing the latest information and instructions for the most current Software Release – especially if you are performing a software update to a higher level. The latest Release Note is always available at www.bintec.de.

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

The information in this manual is subject to change without notice. Additional information, including changes and Release Notes for **BinGO!**, can be retrieved from **BinGO!** at www.bintec.de.

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

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

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

Guidelines and standards **BinGO!** adheres to the following guidelines and standards:

- Voltage guidelines 73/23/EWG according to EN60950
- Adheres to German safety regulations standards

- Interference resistance according to EN50082 -1/1.32
- Class B interference emissions according to EN55022 /-8.94
- Electro-magnetic tolerance according to EU guideline 89/336/EWG
- CE-symbol for all EC countries

Registration:

- BZT D 133451J (CE and German registration)
- BZT D 133457J (EG design test certificate)
- BAKOM (registered)
- CE 0188X (France adheres to the CE guideline)
- EN50082, EN55022
- EN60950

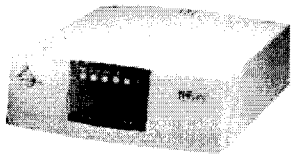
In addition to the CE guideline, **BinGO!** satisfies the ISDN requirements in France and may be connected to Euro-Numeris.

How to reach BinTec

BinTec Communications AG	
Telephone	+49 911 96 73 0
Fax	+49 911 688 07 25
Mail	BinTec Communications AG Südwestpark 94 D-90449 Nürnberg
Internet	www.bintec.de

Version 1.6
Document #71000B
March 1999

1 Welcome!



Congratulations on wisely choosing to buy a personal ISDN Internet access router. In doing so, you have acquired a leading product from the Personal Access range of BinTec Communications AG. This high-performance multiprotocol router allows you affordable networking of smaller networks. In future, your **Bingo!** will make it possible for you to connect either your individual workstation or small company to the Internet and to a corporate network. Moreover, the entry-level router **BinGO!** will provide all the computers on the network with up-to-the-minute means of office communication (communications applications, such as fax, file transfer, terminal emulation).

Where do we go from here?

What your Bingo gives you... ..., what **BinGO!** means for you and exactly what Bingo can do are questions addressed in the following pages.

Getting BinGO! up and running... ...is concisely described in chapter 3, page 33. There we will show you how to connect **BinGO!**; how, within minutes, and with the help of a configuration assistant, the Configuration Wizard, configuring is made quick and easy; how to install other useful online assistants; and, if necessary, how to configure your computer. At the end of that chapter, you will be in a position to surf the Internet, send or receive e-mails or faxes and connect with and exchange data to and from HQ from your computer – indeed, from any computer in your small network.

And on top of all that, you will find extensive explanations in chapter 6, page 117. There you will be shown all the configurations in detail. Even if you do not have a Windows computer, you will find fast ways to configure your **BinGO!**.

If you have already configured BinTec routers... ...or have general experience with configuration, and you want to get started right away, all you really need to know is the preset user name and password.

User name	Password
admin	bintec

Remember, however, to change your user name and password when you log in to your **BinGO!** for the first time. All BinTec routers are supplied with the same passwords. Thus, they are only protected against unauthorized access once you change the access information.

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

1.1 What Do you Need BinGO! For?

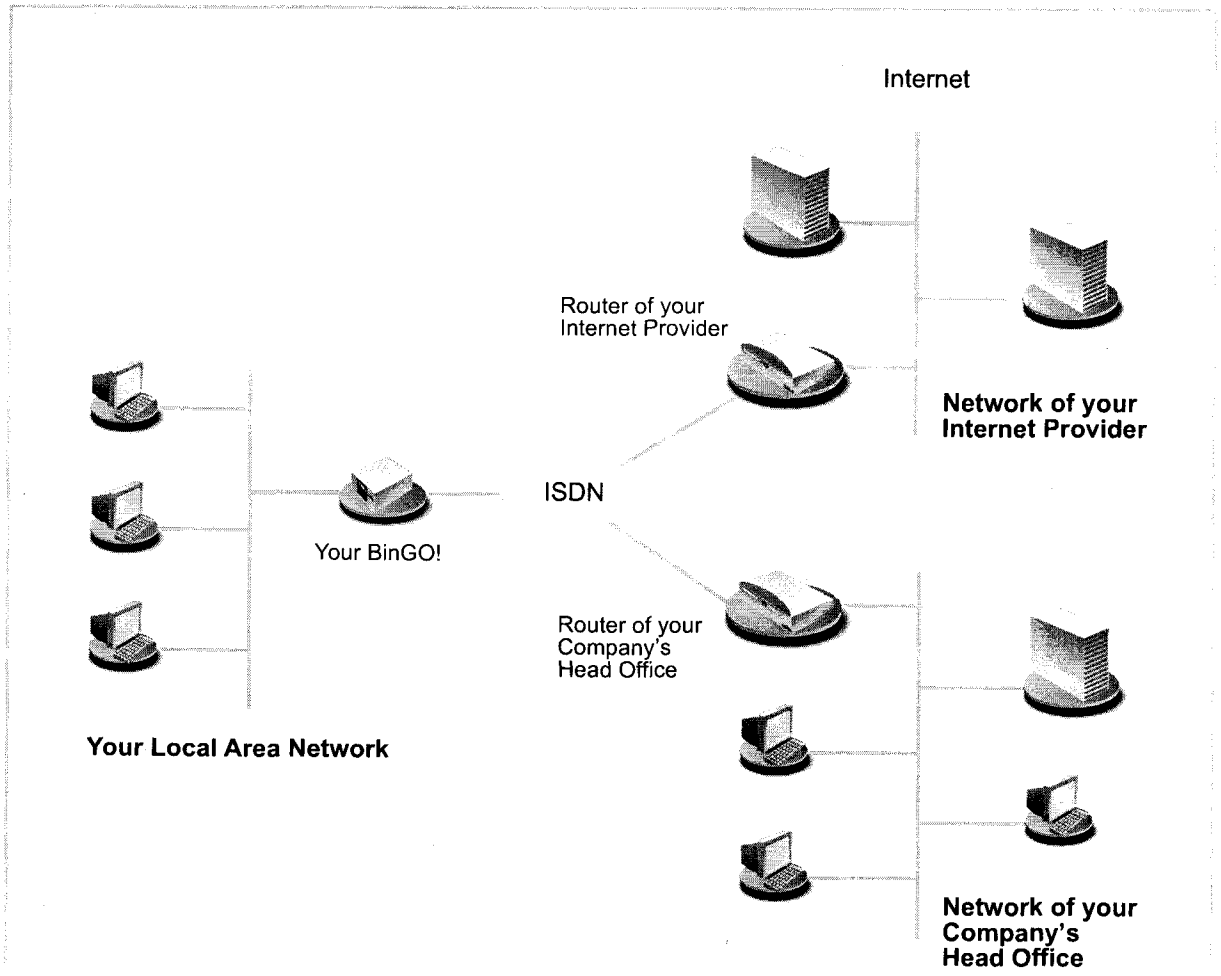


Figure 1-1: Basic scenario

Why BinGO!? Routers are used to connect networks with one another, to exchange information between networks and to make common use of services. Thus, via your router, as shown above, you can connect with the network of your Internet provider and thus avail of the usual services of the Internet, such as the World Wide Web (WWW) or e-mail. By connecting to your company´s head office from your

home or branch office, you can conveniently access any information you may need from the headquarters, even if this is hundreds of kilometers away. The connection of these local networks takes place via ISDN. When these small, single networks, the so-called LANs (Local Area Networks), are connected together the result is a Wide Area Network (WAN). The size of the single network alone – whether it consists of several computers or just one home office – is irrelevant.

As shown in the previous illustration, your **BinGO!** is the essential component for a connection of the networks: it is your link to the outside world. All the routers in the illustration are linked by ISDN lines to ISDN and thus serve as a connection between the single local networks. Within each single LAN, the router is connected to the network like a normal computer. It is designed to transmit information from its own network to an external network (e.g. to the network of your provider or your head office). In order to do so, it must determine the most suitable routes for that transmission. Conversely, it receives information and routes it into its own network.

What can your **BinGO!** do that a modem or ISDN-card cannot do? Your BinGO can do considerably more.

One router for everyone

If you have a local network with several computers, you only need one single router to allow all computers in the network access to the Internet or the head office. Thus, as a result of lower costs for equipment and maintenance, the more computers in the network, the more you save. When using modems or ISDN-cards, on the other hand, every workplace would have to be separately equipped.

Communications applications

The same applies to communications applications (telematic services such as answering machine, fax G3 and G4, file transfer and eurofile transfer) on your computer. All LAN users can avail of these services via an interface designed by BinTec, the Remote CAPI, while the **BinGO!**, however, needs just one single ISDN connection. The only precondition is that all users have the corresponding application software installed which suports the so-called CAPI interface. This standard interface is, however, supported, by most communications applications. The telematic software RVS-COM Lite that covers the spectrum of all the usual telecommunications services is included in the scope of supply of your **BinGO!**.

Automatic dialing and disconnection

Additionally, a significant advantage of your **BinGO!** is the means by which access to networks is achieved. When using a modem/ISDN-card, you must expressly dial your Internet provider in order to send an e-mail, for example. On the other hand, the router decides independently (once configured, that is) if and how a connection to the Internet provider is established. If you submit an external WWW-address with your browser, for example, your **BinGO!** realizes that the requested address lies outside your own LAN, thus automatically establishes a connection with your provider and the Internet. This procedure is particularly economical as your router disconnects you after a predefined time subsequent to a cessation in external data exchange.

The same principle is applicable for conveniently accessing data from your home office. While running Windows, for example, you can connect a network drive with the server of your home office. Simply click the link in Windows Explorer and "surf" the server´s directories and files, just as you would your own hard disc. **BinGO!** takes care of dialing your home office.

Security

Similarly, with regard to security, **BinGO!** has a lot to offer. Your router contains integrated firewall mechanisms, and easily and economically fulfills all requirements concerning access security. It protects your network from unauthorized external access. This is made possible by **BinGO!**´s SAFERNET mechanisms, such as encoding, filtering and monitoring.

Configuration and maintenance

A range of options is available for the configuration of your **BinGO!**. Most methods of configuration are independent of the operating system of your PC.

The simplest method running Windows is with the help of the Configuration Wizard. The configuration assistant leads you step by step through the configuration and supports you with the most important settings on your router. In just a few minutes your **BinGO!** is ready to be used.

A range of other possibilities is available to refine the configuration, such as the Setup Tool, for example. This can be used independently of the operating system.

BinGO! can be remotely configured and administrated. As soon as your router is connected to the ISDN – even in its state of delivery, configuration settings can be carried out from a distant location (e.g. by the administrator of your head office).

You can thus leave the complete configuration of the system to be carried out by someone at HQ.

In summary The main advantages of your **BinGO!** can thus be summarized as follows:

- A connection with the Internet allowing all users in your LAN to avail of the usual Internet services (e.g. e-mail, WWW, file transfer)
- Connection to a head office, for example, (LAN-LAN connection) from a teleworking station or branch office allowing the easy exchange of data to and from HQ
- Common use of communications applications in the LAN (e.g. fax, answering machine)
- Simple configuration for you and remote administration from head office
- Independence from the operating system of your PC

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

1.2 Scope of Supply

BinGO! is shipped with the following:

- Cable sets/mains unit:
  - one cable (RJ-45) each for LAN and ISDN connection
  - serial cable
  - adaptor for serial cable
  - mains unit
- BinTec Companion CD
- Documentation:
  - user´s guide
  - Release Note, if required
- Additional information
  - Quick Install Guide (English and German)
  - license card
  - registration card

1.3 BinTec Companion CD

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

BRICKware

- DIME Tools serve to monitor and administrate your **BinGO!**.
- The Configuration Wizard leads you step by step through the basic configuration of **BinGO!**.
- Using the terminal program BRICK at COM1 or BRICK at COM2, you gain access to **BinGO!** via the serial interface.
- The DIME browser allows you to configure and administrate all BinTec routers in the network via a graphic window. Here you can view all SNMP tables and make adjustments to the variables.
- The Java Status Monitor allows you to request all systems information over an Internet browser.
- Remote CAPI Client:
  The Remote CAPI Client allows you to use communications applications on the standard CAPI interface (e.g. RVS-COM Lite).
- Token Authentication Firewall (TAF) program:
  This software package is required if you are using the security system from Security Dynamics.

More detailed descriptions can be found in our online handbook BRICKware for Windows.

RVS-COM Lite

In addition to BRICKware, your BinTec Companion CD contains RVS-COM Lite, communications software that allows you to avail of all the usual communications applications on your PC, such as an answering service facility, fax or data transfer. We explain how in chapter 3.6, page 60.

What else?

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

- The documentation in electronic form (see chapter 1.4, page 22)
- A copy of the router software (in its unconfigured state)

- UNIX-Tools
- Adobe´s Acrobat Reader
- Configuration examples

1.4 BinTec Documentation

Together with **BinGO!**, you will have received documentation partially in printed form and completely in electronic form (PDF, HTML). The electronic versions of the different documents are included on the BinTec Companion CD. In addition to your CD documentation, you can download all the very latest BinTec documentation from our WWW server at the address www.bintec.de. Here is a list of the available documentation:

- User´s guide (English and German, PDF or printed).
  This manual. The German version is only available in electronic form (PDF) and can, of course, be printed out if required.
- Leaflets to get **BinGO!** operational in just a few minutes (PDF and printed):
  - Quick Install Guide (English)
  - Kurzanleitung (deutsch)
- Reference manuals (English, PDF/HTML)
  - Software reference (PDF)
    Online reference with detailed information on functions described here, a reference for the internal SNMP table structures and the operation of the SNMP shell.
  - Extended Features Reference (PDF)
    Online reference for extra functions only available with a separate license (e.g. VPN).
  - MIB reference
    HTML document with short descriptions about all **BinGO!´s** SNMP tables and variables.
- BRICKware for Windows (English, PDF)
  User´s guide for Windows utility programs (BRICKware)
- Release Notes (English, PDF and /or printed)

Up-to-the-minute information and instructions concerning the latest software release, description of all changes undertaken since the previous release. In the Release Note Logic, you will find instructions to help you upgrade BOOTmonitor and/or Firmware Logic.

- UK info (English, PDF)
  Instructions for the operation of BinTec routers in Great Britain.

1.5 System Requirements

BinGO! can be configured from all conventional platforms. As a stand alone device, **BinGO!** is independent of a connected PC or its operating system. The router communicates with the PC over a LAN interface (10mbps) or a serial connection. Therefore, your router can be used in many and varied, operating-system environments, such as DOS, Windows, UNIX, AS/400, Mackintosh or Novell.

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

- PC with serial interface (V.24)
- Windows 95 or 98 or Windows NT 4.0 or higher
- An installed network card (10 mbps Ethernet)
- An installed Microsoft TCP/IP protocol
  Before we start with the configuration, we will explain how you determine whether the required settings have been made on your PC or, if necessary, how you make these settings yourself.
- High Color Monitor (at least 32000 colors) for the correct display of graphics.

1.6 Warranty

BinGO! is covered by a warranty period of 36 months from the date of purchase. For any warranty claims, consult your specialist dealer.

1.7 About this Manual

1.7.1 Contents

The manual is structured in the following way:

Chapter	Content
1: Welcome!	General introduction, scope of supply, warranty, table of contents
2: General Safety Precautions	General safety precautions
3: Getting Started	Directions to get **BinGO!** operational in a few minutes with the Configuration Wizard, and how to install and configure useful software
4: An Overview	Fundamental information concerning routers and networks
5: Connecting BinGO!	A basis for working with Setup Tool
6: Basic Configuration with Setup Tool	How to get **BinGO!** working with Setup Tool (parallel with Configuration Wizard)
7: Advanced Configuration	How to perform the more advanced settings of Setup Tool
8: Security Mechanisms	How to configure security mechanisms using SAFERNET, e. g. NAT (Network Address Translation) or CLID (Calling Line Identification)
9: Configuration Management	How to administrate configuration files and how to perform software updates
10: Troubleshooting	Important tips concerning fault detection
11: Technical Data	**BinGO!**´s technical data
12: Important Commands	A brief overview of the most important commands of the SNMP shell and BRICKtools for Unix

Chapter	Content
13: General Safety Precautions in 15 Different Languages	General safety precautions in 15 different national languages

1.7.2 Conventions Used in this Guide

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

Symbol	Meaning
	Points out useful and relevant tips and tricks
	Predicts potential pitfalls and explains how to avoid them
	Brings to your attention general and important points
	Explains required fundamental information

Symbol	Meaning
	Brings your attention to important safety precautions. Levels of danger are in accordance with ANSI: ■ Caution (indicates possible danger that, if unheeded, could cause material damage) ■ Warning (indicates possible danger that, if unheeded, could cause bodily harm) ■ Danger (indicates danger that, if unheeded, could lead to serious bodily harm or death)

In order to help you find and interpret the information in this manual, the following typographical elements are used:

Typography	Meaning
➤	Here you are requested to do something
■ –	Lists including two levels
MENU ➧ SUBMENU	Indicates menus and submenus in Setup Tool.
`Non-proportional (Courier), e. g.` `ping 192.168.1.254`	■ Indicates commands (e. g. in the SNMP shell) that you must enter as shown ■ Used for drawings of the Setup Tool
bold, italics, e. g. ***BigBoss***	Indicates example terms
bold, e. g. **➤➤ MIB**	Indicates terms that you can find in the glossary. (For online texts, click the double arrow)
bold, e. g. **biboAdmLoginTable,** **Windows Start menu**	■ Indicates fields in Setup Tool and MIB tables/variables ■ Indicates keys/key combinations and Windows terms
italics, e. g. *none*	Indicates values that can be entered or set in Setup Tool or MIB variables
Online: underlined	Indicates links

Welcome!

2 General Safety Precautions

The following section includes safety precautions you are strongly advised to heed when working with your router.

Transport and storage

- Only transport and store **BinGO!** in its original packaging or use other appropriate packaging to prevent against knocking and shaking.

Placement and operation

- Before setting up this product for operation, please bear in mind the instructions for the most appropriate ambient conditions (cf. technical data). Place on a firm and level surface.
- Condensation may occur externally or internally if this equipment is moved from a colder room to a warmer room. When moving the product under such conditions, allow ample time for the equipment to reach room temperature and to dry completely before operating.
- Make sure the power rating on the label of the mains unit complies with the local power source. **BinGO!** may only be operated with the original BinTec Communications mains unit (5 V DC). BinTec Communications AG accepts no liability for damages caused by the use of other mains units.
- Make sure to follow the correct cabling sequence, as described in the manual. Firstly, connect the LAN, ISDN and serial cables, then connect to the mains, and finally, turn on your **BinGO!**.
- Make doubly sure the cabling is correct – especially the ISDN and LAN cables – before you turn on **BinGO!**. **BinGO!**'s ISDN connection must not be connected with the Ethernet connection of your PC or hub, and neither should **BinGO!**'s LAN connection be connected with the ISDN connection.
- Use only the supplied cables. If you use other cables, BinTec Communications AG can not accept liability for any resulting damage.
- Arrange the cables so as they are not in the way, can not be tripped over and can not be damaged.
- Avoid connecting or disconnecting data lines during lightning storms.

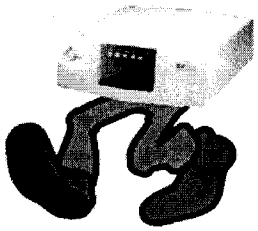
Operate according to the regulations

- **BinGO!** is intended for use in offices. As an ISDN multiprotocol router, **BinGO!** establishes ISDN connections depending on the system configuration. To avoid extra charges, you should carefully monitor the product.
- **BinGO!** corresponds to the relevant safety standards for the use of information technology equipment in offices.
- Operation of the system according to IEC 950/EN 60950 is only guaranteed when the roof of the housing is fitted (cooling, fire-protection, noise suppression)
- Ambient temperature should not exceed 50°C.
- Make sure no foreign objects (e.g. paper clips) or liquids get into the device (electric shock, short circuit).
- In an emergency (e. g. damaged housing or operating elements, liquid spills or the entry of foreign bodies), immediately remove the AC/DC adaptor and notify customer service.

Cleaning and repair

- The device should only be opened by trained personnel. Only service centers authorized by BinTec should carry out any repairs to the device. Your dealer will tell you where the service centers are situated. As a result of unauthorized opening and improper repairs, serious danger can result for the user (e. g. electric shock). In the event of such non-permissible opening of the device, the terms of the guarantee are suspended and BinTec Communications AG accepts no liability.
- Never use water to clean this device. Water spillage can result in serious danger for the user (electric shock) and cause considerable damage to the device.
- Never use scouring or abrasive alkaline cleaning agents on this device.

3 Getting Started



This chapter will help you to configure the most important applications for your local network or your single-user system as quickly as possible. To ensure the simplification of your configuration, the **Configuration Wizard,** a configuration assistant will support you. With its help, you will configure **BinGO!** in a matter of minutes.

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

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

In oder to set up these applications, you must:

- Firstly, set up and connect your **BinGO!** (chapter 3.1, page 35)
- Collect some important data (chapter 3.2, page 38)
- Install Windows software
  - install BRICKware for Windows (chapter 3.3, page 43)
  - configure **BinGO!** with the Wizard (chapter 3.4, page 45)
  - configure the Remote CAPI interface (chapter 3.5, page 58)
- Possibly perform additional settings on your PC (chapter 3.6, page 60)
- Install RVS-COM Lite (chapter 3.7, page 64)

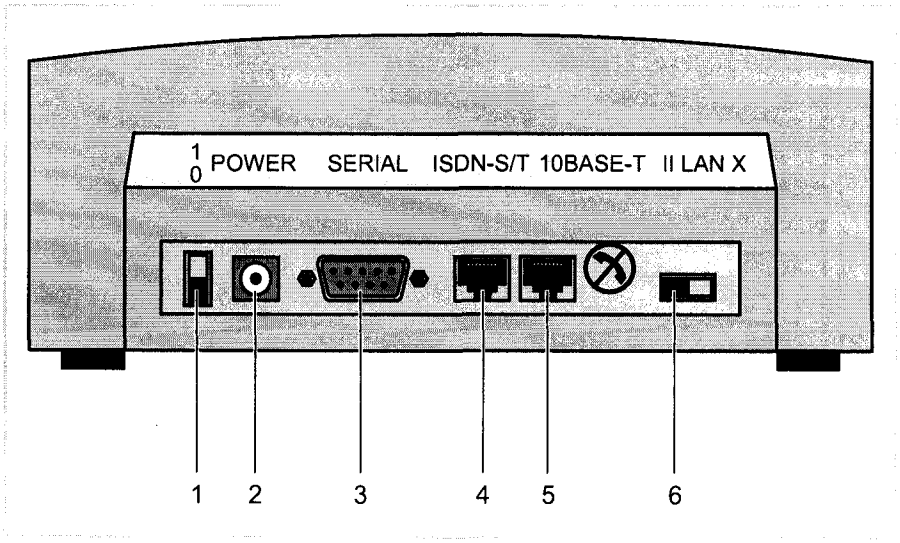
At the end of this configuration, we will explain to you how to test the configuration.

After finishing the basic configuration with the Wizard, you can explore further configuration possibilities in chapter 7, page 181.

If you would like to know how to carry out the basic configuration without the Configuration Wizard (e.g. if you are not using a Windows operating system), read chapter 8, page 227.

This chapter is designed to facilitate quick and easy initial configuration with a minimum of technical details. If, however, you want a little more background, then read chapter 4, page 75.

3.1 Setting up and Connecting



1	Power switch	4	S_0 port
2	Power supply	5	10Base-T interface (LAN)
3	Serial port	6	LAN switch

Figure 3-1: **BinGO!** rear view

Alternatively, you can connect **BinGO!** to the network card of your PC or, if you belong to a small network, to a hub. For the latter, you must merely set the LAN switch (6) at the rear of the device accordingly. How to set the switch is explained below.

Connect **BinGO!** to the ISDN over the ISDN-S/T connection. It makes no difference for **BinGO!** whether you use an ISDN socket, an ➤➤ **NTBA** adaptor or a PBX system as a distant terminal. If, however, you want to use functions specific to a PBX system, connect **BinGO!** to the PBX system. It is thus possible to block phone numbers or to check charges of phone numbers assigned to **BinGO!**.

Caution!

Use of the wrong mains adaptor can cause your router to malfunction!

- Only use the included mains unit (5VDC).
- Make sure that the rated voltage marked on the mains unit matches that of the local voltage supply.
- Never exchange the mains adaptor from **BinGO!** with that of **BinGO! Plus/ Professional**.

Caution!

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

- Only connect **BinGO!**'s LAN interface with the LAN interface of your PC/ hub, and **BinGO!**'s ISDN interface with the ISDN connection.

For connections, follow the following sequence:

- Place **BinGO!** on a firm level surface.
- Set the LAN switch at the rear of the device to:

  || if you connect **BinGO!** to your LAN-hub (cf. figure 3-1, page 35).

  X if you do not connect **BinGO!** to a LAN (because you have no hub), but directly to the network card of your PC (single user system).

  By using the node/hub switch (6), you can use the included 1 to 1 wired cable. A twisted pair (cross-over cable) LAN cable is not necessary.
- Connect the serial port of your PC (COM1 or COM2) with the serial interface of your router (3). Use the serial cable included in the scope of supply and if necessary the adaptor (9-pin on 25-pin).
- Connect **BinGO!** to your hub or to the network card of your PC (single user system). Connect one of the included cables (RJ-45) to the 10Base-T interface (5).
- Connect the second cable (RJ-45, also included) to **BinGO!**'s S_0 interface and your ISDN outlet.
- Connect **BinGO!**'s mains connection to the power supply with the included mains adaptor.

➤ Switch the router on with the power switch (1).

BinGO! performs a self-test. If all cables are correctly connected, the red LED ERR expires at the end of the test; and the green LED PWR (operating display) lights up.

3.2 In Advance of Configuration

3.2.1 Gathering Information

Before you start your configuration, you should keep at hand data for the following purposes – depending on what you want to do with **BinGO!**:

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

In the following table, we have included examples of what the values could look like. You should supplement the table with your personal data under the heading "your values". Then you can refer to the values later when needed.

Basic configuration

For the basic configuration of your **BinGO!**, you need information concerning your ➤➤ **ISDN** connection and your network environment:

Access Data	Examples	Your Values
ISDN telephone numbers (MSNs You received the ISDN numbers with your ISDN connection.	*967310* *967311* *967312*	
BinGO! IP Address	*192.168.1.254*	
BinGO! Netmask	*255.255.255.0*	

The following will be a description of the settings required for a connection of **BinGO!** to an ➤➤ **NTBA** adaptor. If you are connecting to a PBX system, make sure to take into account the special characteristics of your connections and if necessary, refer back to the documentation of your PBX system.

If you are not in a network or do not know how to assign IP addresses in a new network, then simply use our values. Otherwise, consult your system administrator.

For the ISDN numbers, it is sufficient to enter the final digits that distinguishes each number. If your dial numbers (➤➤ **MSNs**) are, for example, the following: ***967310***, ***967311*** and ***967312***, you need only consider the numbers ***10***, ***11***, and ***12***.

License cards

All you need now for the basic configuration is your license card. You should have received this together with your **BinGO!**. On the card you will find a serial number, mask and key which you will need to validate the functions of your **BinGO!.** You will also find the license number for the communications program RVS-COM Lite.

Internet access

If you want to access the Internet, you will need an Internet Service Provider (ISP). If you still haven´t got one, you can not continue with the configuration for Internet access. If you have your ISP, you will also have received your personal access data. The terms of the required access data may vary slightly from provider to provider. Basically, however, the kind of information required to establish your personal access remains the same. In the following table, the access data which your **BinGO!** also needs for a connection to the Internet is compiled.

Access Data	Examples	Your Values
Provider name	*GoInternet*	
Dial number The number with which you call your provider.	*1234567*	
Your user name	*MyName*	
Password	*TopSecret*	

If **BinGO!** is connected to a PBX system for which a leading zero is required for external calls, this leading zero must be considered when entering the dial number.

Some providers such as T-Online require some additional information:

Access Data	Examples	Your Values
T-Online number	*081512345678*	
Mitbenutzerkennung (other user code)	*007*	

Connecting to a corporate network

In order to connect with a WAN partner (e.g. corporate head office), you will need some pieces of information about the remote terminal that should take your call. Likewise, the remote terminal must know information about you. This data must be commonly agreed upon by the equipment on both sides of the connection.

Before every connection, **BinGO!** and the router at HQ check the incoming data to see if they should take the call. In order to protect the network against unauthorized access, acceptance of the call only takes place after correct authentication. This authentication is based on a common password and two codes that you and your partner use for the connection.

Access Data	Examples	Your Values
Partner name Code of head office	*BigBoss*	
Dial number Number of head office´s router	*0911987654321*	
Local name Your own code. Your partner (at head office) must enter this name as a WAN partner name on his router.	*LittleIndian*	
Password Common password for this connection	*Secret*	
Network address of your head office	*10.1.1.0*	
Netmask of your head office	*255.255.255.0*	

How to use other security mechanisms, e.g. authentication by means of the calling number (CLID) or the concealing of your own network to the outside (NAT) is explained in chapter 8, page 227.

If **BinGO!** is connected to a PBX system for which a leading "0" is required for external calls, this leading zero must be considered when entering the dial number.

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

3.2.2 What to Do in Your Windows Network

Now that you have gathered the information that **BinGO!** needs to know, you must ensure that your PCs in the network are properly configured. If not, you will need to adjust some settings.

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

Checking the TCP/IP Protocol

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

➤ Click the Windows **Start** button and point to **Settings** ➧ **Control Panel.**

➤ Double-click **Network.**

Windows 95/98

➤ Look for **TCP/IP** in the list of network components.

➤ If you can´t find the entry, install the TCP/IP protocol, as explained below.

Windows NT

➤ Select the **Protocols** tab and look for **TCP/IP Protocol** in the list of network components.

➤ If you can´t find the entry, install the TCP/IP protocol, as explained below.

Installing the TCP/IP Protocol

Windows 95/98

➤ Click **Add** in the dialog box **Network.**

➤ Select **Protocol** from the list of network components and click **Add**.

➤ Select **Microsoft** as the producer and **TCP/IP** as the network protocol, click **OK**.

➤ If you have an existing network, you may have to undertake further settings at this point. Consult your system administrator.

➤ If you are setting up a new network, click **OK**.

➤ Follow the on-screen instructions and then restart your PC.

➤ Repeat the installation for all PCs in the network.

Windows NT

➤ Click the **Protocols** tab in the dialog box **Network**. Click **Add**.

➤ Select **TCP/IP protocol** from the list network protocols. Click **OK**.

➤ If setting up a new network, click **Yes** to the question.

➤ Consult your system administrator if you have an existing network.

➤ Follow the on-screen instructions and then restart your PC.

In conclusion

➤ Repeat the installation for all PCs on the network where the LAN-LAN connection, Internet access or communications programs should be used over **BinGO!**.

3.3 Installing BRICKware Under Windows

- Close all Windows programs on your PC.
- Place your BinTec Companion CD in the CD-ROM drive of your PC. After a short time, the start window will automatically appear.
- If the start window does not automatically appear, click your CD-ROM drive in Windows Explorer and double-click **setup.exe.**
- Click **BRICKware** in the start window.

  The setup program starts.
- Specify the directory in which BRICKware should be installed.
- Click **Next**.
- Select your router: in this case, **BinGO!**.
- Click **Next**.
- Select the software components you wish to install. Simply choose from the preset list. Be careful not to lift the marking of **Configuration Wizard** in the **Administration Tools** group. Otherwise, you will not be able to carry out basic configuration with the assistance of the Wizard.
- Click **Next.**

  The files are copied. After a short time, a message window appears saying your old autoexec.bat has been saved.
- Click **OK**

  If you have installed DIME Tools, a window appears asking if you want DIME Tools to start automatically.
- Here you can click **No,** as this is not necessary for the basic configuration of **BinGO!**.

  A window appears in which you choose how to configure **BinGO!**.
- Click **Initial BRICK configuration with the Wizard** and then **Next.**

  Another window appears saying you must restart the PC in order to use the Java Status Monitor.
- Click **OK**

  A message appears heralding the Wizard.

➤ Click **OK**.

The Configuration Wizard starts.

3.4 Configuring BinGO! Under Windows

In chapter 3, page 33, you started the Configuration Wizard, now you can configure **BinGO!** with it.

The following configuration options are available:

- Basic Configuration of the Router
- Internet Access
- Connection to a Corporate Network

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

➤ Press **F1** or click **Help.**

If you have already used the Wizard to create an existing configuration, the Wizard can adopt the preset values. At the end, the Wizard transfers the existing configuration to the router and, in addition, saves it to your PC.

Furthermore, you can save the existing configuration file from **BinGO!** at the end of the configuration on the router (under old_cfg), as long as you have not forgotten the password.

If you are operating **BinGO!** behind a PBX system with a system connection, an entry must be made in Setup Tool in addition to the settings under Wizard. In the ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** menu, select *left to right*. The Wizard does not make these settings automatically as this is not the default setting. See also chapter 6.1.4, page 126.

Starting the Wizard

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

➤ Click the Windows Start menu, point to **Program** ➧ **BRICKware** ➧ **Configuration Wizard**.

The Start window of the Configuration Wizard opens:

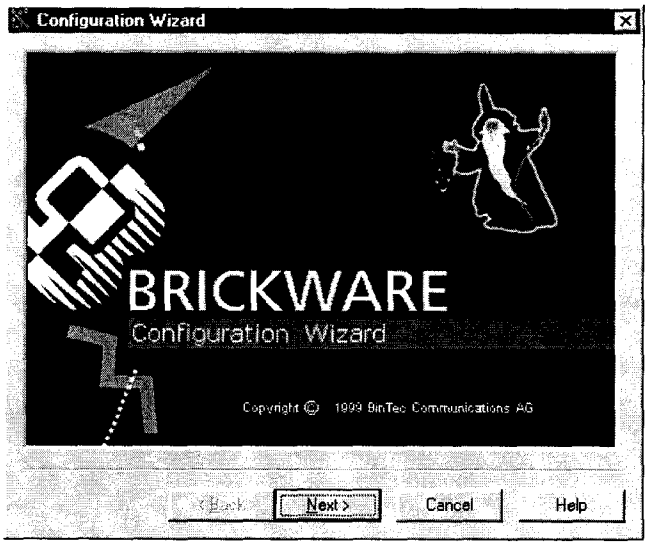


Figure 3-2: Start window of the Configuration Wizard

➤ Click **Next**.

Setting the configuration mode

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

➤ If you are not very familiar with networking technologies, choose **Quick**. The following is an explanation of how to configure using the Quick Mode.

➤ If you are already familiar with networking technologies and the configuration of routers, you could choose **Expert.**

In this mode, you could:

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

➤ Click **Next**.

➤ Click **Next**.

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

Making a serial connection

➤ Click **Next.**

The Wizard establishes a connection to **BinGO!**. After that the router is re-started and the type of router identified: in your case, **BinGO!**.

If the Configuration Wizard can not establish a connection or an error message appears:

➤ Make sure **BinGO!** is correctly connected.

➤ If it is, check to see there is a terminal program (e. g. Hyperterminal) running and occupying the serial interface. If there is, close the program.

➤ Check if **BinGO!**'s Baud rate has changed. The product is shipped set with 9600 bit/s. If you have altered the Baud rate, reset to 9600 Baud.

➤ Before you start the Wizard, **BinGO!** has to be restarted. If this did not happen, disconnect from the mains, wait a moment until the LEDs stop blinking.and then reconnect to the mains.

➤ Click **Next**.

➤ Click **OK** and then **Next**.

Selecting configuration points

➤ Select one or more of the following options:

- **Basic Router Settings**, (chapter 3.4.1, page 48)
- **Internet Access**, (chapter 3.4.2, page 52)
- **Connection to a Corporate Network**, (chapter 3.4.3, page 53)

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

➤ Click **Next**.

3.4.1 Basic Router Settings

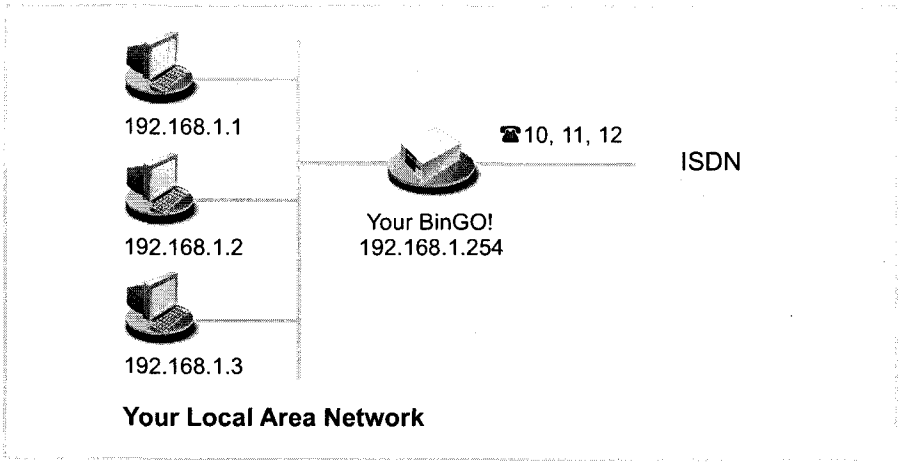


Figure 3-3: **BinGO!'s** basic configuration

Caution!

All BinTec routers are shipped with the same user names and passwords. As long as the password remains unchanged, they are unprotected against unauthorized use.

➤ It is thus essential that you change your password when requested to do so.

➤ Firstly, enter your license data. You will find this on the license information card. Click **Next**.

The Wizard checks the settings of the PC and thus derives proposed values for the configuration.

An unconfigured network

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

➤ Click **Next**.

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

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

➤ Deactivate the field **Use this Configuration.**

➤ Next, enter **BinGO!**'s IP address and the corresponding netmask, e.g. *192.168.1.254* and *255.255.255.0*. Click **Next.**

➤ State whether you want to configure **BinGO!** as a DHCP server. If you do, enter the IP address range for your PCs and define the number of IP addresses to be assigned by **BinGO!**.

After configuration, remember to assign your PCs with fixed IP addresses if no DHCP server is configured (cf. chapter 3.4.3, page 53).

An already configured network

➤ In a network where fixed IP addresses have already been configured, the Wizard asks you in the **Router IP Address** window for **BinGO!**'s IP address and the corresponding netmask. Enter the values, e.g. *192.168.1.254* and *255.255.255.0*.

➤ Click **Next**.

➤ Enter a new password for your access authorization.

➤ Click **Next**.

➤ Enter the phone numbers of your ISDN port that you want to use with **BinGO!**: enter a phone number in the field **Phone numbers** and click **ADD**. Repeat the entry for all other numbers (cf. figure 3-4, page 50).

BinGO!

User´s Guide

Installation and Configuration

Purpose This manual explains the installation and initial configuration of **BinGO!** with the Software Release 4.9.3. It is highly recommended that you read our Release Note containing the latest information and instructions for the most current Software Release – especially if you are performing a software update to a higher level. The latest Release Note is always available at www.bintec.de.

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

The information in this manual is subject to change without notice. Additional information, including changes and Release Notes for **BinGO!**, can be retrieved from **BinGO!** at www.bintec.de.

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

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

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

Guidelines and standards **BinGO!** adheres to the following guidelines and standards:

- Voltage guidelines 73/23/EWG according to EN60950
- Adheres to German safety regulations standards

- Interference resistance according to EN50082 -1/1.32
- Class B interference emissions according to EN55022 /-8.94
- Electro-magnetic tolerance according to EU guideline 89/336/EWG
- CE-symbol for all EC countries

Registration:

- BZT D 133451J (CE and German registration)
- BZT D 133457J (EG design test certificate)
- BAKOM (registered)
- CE 0188X (France adheres to the CE guideline)
- EN50082, EN55022
- EN60950

In addition to the CE guideline, **BinGO!** satisfies the ISDN requirements in France and may be connected to Euro-Numeris.

How to reach BinTec

By ...	At the telephone number or address
Telephone	+49 911 96 73 0
Fax	+49 911 688 07 25
Mail	BinTec Communications AG Südwestpark 94 D-90449 Nürnberg
Internet	www.bintec.de

Version 1.6
Document #71000B
March 1999

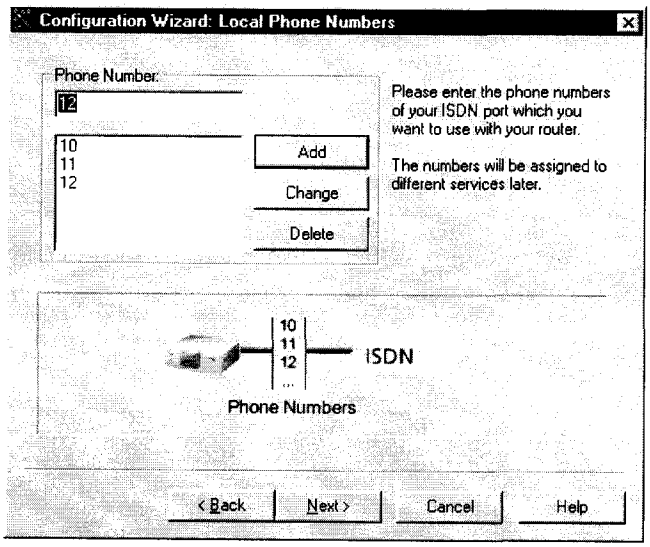


Figure 3-4: Entering dial numbers in the Configuration Wizard

➤ Click **Next.**

The Wizard automatically assigns the numbers to certain services (more on services and users in chapter 4.3, page 80. This allocation can only be changed in the Expert Mode (figure 3-5, page 54).

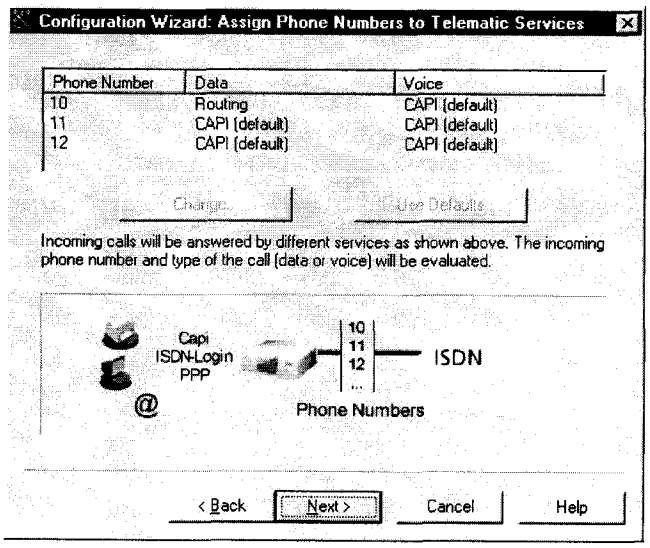


Figure 3-5: Allocation of dial numbers in the Configuration Wizard

➤ Click Next.

The basic configuration is now complete. A summary of the values set in the previous steps appears.

Additionally, the following options are available in the Expert Mode:

- Changing the system data, e.g. contact, name and location of **BinGO!**
- Specifying the IP address of a DNS server
- Receiving system time from a source other than ISDN
- Enabling isdnlogin
- Defining different system passwords
- Assigning communications applications to different users and different phone numbers
- Setting more extensive filters (NetBIOS, CAPI and TAPI clients)
- Recording of system messages

3.4.2 To the Internet with BinGO!

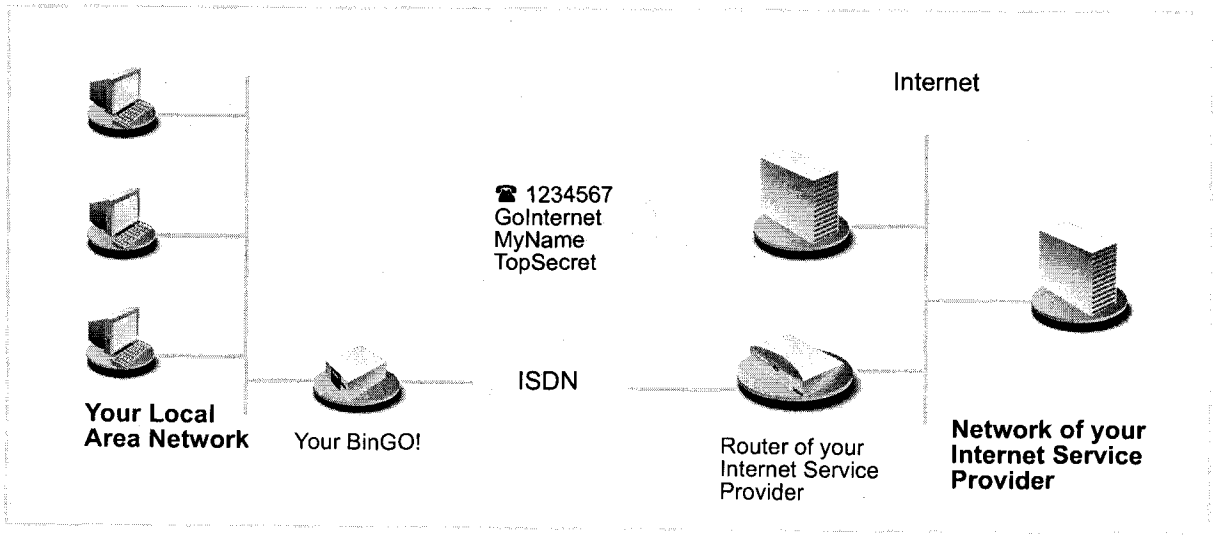


Figure 3-6: **BinGO!** and its Internet provider

➤ Click **Next.**

A message window appears.

➤ Click **Next**, after reading the information in the window.

➤ Firstly, define your Internet provider. Choose between the following:
- Compuserve
- T-Online
- Spacenet
- another provider

➤ Click **Next.**

➤ Enter the name of the provider (if your provider´s name is not listed) and its corresponding dial number, e. g. ***GoInternet*** and ***1234567***.

➤ Click **Next.**

➤ Type in your user name and corresponding password, e. g ***MyName*** and ***TopSecret***.
If your provider is T-Online, also enter the T-Online password and number, as well as the "Mitbenutzerkennung" (other user name) and the "Anschlußkennung" (connection code), e. g. ***081512345678*** and ***0001***.

■ Click **Next**.

The configuration of your Internet connection is complete. A summary of the previous points you have set appears.

Additionally, the following points are covered in Expert Mode:

■ Logging IP connection data

■ Enabling data compression

■ Defining when you receive ISDN charging information and thereby specifying exactly when a connection is terminated (dynamic and static Short Hold)

3.4.3 Connecting BinGO! to a Corporate Network

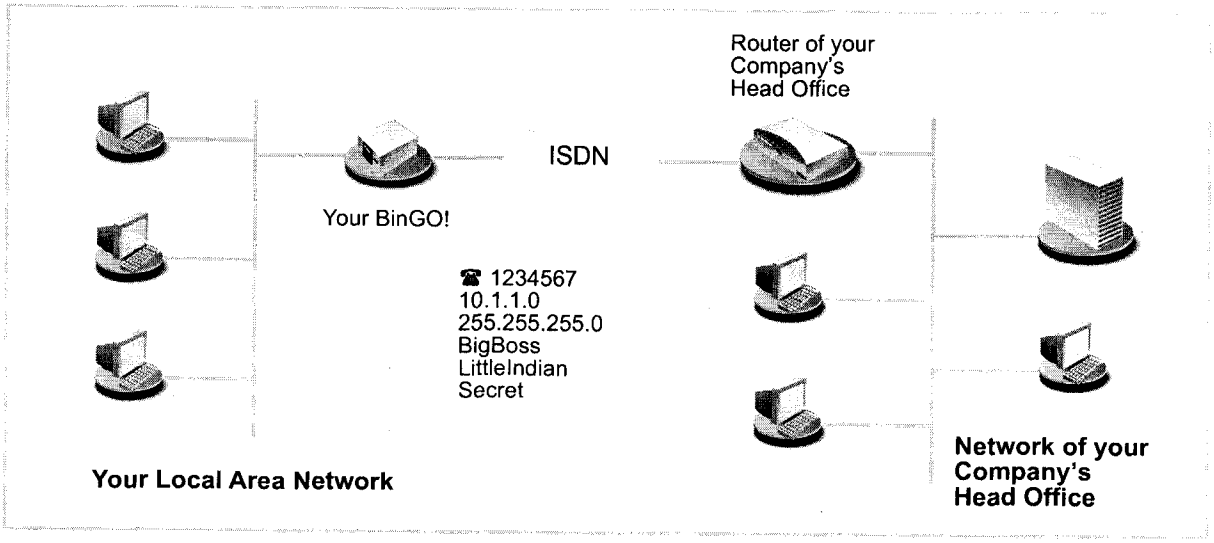


Figure 3-7: **BinGO!** and your head office

➤ Click **Next**.

A message window appears

➤ Click **Next**, after reading the information in the window.

➤ Firstly, enter the name of your WAN partner (e. g. your head office) and the corresponding dial number e.g. ***BigBoss*** and ***0911987654321***.
The name of your WAN partner must be the same name as your partner uses as a local name.

➤ Click **Next**.

➤ Enter your local name and your common password, e. g. ***LittleIndian*** and ***Secret***.
Your local name must be the same name as your partner uses for you as a WAN partner.

➤ Click **Next**.

➤ Add a route to your head office:
If you have not configured Internet access, choose **Use Default Route**.
If you have configured Internet access, then enter the route yourself:
Click **Add**. Enter the network address and netmask, e. g. ***10.1.1.0*** and ***255.255.255.0***. By setting the route, you are fixing the path connecting you to your WAN partner. (e. g. head office) (cf. figure 3-8, page 55).

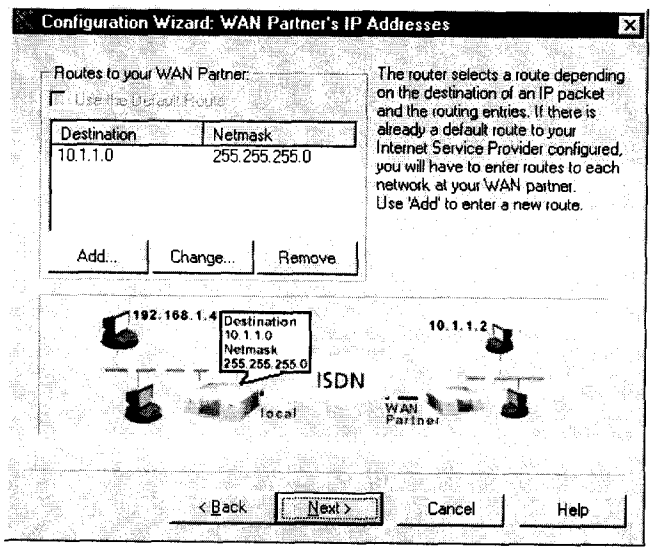


Figure 3-8: Route to the WAN partner in the Configuration Wizard

Each route represents a network or subnet of your WAN partner. A route is fixed by IP addresses/network addresses and netmasks.

Instead of the network address, you can choose and enter any IP address from your partner´s network. By means of the corresponding netmask, Configuration Wizard automatically finds out the network address.

➤ Click **OK**.

➤ If the network of your head office comprises several smaller networks (subnets) and you want access to each of these subnets, you must enter a route for each one of them. (cf. chapter 4-3, page 91).

➤ Click **Next**.

The configuration of your WAN partner is complete. A summary of the previous points you have set appears.

Additionally, the following points are covered in Expert Mode:

- Configuration of an automatic callback function, so that only one of the two partners takes the telephone charges.
- Checking the number of the caller: Calling Line Identification (CLID)

- Keeping a record of IP connection data
- Activating Back Route Verify for the prevention of the import of manipulated data packets
- Data compression, encryption and channel bundling
- Defining when or if you receive ISDN charging information, and specifying exactly when a connection is terminated (dynamic and static Short Hold)

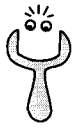
3.4.4 Completing Configuration

➤ Click **Next**.

➤ Select **Save the former configuration on the router** to save an existing configuration before overwriting.

➤ Click **Finish** to conclude configuration.

The Wizard logs onto **BinGO!.** An existing configuration is saved on the router as old_cfg. The new configuration is transferred to **BinGO!** and additionally saved on your PC under the name brick.cfg in the BRICK directory. After a short time, a message appears saying the configuration is complete.



If an error message appears saying the Wizard could not log onto the router, because the password has changed:

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

The Wizard will try to login to **BinGO!**.

➤ If this fails, enter the password again or if you click **Unknown,** the old configuration will be overwritten, the new one saved on the router.

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

The old configuration will be overwritten and the new one saved on the router.

In any case, the Wizard saves your new configuration on the PC, even if errors have occurred during transmission to the router.

The configuration file saved on your PC can be further configured with the Wizard.

➤ Click **OK**.

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

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

A message window opens inquiring if you want to install the CAPI/TAPI server.

➤ Click **Yes**.

The Remote Clients Configuration window opens:

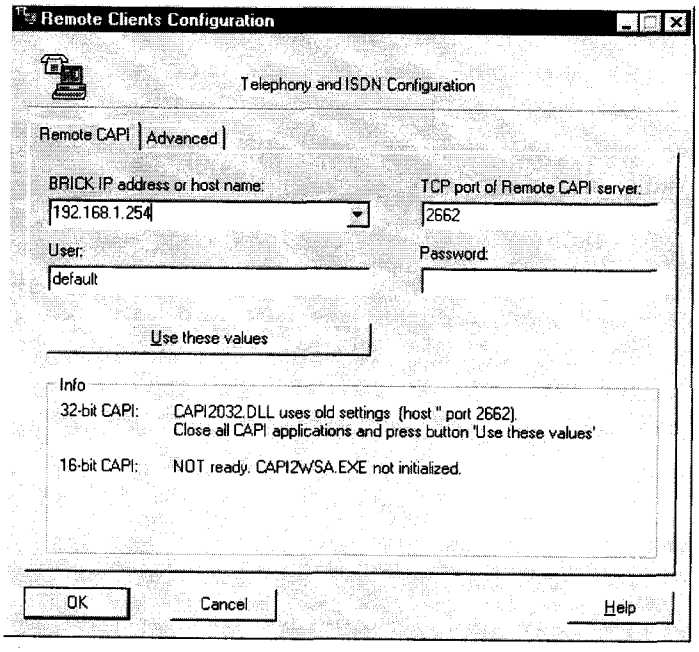


Figure 3-9: Remote clients configuration

3.5 Configuring the Remote CAPI Interface

Enter **BinGO!** as CAPI server in the **Remote CAPI** configuration program.

The **BinGO!** CAPI server makes the following possible:

- Operating communications applications on every PC in the network (fax services with RVS-COM Lite)
- From several PCs simultaneous ISDN access over communications applications.

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

You have already installed BRICKware on the first PC and have opened the configuration window for the Remote CAPI configuration (cf. figure 3-9, page 57). You can proceed with chapter 3.5.2, page 58. For all PCs in the network, you will have to install the CAPI configuration program, as described in chapter 3.5.1, page 58.

3.5.1 Installing the CAPI Configuration Program

➤ If you haven't already done so, install BRICKware as described in chapter 3.3, page 43 up to the window **Configure your BRICK and this PC**.

➤ In the window **Configure your BRICK and this PC**, click **Keep old BRICK configuration**.

➤ Click **Next.**

The Remote CAPI configuration window appears (cf. figure 3-9, page 57)

3.5.2 Configuring Remote CAPI

➤ Enter **BinGO!**'s IP address, e.g. ***192.168.1.254*** in the Remote CAPI tab.

➤ If you have used Quick Mode in Configuration Wizard, retain the entry **default** in the **User** field.

➤ If you have configured several users in the Expert Mode of the Configuration Wizard, then enter your user name and password. The rights you have set for these users during configuration are thereby valid on the current PC.

➤ Click **Use these values**.

A message appears "Remote CAPI is ready".

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

- **BinGO!´s** IP address is correct
- You have entered a valid user name
- The right port number 2662 has been entered
- Your PC has been configured but perhaps has no IP address (see chapter 4.4, page 84)

➤ If no error message appears, click **OK**

➤ Repeat the Remote CAPI installation on all PCs in the network on which you want to enable communications applications (e.g. fax)

You can find a more detailed description of the Remote CAPI configuration in BRICKware for Windows. An explanation of Multibrick for Windows NT is also included there, which allows you to define several BRICKs in the network as CAPI servers.

3.6 Configuring a PC

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

- If you have not configured **BinGO!** as a DCHP server with the Wizard, and the PC has not yet got an IP address, you will have to (according to chapter 3.6.1, page 60):
  - fix the IP addresses now
  - show the PC "the way out" (Gateway, DNS server)

  If you have assumed the Wizard´s standard settings and have configured your PCs as DHCP clients, you can disregard chapter 3.6.1, page 60. In this case, **BinGO!** automatically supplies the necessary information.
- If you have configured a connection to a corporate network, you will certainly want to reach PCs from the partner LAN (e.g. head office) via Windows. To do this, you must proceed as described in chapter 3.6.2, page 61.

3.6.1 Telling the PC IP Addresses, Gateway and DNS Server

If you have not configured **BinGO!** as a DHCP server and your PCs have not yet got an IP address, you must now tell the PCs at which IP address they can be reached. Furthermore, you must tell the PCs the way out, how to get to the Internet. Proceed as follows:

➤ Click the Windows **Start** button, and then point to **Settings** ➧ **Control Panel**.

➤ Doubleclick **Network**

Windows 95/98

➤ Click **TCP/IP** ➧ **Properties**.

➤ Enter the unique IP address of your PC and the netmask in the **IP address** tab, e. g. *192.168.1.1* and *255.255.255.0*.

➤ Enter **BinGO!**´s IP address in the **Gateway** tab, e. g. *192.168.1.254*. Click **Add**.

➤ If you do not have your own DNS server, enter **BinGO!**'s IP address in the **DNS Configuration** tab under **DNS Server Search Order,** e. g. *192.168.1.254*.

Windows NT

➤ Select the **Protocol** tab. Click **TCP/IP Protocol ➧ Properties**.

➤ Click the **IP Address** tab and **Specify an IP Address**, then type in the IP address, netmask and default gateway, e. g. *192.168.1.254*, *255.255.255.0* and *192.168.1.1*. As default gateway, type **BinGO!**'s IP address.

➤ In the **DNS** tab, click **Add** in the **DNS Server Search Order** and type in **BinGO!'s** IP address, e. g. *192.168.1.254*.

And finally,

➤ Confirm all entries and restart your PC.

➤ Repeat the procedure for all the PCs in your network.

3.6.2 Finding PCs on your Partner's Network

By this stage, you have done all you need to on your **BinGO!** to connect with your partner's network. Now you may want to establish contact with a PC from your partner's network, let's say with ***BossPC***.

First, a little background. Every PC in your LAN or in the network of your partner requires a unique address, the IP address. In addition to the use of IP addresses, an alternative means of addressing PCs is by computer or host names (such as ***BossPC***). Computer names are used especially in Windows networks. PCs, however, only understand IP addresses and not names. Thus, it is necessary for the names to be translated (resolved) into their corresponding IP addresses. (chapter 4.5, page 87) Typical examples of services capable of such name resolution are the DNS or the WINS servers. As you normally do not want to set up your own DNS server in a small network, there is an alternative way of resolving host names into their IP addresses: the LMHOSTS file.

In the LMHOSTS file, IP addresses are arranged with their computer names in tabular form. If, for example, you are looking for ***BossPC***, a PC located in your partner's network (e.g. HQ), your PC asks its LMHOSTS file for the corresponding IP address and in this way is able to find the PC.

Caution!

The following configuration can lead to increased connections and higher telephone bills. The conditions that lead to establishing connections are largely dependent on the respective network configuration. You should be aware that when you connect a network drive, in particular, that regular requests will increase the number of connections made.

➤ To avoid unintentional charges, it is essential that you monitor **BinGO!**.

The following process can only be applied if you have not configured extensive NetBIOS filtering in the Expert Mode of the Configuration Wizard. Otherwise certain Windows functions, such as network drive connections, can not be used.

If you require access to the partner network for several PCs in your network, you must save the arrangement of IP address to name on each of these PCs.

Additionally, bear in mind:

- that you and your WAN partner are in the same domain or working group
- that you receive the necessary admission to PCs in the network of your partner from that WAN partner. If in doubt, ask your systems administrator.

You can also register with the Windows NT domain of a partner network. To test such a configuration, BinTec has made available a test access. You can find out more about configuring this access in the FAQ section at www.bintec.de: BRICK/Test access "Router – Router".

By editing the LMHOSTS text file, tell your PC the IP address of ***BossPC*** as follows:

➤ Click the Windows Start button and then point to **Find ➧ Files or Folders....**

➤ Type in `lmhosts.*`.

➤ Click **Find now**.

➤ Double-click the file name, then open the file with a text editor.

➤ Type in the IP address of the PC in the partner network, followed by a tab or space, followed by the name of the PC, e. g. `10.1.1.1 BossPC`. Save and close the file.

➤ Repeat the procedure for each PC in the partner network that you want to reach over Windows.

➤ Click the Windows Start button and then point to **Find** ➧ **Computer...**.

➤ Type in the name of the PC, e. g. ***BossPC***, and click **Find now**.

The name of the PC appears below after a moment.

Creating a shortcut on the Desktop

➤ So that you do not have to look for the PC every time you restart, right-click the PC icon in the Computer window and click **Create Shortcut**.
You are then asked if you want the shortcut to be placed on the desktop.

➤ Click **Yes**.

Now you can connect with the PC ***BossPC*** on your partner´s network at any time.

Connecting a network drive

Alternatively, you could establish a network drive connection:

➤ Open Windows Explorer, click **Tools**, then **Map network drive**.

➤ Specify the drive and type in the path, e.g. ***\\BossPC***.

➤ Click **Reconnect at logon**.

➤ Click **OK.**

3.7 Faxing and Answering Services with RVS-COM Lite

Let´s fax something. But how?

After you have successfully configured your PC and **BinGO!**, install RVS-COM Lite. With RVS-COM Lite it is possible to:

- Send and receive faxes from your PC using **BinGO!** over the network.
- Configure an answering service.
- Data transfer services and eurofile transfer services.

In the following sections, we will describe how to teach your PC and **BinGO!** how to fax with RVS-COM Lite (version 1.56) and how to set up an answering service facility.

With **BinGO!** you have received just one license for RVS-COM Lite. If you want to install RVS-COM Lite on more PCs, contact RVS Datentechnik GmbH. You can retrieve the address from RVS-COM Lite´s online help.

3.7.1 Installing RVS-COM Lite

➤ Place your BinTec Companion CD in the CD-ROM drive of your PC.
The start window should appear automatically.

➤ If the start window does not open automatically, click your CD-ROM drive in Windows Explorer and double-click **setup.exe**.

➤ In the start window, click **RVS-COM Lite**.
The setup program starts.

➤ Enter your RVS-COM license number. The number is on your license card.

➤ Click **Install.**
The start window opens.

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

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

➤ Click **Finish.**

The start window of the installation assistant is now started.

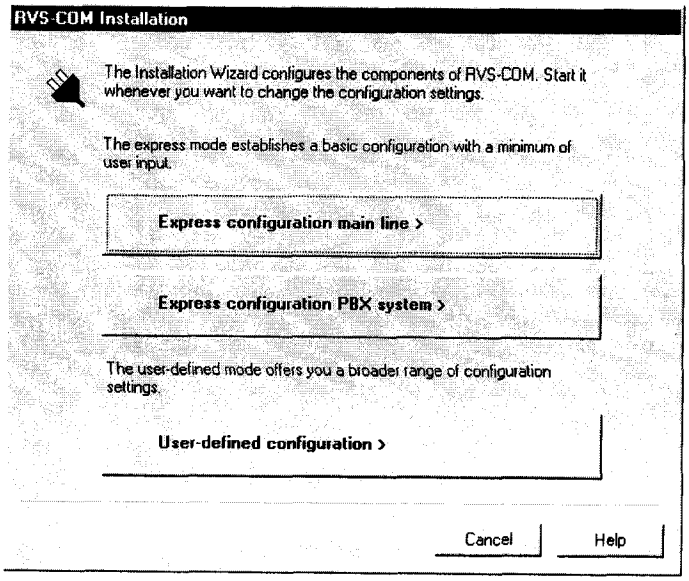


Figure 3-10: Start window of the configuration assistant of RVS-COM Lite

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

➤ make sure **BinGO!** is connected to your ISDN connection.

➤ make sure your Remote CAPI configuration is configured as described in chapter 3.5.2, page 58.

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

➤ If **BinGO!** is connected to a main line (e.g. NTBA adaptor), click **Express configuration main line**.

➤ If **BinGO!** is connected to a PBX system, click **Express configuration PBX system**.

➤ Click **Next**.

A message appears saying you have configured RVS-COM for operation with an ISDN adaptor with a CAPI interface.

➤ Click **Next**.

➤ If a message appears saying you should change the dialing properties (e.g. area code, exchange number). Adjust the settings. (cf. figure 3-11, page 66)

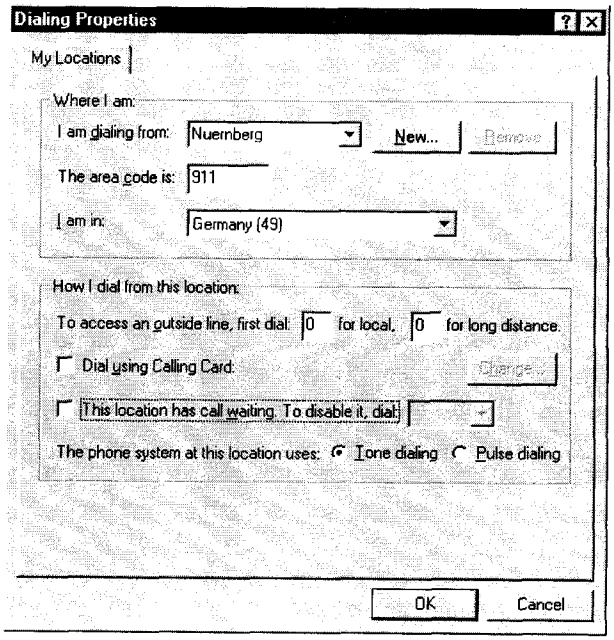


Figure 3-11: Dialing properties

The area code must be given without a leading "0".

You only need the exchange number if you are operating **BinGO!** on a PBX system. Normally, the exchange number for local and long-distance calls are the same (see figure 3-11, page 66),

➤ When you have adjusted the settings, click **Apply**, and then **OK**.

➤ If you selected **Express configuration main line,** enter the dial number of your ISDN connection. Select one of the numbers you have already entered with the Wizard. You can only enter one number with the configuration assistant. Later, it is possible to add more.

➤ If you selected **Express configuration PBX,** enter in the next two windows the extension and ISDN phone numbers (point to multipoint) and dial number and prefix of the extension number (point to point)..

If you are operating **BinGO!** on a PBX system, you must ensure the digit comparison is set properly in Setup Tool (these entries are not made automatically by the Wizard). **In CM-1 BRI, ISDN S0 ➧ Incoming Call Answering** the incoming number must be set to left to right (DDI) for the comparison of numbers, as this is not the default setting. See chapter chapter 6.1.4, page 126.

➤ Click **Next**.

➤ Click **Next** in the following windows and finally **Finish.**

The configuration with the Wizard is now complete.

3.7.2 Configuring RVS-COM Lite

In the following section, the numbers which were set with the Wizard have to be allocated to different services (fax, answering service). The following picture illustrates which number in our configuration example is to be used for a certain facility.

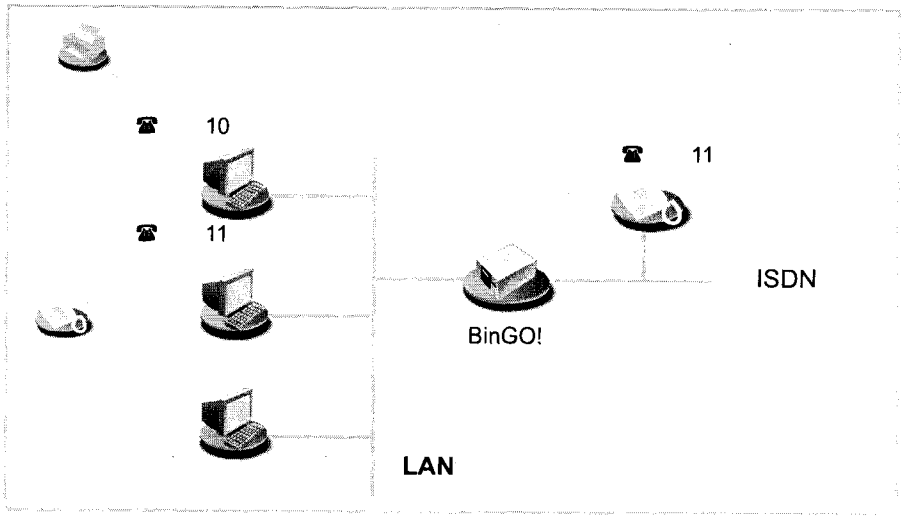


Figure 3-12: Scenario: 1 Telephone, 1 PC with fax and answering service facility

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

- Click the Start button in the Windows menu and point to **Program ➧ RVS-COM Lite ➧ CommCenter**.
- Click **Add** in the **Phone Numbers** tab to enter more phone numbers. Enter the numbers that you have already used with the Wizard (cf. figure 3-13, page 69)

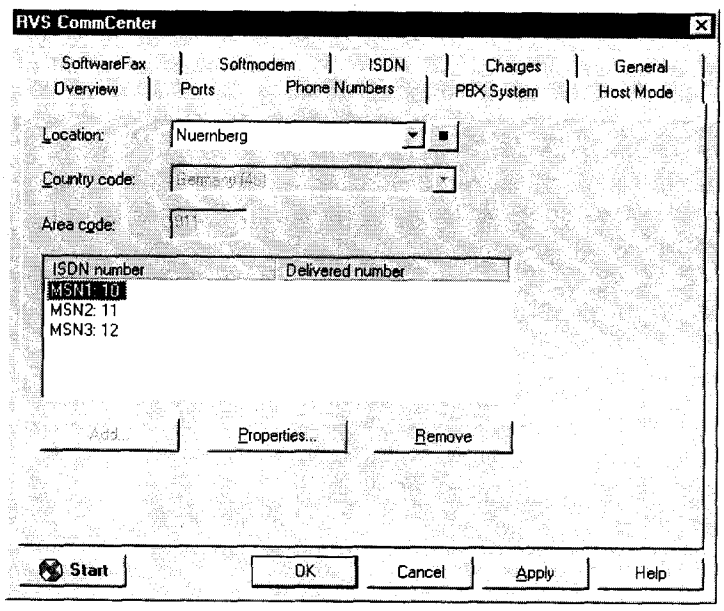


Figure 3-13: Phone number configuration in RVS-COM Lite

➤ Click **Apply** after you have entered all the numbers.

➤ Click **Properties** in the **Ports** tab to allocate the numbers to a service (cf.figure 3-14, page 70)

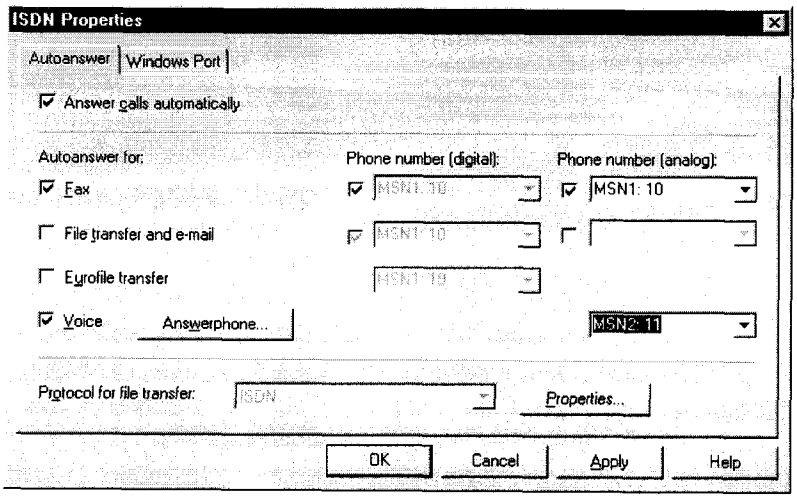


Figure 3-14: Allocation of phone numbers to services in RVS-COM Lite

- Allocate the first phone number to the fax service, the second number to voice (answering machine).
- Leave the other services free (file transfer, eurofile transfer).
- To adjust the answering service facility, click **Answerphone** and change the recorded message if necessary and the number of rings before the call is taken.
- Click **OK.**
- Click **Apply** and finally **OK.** In the list of connections, the message appears: "ISDN: waiting for call." CommCenter is ready to take calls and faxes.

3.8 Testing your Configuration

Your configuration is now complete! Now let's make sure everything works.

3.8.1 Testing Internet Access

➤ Configure your browser if you have not done so already. If you have received the IP address of a proxy server from your Internet provider, you can enter the address. Make sure you configure a connection over your local network (figure 3-15, page 71).

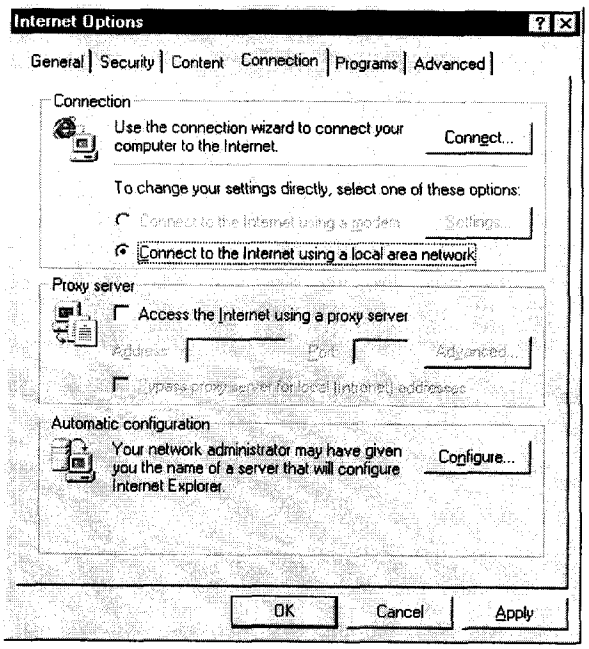


Figure 3-15: Browser configuration for an Internet connection (example using Internet Explorer)

➤ Try contacting us by typing in www.bintec.de in your browser.
The home page BinTec Communications AG appears.

3.8.2 Sending and Receiving E-Mails

Open an account in the e-mail program if you have not already done so. You should have received the servers for incoming and outgoing mail from your Internet provider. Make sure you configure a connection over your local network (figure 3-16, page 72).

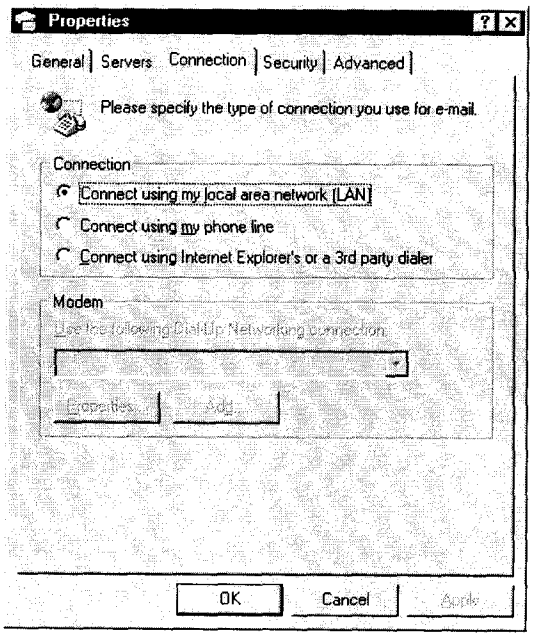


Figure 3-16: Configuration of the e-mail program (example from Microsoft Outlook Express)

➤ Just send an e-mail to a good friend or – if you like – send one to BinTec! Use the e-mail address testmail@bintec.de and type in Test Mail as the subject.

You will receive an immediate reply from us to reassure you that the mail arrived successfully.

3.8.3 Sending a Fax

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

➤ Click the Windows **Start** button and then point to **Program ➧ RVS-COM Lite ➧Create new fax.**

The window **RVS fax: Recipients** appears.

➤ Type in the name of the receiver and the call number, e.g. *9119673.*

➤ Click **Next**.

➤ Type in a subject and a short message, e.g. Test Fax.

➤ Click **Next**.

➤ Select the cover page **Normal**.

➤ Click **Next**.

➤ If you want, you can attach a file to the fax.

➤ Click **Next** and finally **Finish** to send your fax.
The RVS Mail Spooler appears and informs you about the status of the fax being sent.

If you have sent a fax to yourself, you should receive it right away (figure 3.8.4, page 74). This is the best way to assure yourself your fax application is working properly.

You can fax from a program of your choice (e.g. Word):

➤ Write your fax message.

➤ Print the document by using the printer driver RVS FAX from RVS-COM Lite. Point to **Print** in the **File** menu and set the printer driver **RVS Fax.**

➤ Confirm the print request.

➤ Afterwards, the **RVS Fax: Recipient** window opens, which we have just looked at.

3.8.4 Receiving a Fax

As we are dealing with a softfax solution when faxing with **BinGO!** and RVS-COM Lite, the fax software must always be started when you want to receive faxes. On installing RVS-COM Lite, RVS-COM is stored in the Windows Task-bar – as long as you do not close the program, RVS-COM is available at all times.

All incoming and outgoing faxes are displayed in the RVS-COM inbox; as are voice messages you receive over your RVS-COM Answerphone.

➤ Click the Windows **Start** button and then point to **Program ➧ RVS-COM Lite ➧ Inbox**.

All faxes and voice messages received are listed in the inbox

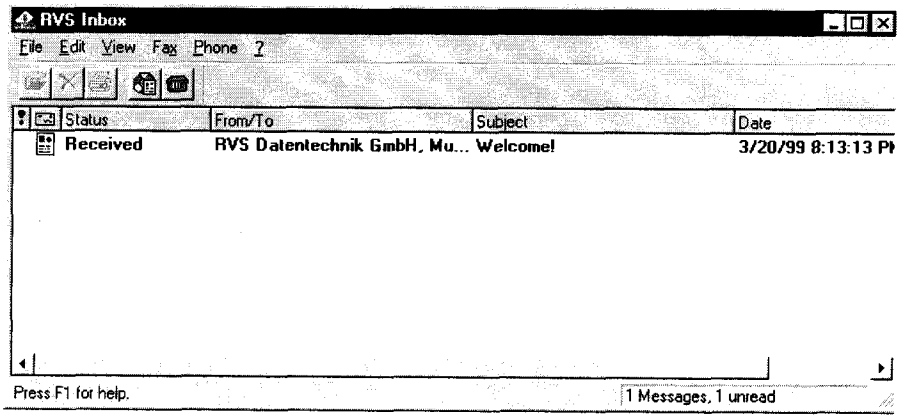


Figure 3-17: RVS Inbox

➤ Double-click the fax entry to open your received fax messages (including the test message from RVS-COM).

The RVS FaxViewer opens. If you have sent yourself a fax, you should find it in the inbox.

4 An Overview

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

If, in the course of the configuration in chapter 3, page 33, you asked yourself the questions listed below or similar ones, you should read this chapter thoroughly. It will not only contribute to your understanding of the chapters to come, but it will also help you to understand the wider context, as well as some of the connections made in the last chapter.

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

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

4.1 The Basics of ISDN

What is ISDN?

ISDN means Integrated Digital Services Network and describes a telecommunications service which is supported worldwide.

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

To transmit data over ISDN, most frequently, the so-called ➤➤ **PPP** protocol is used, (Point-to-Point Protocol).

Every ISDN basic connection (S_0 connection) consists of three channels:

- 2 B-channels
- 1 D-channel

B-channel channel bundling

Data transmission takes place over the B-channels (voice, text, data). Each B-channel has a data transmission rate of 64 kbps. Since you have two B-channels, you can, as you probably know, make telephone calls simultaneously from two different telephones. **BinGO!** can also use both B-channels at the same time in order to exchange data with two different opposite terminals. You can even combine both B-channels in order to transmit data to just one opposite terminal using the collective capacity of both B-channels. Naturally, you must pay for the use of both channels; your data transmission, however, takes half the time it would need using just one channel. You can do this with **BinGO!** by using the function channel bundling. You can only configure channel bundling with Setup Tool. (cf. chapter 7.2.2, page 194)

D-channel

The D-channel transfers control data with a data transmission rate of 16 kbit/s. Such information includes, e. g. the identification of the caller (Calling Party's Number) and the party called (Called Party's Number) by the dial numbers. For example, you can configure your router to accept only calls from certain partners. If the dial number being transmitted over the D-channel does not match a pre-defined number, the call is not taken. This security mechanism is known as Calling Line Identification – or CLID. Other authentication mechanisms check

the user name and password of the opposite terminal. The latter checks take place by means of ➤➤ **PAP/CHAP** authentication.

CLID can only be set in the Expert Mode of the Wizard or in the Setup Tool. PAP/CHAP authentication, however, has already been set in the Quick Mode of the Wizard.

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

Charging information and Short Hold

Many ISDN connections make available charging information. Mostly, you receive this information at the end of a connection, some ISDN connections, however, provide the information even during the connection (AOCD: often it is necessary to apply for this function). **BinGO!** is able to evaluate this information allowing you to save money.

Normally, (in Quick Mode) **BinGO!** is configured so that after a certain time (the standard time is 20 seconds) the connection is ended, if there is no more data exchange. After this fixed time in which there is no further data transfer, **BinGO!** cuts the connection – even if a new charging unit has just begun (static Short Hold).

If you now know for sure that you receive charging impulses during a connection, you can optimize further the automatic disconnection of calls by using to the full charging units which have already begun. Provided **BinGO!** receives regular charging impulses from the ISDN, you can tell your router to disconnect just shortly before the beginning of the next charging unit (dynamic Short Hold). The time range is not calculated here in seconds, but in the form of a percentage value, the reference of which is a charging unit (e. g. the connection should be cut after 80% of the charging unit is used up). Dynamic Short Hold can only be set in the Expert Mode of the Wizard or in Setup Tool.

If you want to use dynamic Short Hold in addition to static Short Hold, static Short Hold should always be set longer than a charging unit, otherwise dynamic Short Hold is ineffectual. (cf. chapter 6.2.1, page 144)

Dial numbers MSN

Normally, you receive three dial numbers with an ISDN basic connection (in Germany), the so-called MSNs (Multiple Subscriber Number). The MSN is a complete telephone number without a prefix. If three dial numbers are not

enough for you, you can usually request more MSNs from your telephone provider.

You have already entered the dial numbers in the Quick Mode of the Wizard. Only the digits were entered that suffice to distinguish between the dial numbers (i.e. usually the last two digits). **BinGO!** begins checking the dial numbers from the back (left to right mode). As soon as the configured number matches the incoming number, the number can be identified and assigned to a service. Thus, it is not necessary to enter the complete MSN every time.

Matters are complicated slightly if you are using extension systems. Normally, an extension system uses a main number and several extension numbers. In this case you should be informed about any special characteristics of your connection. It could be the case that internal dial numbers (S_0-Bus) are registered differently with different extension systems. Since you must always enter the dial number to which **BinGO!** (or also RVS-COM Lite) should react, you should know this registered dial number. If you do not know how your extension system forwards dial numbers, you can find that out using **BinGO!** (see chapter 6.1.4, page 126).

4.2 Speeding Things up Even More...

Compression systems help you to achieve a higher throughput rate in the same amount of time. When using compression processes, you must always ensure that the opposite terminal also supports the compression process. Otherwise, no connection can be made. No compression was activated in the Quick Mode of the Wizard. To do so, you need to use the Expert Mode or the Setup Tool. (cf. chapter 7.2.7, page 205)

BinGO! supports:

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

4.3 Services and Users

Management of a call

All routers use an algorithm in order to react to incoming calls from the ISDN. **BinGO!** can distribute the incoming calls to the following services:

- PPP (routing)
- isdnlogin
- CAPI

What do these services do?

PPP is **BinGO!'s** general routing service. This enables incoming data calls from WAN partners to be connected within your LAN. Thus, partners outside your local network can access PCs in your LAN.

The isdnlogin service allows incoming data calls to access **BinGO!**'s SNMP shell. This is how **BinGO!** can be remotely configured and administrated, for example.

The CAPI service allows incoming data and voice calls a connection with communications applications on hosts in the LAN that access **BinGO!'s** Remote CAPI interface. In this way, connected hosts can receive faxes with **BinGO!**, for example.

CAPI and Remote CAPI

Most applications programs that allow communications applications on a PC use the standardized CAPI interface. This makes possible services, such as answering service, fax G3 and G4, file transfer and eurofile transfer via ISDN. On its own, the CAPI interface allows only one PC to use the services over the ISDN connection. With the support of BinTec's own Remote CAPI, it is possible for all users in the network to use the services, providing, of course, all users have installed the required software. All users share just one single ISDN connection.

What have you configured?

In the Quick Mode of Wizard, you have activated the services PPP (routing) and CAPI. You can only activate isdnlogin in the Expert Mode or in Setup Tool. As

a standard, the Wizard allocates the numbers to the services as follows (the arrangement can only be changed in the Expert Mode):

Dial number	Data service	Voice service
1 (e. g. *10*)	PPP (routing)	CAPI
2 (e. g. *11*)	CAPI	CAPI
3 (e. g. *12*)	CAPI	CAPI

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

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

In our example configuration (cf. figure 3-12, page 68), we used the number *10* as a fax number and the number *11* for an answering service. As you may have noticed, the number *10* was assigned twice: for PPP and CAPI.

Voice or data?

Since on acceptance of the call, besides the dial number, data and voice calls are also distinguished, this doubling of services presents no problem for **BinGO!**. The router realises that an incoming fax with the number *10* must be a voice data and forwards the information to the CAPI service. On the other hand, if a WAN partner dials into your network, it must be digital information (data) and **BinGO!** forwards the data to the PPP service.

Data is:

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

Voice is:

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

Who is faster?

Moreover, we also presumed that you can be reached by telephone connected to the same S_0 bus as **BinGO!** at the number *11*. All devices connected to the same S_0 bus and that can be reached at the same dial number also react to

calls. This means that while your telephone rings on an incoming call at the number *11*, at the same time RVS-COM Lite receives the signal. As you have set the number of ringing tones before the call is taken on RVS-COM Lite, RVS-COM Lite initially waits. If you first lift the handset, you are quicker and take the call. If you do not lift the handset before the number of "rings" of RVS-COM Lite is reached, RVS-COM Lite is faster and takes the call.

Several users

One dial number is not occupied: the *12*. If you have a network with two PCs in the LAN, you could assign each of these two PCs its own fax number. In CommCenter of PC 1, you would leave the number *11* as dial number, in CommCenter of PC 2, you would enter the number *12* as dial number for fax (cf. figure 4-1, page 82).

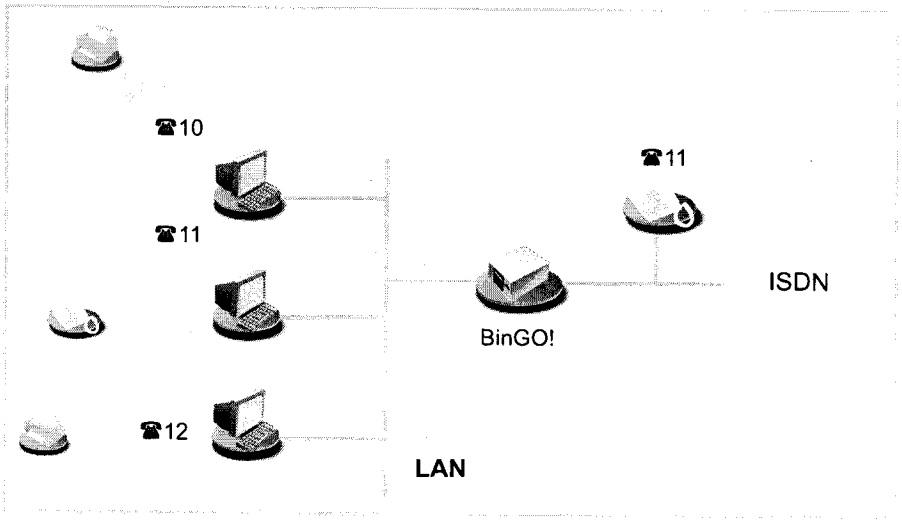


Figure 4-1: Scenario: 2 PCs, 2 fax numbers, 1 telephone

So far, so good. But what if one of either of the two users of PC 1 or PC 2 changes the dial number! Both CommCenters could, for example, react to an incoming call at number *11*. Whoever is faster, gets the fax...

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

More security

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

cess by using a user name and password. The CAPI-user concept thus helps you out of this pickle.

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

Several user accounts Every user who should be allowed certain communications applications receives his own user name and password. The settings for name and password must be made on the router (e. g. with the Wizard in Expert Mode or Setup Tool chapter 7.1.2, page 184) and on the respective PC (Remote CAPI configuration). Additionally, you allocate a dial number to each user on the router. (e. g. fax number). The communications application of the PC, on which the corresponding user is also entered in the CAPI configuration, only reacts to that number.

4.4 BinGO! as a DHCP Server

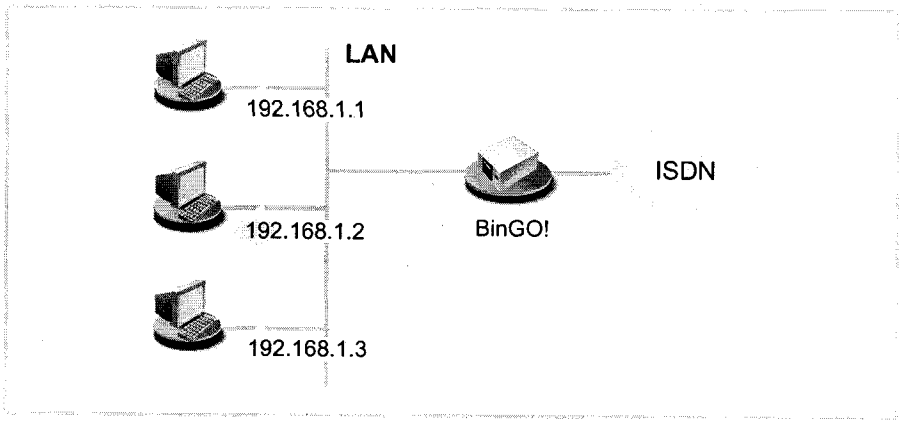


Figure 4-2: Scenario: **BinGO!** as a DHCP server

What do we need IP addresses for?

Every PC in your LAN requires its own IP address, just as **BinGO!** does. Otherwise the devices could not communicate together. When you send a letter by "snail mail", you also have to write the receiver´s and your own address. If you don´t, the letter neither arrives at its destination nor returns to sender.

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

How do I know who I am?

These IP addresses can be fixed on PCs. The disadvantage is that if you are newly configuring or reconfiguring your network, you have to assign each PC individually with its own IP address. This can involve quite a lot of work depending on the number of PCs you have on your network.

You can save yourself all this work with a ➤➤ DHCP server (DHCP=Dynamic Host Configuration Protocol). Automatically, a DHCP server allocates IP addresses to all the PCs on the LAN. The PCs are then DHCP clients. All you have to do is to define a pool of IP addresses that the DHCP server may allocate to computers on the network. In addition, you must tell the PCs that they should request their IP addresses from the server.

BinGO! can not be configured as a DHCP client. It must always have a fixed IP address. It is possible, however, to assign **BinGO!** an IP address over a BootP server. (cf. chapter 6.1.2, page 122)

Moreover, there can not be several DHCP servers with the same address pools in each network.

BinGO! as DHCP server

You can use **BinGO!** as a DHCP server if you do not have another DHCP server. (cf. chapter 6.1.5, page 136) It assigns IP addresses to all PCs in your own network. Perhaps you have already configured **BinGO!** as a DHCP server in the Quick Mode with the Wizard. If you accepted the values suggested, your PCs will receive IP addresses from ***192.168.1.1*** to ***192.168.1.8***.

When are IP addresses allocated?

Every PC that newly enters the network – after booting, for example – sends out an address request and in reply receives its IP address. Usually, the PC retains this address for a specified period of time (you can set the length of time in Setup Tool). Afterwards the address is reassigned, maybe to the same or maybe to another PC. You can also explicitly tell your PC to request an IP address. The Wizard may have done this for you in Quick Mode, if you wanted to configure **BinGO!** as a DHCP server.

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

Calling up WINIPCFG

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

➤ Type in `winipcfg`.

A window appears in which you can see the IP address of your PC and other network information.

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

Calling up IPCONFIG

➤ Click the Windows Start button and then point to **Programs ➧ Command Prompt**.

- Type in `ipconfig` or `ipconfig/all` to request the IP address of your PC and other network information.
- Type in `ipconfig/renew` to reassign an IP address.
- Type in `ipconfig/release` to release an IP address.

4.5 How Does Name Resolution Work?

Now you have heard quite a bit about why you need an IP address. What about if you want to communicate or access data by simply using the name and not the number (IP address), for example, if you want to talk with the PC *BossPC* or you want to see the Internet pages *www.bintec.de*? *BossPC* and *www.bintec.de* are clearly not IP addresses, but names. As computers only understand IP addresses and not names, it is necessary for the names to be translated (resolved) into their corresponding IP addresses.

Name resolution

The following options are available for name resolution:

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

➤➤ **DNS** translates the host names or computer names into their IP address equivalents. A DNS contains tables with lists of computer/host names and their corresponding IP addresses, these can be amended and made known.

DNS servers are structured hierarchically. As soon as the primary DNS receives a request, it tries to translate the name. If it is not able to translate the name, it refers the request to the next higher DNS.

BinGO! as DNS proxy

If you use **BinGO!** as a DNS proxy (usual case), your router forwards all DNS requests to a DNS server (usually the server here is at your ISP).

WINS

A similar service called WINS exists in Windows networks. With WINS you can only translate computer names or NetBIOS names, but not host names. NetBIOS is used analogous with the transport protocol TCP/IP. Generally, computer and host names are identical in Windows networks.

HOSTS and LMHOSTS files

You may have already met the LMHOSTS file in the previous chapter. A table containing computer names and corresponding IP addresses is laid in the LMHOSTS file. The HOSTS file is similarly structured. Instead of computer names, the HOSTS file translates host names into IP addresses.

How does name resolution function in practice?

Internet access

If you have configured Internet access with the Wizard and you do not have your own DNS server, you can obtain the IP address of your provider´s DNS server. The router is known as the DNS proxy by the PCs in the LAN. When a request is made for a name resolution (e. g. for ***www.bintec.de***), the PC asks the router, and the router in turn refers to the provider´s DNS server. Translation of the address can then take place there.

So far, so good. What, however, if, in addition, you configure a corporate network connection?

Internet access and corporate network connection

If, in addition to an Internet connection, you have configured a corporate network connection, entered **BinGO!** as a DNS proxy server, and the DNS settings of your router lead to the Internet provider (a standard setting of the Wizard), all requests for name translation would be sent to your provider. If you want to reach a PC in your partner´s network (***BossPC***), **BinGO!** establishes a connection to the provider and asks for the IP address of ***BossPC***. Unlike "names" such as ***www.bintec.de***, computer names are not known on the Internet. They are only used within a corporate network (domain, working group), The DNS server of the provider is thus usually unable to translate the name. This connection to your provider has been a waste of time, not to mention money. And you still have not reached ***BossPC***.

In order that such unintentional and useless connections are not established, you must prevent such requests about computers in your partner´s network taking place in the first place. This task is carried out by the NetBIOS filter you configured with the Wizard. (see chapter 4.7, page 93). This, however, has not solved your problem. You still want to have the name ***BossPC*** translated into its IP address.

One possibility would be to set up your own Domain Name Server in which all the names of the PCs in your partner´s network and their corresponding IP addresses that you want to reach are listed. As it is not always worth the trouble

setting up your own server, if you only have one or two such entries to make, there is a second alternative:

You save the IP address to name arrangements on your PC. This must be done, however, on all PCs that require the information. You can use the LMHOSTS file for such purposes.

How to add an entry to the LMHOSTS file has already been explained in chapter 3.6.2, page 61.

To ensure the success of our solution, you should bear in mind the following points:

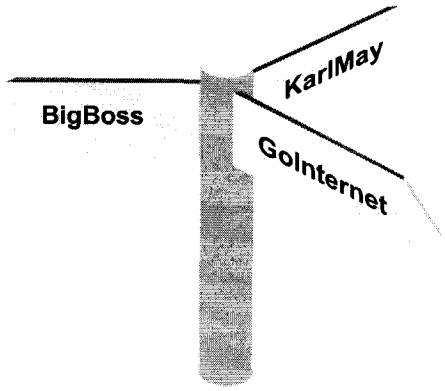
- Domain and working group names must be identical on both sides. Your opposite terminal should have an NT domain where you can register.
- You must be known on the far end as a user.
- You must not have set extensive NetBIOS filtering with the Wizard, otherwise certain Windows functions such as a network drive connection could not be used.

The subject "Connections of Windows Networks" is extensive and complex. A range of factors determine the success of such a project. As a more detailed treatment of the subject would exceed the scope of this manual, we can only refer you at this point to related technical literature: e.g. "Windows NT Connectivity Guide" by Richard Grace (ISBN 0-7645.3160-3)

4.6 What Are Routes and Default Routes?

Routing

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



This is why we define the routes *to* those destinations. The routes lead to a certain network with a defined ➤➤ **network address** and ➤➤ **netmask**. You must specify the route to every network you want to access. You could define, for example, the route to your WAN partner (e. g. head office). All packets whose IP addresses belong to the netmask and network address are sent to the partner network.

But where do all the other IP packets go?

Default route

By means of a so-called default route, you can decide that all packets whose destination is unknown to **BinGO!** be sent to a certain network. Generally, the route to the Internet provider is used as the default route, because most unknown packets are bound for the Internet anyway (e. g. ***www.bintec.de***). The Wizard automatically enters the route to your provider as the default route, as long as you have configured for Internet access. If you have only configured a partner network and not an Internet provider, the Wizard simply uses the route to your partner´s network as a default route.

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

Due to the fact that your default route leads all unknown packets to your head office, and there another default route in turn sends all unknown packets to its Internet provider, you can access the Internet via your partner´s network.

Several routes for the one WAN partner

Your corporate network can consist of several LANs with different network addresses and netmasks (subnets). In this case, you must specify the route to each subnet you want to reach. (cf. figure 4-3, page 91).

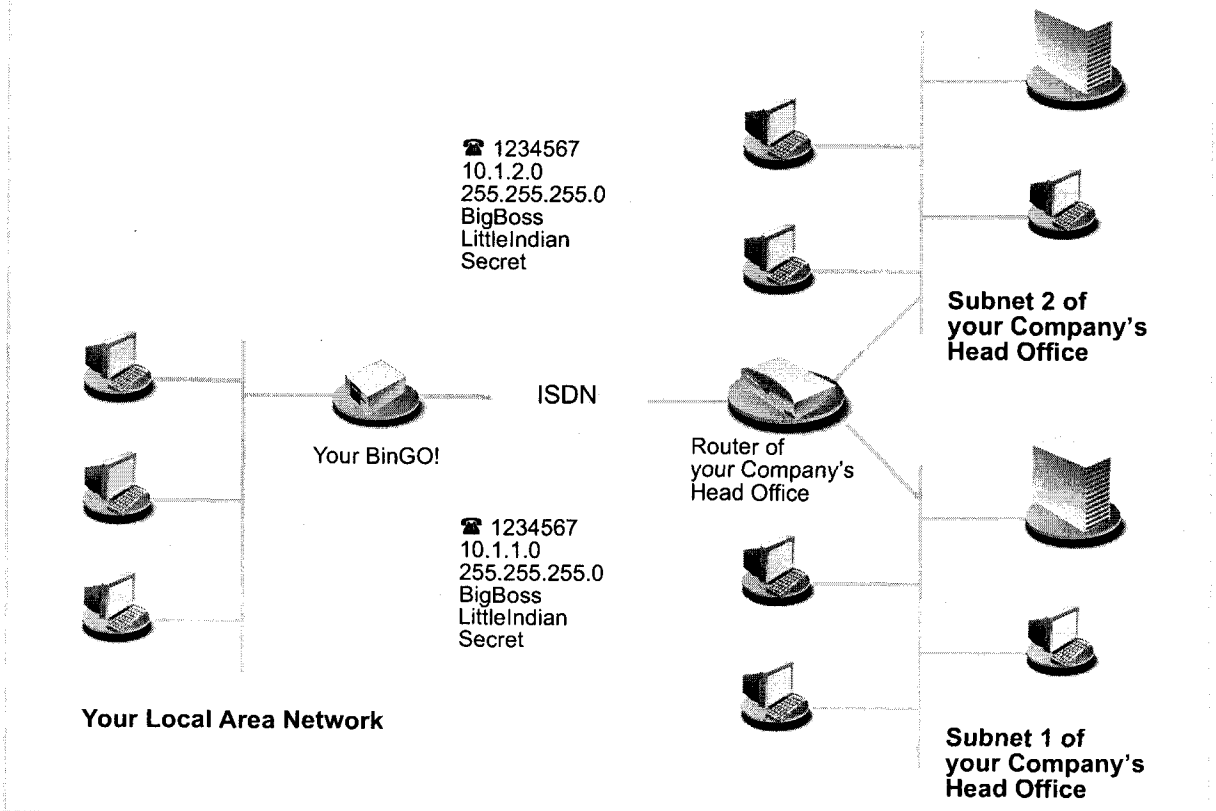


Figure 4-3: Scenario: WAN partner with two subnets

Routes, name resolution and Gateways

Not only does **BinGO!** avail of a default route, your PC also has one: the gateway. All packets whose destinations are not within the local network are sent by your PC to this gateway. **BinGO!** serves as this gateway. As soon as your router receives such a packet, it forwards it in turn to one of its known routers (e.g. to the provider or to another partner´s network).

Let´s assume your default route leads to an Internet provider, your PCs are DCHP clients and are assigned their IP addresses from **BinGO!**. In such a case, the PCs also get their IP addresses after name resolution from **BinGO!**

acting as a DNS proxy server and gateway. (The example also applies if your PCs are not DHCP clients, but are configured in such a way that **BinGO!**´s IP address is entered as the DNS server and gateway.)

As soon as you enter ***www.bintec.de***, for example, in the browser, the PC sends a DNS request to **BinGO!** – as **BinGO!** is known as a DNS proxy server. **BinGO!** can not translate the name itself and sends the packet with the DNS request along the default route to the provider. There the name ***www.bintec.de*** can be resolved. The DNS request is successful and in reply the PC receives the IP address for the name ***www.bintec.de***. Now the packet can be sent on its actual journey to ***www.bintec.de***. As **BinGO!** is entered as a gateway, and the packet has an IP address whose destination is an external LAN, the packet is sent out via the gateway (**BinGO!**). Since no route is entered for the IP address for ***www.bintec.de***, **BinGO!** uses the default route.

4.7 Filters and NetBIOS

You have just learned a fair bit about names resolution and routing. This is all very practical, but...

Why Filters? All Windows networks use computer names, e. g. one could be called Winnetou in the network, another Old Shatterhand. These computer names are not known on the Internet as they are only used within a corporate network (as opposed to "names" such as *www.bintec.de*). These computer names are resolved in all Windows networks via the service NetBIOS. NetBIOS in turn tries to have these computer names resolved by your provider. As they are only known in your network (domain, working group), **BinGO!** would constantly establish unnecessary connections with your provider (the requests are approximately every 12 to 15 minutes and thus quite frequent!) who would not be able to resolve the WINS names.

This is where filters come in.

Simple filters If you have activated the simple NetBIOS filter with the Wizard, all IP packets that are sent to **BinGO!** to have their names resolved are discarded. The Wizard always configures a simple filter in the Quick Mode.

Extensive filters *Extensive filtering can only be set in the Expert Mode or with Setup Tool.* With the extensive filter, all NetBIOS data traffic (NetBIOS broadcasts) is filtered – that means not just requests for name resolution. The only disadvantage is that as soon as several WAN partners (e. g. Internet and corporate network connections) are configured, all NetBIOS services such as the common use of drives *and printers can not be used.*

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

Not only are unintentional connections prevented with filter mechanisms, the primary function of filtering is the security of the internal network against intrusion from outside. (cf. chapter 8.2.8, page 250)

4.8 MIB and SNMP

What is SNMP?

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

What is MIB?

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

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

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

5 Connecting BinGO!

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

You will learn:

- how to access **BinGO!**
- how to log on
- which methods of configuration are available to you
- how the ➤➤ **Setup Tool** is constructed

5.1 Connection Methods

In order to configure your ➤➤ **router**, you must firstly connect it. There are three ways to do this.

- Over a serial connection
- Over your ➤➤ **LAN**
- Over an ➤➤ **ISDN** *connection*

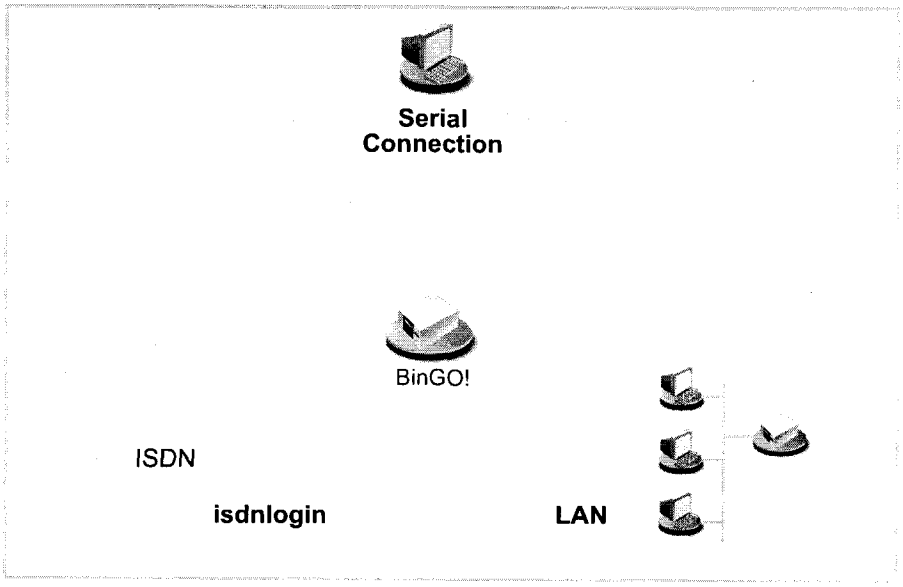


Figure 5-1: Possible connections to **BinGO!**

Initially, we will present the various methods to you, then you can choose the way you feel most suits your needs. Regardless of the method of access you choose, the ➤➤ **SNMP shell** of your **BinGO!**, a window in which you will configure your router via the Setup Tool, will appear on your monitor screen.

5.1.1 Connecting over the Serial Port

Initial configuration

A serial port connection is the most appropriate method if you are configuring your **BinGO!** for the first time. To access the router over the serial port, proceed as explained in chapter 3.1, page 35.

Windows

If you are using a Windows PC, you will need a terminal program, e.g. HyperTerminal, for the serial connection. You will have installed this assistant already together with BRICKware for Windows in chapter 3.3, page 43.

➤ Click the Windows Start button and then **Programs** ➧ **BRICKware** ➧ **Brick at COM1** (or ➧ **Brick at COM2**, if you are using the PC´s COM2 interface), to start **HyperTerminal.**

➤ Press **Return** (at least once), after the HyperTerminal window opens.
A window with the login prompt appears. You are now in **BinGO!**´s SNMP shell. Continue with chapter 5.2, page 103.

If the login prompt does not appear after several attempts pressing **Return**, the connection to **BinGO!** has not been successful. Check the settings of COM1 or COM2.

➤ Click **File** ➧ **Properties**

➤ Click **Configure** in the **Phone Numbers** registry...
The following parameters are necessary
- Bits per second: 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

➤ Enter the values and click **OK.**

➤ Set in the **Settings** registry:
Emulation: auto detect

➤ Click OK.

You can use any other terminal program that can be adjusted to 9600 bit/s, 8N1 (8data bits, no parity, 1 stop bit), software handshake (XON, XOFF) and VT100 emulation.

Unix If you are using a Unix PC, you can not use HyperTerminal. You will require a terminal program such as **cu** (under system V) or **tip** (under BSD) or **minicom** (under Linux). The parameters for these programs are the same as listed above.

5.1.2 Connecting over a LAN

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

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

➤ Connect **BinGO!** with your LAN as explained in chapter 3.1, page 35.

Assigning IP addresses

To assign your **BinGO!** an IP address (if necessary), proceed as follows:

➤ Click the Windows Start button and then **Programs** ➧ **BRICKware** ➧ **DIME Tools**.
A ➤➤ **bootP** server window will appear after a short time if **BinGO!** is unconfigured.

➤ Enter the name and IP address of your **BinGO!** in the window under **BRICK Parameter** (if you are unsure, refer to chapter 3.2, page 38).

➤ Click **OK**.

➤ Close **DIME Tools**.

Running telnet Now establish a connection to **BinGO!** with telnet:

Windows

➤ Click **Run** in the Windows Start menu.

➤ Type `telnet <IP address of your BinGO!>`,

➤ Click OK.

A window with the login prompt will appear. You are now in **BinGO!**'s SNMP shell. Continue with chapter 5.2, page 103.

Unix

➤ Type `telnet <IP address of your BinGO!>` in the Terminal window.

A window with the login prompt will appear. You are now in **BinGO!**'s SNMP shell. Continue with chapter 5.2, page 103.

5.1.3 Accessing over ISDN

Remote configuration Access over ➤➤ **ISDN** with ➤➤ **isdnlogin** is particularly useful when **BinGO!** is situated at a different location and you want to configure it and administrate it from a distance. This is also possible when **BinGO!** has not even been initially configured. You must have, however, an already configured BinTec router at your disposal (in LAN 1), you must also know the telephone number of your (new) router (in LAN 2). It is thus possible for the administrator of a head office to configure the router of a colleague in a home office who is hundreds of kilometers away. The **BinGO!** in the home office merely has to be connected to an ISDN outlet and turned on.

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

➤ Connect **BinGO!** to the ISDN as explained in chapter 3.1, page 35.

To reach **BinGO!** over isdnlogin, proceed as follows:

➤ Login to your other BinTec router (in LAN 1) in the usual way.

➤ Type in `isdnlogin <telephone number of your BinGO!>` in the SNMP shell.

The login prompt will appear in the window. You are now in the SNMP shell of your **BinGO!**. Continue with chapter 5.2, page 103.

5.2 Logging in

Regardless of how you access **BinGO!**, the ➤➤ **SNMP shell** with the login prompt is always the first thing to appear:

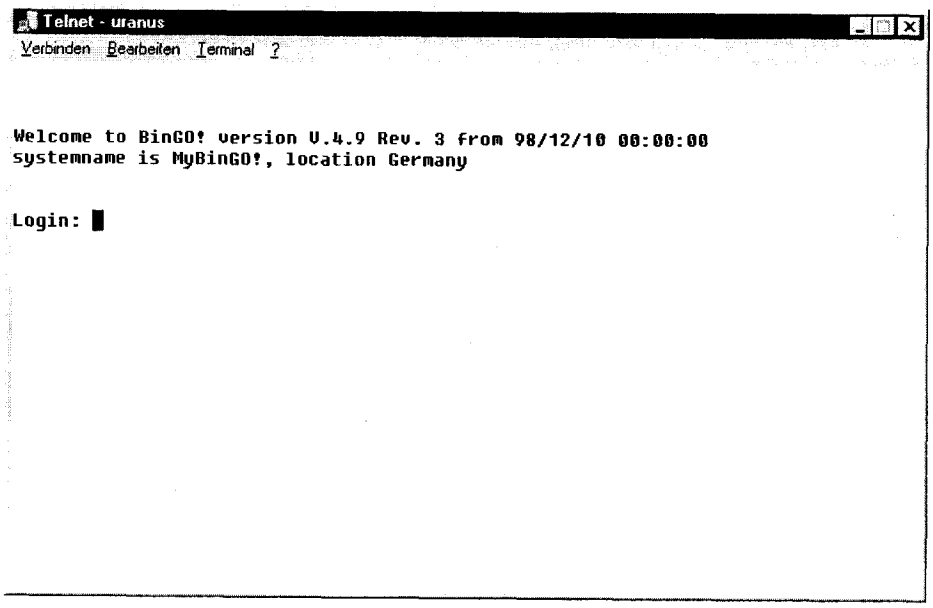


Figure 5-2: Login prompt

In order to login, you need to know the user name and password. In its unconfigured state, **BinGO!** is provided with the following user names and passwords.

User Name	Password	Permission
admin	bintec	Read and change system variables, save configurations, use the Setup Tool
write	public	Read system variables (changes are lost when **BinGO!** is turned off)
read	public	Read system variables
http	bintec	Call up **BinGO!'s** HTTP status page and Java Status Monitor, read system variables, no login

Table 5-1: User names and passwords as when shipped

As you can see, it is only possible to change and save configurations when you login with the user name `admin`.

For security reasons, it is only possible to read access data by logging in with the user name `admin`. With the user name `read`, for example, it is possible to read all system variables, but no access data. Thus, it is impossible to login with `read`, read the password of the admin user and subsequently login with the `admin` user name and password and effect changes to the configuration.

This is how you login:

- Type in your user name (e.g. `admin`) and press **Return**.
- Type in your password (e.g. `bintec`) and press **Return**.

  Your router then issues an input prompt (e.g. `brick:>`). The login was successful.

Caution!

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

- Change the passwords as described in chapter 6.1.2, page 122.

Close the SNMP shell

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

5.3 Configuration Options

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

5.3.1 Methods of Configuration

The following are **BinGO!**'s configuration methods:

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

Configuration Wizard You have already met the Configuration Wizard in chapter 3.4, page 45. It is useful for quick, initial configuration and can be used if you have a Windows PC. This usually covers most cases. If, however, you require further settings, you can avail of the other aforementioned options. You could firstly configure **BinGO!** with the Configuration Wizard and subsequently extend or change these initial configurations with one of the other tools. In many cases, though, the Configuration Wizard will be entirely sufficient!

Setup Tool The Setup Tool is a menu-driven tool for the configuration and administration of **BinGO!**. Configuration with Setup Tool is considerably easier and clearer than configuration with SNMP commands, although not all settings can be performed with Setup Tool. Besides the assistance of the Configuration Wizard, this manual only explains how to configure with Setup Tool. Setup Tool is independent of the operating system on your PC. If, as in a few isolated cases, a configuration step is only possible with the help of an SNMP command, the procedure will be additionally explained.

SNMP ➤➤ **SNMP**(Simple Network Management) is a ➤➤ **protocol** over which you can access the configuration settings. All configuration settings are located in

➤➤ **MIB** (Management Information Base) in the form of MIB tables and MIB variables. You can access these directly via the SNMP shell.

DIME Browser and other SNMP managers

BinTec Communications AG makes available DIME Browser, an SNMP manager for Windows PCs. A surface based on the Microsoft Explorer, you can access all **BinGO!**'s MIB tables and variables. You can use other SNMP managers, such as SNM, HP-Open View or Transview to access and modify the MIB tables and variables. However, more detailed knowledge of the structure and interrelations of **BinGO!** would be a prerequisite: this is thus a method suitable for more experienced users. This manual does not go into the subject of MIB tables and variables, if you want more information on the subject, refer to the Software Reference and MIB Reference.

5.3.2 Setup Tool

If you have logged into **BinGO!**, you can call up Setup Tool:

➤ Type `setup` after the input prompt and press **Return**.
The main menu of the Setup Tool appears.

Main menu

```
BinGO! Setup Tool                                BinTec Communications AG
                                                                MyBinGO!

Licenses                    System

LAN Interface:   CM-BNC/TP, Ethernet
WAN Interface:   CM-1BRI, ISDN S0

WAN Partner
IP       IPX       PPP       ISDN      CAPI

Configuration Management
Monitoring and Debugging

Exit

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

To use Setup Tool, you must login with the user name admin! If you don´t know the corresponding password, you can not open Setup Tool (see chapter 5.2, page 103).

Setup Tool, you will find, is easy to use. After a few minutes, you will have no problem finding your way around. Nevertheless, by way of introduction, we would first like to point out a few things you should be aware of when using Setup Tool.

Menu layout

Every Setup Tool menu consists of three parts: the menu line, on the top; the main configuration window, in the middle; and the help line, on the bottom.

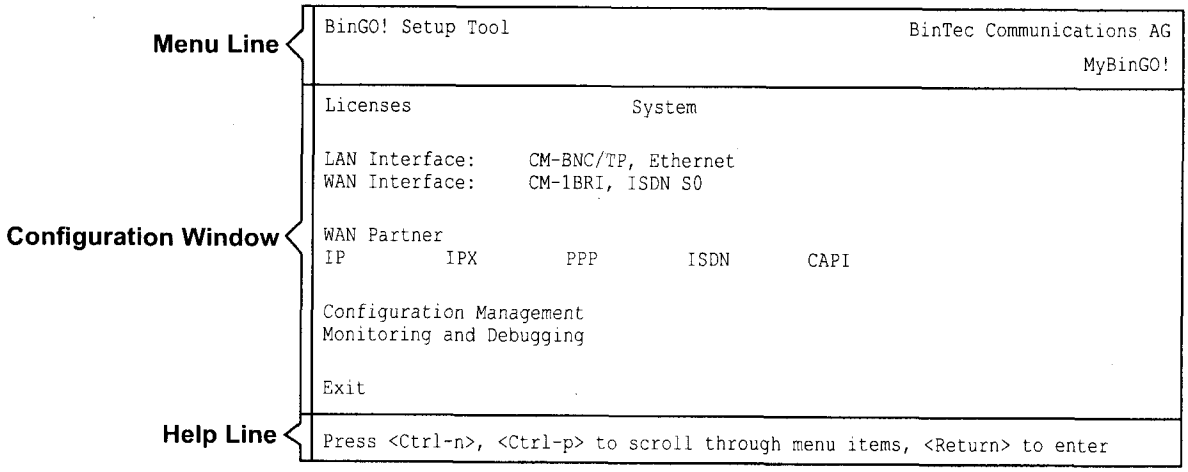


Figure 5-3: Setup Tool menu layout

In the menu line a navigation aid shows you where you currently are in the Setup Tool menu system. In addition, **BinGO!**´s system name is displayed. This is especially helpful if you are using several BinTec routers with different system names.

The configuration window is where the actual entries are made or where the respective settings are displayed. The cursor marks the entire field it is on.

The help line at the bottom of the window gives you command options and tells you how to move around or how to change entries in the configuration window currently being displayed.

Menu navigation While using the Setup Tool, the following keys or key combinations can be used to navigate the various menus:

Key Combination	Purpose
Tabulator	To move to the next field.
Return	To open a submenu or to activate a menu command (e.g. **SAVE**).
up or **down**	To move forwards or backwards among menu fields.
left or **right**	To scroll backwards or forwards on the same field to reveal a list of possible entries.
Esc Esc	Esc twice in succession: to return to the previous menu. Aborts any changes made.
Space	To toggle the delete flag for special entries that may be deleted. Entries thus tagged are marked D. By pressing **Space** again, the tagging is lifted.
Ctrl - l	To redraw the screen.
Ctrl - n	To jump to the next item in a list.
Ctrl - p	To jump to the previous item in a list.
Ctrl - 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).
Ctrl - 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).
Ctrl - c	Leave Setup Tool

Table 5-2: Navigation in the Setup Tool

Menu commands When you start moving around in Setup Tool, you will notice that some menus have different command options in the help line (lower portion of the menu) such as the **DELETE, SAVE** and **CANCEL** commands shown below. There are

a few slight differences between these commands which you should be aware of.

Menu Command	Meaning
ADD	To create or add an item to a list. A submenu appears where you can enter the item.
CANCEL	To discard all changes made within the current menu. Note: ONLY the current menu.
DELETE	To delete all entries tagged with the space-bar 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 memory.
SAVE	All variables set in the current menu, as well as its submenus, are saved to memory. These changes become effective immediately.
EXIT	To leave the current menu and to return to the previous menu. If entries have been made, they are lost.

Table 5-3: Menu commands in Setup Tool

Searching lists Several Setup Tool menus contain lists of items, e.g. the WAN Partner menu lists all the ➤➤ **WAN partners** which are currently configured.

```
BinGO! Setup Tool                                   BinTec Communications AG
[WAN]: WAN Partners                                                 MyBinGO!

Current WAN Partner Configuration

    Partnername          Protocol             State

    BigBoss              ppp                  dormant      ^
    T_ONLINE             ppp                  dormant      |
    Partner1             ppp                  dormant      |
    Partner2             ppp                  dormant      |
    PROVIDER             ppp                  dormant      =

ADD              DELETE                EXIT

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

These lists are in alphabetical order according to the contents of the first field. There is a search function which allows you to search long lists for an item.

Proceed as follows:

- Enter the first letter (upper or lowercase) of the item you are looking for.
- As long as the search is active, you can enter more characters to refine the search.
- The **Backspace** key (and possibly **Delete** depending on terminal settings) can be used to edit the search string.
  The cursor automatically jumps to the first match it finds in the list.

The characters entered for the search are displayed in the help line.

Avoid invisible entries, such as **Tabulator** or **Space**, they cause the search to be discontinued and could lead to a key-related function being initiated.

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

Example:

Using the menu ***WAN PARTNER*** menu shown above, the following entries would yield the following search results:

Entry	Result
p or P	Partner 1
pr, Pr,pR, PR	PROVIDER
p a r t n e r 2	Partner1, on entering 2 to Partner2

Table 5-4: Search results

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

MENU ➧ SUBMENU ➧ SUBMENU

For example:

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

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

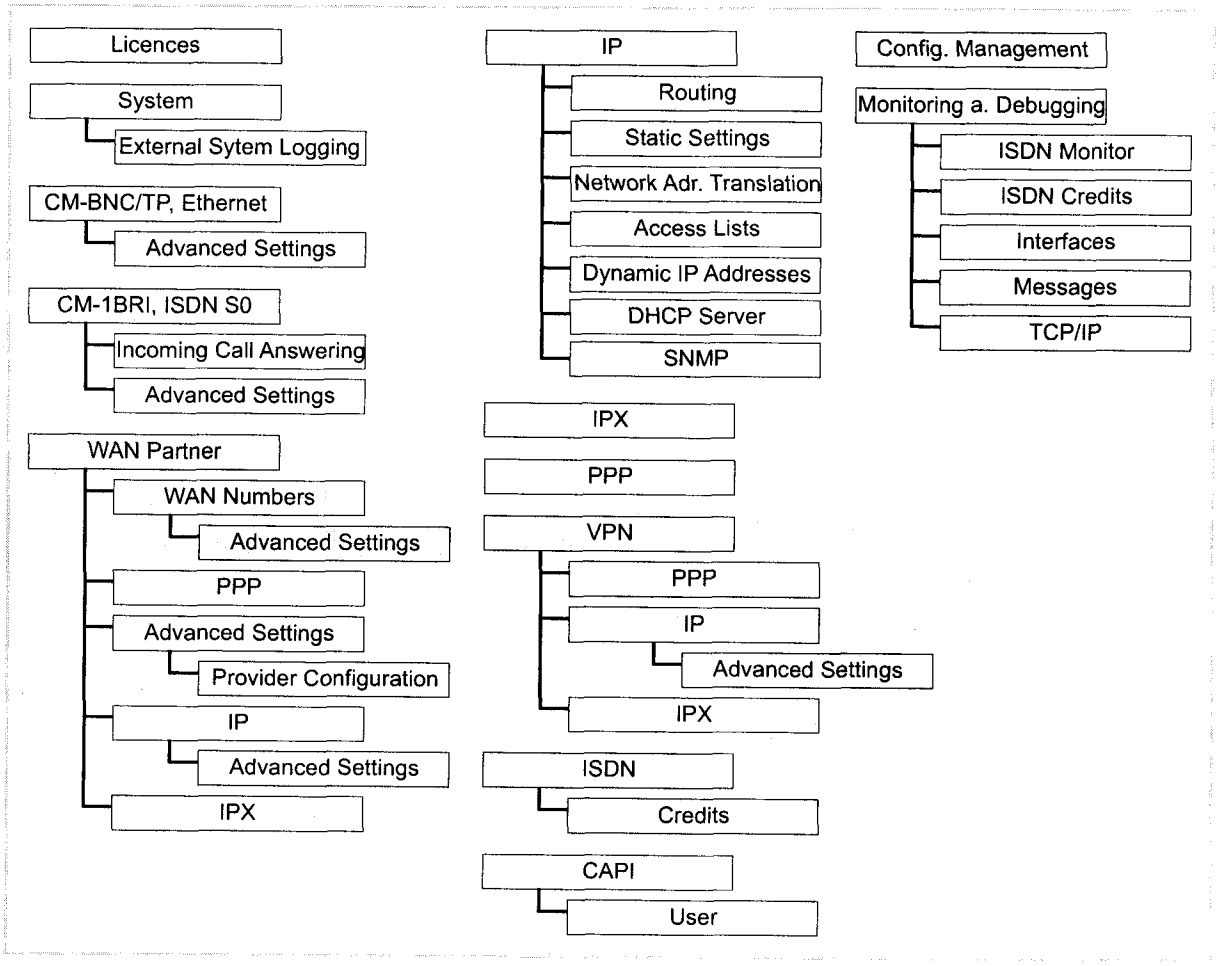


Figure 5-4: Setup Tool menu structure

figure 5-4, page 112 illustrates all menus of the Setup Tool available to **BinGO!**. Not all functions are available on all routers (e.g. VPN). To use them, an additional license you can acquire from BinTec Communications AG is required. When you activate the necessary license, **BinGO!** recognizes it and displays the corresponding menus (to enter licenses see chapter 6.1.1, page 120).

Summary As an appendix to the above depiction of the menu structure and to help you find your bearings prior to configuration, here are some brief explanatory re-

marks about the items in the main menu. A more detailed account of each in terms of the configuration steps necessary for the required settings is given in the following chapters.

Menu	Function
LICENSES	Here you type the licensing information that is on your license card. This is also where the extra licenses are activated.
SYSTEM	Here you enter **BinGO!**'s basic settings, such as system name and passwords.
CM-BNC/TP, ETHERNET	In this menu, **BinGO!**'s ➤➤ **LAN** interface is configured. Here you enter the IP address and netmask of your router, for example.
CM-1BRI, ISDN S0	Here you configure **BinGO!**'s ➤➤ **WAN interface** by entering such information as the kind of ISDN connection your **BinGO!** is connected to. In the submenu ***WAN INTERFACE*** ➧ ***INCOMING CALL ANSWERING***, you assign certain services (e.g. ➤➤ **PPP** Routing, ➤➤ **CAPI**, isdnlogin) to the available ISDN numbers.
WAN PARTNER	Here you define all your WAN partners, e.g. your ➤➤ **Internet** Service Provider (➤➤ **ISP**). You can include an unlimited number of WAN partners. All these partners are displayed in a list that includes name of partner, protocol used and the current status of each.

Menu	Function
IP	Here you enter the settings that relate to the ➤➤ **IP** protocol. It consists of several submenus: ***IP*** ➧ ***ROUTING*** includes **BinGO!**'s IP routing table. Here you enter routes to your partners (e.g. default routes, network routes), which ensure that your **BinGO!** sends all the ➤➤ **data packets** to the correct addresses. In ***IP*** ➧ ***STATIC SETTINGS***, you enter some important settings, e.g. your domain name, the IP address of additional ➤➤ **servers** (e.g. Domain Name Server), system time specifications. In ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***, configure the interfaces to the partners for which you want to use the function Network Address Translation (➤➤ **NAT**). In ***IP*** ➧ ***ACCESS LISTS***, you define ➤➤ **filters**, in order to allow or prevent access from or to the different hosts in closed networks. You can thus prevent your **BinGO!** from establishing unintended connections to the ISDN. In ***IP*** ➧ ***DYNAMIC IP ADDRESSES***, you can set up a pool of IP addresses that your **BinGO!** as a dynamic IP address server can assign to partners who can then dial in from a WAN. In ***IP*** ➧ ***DHCP SERVER***, you configure **BinGO!** as a ➤➤ **DHCP** server. As a DHCP server, **BinGO!** dynamically assigns the hosts in the LAN their IP addresses. In ***IP*** ➧ ***SNMP***, you can change the basic ➤➤ **SNMP** settings.
IPX	Here you make the entries that concern the IPX protocol. ➤➤ **IPX** is used especially in Novell networks.
PPP	Includes generally valid ➤➤ **PPP** settings, e.g. authentication protocol that does not just refer to particular partners. **BinGO!** can thus perform an authentication procedure for incoming calls, even when the Calling Line Number can not be identified (e.g. because the call is made from an analog line that does not carry the Calling line Number).

Menu	Function
VPN	Here the necessary settings for Virtual Private Networking (VPN) are made. It only appears if you have entered the relevant valid license. To use the function, you need a VPN server from Security Dynamics. The license can be optionally acquired. You will find more detailed explanations and instructions in Extended Features Reference.
ISDN	Here you administrate your **BinGO!**'s Credits Based Accounting System.
CAPI	Includes the settings for the ➤➤ **CAPI** User Concept from BinTec. You can thus assign user names and passwords to **BinGO!** users of the CAPI applications.This is how you can ensure that only authorized users can receive incoming calls and establish outgoing connections via CAPI.
CONFIGURATION MANAGEMENT	Here you can manage your **BinGO!**'s configuration files. You can save them either locally on **BinGO!** or on your PC, for example.
MONITORING AND DEBUGGING	Includes submenus that enable the location of problems in your network and the monitoring of activities, e.g. at **BinGO!**'s WAN interface.
EXIT	With exit you leave Setup Tool. With **Exit** ➧ **Save as boot configuration and exit**, you save the configuration file to the Flash memory, after **BinGO!** is restarted, this file is loaded. With **Exit** ➧ **Exit without saving**, all settings made since **BinGO!** was last started are lost.

Table 5-5: Menus in the Setup Tool

6 Basic Configuration with Setup Tool

This chapter explains the basic configuration of **BinGO!** with ➤➤ **Setup Tool,** which covers the same subjects as were configured with the Configuration Wizard, explained in chapter 3.4, page 45. However, the Setup Tool is independent of the operating system and, in addition, is capable of more settings.

Initial configuration

The basic configuration of **BinGO!** includes:

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

The basic router settings are essential for the working of **BinGO!.** Depending on your needs, you can configure for Internet access and or corporate access right away or at a later time.

Extending existing configuration

Even if your **BinGO!** has already been initially configured and you want to modify your existing configuration, you will find lots of useful tips in this chapter, for example:

- how to include additional ➤➤ **WAN partners**
- how to change passwords
- how to enter additional licenses
- how to organize Incoming Call Answering
- how to setup **BinGO!** as a ➤➤ **DHCP** server
- how to define a simple ➤➤ **NetBIOS** filter
- how to make routing entries

How to supplement and improve your configuration after finishing the basic configuration is explained in chapter 7, page 181.

How to configure the security mechanisms according to SAFERNET is explained in chapter 8, page 227.

6.1 Basic Router Settings

The configuration of the basic router settings concerns both your **BinGO!** and your local network. The relevant detail from figure 6-1, page 119 is illustrated in figure 6-1, page 119. There you will find, for example: names, ➤➤ **IP addresses**, phone numbers, etc. If you are setting up a new Local Area Network (LAN) together with your **BinGO!** and have not been assigned any IP addresses (e. g. from the system administrator at your head office), simply use the IP addresses given as examples. You can, of course, use any other relevant values you may have.

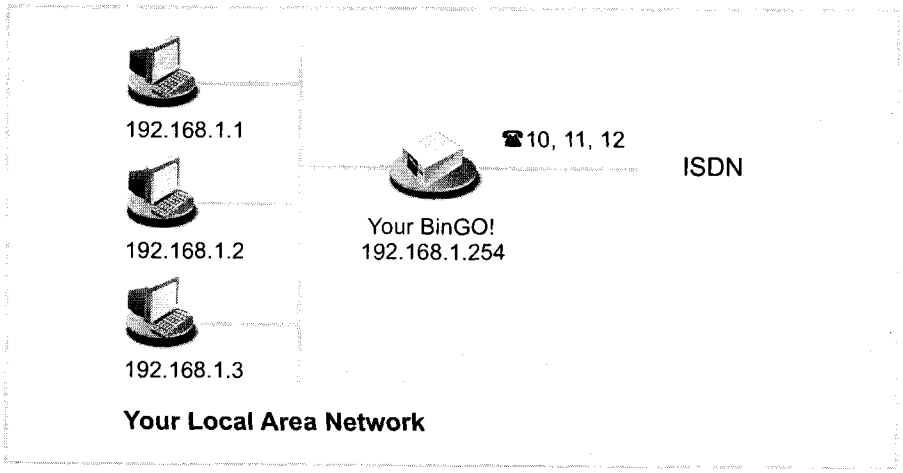


Figure 6-1: Basic router settings

The following steps are necessary:

- enter a license
- enter system data (e. g. passwords)
- configure the LAN interface
- configure the ➤➤ **WAN interface**
- configure **BinGO!** as a DHCP ➤➤ **server** (optional)
- set ➤➤ **filters** (optional, extensively explained in chapter 8.2.8, page 250)

Let´s go:

6.1.1 Entering a License

License card

After logging in to your **BinGO!** with the user name `admin` and calling up Setup Tool with `setup`, as described in chapter 5.2, page 103, you should now enter the license information. This is written on the included license card. You thereby activate all **BinGO!**´s functions.

➤ Go to ***LICENSES***:

```
BinGO! Setup Tool                                   BinTec Communications AG
[LICENSE]: Licenses                                                MyBinGO!

Available Licenses:

IP (builtin), EXTENDLAN (not_valid), TUNNEL (not_valid), STAC (valid),
CAPI (valid), IPX (valid)

Serialnumber        Mask        Key         State
101546              51          88PNUPZ     ok


ADD                        DELETE                          EXIT

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

Listed under Available Licenses are all subsystems available to **BinGO!**, as well as their current status (*builtin* - always available, *valid* - activated, *not_valid* - not activated).

Beneath that, the license entries are shown (*Serialnumber*, *Mask*, *Key*).

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

Subsystems The following subsystems can be activated on your **BinGO!**:

Subsystems	Meaning
IP	IP *routing*
EXTENDLAN	An unlimited number of LAN partners (only with an extra license)
TUNNEL	Virtual Private Networking VPN (only with extra license)
STAC	➤➤ **STAC** ➤➤ **data compression**
CAPI	➤➤ **Remote CAPI** interface makes possible communications applications on your PC, e.g. sending and receiving faxes.
IPX	➤➤ **IPX** routing

Table 6-1: Subsystems

To Do To enter your license, proceed as follows:

➤ Press **ADD**.

Another window menu opens.

➤ Type in the *Serial Number.*

➤ Type in the *Mask.*

➤ Type in the *Key.*

➤ Press **SAVE.**

You have returned to the ***LICENSES*** menu. The subsystems activated by your license data are now listed. Your license has been entered, its current status *ok* is displayed under State.

If you have entered a valid license, *ok* appears under State. If your license was invalid (due to a typing error, perhaps):

➤ Try again.

6.1.2 Entering System Data

Passwords, System names

Next you should enter the basic system data for the identification of your **BinGO!**.

➤ Go to ***SYSTEM***:

```
BinGO! Setup Tool                                BinTec Communications AG
[SYSTEM]: Change System Parameters                                MyBinGO!

System Name                                      MyBinGO!
Local PPP ID (default)                           LittleIndian
Location                                         3rd floor
Contact                                          admin@BigBoss.com

admin Login Password/SNMP Community              secret
read Login Password/SNMP Community               secret1
write Login Password/SNMP Community              secret2

HTTP Server Password                             secret3
Syslog output on serial console                  no
Message level for the syslog table               info
Maximum Number of Syslog Entries                 20

External System Logging>

            SAVE                                    CANCEL

Enter string, max length = 34 chars
```

The following parts of the menu are relevant for the entry of system data:

Field	Meaning
System Name	Defines **BinGO!´s** system name; is also used as a PPP host name; is also used as login prompt. If no system name is registered, a warning message appears on logging in with the user name `admin`.
Local PPP ID	If a non-partner-specific ➤➤ **PPP authentication** is being performed (e.g. ➤➤ **PAP** or ➤➤ **CHAP**), this entry is necessary for the identification of your **BinGO!**. (see chapter 7.4.1, page 219)
Location	(optional) Enter the location of your **BinGO!**.
Contact	(optional) States the contact responsible. If the person can be reached from **BinGO!´s** HTTP status page, a valid e-mail address must be entered here.
admin Login Password	Password for user name admin

Field	Meaning
read Login Password	Password for user name read
write Login Password	Password for user name write
HTTP Server Password	Password for **BinGO!´s** HTTP status page

Table 6-2: ***SYSTEM***

Caution!

All BinTec routers are supplied with the same user names and passwords. Consequently, they are not protected against unauthorized access.

➤ To prevent unauthorized access to **BinGO!**, you must change your passwords.

The permission attached to the various user names and passwords allowed (read, write) can be found in chapter 5.2, page 103.

To Do To enter the relevant system data, proceed as follows:

➤ Type in the *System Name* of your **BinGO!**, e. g. your ***MyBingo***.

➤ Type in the *Local PPP ID*. The entry can be identical to the *System Name*.

➤ Type in the *Location*, e. g. ***Europe***.

➤ Type in your *Contact*, e. g. ***SysAdmin***.

➤ Type in the *admin Login Password*.

➤ Type in the *read Login Password*.

➤ Type in the *write Login Password*.

➤ Type in the *HTTP Server Password*.

➤ Press **SAVE**.

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

6.1.3 Configuring the LAN Interface

➤➤ **IP addresses**
➤➤ **Netmasks**
➤➤ **Encapsulation**

The next step is to configure your **BinGO!´s** LAN interface. The LAN interface is the physical interface to the local network. In the following menu, enter your **BinGO!´s** address where it can be reached in the LAN. As long as **BinGO!** does not have this entry, it can not be recognized by other hosts as a part of the LAN.

You may have already assigned your **BinGO!** its IP address and netmask before the basic configuration, e. g. with the help of the ➤➤ **BootP** server of ➤➤ **DIME** Tools. If you have, check the entries in the following menu anyway.

➤ Go to ***CM-BNC/TP, ETHERNET***:

```
BinGO! Setup Tool                                BinTec Communications AG
[LAN]: Configure Ethernet Interface                              MyBinGO!

IP-Configuration
local IP-Number          192.168.1.254
local Netmask            255.255.255.0
Encapsulation            Ethernet II

IPX-Configuration
local IPX-Netnumber      0
Encapsulation            none

Advanced Settings>

            SAVE                              CANCEL

Enter IP address (a.b.c.d or resolvable hostname)
```

Entries for IP configuration and ➤➤ **IPX** configuration are possible in the menu. This chapter will only explain the configuration of ➤➤ **IP**.

Retain the preset values under IPX configuration. If you wish to use the IPX ➤➤ **protocol**, you can find an explanation of how to configure the LAN interface under IPX in chapter 7.4, page 219.

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

Field	Meaning
local IP-Number	**BinGO!´s** IP address in the LAN
local Netmask	Netmask of the network where **BinGO!** is located
Encapsulation	Defines the kind of header added to the IP packets which run over this LAN interface. Possible values: ■ *Ethernet II (conforms with IEEE 802.3)* ■ *Ethernet SNAP.* In general, you can retain the preset value *Ethernet II*. With *Ethernet II* the LAN interface is called en 1, with *Ethernet SNAP: en1-snap*

Table 6-3: ***CM-BNC/TP, ETHERNET***

To Do To configure your **BinGO!´s** LAN interface, proceed as follows:

➤ Type in **BinGO!´s** *local IP-Number*, e. g. ***192.168.1.254***.

➤ Type in the *local Netmask*, e. g. ***255.255.255.0***.

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

➤ Press **SAVE**.

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

6.1.4 Configuring the WAN Interface

Interface to ISDN

■ The next step involves configuring your **BinGO!´s ➤➤ WAN interface**. The WAN interface is the physical interface to the ➤➤ **ISDN**. Its configuration entails taking two steps:

■ Enter the settings of your ISDN connection:
Here, just the most important parameters of your ISDN connection are set.

- Configuring Incoming Call Answering:
  Here, you tell the ➤➤ **router** how it should react to incoming calls from the WAN.

Autoconfiguration, ISDN Switch Type

Firstly, enter the settings for your ISDN connection.

➤ Go to ***CM-1BRI, ISDN S0***:

```
BinGO! Setup Tool                                BinTec Communications AG
[WAN]: WAN Interface                                            MyBinGO!

    Result of Autoconfiguration: Euro ISDN, point to multipoint

    ISDN Switch Type             autodetect on bootup

    D-Channel                    dialup
    B-Channel 1                  dialup
    B-Channel 2                  dialup


    Incoming Call Answering>
    Advanced Settings>

                      SAVE                        CANCEL

Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
Result of Autoconfiguration	Status of the ISDN autoconfiguration. Automatic ➤➤ **D-channel** recognition runs until a setting has been found or until the ISDN protocol has been entered manually under ISDN switch type.
ISDN Switch Type	Defines the ISDN protocol that your ISDN provider has made available. The following protocols are supported: ■ Euro ISDN ■ 1TR6 ■ National ISDN 1 AT&T NI1, EWSD NI1 ■ AT&T 5ESS Custom ISDN ■ National ISDN 1 Northern Telecom DMS100 ■ Japan NTT INS64

Field	Meaning
D-Channel	D-channel configuration. The dialup value can not be changed.
B-Channel 1	Configuring the first ➤➤ **B-channel**. Possible settings: ■ dialup (this is the standard setting) ■ not used
B-Channel 2	Configuring the second B-channel. possible settings: ■ dialup (this is the standard setting), ■ not used.
SPID B-Channel 1+2	Required for the AT&T protocol. Sets SPID (Service Profile Identifier) for both B-channels.
SPID B-Channel 1	Required for the National ISDN 1 Northern Telecom protocol. Sets the SPID (Service Profile Identifier) for the first B-channel.
SPID B-Channel 2	Required for the National ISDN 1 Northern Telecom protocol. Sets the SPID (Service Profile Identifier) for the second B-channel.
Incoming Call Answering B1	Required for the National ISDN 1 Northern Telecom protocol. The settings for Incoming Call Answering have to be set separately for each B-channel.
Incoming Call Answering B2	Required for the National ISDN 1 Northern Telecom protocol. The settings for Incoming Call Answering have to be set separately for each B-channel.

Table 6-4: ***CM-1BRI, ISDN S0***

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

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

This setting enables **BinGO!** to use its automatic D-channel recognition. As long as the D-channel recognition is running, *running* appears next to *Result of Autoconfiguration*. Once the setting has been found, it is displayed, e.g. *Euro ISDN, point to multipoint*.

If the ISDN protocol is not recognized, it can be entered manually under *ISDN Switch Type*. *The* automatic D-channel recognition is then switched off.

An incorrectly set ISDN protocol prevents successful ISDN data transmission.

➤ Select *B-Channel 1*: *dialup*.

➤ Select B-Channel 2: *dialup*.

➤ Press **SAVE**.

You have returned to the menu ***CM-1BRI, ISDN S0***, and the entries have been saved.

Incoming Call Answering Now you must tell **BinGO!** how it should react to incoming calls from the ISDN. According to the settings in the following menus, **BinGO!** distributes the incoming calls to the appropriate internal services.

BinGO! supports the following services:

- PPP (Routing):
  The ➤➤ **PPP** service is **BinGO!´s** general routing service. Incoming data calls from WAN partners are thus connected with your LAN. In this way, partners outside your own LAN can access hosts within your local network.
- ISDN Login:
  The ➤➤ **isdnlogin** service allows incoming data calls access to the ➤➤ **SNMP shell** of your **BinGO!**. This is how **BinGO!** can, for example, be remotely configured and administrated.
- CAPI:
  The ➤➤ **CAPI** service allows incoming data and voice calls a connection with communications applications on hosts within the LAN that access the data via the ➤➤ **Remote CAPI** interface. This is how hosts connected to **BinGO!** receive faxes, for example.

When a call arrives, **BinGO!** firstly checks the Called Party Number (CPN) that is transmitted by ISDN, and then the type of call (data or voice call). Finally, the call is connected with the appropriate service.(see also figure 6-2, page 131).

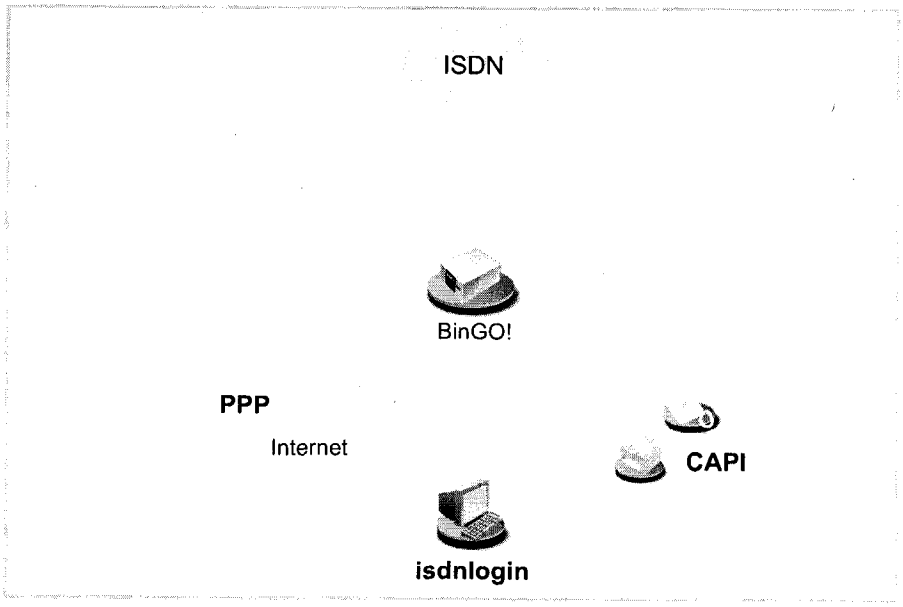


Figure 6-2: DIstribution of incoming calls to services

If your ISDN connection has three phone numbers, a sensible system of distribution could look like this:

Called Party Number	Data Service	Voice Service
11	PPP (Routing)	
12	CAPI	CAPI
13	isdnlogin	

If you do not make any entries in the following menu, all incoming calls will be taken by the service isdnlogin. To avoid this, be sure to make the necessary entries here.

As soon as you have made one or more entries in this menu, the matching incoming calls are distributed to the corresponding services.

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

Now set the entries for Incoming Call Answering:

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

```
BinGO! Setup Tool                                BinTec Communications AG
[WAN][INCOMING]: Incoming Call Answering                          MyBinGO!


Item                          Number       Mode              Username
CAPI 1.1 EAZ 1 Mapping        11           right to left
CAPI 1.1 EAZ 1 Mapping        11           right to left
ISDN Login                    12           right to left
PPP (routing)                 10           right to left

    ADD                  DELETE               EXIT

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

In this menu the allocation of services to phone numbers is listed.

To make entries to the list, proceed as follows:

➤ Include a new entry with **ADD** or select an existing entry, and press **RETURN** to change it.

Another menu window opens:

```
BinGO! Setup Tool                              BinTec Communications AG
[WAN][INCOMING][ADD]:Incoming Call Answering                    MyBinGO!


    Item                        PPP (routing)
    Number                      10
    Mode                        right to left
    Username
    Bearer                      data

                SAVE                        CANCEL

Use <Space> to select
```

The menu includes the following fields

Field	Meaning
Item	A service to which a call should be allocated to the *Number* below.
Number	A dial number at which the above service (*item*) can be reached.
Mode	A mode with which **BinGO!** carries out the numerical comparison *Number* with the Called Party Number of the incoming call: ■ right to left: this is standard. ■ left to right (DDI): Always select, when **BinGO!** is connected with a Point-to-Point connection.
Username	CAPI user name. Only necessary if you want to use the CAPI User Concept. (see chapter 7.1.2, page 184)

Field	Meaning
Bearer	Type of incoming call. Possible settings: ■ data: data call ■ voice: voice call ■ any: data as well as voice calls

Table 6-5: ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** ➧ **ADD**

The *Item* field includes the following selection:

Possible Values	Meaning
PPP (routing)	Standard setting for ➤➤ **PPP** routing. Also applicable for the PPP connections below.
ISDN Login	Enables logging in with ➤➤ **isdnlogin**
PPP 64k	Enables 64 kbps PPP data connections.
PPP 56k	Enables 56 kbps PPP data connections.
PPP Modem	unavailable on **BinGO!**
PPP DOVB	Data transmission Over Voice Bearer - useful in the USA, for example, where voice connections are sometimes cheaper than data connections.
PPP V.110 (1200...38400)	Enables PPP connections with V.110 with bitrates of 1200 bps, 2400 bps,..., 38400 bps.
Pots	unavailable on **BinGO!**
PPP Modem Profile 1...8	unavailable on **BinGO!**
CAPI 1.1 EAZ 0...9 Mapping	Enables connections with Remote CAPI applications. Required for CAPI 1.1 applications only.
X.25 PAD	unavailable on **BinGO!**

Table 6-6: *Item*

To Do Make the following entries:

- ➤ Select *Item*, e. g. ***PPP (routing)***.
- ➤ Select *Number*, e. g. ***11***.
- ➤ Select *Mode*, e. g. ***right to left***.
- ➤ Select *Bearer*, e. g. ***data***.
- ➤ Press **SAVE**.

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

  You have thus assigned a service (***PPP (routing)***) to one of your phone numbers (***11***). This means that when a data call is received by Called Party Number 11, it is put through to the service PPP (routing).

Because **BinGO!** forwards to the ➤➤ **CAPI** service all incoming calls that do not match any entry in the menu, it is not entirely necessary to enter CAPI! (Except CAPI 1.1 applications.)

- ➤ Repeat these steps until all phone numbers are assigned to services which can be reached at those numbers.

  You have now finished configuring Incoming Call Answering, your **BinGO!** will distribute the incoming calls to the internal services.

Make sure to enter the right *Number* that means the actual number that arrives at **BinGO!**. If your **BinGO!** is connected to a ➤➤ **PABX** system, only the extension number arrives at **BinGO!**.

If you are not sure of the number arriving ar **BinGO!**, proceed as follow:

- ➤ Call **BinGO!** with a conventional telephone using one of its numbers.
- ➤ Go to ***MONITORING AND DEBUGGING*** ➧ ***ISDN MONITOR***.
  In the menu, you can see the incoming call.
- ➤ Place the cursor on the call and type in d (details).
- ■ Under Local Number, you can see the part of the number that arrives at **BinGO!**.
- ■ Type in this part of the number in ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** ➧ ***ADD*** under *Number*.

Using the CAPI User Concept (see chapter 7.1.2, page 184), you can reserve access to the CAPI services for certain users with their own passwords.

6.1.5 Configuring BinGO! as a DHCP Server

Every PC in your ➤➤ **LAN**, as well as your **BinGO!**, requires its own IP address. If you configure **BinGO!** as a ➤➤ **DHCP** (Dynamic Host Configuration Protocol) server, it automatically assigns those PCs in the LAN ➤➤ **IP addresses**, out of a pre-defined IP address pool. A PC sends out an address request and in turn receives its IP address from **BinGO!**. You do not have to bother assigning PCs fixed IP addresses, you have, as a result, less configuring to do in your network. To do this, you must set up a pool of IP addresses, from which **BinGO!** assigns IP addresses to hosts in the LAN, albeit for a defined period of time. A DHCP server also forwards the addresses of the Domain Name Server (➤➤ **DNS**), ➤➤ **NetBIOS** name servers (WINS) and the standard ➤➤ **Gateway**.

➤ Go to ***IP*** ➧ ***DHCP SERVER*** ➧ **ADD**:

```
BinGO! Setup Tool                              BinTec Communications AG
[IP][DHCP][ADD]: Add range of IP Addresses                      MyBinGO!

    Interface                              en1
    IP Address                             192.168.1.1
    Number of consecutive addresses        8
    Lease Time (Minutes)                   120
    MAC Address

        SAVE                          CANCEL

Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
Interface	An interface to which the address pool is assigned. When an address request comes in over *Interface* one of the addresses in the pool is assigned.
IP Address	First IP address in the address pool.
Number of consecutive addresses	Total number of IP addresses in the IP address pool, including the first IP address.
Lease Time (Minutes)	Specifies the length of time an address from the pool can be assigned to a host. After the *Lease Time (Minutes)* expires, the address can be reassigned elsewhere.
MAC Address	(optional) Only when *Number of consecutive addresses = 1:* IP address is only assigned to a device with a *MAC Address*

Table 6-7: ***IP*** ➧ ***DHCP SERVER*** ➧ **ADD**

ToDo To set up **BinGO!** as a DHCP server, proceed as follows:

➤ Select *Interface*, e. g. ***en1***.

➤ Type in *IP Address*, e. g. ***192.168.1.1***

- Type in *Number of consecutive addresses*, e. g. *8*.
- Type in *Lease Time (in minutes)*, e. g. *120*.
- Type in *MAC Address* (optional).
- Press **SAVE**.

  You have returned to ***IP*** ➧ ***DHCP SERVER***, where the IP address pool is listed. The entries have been saved.

By also creating several entries, you can define unconnected address ranges, e.g. 192.168.1.20; 192.168.1.29 and 192 168.1.40 and so on.

6.1.6 Setting Filters

NetBIOS filters

If you are working with Windows in your local network, you should set the ➤➤ **NetBIOS** filter, in order to reduce expenses. This prevents **BinGO!** establishing connections to your Internet Service Provider (➤➤ **ISP**), for example, in order to forward WINS requests from PCs in your network. This means that **BinGO!** asks your ISP which ➤➤ **host name** can be assigned an IP address. Because the ISP can not resolve WINS names, these connections are unnecessary and cost money.

A more detailed explanation of the subject of ➤➤ **filters** can be found in chapter 8.2.8, page 250.

To prevent these unnecessary connections, proceed as follows:

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

- Use the serial interface or isdnlogin on **BinGO!** for filter configuration.
- If you use telnet: In the ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES*** ➧ **EDIT** menu, select *First Rule*: *none*.
- Go to ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER*** ➧ **ADD**:

```
BinGO! Setup Tool                              BinTec Communications AG
[IP][ACCESS][FILTER][ADD]: Configure IP Access Filter          MyBinGO!

    Description                wrong_dns
    Index                      1

    Protocol                   udp

    Source Address
    Source Mask
    Source Port                specify
    Specify Port               137

    Destination Address
    Destination Mask
    Destination Port           specify
    Specify Port               53

                      SAVE                          CANCEL

Enter string, max length = 48 chars
```

To Do Make the following entries:

- Type in *Description*: *wrong_dns*.
- Select *Protocol*: *udp*.
- Select *Source Port*: *specify*.
- Select *Specify Port*: *137*.
- Select *Destination Port*: *specify*.
- Type *in Specify Port*: *53*.
- Press **SAVE**.

  You have returned to ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER***. The entries have been saved.

Now define a second filter as follows:

- Go back to ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER*** ➧ **ADD**.
- Type in *Description*: *all*.
- Select *Protocol*: *any*.
- Select *Source Port*: *any*.
- Select *Destination Port*: *any*.

➤ Press **SAVE**.

You have returned to ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER***. The entries have been saved, both filters are now listed.

To define rules for these filters, proceed as follows:

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

```
BinGO! Setup Tool                                BinTec Communications AG
[IP][ACCESS][RULE][ADD]: Configure IP Access Rules              MyBinGO!

    Action                deny M
    Filter                wrong_dns (1)

                  SAVE                        CANCEL

Use <Space> to select
```

ToDo Make the following entries:

➤ Select *Action*: *deny M*.

➤ Select *Filter*: *wrong_dns (1)*.

➤ Press **SAVE**.

You have returned to ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES***. The entries have been saved.

Now define a second rule as follows:

➤ Return to ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **ADD**:

➤ Select *Insert behind Rule*: *RI 1 FI 1 (wrong_dns)*.

➤ Select *Action*: *allow M*.

➤ Select *Filter*: *all (2)*.

➤ Press **SAVE**.

You have returned to ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES***. The entries have been saved and listed.

```
BinGO! Setup Tool                                BinTec Communications AG
[IP][ACCESS][RULE]: Configure IP Access Rules                    MyBinGO!

Abbreviations:  RI (Rule Index)  M  (Action if filter matches)
                FI (Filter Index)!M (Action if filter does not match)
                NRI (Next Rule Index)

RI  FI  NRI     Action  Filter      Conditions
1   1   2       deny  M wrong_dns   udp, sp 137, dp 53
2   2   0       allow M all

        ADD             DELETE          REORG           EXIT

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

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

```
BinGO! Setup Tool                                BinTec Communications AG
[IP][ACCESS][INTERFACES]: Configure First Rule                   MyBinGO!

    Configure first rules for interfaces

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


    EXIT

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

To Do Make the following entries:

➤ Select **BinGO!**´s LAN interface (*en1* or *en1-snap*) and press **Return.**

➤ Select *First Rule*: *RI 1 FI 1 (wrong_dns).*

➤ Press **SAVE.**

➤ These entries ensure that all data traffic which passes from source ➤➤ **port** 137 to destination port 53 will be discarded. This means, in turn, that no unnecessary connections will be established to resolve WINS names.

➤ Leave ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES*** via **EXIT**.

➤ Leave ***IP*** ➧ ***ACCESS LISTS*** via **EXIT**.

➤ Leave ***IP*** via **EXIT**.

You have returned to the main menu.

The basic configuration of the router settings is complete.

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

The settings are thus saved to the Flash and will not be lost when **BinGO!** is switched off (chapter 6.3, page 179).

6.2 BinGO! and the WAN

If you have carried out the configuration steps in chapter 6.1, page 119, **BinGO!** is set up for your ➤➤ **LAN**. If you also want to access hosts outside your LAN, e.g. to surf the ➤➤ **Internet,** then this chapter will be of interest to you.

The following points will be considered:

- Configuring ➤➤ **WAN partners**:
  To enable **BinGO!** to make connections to networks outside your LAN, you must configure on your **BinGO!** those partners you want to connect with as WAN partners. This applies for outgoing connections (**BinGO!** dials its WAN partner), as well as for incoming connections (a WAN partner dials the number of your **BinGO!**). Consequently, if you want to access the Internet, you must set up your Internet Service Provider (➤➤ **ISP**) as a WAN partner. If you wish to establish a LAN-LAN connection, e.g. between your LAN and the LAN of your head office (central site connection), you have to configure the LAN of your head office as a WAN partner.
  How to set up a WAN partner on your **BinGO!** is explained in general terms in chapter 6.2.1, page 144.

- Configuring for Internet access by means of examples:
  In chapter 6.2.2, page 169, you will find examples of how to set up an ISP as a WAN partner. If you want to access the Internet with one of the following providers, you will find a convenient procedure to connect to the Internet with **BinGO!**:
  - T-Online
  - Compuserve

- Connecting with a corporate network by means of an example:
  In chapter 6.2.3, page 175, you will find an example of how to establish a corporate network connection with your **BinGO!**. In many cases, this fast procedure should be entirely sufficient.

A basic scenario is illustrated in figure 6-3, page 144, giving an idea of how connections to the WAN partners, ISP and corporate head office, could look!

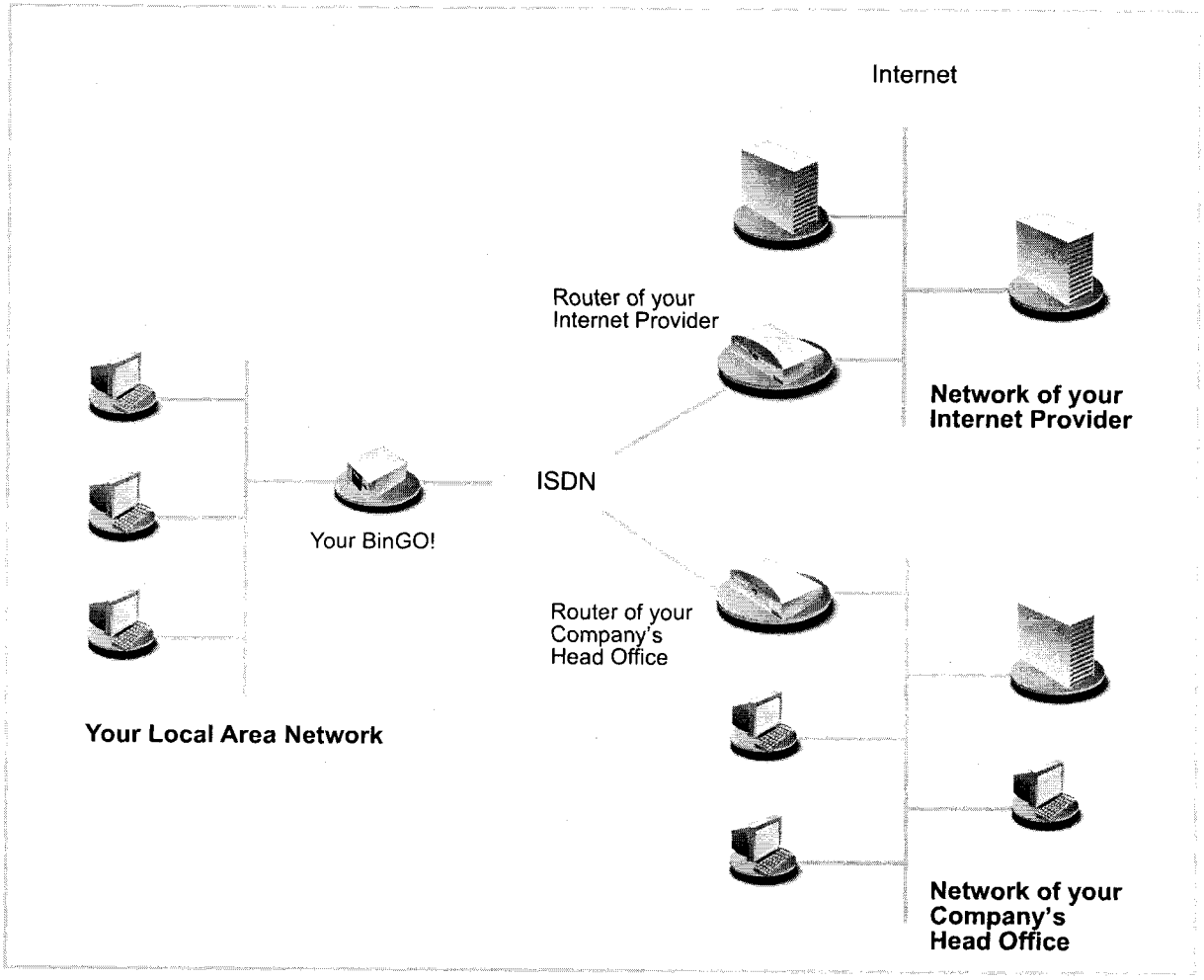


Figure 6-3: Basic scenario

6.2.1 Configuring a WAN partner

In general, establishing a WAN partner involves the following steps:

- Enter the WAN partner
  - Determine a ➤➤ **protocol**

- Enter dial number(s)
- Determine ➤➤ **PPP** settings for authentication
- Define ➤➤ **Short Hold**
- Carry out IP configuration

■ Create routing entry

■ Activate Network Address Translation (➤➤ **NAT**) (optional)

Off we go!:

Entering a WAN partner

Configuring a WAN partner

Here you are going to establish access to your chosen WAN partner, e.g. your Internet Service Provider (ISP). Before you get down to it, you should collect the necessary access information that you received from your ISP or system administrator (see chapter 3.2.1, page 38). The terms used may vary slightly from provider to provider.

To enter a WAN partner, proceed as follows:

➤ Go to ***WAN PARTNER***:

```
BinGO! Setup Tool                                BinTec Communications AG
[WAN]: WAN Partners                                              MyBinGO!

Current WAN Partner Configuration

    Partnername              Protocol        State
    BigBoss                  ppp             dormant



ADD                  DELETE              EXIT

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

This is where all WAN partners currently configured are listed with the corresponding *Partnername*, *Protocol* and *State*. *State* can have the following values:

■ *up:* connected

- *dormant:* not connected
- *blocked:* not connected (on establishing a connection an error arose, a renewed attempt is only possible after a specified number of seconds, see chapter 7.2.1, page 193)
- *down:* set to down by administration

To make an entry in the list, proceed as follows:

➤ Select **ADD** to create a new entry or select an existing entry and press **Return** to modify it.

Another menu window opens:

```
BinGO! Setup Tool                              BinTec Communications AG
[WAN][ADD]:Configure WAN Partner                                MyBinGO!

    Partner Name                  BigBoss

    Encapsulation                 PPP
    Compression                   none
    Encryption                    none
    Calling Line Identification   no

    WAN Numbers >
    PPP >
    Advanced Settings >

    IP >
    IPX >

                      SAVE                      CANCEL

Enter string, max length = 25 chars
```

The menu contains the following fields:

Field	Meaning
Partner Name	Enter a name with which to identify the WAN partner.

Field	Meaning
Encapsulation	➤➤ **Encapsulation**. Defines the type of header added to the ➤➤ **data packets** that run to this WAN-Partner over the interface. ■ *PPP* ■ *Multi-Protocol LAPB Framing* ■ *Multi-Protocol HDLC Framing* ■ *Async PPP over X.75* ■ *Async PPP over X.75/T.70/BTX* ■ *X.25_PPP:* not available on **BinGO!** ■ *X.25:* not available on **BinGO!** ■ *HDLC Framing (only IP)* ■ *LAPB Framing (only IP)* ■ *X31 B-Channel:* not available on **BinGO!** ■ *X.25 No Signalling:* not available on **BinGO!** ■ *X.25 PAD:* not available on **BinGO!** ■ *X.25 No Configuration:* not available on **BinGO!** ■ *Frame Relay:* not available on **BinGO!** ■ *X.25 No Configuration, No Signalling:* not available on **BinGO!**

Field	Meaning
Compression	Establishes the type of compression that should be used for data traffic with the WAN partner. Possible values: ■ *STAC*: only when *Encapsulation = PPP* ■ *MS-STAC*: only when *Encapsulation = PPP* ■ *MPPC*: not available on **BinGO!** ■ *V.42bis*: only with *Multiprotocol LAPB Framing* or *LAPB framing (only IP)* encapsulation ■ *none*
Encryption	Defines the type of encryption that should be used for data traffic with the WAN partner. Only possible if STAC compression is not activated for the connection. Possible values: ■ MPPE 40: only when *Encapsulation = PPP* ■ MPPE 128: only when *Encapsulation = PPP and Authentication = MS-CHAP* ■ none:
Calling Line Identification	Displays whether calls from this WAN partner should be identified by means of the Calling Party's Number (➤➤ **CLID**). The value of this field is dependent on *Direction* in the submenu ***WAN NUMBERS***.

Table 6-8: ***WAN PARTNER*** ➧ **ADD**

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

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

Table 6-9: Encapsulation and compression

To Do Make the following entries:

- ➤ Type in *Partner Name*, e. g. ***BigBoss***.
- ➤ Select *Encapsulation*, e. g. ***PPP***.
- ➤ Select *Compression*, e.g. ***none***.
- ➤ Select *Encryption*, e. g. ***none***.
- ➤ Select ***WAN PARTNER*** ➧ **ADD** ➧ *WAN Numbers*:

Entering dial numbers

```
BinGO! Setup Tool                                BinTec Communications AG
[WAN][ADD][WAN Numbers]: WAN Numbers (BigBoss)                  MyBinGO!

    WAN Numbers for this partner:

        WAN Number          Direction
        0911987654321       outgoing


    ADD                 DELETE                  EXIT

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

This is where the phone numbers of all WAN partners currently listed are shown.

To make an entry in the list, proceed as follows:

➤ Select **ADD** to create a new entry or select an existing entry and press **Return** to modify it.

Another menu window opens:

```
BinGO! Setup Tool                                    BinTec Communications AG
[WAN][ADD][WAN NUMBERS][ADD]:Add or Change WAN Numbers(BigBoss)
                                                                    MyBinGO!


    Number                    0911987654321
    Direction                 outgoing

    Advanced Settings >


              SAVE                              Cancel

Enter string, max length = 40 chars
```

The menu contains the following fields:

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

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

The *Direction field contains the following selection*:

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

Table 6-11: *Direction*

When **BinGO!** is connected to a PABX system for which a leading "0" is necessary for an external call, this "0" must be considered when entering the dial number.

Wildcards

When entering the *Number*, you can either enter the sequence digit for digit or you can replace single numbers or groups of numbers with wildcards.

You can use the following wildcards, which have different effects for incoming and outgoing calls:

Wildcard	Meaning		Example		
	Incoming calls	Outgoing calls	Number	**BinGO!** accepts incoming calls e.g. with:	Outgoing calls: **BinGO!** makes connections to WAN partners with:
*	Matches none or more digits.	Is ignored.	123*	123, 1234, 123789	123
?	Matches any single digit.	Is replaced by 0.	123?	1234, 1238, 1231	1230
[a-b]	Denotes a range of possible digits to match.	The first digit of the specified range is used.	123[5-9]	1235, 1237, 1239	1235
[^a-b]	Specifies a range of excluded digits.	The first digit after the specified range is used.	123[^0-5]	1236, 1238, 1239	1236
{ab}	Optional sequence to match.	Sequence is used.	{00}1234	00123 and 123	00123

Table 6-12: Wildcards for incoming and outgoing calls

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

To Do Make the following entries:

- Enter the *Number*, e. g. ***0911987654321***.
- Select the *Direction*, e. g. ***outgoing***.
- Press **SAVE**.
  The entries have been saved and are listed.
- Leave ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS*** with **EXIT**.

➤➤ PPP authentication

Next enter the PPP settings of your WAN partner. They serve to authenticate your connecting partner.

When a call comes in, the Calling Line Number is always given over the ISDN ➤➤ **D-channel**. This number allows **BinGO!** to identify the caller (➤➤ **CLID**), provided the caller is entered as a WAN partner. After identification with CLID, **BinGO!** can additionally carry out PPP authentication with the WAN partner before it takes the call. In order to do this, it needs the necessary data that you should enter here. Firstly, establish the type of authentication process that should be performed. Then enter a common password and two user names. You will get this data from your WAN partners, e.g. from your Internet Service Provider (ISP) or the system administrator at your head office. The call is only taken if the data entered on the **BinGO!** matches the caller's data.

To set WAN partner PPP authentication, proceed as follows:

- Go to **WAN partner** ➧ **ADD** ➧ ***PPP***:

```
BinGO! Setup Tool                              BinTec Communications AG
[WAN][ADD][PPP]: PPP Settings (BigBoss)                        MyBinGO!


    Authentication              CHAP + PAP
    Partner PPP ID              BigBoss
    Local PPP ID                LittleIndian
    PPP Password                Secret

    Keepalives                  off
    Link Quality Monitoring     off


                OK                                CANCEL

Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
Authentication	Authentication protocol
Partner PPP ID	ID of WAN partner
Local PPP ID	ID of **BinGO!**
PPP Password	Password
Keepalives	Activates keepalive packets
Link Quality Monitoring	PPP Link Quality Monitoring acc. to RFC 1989

Table 6-13: ***WAN PARTNER ➧ ADD ➧ PPP***

The *Authentication* field contains the following selection

Possible Values	Meaning
PAP	Only ➤➤ **PAP** (PPP Password Authentication Protocol), password is transferred uncoded.
CHAP	Only ➤➤ **CHAP** (PPP Challenge Handshake Authentication Protocol acc. to RFC 1994), password is transferred coded
CHAP + PAP	Primarily CHAP, or else PAP
MS-CHAP	Only MS-CHAP (MS Challenge Handshake Authentication Protocol)
CHAP + PAP + MS-CHAP	Primarily CHAP, on denial, the authentication protocol required by the WAN partner
none	No PPP authentication protocol

Table 6-14: *Authentication*

To Do Make the following entries:

- ➤ Select *Authentication*, e. g. *CHAP*.
- ➤ Type in *Partner PPP ID*, e. g. ***BigBoss***.
- ➤ Type in *Local PPP ID*, e. g. ***LittleIndian***.
- ➤ Type in *PPP Password*, e. g. ***Secret***.
- ➤ Select *Keepalives*, e. g. ***off***.
- ➤ Select *Link Quality Monitoring*, e. g. ***off***.
- ➤ Press **OK**.

  You have returned to ***WAN PARTNER*** ➧ **ADD**.

In some cases, the caller can not be identified with ➤➤ **CLID**, although he has been entered as a WAN partner. In this case, your **BinGO!** does not know which authentication protocol was set for this WAN partner. Nevertheless, in order that the call can be taken, **BinGO!** refers back to general settings, which you can change, if necessary (see chapter 7.1.4, page 190).

Setting Short Hold

Next you can save money by setting Short Hold. **BinGO!** cuts the ISDN connection when there is no further data exchange. Either a static or dynamic Short Hold setting tells **BinGO!** when to cut the ISDN connection.

Static

The static ➤➤ **Short Hold** setting determines how much time should pass between the sending or receiving of the last ➤➤ **data packet** and the cutting of the ISDN connection. You specify a fixed period of time in seconds.

Dynamic

With the dynamic Short Hold setting, no fixed period of time is specified, instead, the length of an ISDN charging unit is considered. Dynamic Short Hold is guided by AOCD (advice of charge during the call).

When fixing dynamic Short Hold, you specify how much time should pass after the last exchange of data before the connection is cut. A percentage that refers to the last charging unit is given. Thus the value of Idle Timer can change, just as the length of the charging unit changes (according to the time of day, weekend, weekday etc.). If you specify 50%, then Idle Timer will take 60 seconds if the previous charging unit was 120 seconds long and 300 seconds if the previous charging unit was 600 seconds long. The connection is ended after Idle Timer runs out and shortly before the start of the next charging unit.

Bear in mind that you can only use dynamic Short Hold if, when connected, you receive charging information. Ask your telephone company!

When using dynamic Short Hold, it is essential to additionally set static Short Hold so that if AOCD fails, you do not get a permanent switched connection.

You should be aware that static Short Hold engages later than dynamic. However, **BinGO!** always cuts the connection according to static Short Hold, leaving dynamic without a chance to disconnect. In this case, specify a value for static Short Hold more than the expected maximum dynamic inactivity interval.

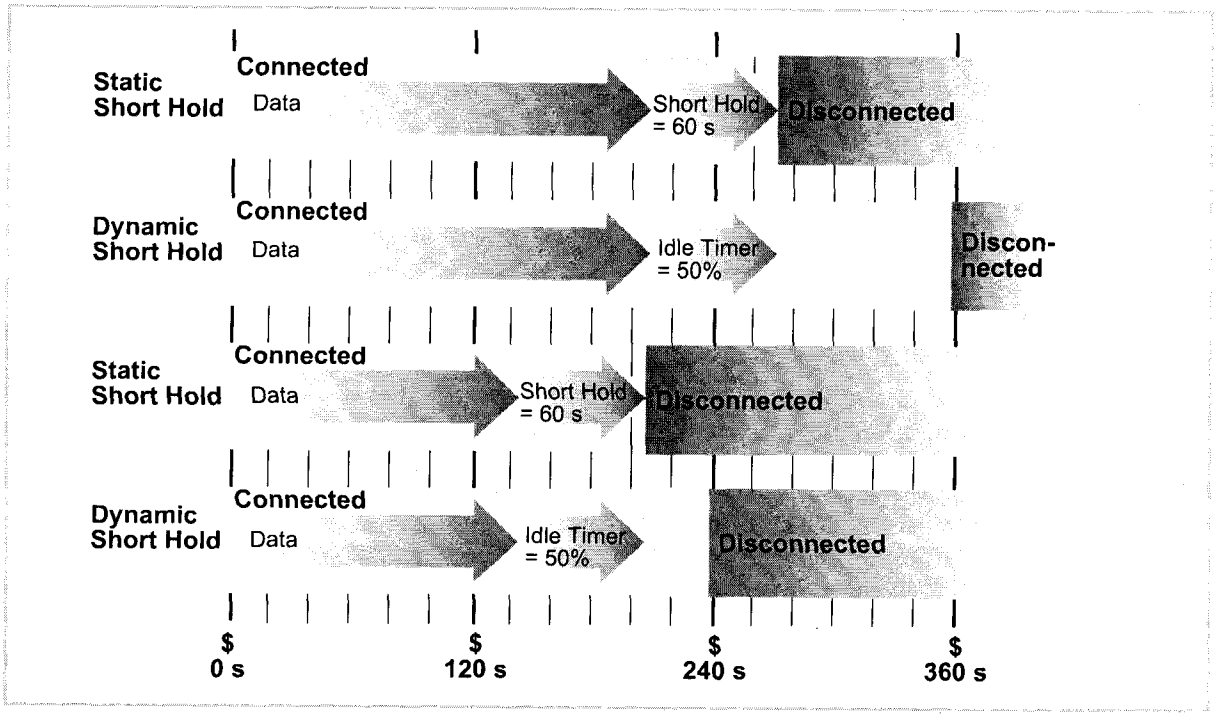


Bild 6-4: Dynamic and static Short Hold

Proceed as follows:

➤ Select ***WAN PARTNER*** ➧ **ADD** ➧ *Advanced Settings:*

```
BinGO! Setup Tool                                BinTec Communications AG
[WAN][ADD][ADVANCED]: Advanced Settings (BigBoss)              MyBinGO!

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

Channel-Bundling                          no

Layer 1 Protocol                          ISDN 64 kbps

                OK                                        CANCEL

Use <Space> to select
```

The following parts of the menu are relevant for these configuration steps:

Field	Meaning
Static Short Hold (sec)	Inactivity interval in seconds for static Short Hold. Example values for a long-distance call: 60, if charging information are transmitted during the connection. (AOCD) Otherwise 20.
Idle for Dynamic Short Hold (%)	Inactivity interval as a percentage for static Short Hold. Only effective if charging impulses are transmitted during the connection. (AOCD).

Table 6-15: WAN Partner ➧ ADD ➧ Advanced Settings

To Do Make the following entries:

- Type in seconds in *Static Short Hold*, e. g. *20*.
- Type in % in *Idle for Dynamic Short Hold*, e. g. *0*.
- Press **OK**.

  You have returned to ***WAN PARTNER*** ➧ **ADD**.

Tips for the entry of Idle for dynamic Short Hold %:

- For interactive connections (e.g. ➤➤ **telnet**, specify a high value (e.g. 80...90)to avoid connection cuts during short phases without data exchange.
- For Internet connections (e.g. WWW, http, etc), specify a middle to high value (e.g. 50...80) to avoid connection cuts while waiting.
- For data connections (e.g. ➤➤ **ftp**), specify a low value (e.g. 10...40) to avoid the unnecessary continuation of a connection after data has been transferred.

You will find a more detailed explanation about static and dynamic Short hold in the Software Reference.

IP configuration

Now we´ll move on to the IP configuration of your WAN partner. Here you will enter the ➤➤ **IP address** and ➤➤ **netmask** of your partner.

Proceed as follows:

➤ Select ***WAN PARTNER*** ➧ **ADD** ➧ *IP*

```
BinGO! Setup Tool                                BinTec Communications AG
[WAN][ADD][IP]: IP Configuration (BigBoss)                       MyBinGO!

    IP Transit Network                    no

    Partner's LAN IP Address              10.1.1.0
    Partner's LAN Netmask                 255.255.255.0

    Advanced Settings >

                    SAVE                        CANCEL

Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
IP Transit Network	Determines if **BinGO!** establishes a transit network to the WAN partner.
local ISDN IP Address	ISDN IP address of **BinGO!** in the transit network.
Partner's ISDN IP Address	ISDN IP address of WAN partner in the transit network.
Partner's LAN IP Address	IP address of the LAN of the WAN partner.
Partner's LAN Netmask	Netmask of the LAN of the WAN partner. If no entry is made, **BinGO!** enters a standard netmask for the netclass used under the partner´s LAN IP address.

Table 6-16: ***WAN PARTNER*** ➧ **ADD** ➧ ***IP***

To Do Make the following entries (normally sufficient for a corporate network connection):

- ➤ Select *IP Transit Network*: e. g. ***no***.
- ➤ Type in *Partner's LAN IP Address*, e.g. ***10.1.1.0***.
- ➤ Enter *Partner's LAN Netmask*, e.g. ***255.255.255.0***.

➤ Press **SAVE**.

➤ Press **SAVE** again.

You have returned to ***WAN PARTNER***. Your entries have been saved.

If you are setting up access to the Internet, you do not normally know the IP address of your Internet Service Provider (ISP). Either your **BinGO!** is dynamically (for the duration of the connection) assigned its *local ISDN IP Address* or statically from the ISP. In such a case, make the following settings in the menu: ***WAN PARTNER*** ➧ **ADD** ➧ ***IP***:

➤ IP address is dynamically assigned
- Select *IP Transit Network*: *dynamic client.*

➤ IP address is statically assigned:
- Select *IP Transit Network*: yes.
- *Local ISDN IP address*: **BinGO!**´s static IP address you get from your ISP (often termed your Gateway or your router address).
- *Partner´s ISDN IP address*: Partner ´s IP address (if known) or else **BinGO!**´s static IP address you get from your ISP.
- No entries for *partner´s LAN IP address* and *partner´s LAN netmask.*

If you want to know more about what a transit network actually is, for example, and what you need it for, see chapter 7.2.4, page 197.

To be able to use the Domain Name Server of the ISP while connected, adjust the following setting in the menu: ***WAN PARTNER*** ➧ **ADD** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***:

➤ Select *Dynamic Name Server Negotiation*: *client (receive).*

This setting is only necessary if you have not entered IP addresses for DNS servers on the PCs of your LAN.

Creating Routing Entries

Routing entry

You have just entered a WAN partner on your **BinGO!**. For every WAN partner entered, a routing entry in the routing table of your **BinGO!** is automatically created. You can edit existing IP routes and add new ones. For the connection to your Internet Service Provider, you should always configure the default route.

Proceed as follows:

➤ Go to ***IP*** ➧ ***ROUTING***:

```
BinGO! Setup Tool                                BinTec Communications AG
[IP][ROUTING]: IP Routing                                       MyBinGO!

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

Destination Gateway          Mask          Flags   Met Interface    Pro
192.168.1.1 192.168.1.254    255.255.255.0US       0   en1          loc
10.1.1.0                     255.255.255.0DI       0   BigBoss      mgmt
default                      0.0.0.0       DI      0   GoInternet   mgmt

    ADD              DELETE                EXIT

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

All IP routes entered are listed here. Under *Flags* the current status (Up, Dormant, Blocked) and the type of route (Gateway Route, Interface Route, Subnet Route, Host Route) are displayed. The protocol with which **BinGO!** has "learned" the routing entry is displayed under *Pro*.

To define a route, proceed as follows:

➤ To add a new IP route select **ADD** or select an existing entry and press **Return** .

Another menu window opens:

```
BinGO! Setup Tool                                BinTec Communications AG
[IP][ROUTING][ADD]: IP Routing                                   MyBinGO!


    Route Type                    Network route
    Network                       WAN without transit network


    Destination IP-Address        10.1.1.0
    Netmask                       255.255.255.0
    Partner / Interface           BigBoss

    Metric                        1


                  SAVE                        CANCEL

Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
Route Type	Type of route. Possible values: ■ *Host route:* Route to a single host ■ *Network route:* Route to a network ■ *Default route:* Is only used when no other suitable route is available
Network	Specifies the type of connection (LAN, WAN).
Destination IP-Address	IP address of the destination host or LAN.
Netmask	Netmask of the partner LAN (only possible for *Route Type* = *Network route*, if no entry is made the router uses a standard netmask).
Partner / Interface	WAN partner (only possible for *Network* = *WAN without transit network*).
Gateway IP-Address	IP address of the host to which **BinGO!** should forward the data packet.
Metric	The lower the value, the higher the priority of the route. (range of values 1...14)

Table 6-17: ***IP ➧ ROUTING ➧ ADD***

The *Network* field contains the following selection:

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

Table 6-18: *Network*

You can only configure one default route on your **BinGO!**. So, if you are setting up access to the Internet, then set up the route to your ISP as a default route. If you are connecting to a corporate network, then set up the default route to head office only if you are not setting up access to the Internet over the **BinGO!**.

If you are configuring Internet access as well as a connection to a corporate head office, use the default route to your ISP and configure a network route to your headquarters.

Default route

➤ To set up a default route, proceed as follows:

➤ Select *Route Type*: *Default Route*.

➤ Select *Network*: *WAN without transit network*.

➤ Select *Partner / Interface*: e. g. ***GoInternet***.

➤ Enter *Metric*: e. g. *1*.

➤ Press **SAVE**.

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

The corporate network can consist of several LANs with different IP addresses and netmasks (➤➤ **subnets**). If you do not want to access your head office as a default route (e. g. because you set up your Internet access as a default route), then, for all the networks you want to reach at the central site, a separate routing entry must be made.

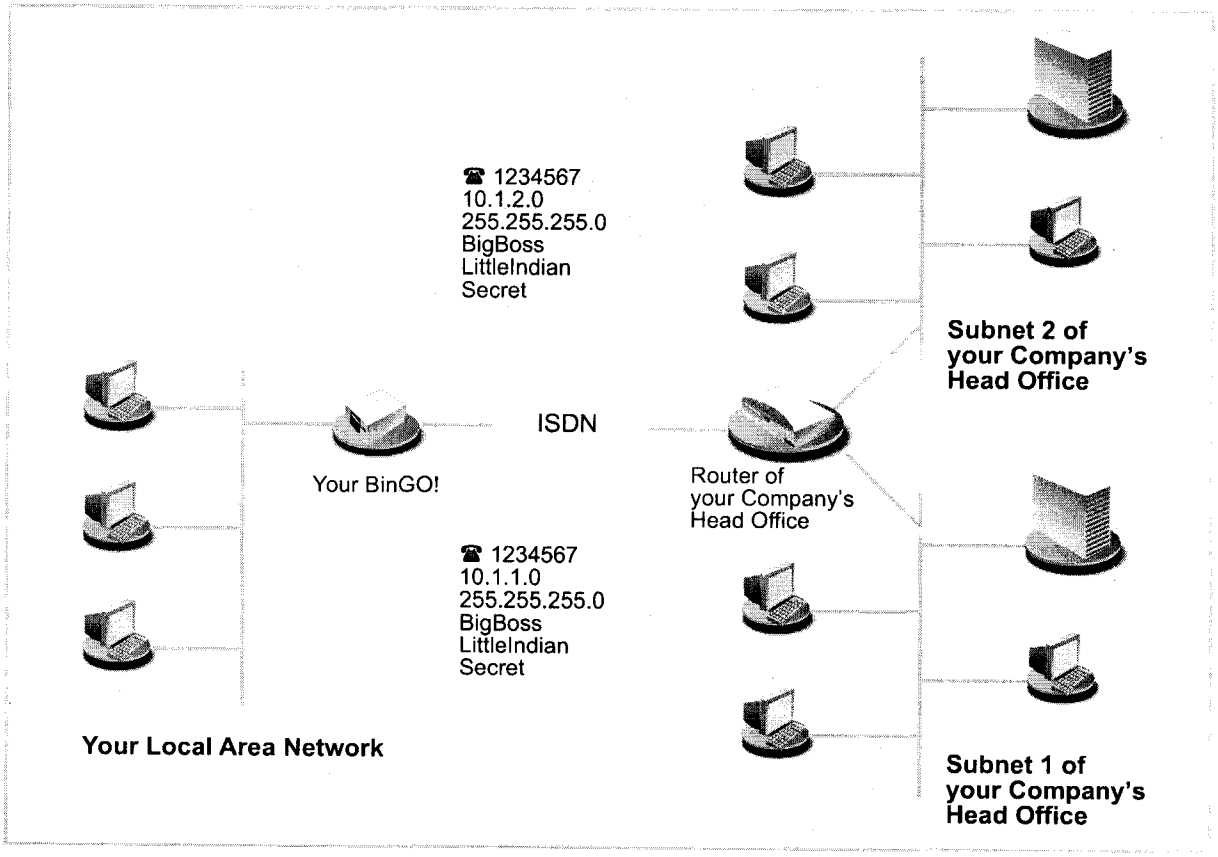


Figure 6-5: Corporate network with several connected LANs

Network route

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

- Select *Route Type*: *network route*.
- Select *Network*: *WAN without transit network*.
- Type in *Destination IP-Address*, e. g. ***10.1.2.0***.
- Type in *Netmask*, e. g. ***255.255.255.0***.
- Type in *Partner / Interface*, e. g. ***BigBoss***.
- Type in *Metric*, e. g. *1*.
- Press **SAVE**.

  You have returned to ***IP*** ➧ ***ROUTING***. The entries have been saved, the newly entered or modified routes are listed.

  Repeat these steps if you have to enter several routes.

Activating Network Address Translation (NAT)

Activating NAT

Here, you can activate Network Address Translation (➤➤ **NAT)** for your WAN partner. You thus present your whole network to the outside with just the one IP address. It is most advisable do this for your connection to the Internet Service Provider.

More information about Network Address Translation (NAT) can be found in chapter 8.2.7, page 244.

To activate NAT, proceed as follows:

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

```
BinGO! Setup Tool                                    BinTec Communications AG
[IP][NAT]: NAT Configuration                                        MyBinGO!

Select IP Interface to be configured for NAT

GoInternet
BigBoss
en1
en1-snap


EXIT

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

➤ Mark the interface or the WAN partner for which you want to activate NAT (e. g. GoInternet) and press **Return.**

Another menu window opens:

```
BinGO! Setup Tool                                    BinTec Communications AG
[IP][NAT][CONFIG]: NAT Configuration (GoInternet)                   MyBinGO!

Network Address Translation      on

Configuration for sessions requested from outside

Service      Destination      Source Dep.      Dest. Dep.   Port Remap


    ADD              DELETE               SAVE             CANCEL

Use <Space> to select
```

To Do Make the following entries:

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

➤ Press **SAVE**.

Network Address Translation is activated for the selected interface or WAN partner.

➤ Leave ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** with **EXIT**.

➤ Leave ***IP*** with **EXIT**.

You have returned to the main menu, after configuring a WAN partner.

6.2.2 Provider-Specific Internet Access

Subsequent to chapter 6.2.1, page 144 where general procedures applicable to all Internet Service Providers (ISP) were described, here are a few concrete examples. Quickly and easily, they show you how to set up Internet access with certain providers.

- Example 1: T-Online
- Example 2: Compuserve

Keep at hand the access information you received from your ISP (see chapter 3.2.1, page 38). The terms may vary slightly from provider to provider.

Off we go:

Example 1: T-Online

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

Configuring a WAN partner

- Go to ***WAN PARTNER*** ➧ **ADD**.
- Type in the *Partner Name* (= provider name): *T_ONLINE.*
- Select *Encapsulation*: *PPP.*
- Select *Compression*: *none.*
- Select *Encryption*: *none.*

Entering a dial number

- Select *WAN Numbers* and press **Return**.
- Add a new entry with **ADD**.
- Type in the *Number* (= dial-in number): *0191011.*
- Select *Direction*: *outgoing.*
- Press **SAVE**.

  The dial number you use to call T-Online is now in the list.
- Leave ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS*** with **EXIT**.

Setting PPP authentication

- Select *PPP* and press **Return**.
- Select *Authentication*: *CHAP + PAP.*

- Type in your *Partner PPP ID* (=provider name): *T_ONLINE*.
- Type in your *Local PPP ID* (=Anschlußkennung + T-Online number + Mitbenutzerkennung), e. g. *123456789012081512345678#0001*.
- Type in *PPP Password*.
- Deactivate *Keepalives*: *off*.
- Deactivate *Link Quality Monitoring*: *off*.
- Press **OK**.
  You have returned to ***WAN PARTNER*** ➧ **ADD**.

Setting Short Hold

- Select *Advanced Settings* and press **Return**.
- Select *Callback*: *no*.
- Type in *Static Short Hold (sec)*, e. g. *60*.
- Type in *Idle for Dynamic Short Hold (%)*, e. g. *0*.
- Type in *Delay after Connection Failure (sec)*, e. g. *300*.
- Select *Channel-Bundling*: *no*.
- Select *Layer 1 Protocol*: *ISDN 64 kbps*.
- Press **OK**.
  You have returned to ***WAN PARTNER*** ➧ **ADD**.

IP configuration

- Select *IP* and press **Return**.
- Select *IP Transit Network*: *dynamic client*.
- Select *Advanced Settings* and press **Return**.
- Select *RIP Send*: *none*.
- Select *RIP Receive*: *none*.
- Activate *Van Jacobson Header Compression*: *on*.
- Select *Dynamic Name Server Negotiation*: client (receive)
- Deactivate *IP Accounting*: *off*.
- Deactivate *Back Route Verify*: *off*.
- Select *Route Announce*: *up or dormant*.

➤ Select *Proxy Arp*: *off*.

➤ Press **OK**.

➤ Press **SAVE**.

➤ Press **SAVE** again.

➤ Leave ***WAN PARTNER*** with **EXIT**.

Setting routing entries

➤ Go to ***IP*** ➧ ***ROUTING***.

➤ Press **ADD** to enter a new entry.

➤ Select the entry with the interface T_Online and press **Return**.

➤ Select *Route Type*: *Default route*.

➤ Select *Network*: *WAN without transit network*.

➤ Select *Partner / Interface*: *T_Online*.

➤ Type in *Metric*, e. g. *1*.

➤ Press **SAVE**.

➤ Leave ***IP*** ➧ ***ROUTING*** with **EXIT**.

Activating NAT

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

➤ Select the IP Interface T_Online and press **Return**.

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

➤ Press **SAVE**.

➤ Leave ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** with **EXIT**.

➤ Leave ***IP*** with **EXIT**.

You have returned to the main menu.

Configuration of Internet access over T-Online is complete.

Example 2: Compuserve

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

Access to Compuserve over a direct dial-in to a Compuserve network node is explained here.

If you want to reach Compuserve indirectly over T-Online´s compuserve Gateway, replace with the following at the appropriate places in the configuration sequence:

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

Setting up a WAN partner

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

Entering the dial number

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

  The dial number you call Compuserve with is now in the list.
- Leave ***WAN PARTNER*** ➧ **ADD** ➧ ***WAN NUMBERS*** with **EXIT**.

Setting PPP authentication

- Select *PPP* and press **Return**.
- Select *Authentication*: *none*.
- Deactivate *Keepalives*: *off*.
- Deactivate *Link Quality Monitoring*: *off*.
- Press **OK**.

  You have returned to the main menu ***WAN PARTNER*** ➧ **ADD**.

Setting Short Hold

- ➤ Select *Advanced Settings* and press **Return**.
- ➤ Select *Callback*: *no.*
- ➤ Type in *Static Short Hold (sec)*, e. g. *120.*
- ➤ Type in *Idle for Dynamic Short Hold (%)*, e. g. *0.*
- ➤ Type in *Delay after Connection Failure (sec)*, e. g. *300.*
- ➤ Select *Channel-Bundling*: *no.*
- ➤ Select *Layer 1 Protocol*: *ISDN 64 kbps.*

Setting authentication

- ➤ Select *Provider Configuration* > and press **Return**.
- ➤ Select *Provider*: *Compuserve Network.*
- ➤ Type in *Host*: *CIS.*
- ➤ Type in *User ID* (= your user name).
- ➤ Type in *Password.*
- ➤ Press **OK**.
- ➤ Press **OK** again.

  You have returned to the main menu ***WAN PARTNER*** ➧ **ADD**.

IP configuration

- ➤ Select *IP* and press **Return**.
- ➤ Select *IP Transit Network*: *dynamic client.*
- ➤ Select *Advanced Settings* and press **Return**.
- ➤ Select *RIP Send*: *none.*
- ➤ Select *RIP Receive*: *none.*
- ➤ Deactivate *Van Jacobson Header Compression*: *off.*
- ➤ Select *Dynamic Name Server Negotiation*: *client (receive).*
- ➤ Deactivate *IP Accounting*: *off.*
- ➤ Deactivate *Back Route Verify*: *off.*
- ➤ Select *Route Announce*: *up or dormant.*
- ➤ Select *Proxy Arp*: *off.*
- ➤ Press **OK**.

➤ Press **SAVE**.

➤ Press **SAVE** again.

➤ Leave ***WAN PARTNER*** with **EXIT**.

Setting routing entries

➤ GO to ***IP*** ➧ ***ROUTING***.

➤ Press **ADD** to enter a new entry.

➤ Select *Route Type*: *Default route*.

➤ Select *Network*: *WAN without transit network*.

➤ Select *Partner / Interface*: *COMPUSERVE*.

➤ Type in *Metric*, e. g. *1*.

➤ Press **SAVE**.

➤ Leave ***IP*** ➧***ROUTING*** with **EXIT**.

Activating NAT

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

➤ Select the IP Interface COMPUSERVE and press **Return**.

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

➤ Press **SAVE**.

➤ Leave ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** with **EXIT**.

➤ Leave ***IP*** with **EXIT**.

You have returned to the main menu.

Configuration of Internet access over Compuserve is complete.

6.2.3 Connecting to a Corporate Network

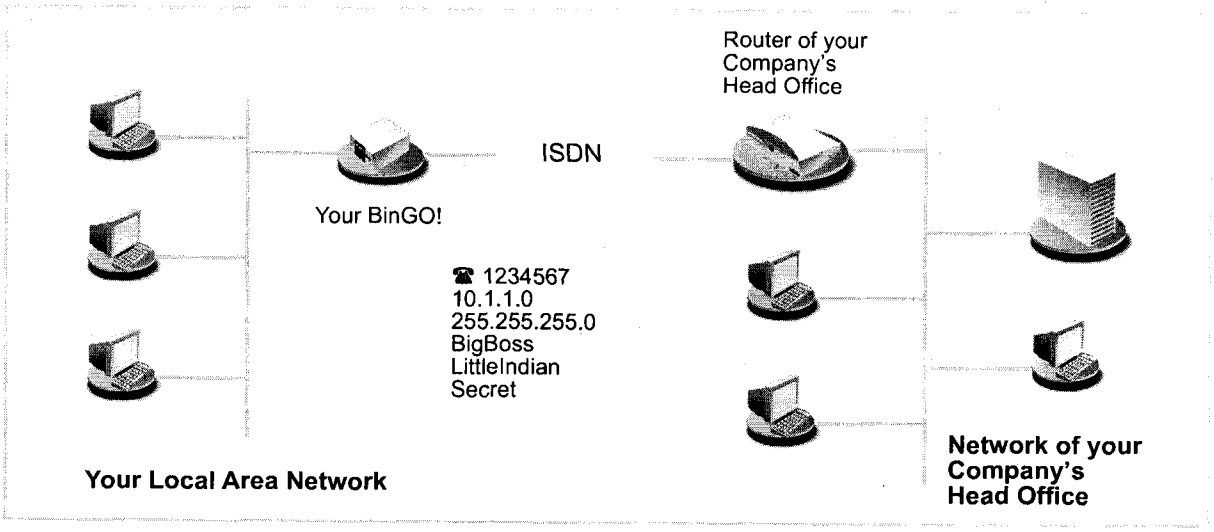


Figure 6-6: **BinGO!** and your head office

This chapter explains in quick and easy steps how to configure your **BinGO!** for a corporate network connection (LAN-LAN connection). Keep at hand the data you should have received from the system administrator of your head office (see also chapter 3.2.1, page 38). If you are not sure about some points, refer to chapter 6.2.1, page 144.

Proceed as follows:

Configuring a WAN partner

- Go to ***WAN PARTNER*** ➧ **ADD**.
- Enter *Partner Name*: e. g. *BigBoss*.
- Select *Encapsulation*: *PPP*.
- Select *Compression*: *STAC*.
- Select *Encryption*: *none*.

Entering a dial number

- Select *WAN Numbers* and press **Return**.
- Add a new entry with **ADD**.
- Enter the *Number* (= the dial number of your head office´s router), e. g. *030987654321*.

➤ Select *Direction*: *outgoing*.

➤ Press **SAVE**.

The number you dial your head office with is now in the list.

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

Setting PPP authentication

➤ Select *PPP* and press **Return**.

➤ Select *Authentication*: *CHAP + PAP*.

➤ Type in *Partner PPP ID* (= head office ID), e. g. *BigBoss*.

➤ Type in *Local PPP ID* (= your own ID), e. g. *LittleIndian*.

➤ Type in *PPP Password* (= common password for this connection).

➤ Deactivate *Keepalives*: *off*.

➤ Deactivate *Link Quality Monitoring*: *off*.

➤ Press **OK**.

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

Setting Short Hold

➤ Select *Advanced Settings* and press **Return**.

➤ Select *Callback*: *no*.

➤ Type in *Static Short Hold (sec)*, e. g. *20*.

➤ Type in *Idle for Dynamic Short Hold (%)*, e. g. *0*.

➤ Type in *Delay after Connection Failure (sec)*, e. g. *300*.

➤ Select *Channel-Bundling*: *no*.

➤ Select *Layer 1 Protocol*: *ISDN 64 kbps*.

➤ Press **OK**.

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

IP configuration

➤ Select *IP* and press **Return**.

➤ Select *IP Transit Network*: *no*.

➤ Type in *Partner's LAN IP Address* : e. g. *10.1.1.0*.

➤ Enter *Partner's LAN Netmask*: e. g. *255.255.255.0*

➤ Select *Advanced Settings* and press **Return**.

- ➤ Select *RIP Send*: *none*.
- ➤ Select *RIP Receive*: *none*.
- ➤ Deactivate *Van Jacobson Header Compression*: *off*.
- ➤ Select *Dynamic Name Server Negotiation*: *yes* (If you have not configured Internet access) or *off* (If you have configured Internet access).
- ➤ Activate *IP Accounting*: *on*.
- ➤ Activate *Back Route Verify*: *on*.
- ➤ Select *Route Announce*: *up or dormant*.
- ➤ Select *Proxy Arp*: *off*.
- ➤ Press **OK**.
- ➤ Press **SAVE**.
- ➤ Press **SAVE** again.
- ➤ Leave ***WAN PARTNER*** with **EXIT**.

  You have returned to the main menu.

  Configuration of corporate network access is complete.

Setting routing entries

If have not configured for Internet access, you can set up a default route to your head office (see chapter 6.2.1, page 144):

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

If the corporate network consists of several LANs (subnets) and you do not set up a default route to your head office, you must set up a separate routing entry for each LAN you want to reach. Bear in mind the notes in chapter 6.2.1, page 144 and figure 6-5, page 166.

- ➤ Repeat the steps for the addition of new routing entries as often as it takes to enter all the necessary routes to the LANs.

- Press **SAVE**.
- Leave ***IP*** ➧ ***ROUTING*** with **EXIT**.
- Leave ***IP*** with **EXIT**.

6.3 Saving the Configuration File

After creating a functioning configuration on your **BinGO!**, make sure to save it:

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

Another menu window opens:

```
BinGO! Setup Tool                                BinTec Communications AG
[EXIT]: Exit Setup                                              MyBinGO!

            Back to Main Menu

            Save as boot configuration and exit
            Exit without saving
```

You have three alternatives:

➤ Select **Back to Main Menu** to return to the Setup Tool main menu.

➤ Select **Save as boot configuration and exit** to save all settings made in this session and to save them to Flash. The file will be named boot.cf.

After creating the Flash file, you are returned to the SNMP shell prompt of your **BinGO!**. The next time you start your **BinGO!**, the configuration file you have just saved will be loaded.

➤ Select **Exit without saving** to leave Setup Tool and to return to the SNMP shell prompt of your **BinGO!**. All settings or changes you have made will be lost when you turn off your router.

7 Advanced Configuration

This chapter contains more **BinGO!** configuration options for the advanced user. This is the right chapter if you would like to make additional settings that were not covered by the Configuration Wizard or in chapter 6, page 117.

The following configuration steps are described:

- General ➤➤ **WAN** settings
- Settings specific to WAN partners
- Basic ➤➤ **IP** settings
- ➤➤ **IPX** settings
- Extra license functions

7.1 General WAN Settings

General WAN functions:

- **BinGO!** as dynamic IP address ➤➤ **server**
- ➤➤ **CAPI** user concept
- Credits based accounting system
- General ➤➤ **PPP** settings

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

7.1.1 Dynamic IP Address Server

IP address pools

BinGO! can operate as a dynamic IP address server for PPP connections. You can use this function by providing one or more pools of ➤➤ **IP addresses**. These IP addresses can be assigned to a dial-in WAN partner for the duration of the connection.

Any host routes entered always have priority over IP addresses from the address pools. That is, when an incoming call has been authenticated, **BinGO!** first checks whether a host route is entered in the routing table for this caller. If not, **BinGO!** can assign an IP address from an address pool (if available).

If address pools have more than one IP address, you cannot specify which WAN partner receives which address. The addresses are initially assigned in order. If a new dial-in takes place within an interval of one hour, **BinGO!** does try to assign the IP address that this partner was assigned the last time.

The configuration is made in

- *IP* ➧ *DYNAMIC IP ADDRESSES (SERVER MODE)*
- *WAN PARTNER* ➧ *EDIT* ➧ *IP*
- *WAN PARTNER* ➧ *EDIT* ➧ *IP* ➧ *ADVANCED SETTINGS*

Field	Meaning
Pool ID	Unique number for identification of the address pool. A pool can comprise several address areas.
IP Address	First IP address of the address pool.
Number of consecutive addresses	Number of IP addresses in the address pool, including the first IP address (*IP Address*).

Table 7-1: ***IP*** ➧ ***DYNAMIC IP ADDRESSES (SERVER MODE)***

Field	Meaning
IP Transit Network	Defines whether a transit network is to be used between **BinGO!** and the LAN of the WAN partner. You must select *dynamic server* here if you assign an address pool.

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

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

Table 7-3: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

To Do Proceed as follows:

- Go to ***IP*** ➧ ***DYNAMIC IP ADDRESSES (SERVER MODE)*** ➧ **ADD**.
- Enter *Pool ID*.
- Enter *IP Address*.
- Enter *Number of consecutive addresses*.
- Press **SAVE**.

- Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** to assign an address pool to a WAN partner.
- Select *IP Transit Network*: *dynamic server*.
- Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.
- Enter *IP Address Pool*: *Pool ID*.
- Confirm with **OK**.
- Press **SAVE**.

7.1.2 CAPI User Concept

User name and password

The CAPI user concept is used to check access to the ➤➤ **CAPI** service. This ensures that only users entered with a user name and password can use **BinGO!**'s CAPI services.

Example

This means, for example, that an incoming fax for the user Winnetou is only passed to Winnetou and not to a user such as Old Shatterhand, who is located in the same LAN. If the CAPI user concept is not used (see chapter 6.1.4, page 126), all incoming calls passed to the CAPI service are offered to all CAPI applications in the LAN. The first user to respond receives the call. So if Old Shatterhand is quicker off the mark ...

The configuration is made in

- ***CAPI*** ➧ ***USER***
- ***CM-1BRI, ISDN S0*** ➧ Incoming Call Answering

Field	Meaning
Name	Name of user who is to be allowed or denied access to the CAPI service (maximum 16 characters).
Password	Password with which the user *Name* must identify himself to obtain access to the CAPI service.
CAPI	Defines whether access to the CAPI service for the user *Name* is allowed or denied. Possible values: ■ *enabled*: access to CAPI allowed ■ *disabled*: access to CAPI denied

Table 7-4: ***CAPI ➧ USER***

Field	Meaning
Item	Service to which a call to the *Number* below is to be assigned.
Number	Phone number under which the service (*Item*) entered above can be reached.
Mode	Mode in which **BinGO!** compares the digits of *Number* with the called party number of the incoming call: *right to left*: default mode. *left to right (DDI)*: Always select this mode if **BinGO!** is connected to a point-to-point line (system line).
Username	Corresponds to *Name* in ***CAPI*** ➧ ***USER***. User to whom an incoming call to the CAPI service under *Number* is to be passed.
Bearer	Type of incoming call. Possible values: ■ *data*: data call ■ *voice*: speech call ■ *any*: either data or speech call

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

If there is no entry in ***CAPI*** ➧ ***USER*** when you start **BinGO!**, a standard entry without password is created automatically (with *Name* = *default* and *CAPI* = *enabled*).

To Do Proceed as follows:

➤ Go to ***CAPI*** ➧ ***USER***:

➤ Select an existing entry and confirm with **Return** or add a new entry with **ADD**.

➤ Enter *Name*.

➤ Enter *Password*.

➤ Select *CAPI*.

➤ Press **SAVE**.

➤ Repeat these steps for every user in the LAN.

➤ Go to ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING***.
Make an entry here for every user in the LAN who has access to the CAPI service:

➤ Select an existing entry and confirm with **Return** or add a new entry with **ADD**.

➤ Select *Item*: *CAPI*.

If you use a communication application on your computer that is based on Remote CAPI 1.1 (current version: Remote CAPI 2.0), **BinGO!** must translate the ➤➤ **MSN**s (=*Number*, multidigit) of the incoming call to ➤➤ **EAZ**s (single digit) (CAPI 1.1 can only detect single-digit numbers). This is the reason why the CAPI entry under *Item* is not simply called *"CAPI"*, but *"CAPI 1.1 EAZ x Mapping"*.

So if you use CAPI 1.1, make sure that you "map" each *Number* to a separate EAZ. For example, select the entry *Item = CAPI 1.1 EAZ **0** Mapping* for *Number = 1234* and the entry *Item = CAPI 1.1 EAZ **1** Mapping* for *Number = 5678*.

CAPI 2.0 evaluates the MSN directly and "translation" to EAZ is not necessary. You can use the same CAPI 1.1 EAZ x Mapping entry for each number.

➤ Enter *Number*.

➤ Select *Mode*.

➤ Enter *Username*.

➤ Select *Bearer*.

➤ Press **SAVE**.

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

7.1.3 Credits Based Accounting System

ISDN charges

BinGO!'s credits based accounting system helps you to keep an eye on the ISDN call charges. The system enables you to define the maximum number of connections allowed in a certain period of time. You can make settings for each subsystem (➤➤ **PPP**, ➤➤ **CAPI**, ➤➤ **isdnlogin**) to define the number of connections, the connection time and the charges billed. If the defined time limit is exceeded, **BinGO!** cannot set up any more connections within the defined period of time. This means you can detect configuration errors in good time, before your telephone bill gets too big!

Syslog messages

Syslog messages are generated if the number of connections reaches 90% and 100% of the limit and if a connection is prevented by the credits based accounting system because the limit is exceeded.

The whole account is available again if you switch **BinGO!** off and then switch it on again (reboot).

The configuration is made in ***ISDN*** ➧ ***CREDITS***:

Field	Meaning
Surveillance	Defines whether the credits based accounting system for the respective subsystem is to be activated. Possible values: *off*, *on*. With *on*, you can define the parameters listed below.
Measure Time (sec)	Time in seconds for which the limit applies.
Maximum Number of Incoming Connections	Number of incoming connections allowed during *Measure Time (sec)*. If you activate this setting with *on*, you can enter the desired value in the line below.
Maximum Number of Outgoing Connections	Number of outgoing connections allowed during the *Measure Time (sec)*. If you activate this setting with *on*, you can enter the desired value in the line below.
Maximum Charge	Maximum number of charge units allowed during the *Measure Time (sec)*. If you activate this setting with *on*, you can enter the desired value in the line below.
Maximum Time for Incoming Connections (sec)	Maximum time in seconds allowed for incoming connections during the *Measure Time (sec)*. If you activate this setting with *on*, you can enter the desired value in the line below.
Maximum Time for Outgoing Connections (sec)	Maximum time in seconds allowed for outgoing connections during the *Measure Time (sec)*. If you activate this setting with *on*, you can enter the desired value in the line below.

Table 7-6: ***ISDN*** ➧ ***CREDITS***

To Do Proceed as follows:

➤ Go to ***ISDN*** ➧ ***CREDITS***.

➤ Select *Subsystem* and confirm with **Return**.

- Select *Surveillance*: *on*, if you want to use the credits based accounting system for the selected *Subsystem*.
- Enter *Measure Time (sec)*, e.g. *86400* (= 24 hours).
- Activate *Maximum Number of Incoming Connections*, if applicable, and enter the desired value.
- Activate *Maximum Number of Outgoing Connections*, if applicable, and enter the desired value.
- Activate *Maximum Charge*, if applicable, and enter the desired value.
- Activate *Maximum Time for Incoming Connections (sec)*, if applicable, and enter the desired value.
- Activate *Maximum Time for Outgoing Connections (sec)*, if applicable, and enter the desired value.
- Press **SAVE**.

7.1.4 General PPP Settings

Authentication You must enter the ➤➤ **PPP** settings for each WAN partner, e.g. the settings needed for authentication of connection partners with ➤➤ **CHAP** or ➤➤ **PAP** (see chapter 6.2.1, page 144). If a call is received, **BinGO!** then recognizes the calling WAN partner from the calling party's number with the aid of ➤➤ **CLID** (Calling Line Identification) and thus knows what authentication negotiations it has agreed with this partner. The call is answered if the authentication is correct.

CLID In some cases it is not possible to identify an incoming call via CLID. This is the case, for example,

- if the call is made via an analog line (the caller dials into your router via the ➤➤ **Modem**),
- if the MS-CHAP authentication protocol has been agreed with the calling WAN partner.

In both cases **BinGO!** receives no calling line number and therefore cannot identify the caller via CLID, even if the caller is entered as a WAN partner. In

this case, **BinGO!** does not know which ➤➤ **PPP authentication** protocol to use to identify the incoming call.

General PPP settings

In order to answer the call in spite of the identification problem, **BinGO!** executes the PPP authentication protocol with the caller. This protocol has been defined generally and therefore does not refer to a certain WAN partner. If the data obtained by executing the authentication protocol, e.g. password, are the same as the data of an entered WAN partner, **BinGO!** answers the call.

The general PPP settings are configured in ***PPP***:

Field	Meaning
Authentication Protocol	Defines the PPP authentication protocol offered to the caller first. Possible values: ■ *PAP*: PAP only ■ *CHAP*: CHAP only ■ *CHAP + PAP*: first CHAP, then PAP ■ *MS-CHAP*: MS-CHAP only ■ *CHAP + PAP + MS-CHAP*: first CHAP, if rejected then the protocol required by the WAN partner ■ *none*: no PPP authentication
Radius Server Authentication	Not available in **BinGO!**.
PPP Link Quality Monitoring	Defines whether Link Quality Monitoring is executed for PPP connections. Possible values: ■ *no*, is not executed. ■ *yes*, the connection statistics are stored in the ➤➤ **MIB** table **biboPPPLQMTable**.

Table 7-7: ***PPP***

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

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

7.2 Settings Specific to WAN Partners

Specific functions for ➤➤ **WAN partners** make it possible to define the characteristics for connections to WAN partners individually. Carry out the configuration steps described separately for each WAN partner.

- Delay after Connection Failure
- Channel Bundling
- Layer 1 Protocol
- IP Transit Network
- Transfer of DNS and WINS Server IP addresses to WAN partner
- ➤➤ **RIP**
- Compression: ➤➤ **VJHC**, ➤➤ **STAC**, MS-STAC
- ➤➤ **Proxy ARP**

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

7.2.1 Delay after Connection Failure

You can use this function to set a delay after a connection setup failure.

The configuration is made in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***:

Field	Meaning
Delay after Connection Failure (sec)	Block timer. Indicates how many seconds must pass after a connection setup failure before it is possible to dial into **BinGO!** again.

Table 7-8: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***

To Do Proceed as follows:

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

➤ Enter *Delay after Connection Failure (sec)*.

➤ Confirm with **OK**.

➤ Press **SAVE**.

7.2.2 Channel Bundling

BinGO! supports dynamic and static ➤➤ **channel bundling**.

Dynamic Dynamic channel bundling means that **BinGO!** connects the second ➤➤ **ISDN** B-channel to increase the throughput for connections to the WAN partner, if this is required, e.g. for large amounts of data. If the amount of data traffic drops, the second ➤➤ **B-channel** is closed again. Only one B-channel is opened initially when setting up a connection.

Static In static channel bundling, you specify right from the start whether **BinGO!** uses one or two B-channels for connections to the WAN partner, regardless of the amount of data transferred.

The configuration is made in ***WAN PARTNER*** ➧ **ADD** ➧ ***ADVANCED SETTINGS***:

Field	Meaning
Channel-Bundling	Defines whether and which type of channel bundling is to be used for connections to the WAN partner.
Total Number of Channels	For dynamic channel bundling: defines the maximum number of B-channels that may be opened. For static channel bundling: defines the number of B channels that are open during the complete connection. Possible values: *1*, *2*.

Table 7-9: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***

The *Channel-Bundling* field contains the following selection options:

Possible Values	Meaning
no	No channel bundling, only one B-channel is ever available for connections.
dynamic	Dynamic channel bundling.
static	Static channel bundling.

Table 7-10: *Channel Bundling*

To Do Proceed as follows:

- Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***.
- Select *Channel-Bundling*.
- Enter *Total Number of Channels*.
- Confirm with **OK**.
- Press **SAVE**.

7.2.3 Layer 1 Protocol (ISDN B-Channel)

ISDN B-channel You can define the Layer 1 Protocol of the ISDN ➤➤ **B-channel** that **BinGO!** is to use for connections to the WAN partner. The default setting is the protocol for ISDN data connections at 64 kbps, which is the default value of the B-channel. Only change the setting if this is expressly required.

The configuration is made in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***:

Field	Meaning
Layer 1 Protocol	Defines which Layer 1 Protocol **BinGO!** is to use. This setting applies only to outgoing calls to the WAN partner and to incoming calls from the WAN partner, if they have been identified from the calling party's number.

Table 7-11: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***ADVANCED SETTINGS***

For incoming calls that cannot be identified from the calling party's number, **BinGO!** uses the settings under *Item* in ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** as the Layer 1 Protocol (see chapter 6.1.4, page 126).

Layer 1 Protocol contains the following selection options:

Possible Values	Meaning
ISDN 64 kbps	For 64-kbps ISDN data connections. This is the default value.
ISDN 56 kbps	For 56-kbps ISDN data connections.
Modem	Not available in **BinGO!**.
DOVB	Data transmission Over Voice Bearer - useful in the USA, for example, where voice connections are sometimes cheaper than data connections.
V.110 (1200 ... 38400)	For connections to V.110 at bit rates of 1200 bps, 2400 bps,..., 38400 bps.
Modem Profile 1 ... 8	Not available in **BinGO!**.
PPTP PNS	VPN interface

Table 7-12: *Layer 1 Protocol*

Most of the entries for *Layer 1 Protocol* correspond to the entries for *Item* in ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING*** (see chapter 6.1.4, page 126).

To Do Proceed as follows:

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

7.2.4 IP Transit Network

If you enter a WAN partner in **BinGO!**, there are various options for entering the IP address of the partner network:

- Simply enter ➤➤ **IP address** and ➤➤ **netmask** of the partner network. You must obviously know these.
- Use an additional ISDN IP address and ISDN netmask for both **BinGO!** and the WAN partner. You thus set up a virtual IP network during the connection, a so-called transit network. You do not need this setting normally, only for some special configurations.
- Assign the WAN partner a dynamic IP address from a specified IP address pool for the duration of the connection.
- Get the WAN partner to assign you a dynamic IP address for the duration of the connection.

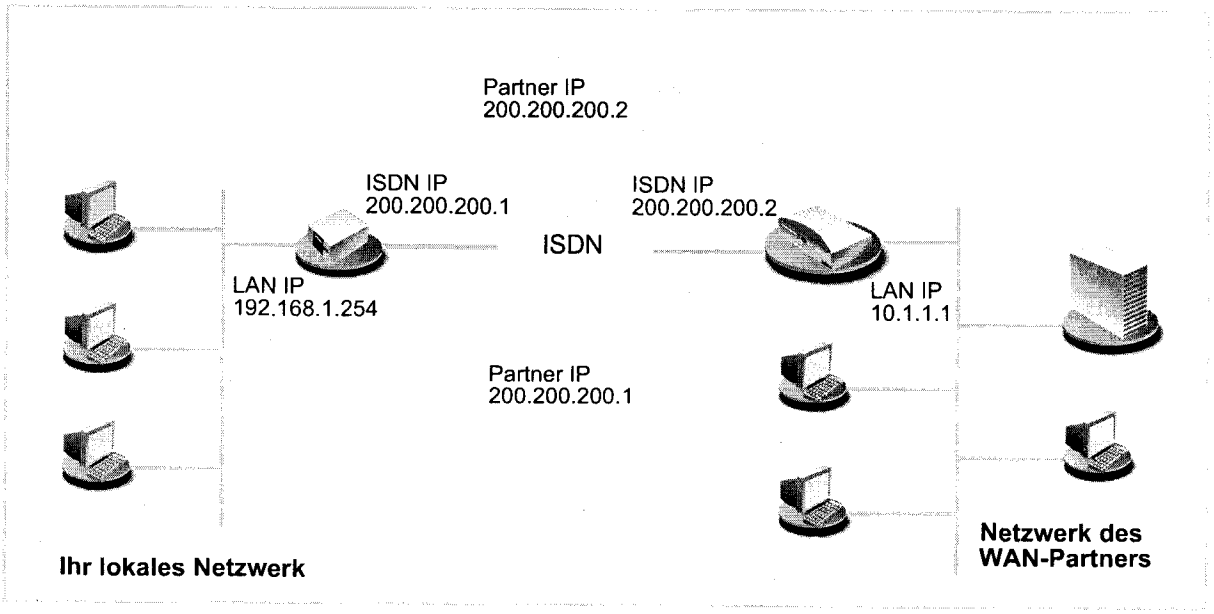


Figure 7-1: LAN-LAN link with transit network

The configuration is made in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***:

Field	Meaning
IP Transit Network	Defines whether **BinGO!** sets up a transit network to the WAN partner.
local ISDN IP Address	**BinGO!**'s ISDN IP address in the transit network.
Partner's ISDN IP Address	WAN partner's ISDN IP address in the transit network.
Partner's LAN IP Address	WAN partner's LAN IP address.
Partner's LAN Netmask	WAN partner's LAN netmask. If you make no entry, **BinGO!** enters a default netmask for the net class used under *Partner's LAN IP Address*.

Table 7-13: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***

IP Transit Network contains the following selection options:

Possible Values	Meaning
yes	A transit network is used.
dynamic client	**BinGO!** receives its IP address for the duration of the connection from the WAN partner.
dynamic server	**BinGO!** assigns the ➤➤ **Remote** WAN partner an IP address for the duration of the connection. In this case, **BinGO!** must be configured as a dynamic IP address server, i.e has an IP address pool available (see chapter 7.1.1, page 182).
no	No transit network. This setting is adequate for most WAN partners.

Table 7-14: *IP Transit Network*

To Do Proceed as follows:

- ➤ Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***.
- ➤ Select *IP Transit Network*.
- ➤ Enter *local ISDN IP Address*, if applicable.
- ➤ Enter *Partner's ISDN IP Address*, if applicable.
- ➤ Enter *Partner's LAN IP Address*, if applicable.
- ➤ Enter *Partner's LAN IP Address*, if applicable.
- ➤ Press **SAVE**.

7.2.5 Transfer of DNS and WINS Server IP Addresses to WAN Partner

IP address = ? A Domain Name Server (➤➤ **DNS**) or Windows Internet Name Server (WINS) is needed for translating host names and ➤➤ **NetBIOS** names into IP addresses (name resolution). Domain Name Servers form a hierarchical tree structure. As soon as a request is sent to your primary DNS, it tries to execute name resolution using its internal tables. If it cannot find the name, it asks a higher-level DNS that it knows.

When you enter a WAN partner in **BinGO!**, you can define whether **BinGO!** sends or answers requests for WINS or DNS IP addresses.

The configuration is made in

- ***IP*** ➧ ***STATIC SETTINGS***
- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

Field	Meaning
Primary Domain Name Server	IP address of **BinGO!**'s first Domain Name Server (DNS).
Secondary Domain Name Server	IP address of another Domain Name Server.
Primary WINS	IP address of **BinGO!**'s first WINS (Windows Internet Name Server) or NBNS (NetBIOS Name Server).
Secondary WINS	IP address of another WINS or NBNS.

Table 7-15: ***IP ➧ STATIC SETTINGS***

Field	Meaning
Dynamic Name Server Negotiation	Defines whether **BinGO!** receives IP addresses for *Primary Domain Name Server*, *Secondary Domain Name Server*, *Primary WINS* and *Secondary WINS* from the WAN partner or sends them to the WAN partner.

Table 7-16: ***WAN PARTNER ➧ EDIT ➧ IP ➧ ADVANCED SETTINGS***

The *Dynamic Name Server Negotiation* field contains the following selection options:

Possible Values	Meaning
off	**BinGO!** does not send or answer requests for WINS or DNS IP addresses.
yes	The response is linked to the mode for issuing / receiving an IP address (setting under *IP Transit Network* in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP***): ■ **BinGO!** sends requests for WINS and DNS IP addresses to the WAN partner, if *dynamic client* is selected. ■ **BinGO!** answers requests for WINS and DNS IP addresses from the WAN partner, if *dynamic server* is selected. ■ **BinGO!** does not send or answer requests for WINS and DNS IP addresses, if *yes* or *no* is selected.
client (receive)	**BinGO!** sends requests for WINS and DNS IP addresses to the WAN partner.
server (send)	**BinGO!** answers requests for WINS and DNS IP addresses from the WAN partner.

Table 7-17: *Dynamic Name Server Negotiation*

DNS in the LAN If you have set up a DNS in your LAN, enter its IP address.

To Do Proceed as follows, if you have not made this entry already (chapter 7.3.2, page 214):

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

➤ Enter *Primary* or *Secondary Domain Name Server*, if applicable.

➤ Enter *Primary* or *Secondary WINS*, if applicable.

➤ Press **SAVE**.

Proceed as follows if you want **BinGO!** to report the DNS or WINS entered to the WAN partner (Server Mode) or if DNS/WINS addresses other than those in the LAN are to be used for connections to the WAN partner (Client Mode, e.g. for dialing into an Internet Service Provider).

- Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.
- Select *Dynamic Name Server Negotiation*.
- Confirm with **OK**.
- Press **SAVE**.

If you do not have a Domain Name Server in your LAN (smaller networks often have no DNS of their own), the name resolution can be carried out, for example, via your Internet Service Provider (Client Mode). However, this requires ISDN connections, which involve charges.

If you work with Windows, you can also obtain name resolution without asking for a DNS. To do this, you must adapt the LMHOSTS file on all PCs in the LAN. Detailed information about this is given in chapter 3.6.2, page 61.

7.2.6 RIP (Routing Information Protocol)

Routing In general, routing can be described as follows: the➤➤ **router** receives ➤➤ **data packets**, each of which contains data about the destination host. On the basis of the entries in the so-called Routing Table (see chapter 6.2.1, page 144), the router decides which route to use to forward the data packet to ensure that it arrives at its destination as quickly and cheaply as possible (with the fewest possible intermediate stations). That is, the router propagates a route. The entries in the Routing Table can be defined statically or the Routing Table can be updated constantly by a dynamic exchange of routing information between several routers. This exchange is controlled by a so-called Routing Protocol, e.g. RIP (Routing Information Protocol).

RIP Routers using the ➤➤ **RIP** protocol exchange the information stored in their Routing Tables by communicating with each other at regular intervals to mutually supplement and renew their routing entries. **BinGO!** supports both version 1 and version 2 of RIP, either exclusively or parallel.

RIP is configured separately for LAN and WAN.

Active and passive

Routers can be defined as active or passive routers: active routers offer their routing entries to other routers via ➤➤ **broadcasts**. Passive routers accept the information from the active routers and store it, but do not pass on their own routing entries. **BinGO!** can do both.

WAN partner

If you negotiate to receive and/or send RIP packets to your WAN partner, **BinGO!** can exchange routing information dynamically with the routers in the LAN of the WAN partner.

Receiving Routing Tables via the RIP is possibly a security loophole, as external computers or routers can change **BinGO!**'s routing functionality.

RIP packets do not set up or hold ISDN connections.

The configuration is made in

- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***
- ***CM-BNC/TP, ETHERNET***

Field	Meaning
RIP Send	Enables RIP packets to be sent via the interface to the WAN partner and LAN interface.
RIP Receive	Enables RIP packets to be received via the interface to the WAN partner and LAN interface.

Table 7-18: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** and ***CM-BNC/TP, ETHERNET***

RIP Send and *RIP Receive* contain the following selection options:

Possible Values	Meaning
none	Not activated.
RIP V1	Enables sending and receiving of RIP packets in version 1.
RIP V2	Enables sending and receiving of RIP packets in version 2.
RIP V1 + V2	Enables sending and receiving of RIP packets in both version 1 and version 2.

Table 7-19: *RIP Send* and *RIP Receive*

To Do Proceed as follows:

- Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.
- Select *RIP Send*.
- Select *RIP Receive*.
- Confirm with **OK**.
- Press **SAVE**.
- Go to ***CM-BNC/TP, ETHERNET***.
- Select *RIP Send*.
- Select *RIP Receive*.
- Press **SAVE**.

7.2.7 Compression

Data compression

You can increase the data throughput and thus reduce the connection costs by using ➤➤ **data compression**. **BinGO!** supports several options, depending on the ➤➤ **encapsulation** selected, e.g. PPP (see chapter 6.2.1, page 144):

- ➤➤ **STAC**:
  The industry standard STAC data compression (Check Mode 3 in RFC 1974) implemented in **BinGO!** can increase the data throughput on the PPP ISDN connections.
- MS-STAC:
  STAC data compression for Windows ➤➤ **clients** (Check Mode 4 in RFC 1974). Select this if you dial into a Windows Remote Access Server.
- ➤➤ **V.42bis**:
  Compression algorithm which requires a security layer. Only possible with *Encapsulation = Multi-Protocol LAPB Framing* or *LAPB Framing (only IP)*.
- Van Jacobson Header Compression (➤➤ **VJHC**):
  Reduces the size of ➤➤ **TCP/IP** packets. Van Jacobson Header Compression can be used in addition to the above-mentioned compression algorithms.

It is not advisable to set both STAC and V.42bis for one connection.

If the far station does not support data compression or its data compression is not activated, **BinGO!** detects this during the ➤➤ **PPP** negotiation phase and deactivates data compression for this connection.

The configuration is made in

- ***WAN PARTNER*** ➧ ***EDIT***
- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

Field	Meaning
Compression	Defines the type of compression for connections to the WAN partner.

Table 7-20: ***WAN PARTNER*** ➧ ***EDIT***

The *Compression* field contains the following selection options:

Possible Values	Meaning
none	No compression.
STAC	Enables STAC data compression (if *Encapsulation = PPP*).
MS-STAC	Enables STAC data compression for dialing into a Windows Remote Access Server (if *Encapsulation = PPP*).
MPPC	Not available in **BinGO!**.
V.42bis	Enables data compression with V.42bis (if *Encapsulation = Multi-Protocol LAPB Framing* or *LAPB Framing (only IP)*).

Table 7-21: *Compression*

Field	Meaning
Van Jacobson Header Compression	Enables VJHC.

Table 7-22: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

STAC, MS-STAC, V.42bis

Proceed as follows to set STAC, MS-STAC or V.42bis:

➤ Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.

➤ Select *Compression*.

➤ Press **SAVE**.

VJHC Proceed as follows to set VJHC:

- ➤ Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.
- ➤ Activate *Van Jacobson Header Compression*: *on*.
- ➤ Confirm with **OK**.
- ➤ Press **SAVE**.

7.2.8 Proxy ARP (Address Resolution Protocol)

ARP Requests **BinGO!** can answer ➤➤ **ARP** Requests from the LAN with the aid of ➤➤ **Proxy ARP**. That is, if a host in the LAN wants to set up a connection to another host in the LAN or to a WAN partner but doesn't know its hardware address, it sends a so-called ARP Request into the network as a ➤➤ **broadcast**. This is actually a question to all those in the network: "What is the hardware address of host x ?". If Proxy ARP is activated in **BinGO!** and the desired host can be reached in the LAN or via a defined WAN connection, **BinGO!** answers the ARP Request with its own address. This is sufficient for connection setup: the ➤➤ **data packets** are sent to **BinGO!**, which then passes them to the desired

host. If Proxy ARP is not activated, only the host with the requested address can answer.

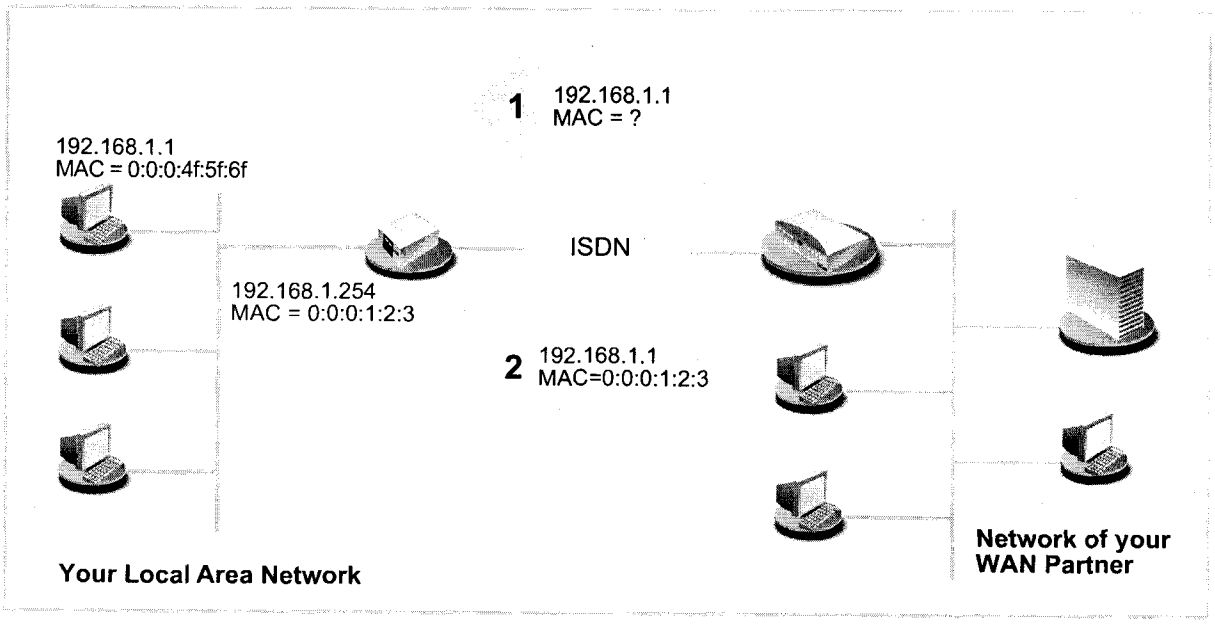


Figure 7-2: Proxy ARP

Example If computers in the LAN are assigned their IP addresses dynamically via DHCP, no static host routes can be entered in **BinGO!** for a connection to these hosts. MAC and IP addresses can, however, still be assigned using Proxy ARP.

Further information (with example) about Proxy ARP is contained in the Software Reference.

The configuration is made in

- ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***
- ***CM-BNC/TP, ETHERNET***

Field	Meaning
Proxy Arp	Enables **BinGO!** to answer ARP Requests.

Table 7-23: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** and ***CM-BNC/TP, ETHERNET***

Proxy Arp in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS*** contains the following selection options:

Possible Values	Meaning
off	Disables Proxy ARP via the interface to the WAN partner.
on (up or dormant)	**BinGO!** answers an ARP Request only if the status of the connection to the WAN partner is *up* (active) or *dormant* (idle). In the case of *dormant*, **BinGO!** only answers the ARP Request; the connection is not set up until someone actually wants to use the route.
on (up only)	**BinGO!** answers an ARP Request only if the status of the connection to the WAN partner is *up* (active). This ensures that **BinGO!** only answers an ARP Request if a connection is already open to the WAN partner.

Table 7-24: *Proxy Arp*

Proxy Arp in ***CM-BNC/TP, ETHERNET*** contains the following selection options:

Possible Values	Meaning
off	Disables Proxy ARP via the LAN interface.
on	Enables Proxy ARP via the LAN interface.

Table 7-25: *Proxy Arp*

To Do Proceed as follows:

- ➤ Go to ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.
- ➤ Select *Proxy Arp*.
- ➤ Press **SAVE**.
- ➤ Go to ***CM-BNC/TP, ETHERNET***.
- ➤ Select *Proxy Arp*.

➤ Press **SAVE**.

7.3 Basic IP Settings

Here you will find a number of basic settings that you can define in **BinGO!**:

- Deriving system time
- Name resolution (➤➤ **DNS**) in **BinGO!**
- ➤➤ **Port** numbers
- ➤➤ **BOOTP** Relay Agent

The necessary configuration steps are explained below.

7.3.1 System Time

System time

You need the system time to obtain correct timestamps for recording connection data (accounting).

The configuration is made in ***IP*** ➧ ***STATIC SETTINGS***:

Field	Meaning
Time Protocol	Protocol used to derive the current time. Possible values: ■ *TIME/UDP* ■ *TIME/TCP* ■ *SNTP* ■ *ISDN* ■ *none*
Time Offset (sec)	Number of seconds added to or subtracted from the derived time. If you enter values between -24 and +24, **BinGO!** interprets the input as a number of hours and converts it automatically to the corresponding number of seconds. Note: if you select *isdn* as *Time Protocol*, you must set the *Time Offset* to *0*. If you change *Time Offset (sec)* (turn back the time), there should be no data flow.
Time Update Interval (sec)	Time interval in seconds after which the system time is checked and updated if necessary. If you enter values between 1 and 24, **BinGO!** interprets the input as the number of hours and converts it automatically to the corresponding number of seconds. For *Time Protocol* = *TIME/UDP*, *TIME/TCP* or *SNTP*: current time is checked after every *Time Update Interval* in seconds. For *Time Protocol* = *ISDN:* current time is checked for each first ISDN connection after expiry of the *Time Update Interval*.

Field	Meaning
Time Server	IP address of the time➤➤ **server** used by **BinGO!**. *Time Server* is not needed if you set *ISDN* as *Time Protocol*.

Table 7-26: ***IP*** ➧ ***STATIC SETTINGS***

The *Time Protocol* field contains the following selection options:

Possible Values	Meaning
TIME/UDP	System time (RFC 868) via ➤➤ **UDP**
TIME/TCP	System time (RFC 868) via ➤➤ **TCP**
TIME/SNTP	SNTP (Simple Network Time Protocol, RFC 1769) via UDP
ISDN	System time from ISDN ➤➤ **D-channel** (free)
none	System time not derived

Table 7-27: *Time Protocol*

ISDN Proceed as follows to derive the system time via ISDN:

- ➤ Go to ***IP*** ➧ ***STATIC SETTINGS***.
- ➤ Select *Time Protocol*: *ISDN*.
- ➤ Enter *Time Offset (sec)*: *0*.
- ➤ Enter *Time Update Interval (sec)*, e.g. *86400* (corresponds to 24 hours).
- ➤ Press **SAVE**.

  After the first ISDN connection has been completed, **BinGO!** derives the system time from the ISDN.

Time server Proceed as follows to derive the system time from a time server:

- ➤ Go to ***IP*** ➧ ***STATIC SETTINGS***.
- ➤ Select *Time Protocol*, e.g. *TIME/UDP*.
- ➤ Enter *Time Offset (sec)*, e.g. *0*.

➤ Enter *Time Update Interval (sec)*, e.g. *86400* (corresponds to 24 hours).

➤ Enter IP address or host name for *Time Server*.

➤ Press **SAVE**.

BinGO! then derives the system time via a time server. **BinGO!** adjusts its system time to the time set on the time server every 24 hours.

➤➤ **DIME Tools** contains a time server. If you enter the IP address of your PC for *Time Server*, you must therefore ensure that **DIME Tools** is active on your PC every time you start **BinGO!**.

If your computer has no fixed IP address but is assigned its IP address dynamically via ➤➤ **DHCP**, you cannot use your computer as time server.

7.3.2 Name Resolution in BinGO!

Domain name

To enable **BinGO!** to resolve host names and computer names in the LAN (e.g. for `ping` or `telnet`), enter **BinGO!**'s domain name and the IP address of DNS or WINS servers in the LAN.

The configuration is made in ***IP*** ➧ ***STATIC SETTINGS***

Field	Meaning
Domain Name	Defines **BinGO!**'s Domain Name.
Primary Domain Name Server	IP address of **BinGO!**'s first Domain Name Server (DNS).
Secondary Domain Name Server	IP address of another Domain Name Server.
Primary WINS	IP address of **BinGO!**'s first WINS (Windows Internet Name Server) or NBNS (NetBIOS Name Server).
Secondary WINS	IP address of another WINS or NBNS.

Table 7-28: *Time Protocol*

To Do Proceed as follows:

- ➤ Go to ***IP*** ➧ ***STATIC SETTINGS***.
- ➤ Enter *Domain Name*, e.g. *bricks.com*.
- ➤ Enter *Primary* or *Secondary Domain Name Server, if applicable*.
- ➤ Enter *Primary* or *Secondary WINS, if applicable*.
- ➤ Press **SAVE**.

7.3.3 Port Numbers

What is a ➤➤ port? **BinGO!** is equipped with a number of services and applications, e.g. HTTP, ➤➤ **Telnet**, ➤➤ **FTP**, etc. In order to reach several services on the same host and to indicate an exact destination for the IP packet within the host, you also enter a port as well as the IP address for a connection to **BinGO!**. This addresses the relevant application. Ports are only used in the TCP and UDP protocols!

BinGO! forwards incoming ➤➤ **data packets** to the port with the number associated with the desired application. This addresses the relevant **BinGO!** application and the incoming data can be processed.

You can define some important port numbers in ***IP*** ➧ ***STATIC SETTINGS***:

The settings are normally correct and you should only make changes here if necessary.

Field	Meaning
Remote CAPI Server TCP port	Port number for ➤➤ **Remote CAPI** connections: 2662 (defined by IANA, www.iana.com).
Remote TRACE Server TCP port	Port number for TRACE Requests. Default value: 7000.
RIP UDP port	Port number for ➤➤ **RIP** (Routing Information Protocol). Default value: 520. RIP can be disabled with *RIP UDP port = 0*.
HTTP TCP port	Port number for HTTP Requests. Default value: 80. *HTTP TCP port = 0* disables access to **BinGO!**'s HTTP status page (see chapter 8.1.3, page 236).

Table 7-29: ***IP*** ➧ ***STATIC SETTINGS***

To Do Proceed as follows to change one of the port numbers:

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

➤ Enter *Remote CAPI Server TCP port*, *Remote TRACE Server TCP port*, *RIP UDP port* and/or *HTTP TCP port*.

➤ Press **SAVE**.

7.3.4 BOOTP Relay Agent

Bootstrap protocol

The Bootstrap Protocol (➤➤ **BOOTP**) defines how a host (BOOTP-➤➤ **client**) in a TCP/IP network receives his IP address and other configuration information on booting. The BOOTP client sends a BOOTP Request, a BOOTP server answers the Request with a BOOTP Response and supplies the client with the necessary information. As the server only hears Requests from the LAN in which it is located, it is sometimes advisable to set up a BOOTP Relay Agent. The Agent forwards all Requests and Responses between the client and server via a WAN connection to this server.

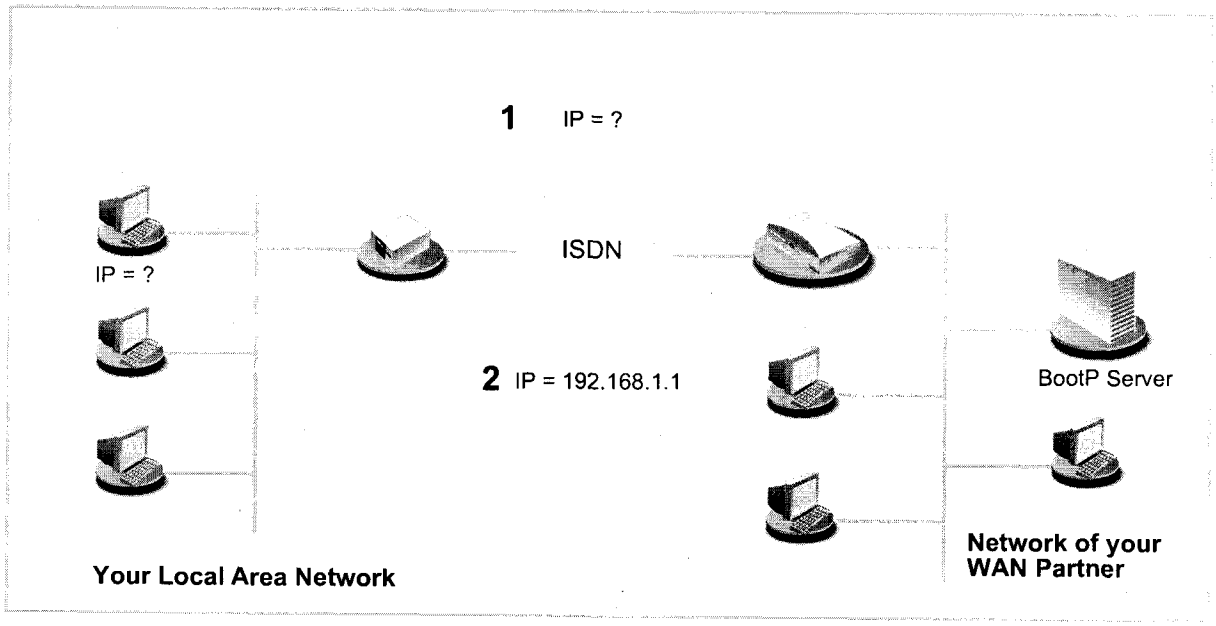


Figure 7-3: **BinGO!** as BOOTP Relay Agent

The configuration is made in ***IP*** ➧ ***STATIC SETTINGS***:

Field	Meaning
BOOTP Relay Server	IP address of the BOOTP server.

Table 7-30: ***IP*** ➧ ***STATIC SETTINGS***

To Do Proceed as follows:

- Go to ***IP*** ➧ ***STATIC SETTINGS***.
- Enter *BOOTP Relay Server*.
- Press **SAVE**.

If an ISDN connection is needed for the connection between the BOOTP server and BOOTP client, you must set up an appropriate WAN partner (see chapter 6.2.1, page 144).

7.4 IPX Settings

The ➤➤ **IPX** Protocol (Internet Packet Exchange Protocol) is a network protocol that is used mainly in Novell networks. Novell ➤➤ **clients** and Novell ➤➤ **servers** can use IPX to communicate via LAN/WAN connections.

The configuration steps necessary for IPX connections are explained below:

- General settings
- Configuring the LAN interface
- Setting up WAN partners

7.4.1 General Settings

These settings are global parameters for IPX and apply to all **BinGO!** IPX connections.

The configuration is made in ***IPX***:

Field	Meaning
Local System Name	IPX system name of **BinGO!** in capital letters. Exclamation marks, full stops and underlining are not permitted.
Internal Network Number	**BinGO!**'s internal network number. This value must be unique among all the network numbers in the LAN and normally comprises the last four bytes of **BinGO!**'s ➤➤ **MAC address**. Only change this value if a ➤➤ **Remote** IPX router has the same *Internal Network Number*.
enable IPX spoofing	Enables and disables NCP session watchdog spoofing and handling of "broadcast message waiting" packets. Possible values: ■ *yes* ■ *no*
enable SPX spoofing	Enables and disables spoofing of SPX session watchdog packets. Possible values: ■ *yes* ■ *no*: disables SPX sessions via WAN connections.
NetBIOS Broadcast replication	Defines how **BinGO!** handles ➤➤ **NetBIOS** packets.

Table 7-31: ***IPX***

NetBIOS Broadcast replication contains the following selection options:

Possible Values	Meaning
yes	All NetBIOS hosts in the network can access each other, even if WAN connections must be set up frequently.
no	NetBIOS hosts in different LANs have no access to each other.
on LAN only	NetBIOS hosts in the LAN can only access each other if they do not need WAN connections to be set up.

Table 7-32: NetBIOS Broadcast replication

To Do Proceed as follows:

- Go to ***IPX***.
- Enter *Local System Name*.
- Enter *Internal Network Number*, if applicable (only if necessary!).
- Activate *enable IPX spoofing, if applicable*.
- Activate *enable SPX spoofing*, if applicable.
- Select *NetBIOS Broadcast replication*.
- Press **SAVE**.

7.4.2 Configuring the LAN Interface

The next step is to configure **BinGO!**'s LAN interface to the IPX network. The LAN interface is the physical interface to the local network. In the following menu, you give the router the address under which it can be reached in the LAN. As long as **BinGO!** does not have these entries, it cannot be recognized as part of the LAN by other hosts.

The configuration is made in ***CM-BNC/TP, ETHERNET***:

Field	Meaning
local IPX-NetNumber	The IPX network number of the LAN to which **BinGO!** is connected.
Encapsulation	Defines which type of header is added to the IPX packets that run via this LAN interface. Possible values: ■ *none* ■ *Ethernet II* ■ *Ethernet 802.2 LLC* ■ *Ethernet SNAP* ■ *Ethernet NOVELL 802.3*

Table 7-33: ***CM-BNC/TP, ETHERNET***

The available types of IPX ➤➤ **encapsulation** also partly support IP packets:

IPX encapsulation	Protocols supported	
	IP	IPX
Ethernet II	X	X
Ethernet SNAP	X	X
Ethernet 802.2 LLC		X
Novell 802.3		X

Table 7-34: IPX encapsulations

To Do Proceed as follows:

➤ Go to ***CM-BNC/TP, ETHERNET***.

➤ Enter *local IPX-NetNumber*.

➤ Select *Encapsulation*.

➤ Press **SAVE**.

7.4.3 Setting Up WAN Partners

If the connection to one or more WAN partners is implemented with the IPX protocol, you must define a number of settings.

The configuration is made in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IPX***:

Field	Meaning
Enable IPX	Enables IPX for the WAN partner. Possible values: ■ *yes* ■ *no*
IPX NetNumber	IPX network number of the WAN connection. Is required by some IPX routers.
Send RIP/SAP Updates	Defines how often **BinGO!** sends ➤➤ **RIP** (Routing Information Protocol) and SAP (Service Advertising Protocol) packets to the WAN partner. RIP and SAP packets are sent in IPX networks as ➤➤ **broadcasts** in linked networks to provide information about current routes and services and to update these. The data flow caused by this is okay in the LAN, but you must make a setting here for networks connected via WAN connections.
Update Time	Defines the time intervals at which periodic updates are sent.
Age Multiplier	If routes and services entered are not renewed during *Update Time* x *Age Multiplier*, they are deleted. This prevents accumulation of unnecessarily large numbers of routes and services that are not used.

Table 7-35: ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IPX***

The *Send RIP/SAP Updates* field contains the following selection options, which are explained with the aid of a table

Possible values	New connection opened?	Updates?	Periodic updates?	Description
off	never	no	no	All routes and services must be entered statically.
triggered + piggyback (on changes, per. if link active)	only for changes	yes	yes	The default setting, which is sufficient in most cases.
triggered (on changes)	only for changes	yes	no	Less data traffic than *triggered + piggyback*, but also less reliable.
piggyback (only if link active)	never	yes	yes	At least 1 route or service must be entered for the WAN partner.
passive triggered (on changes only if link active)	never	yes	no	At least 1 route or service must be entered for the WAN partner.
time update (always)	always	yes	yes	Can cause higher ISDN charges.

Table 7-36: *Send RIP/SAP Updates*

To Do Proceed as follows:

- Select *Enable IPX*.
- Enter *IPX NetNumber*.
- Select *Send RIP/SAP Updates*.
- Enter *Update Time, if applicable*.
- Enter *Age Multiplier*, if applicable.
- Confirm with **OK**.
- Press **SAVE**.

7.5 Extra License Functions

This chapter briefly describes the **BinGO!** functions you can enable with an extra license.

7.5.1 VPN (Virtual Private Network)

BinGO! can set up a VPN using the PPTP (Point to Point Tunneling Protocol). This offers secure (encrypted) transmission of data via WAN connections, e.g. over Internet. It could be used, for example, to provide field service staff with low-cost access to data in the company network via Internet and laptop (dialling in via a local Internet Service Provider).

You can find detailed information and configuration instructions (with examples) in Extended Feature Reference.

7.5.2 Unlimited Number of LAN Partners

You can cancel the limitation to 8 LAN partners by obtaining an extra license.

8 Security Mechanisms

SAFERNET

The **BinGO!** from BinTec Communications AG gives you a high degree of security for your network and connections. The security functions available offer monitoring of activities via the router and effective access and line tapping security. The necessary configuration steps are described in this chapter.

Some of the features can only be configured by making entries directly in the ➤➤ **MIB** tables and not by using the Setup Tool. The relevant tables and variables are given in the respective section.

You can make MIB entries either by commands in the ➤➤ **SNMP shell** or via external SNMP managers. A description of the SNMP commands is given in the Software Reference.

This chapter is broken down as follows:

- Activity Monitoring
- Access Security
- Line Tapping Security
- Special Features
- Checklist

8.1 Activity Monitoring

A major requirement for a high degree of security is accurate monitoring of all activities in and via the router. BinTec Communications AG offers you many facilities for monitoring activities.

8.1.1 Syslog Messages

All major events on **BinGO!**'s various subsystems (➤➤ **ISDN**, ➤➤ **PPP**, ➤➤ **CAPI**, etc.) are logged in the form of syslog messages (system logging messages).

The number of details shown depends on the level set (eight levels from critical to info to debug). **BinGO!** saves the logged data in a list that can be adjusted in length. All information can be and should be passed to one or more external computers for saving and further processing, e.g. to the System Administrator computer. The syslog messages are lost if you restart **BinGO!.**

Avoid forwarding syslog messages to log hosts reachable over a dialup connection. This raises your telephone bill unnecessarily.

Make sure that you only pass syslog messages to a safe computer. Check the data regularly and ensure that there is always enough free capacity available on the hard disc of your PC.

Syslog Demon

All Unix operating systems support the recording of syslog messages (setting up a Syslog Demon in Unix: see the Software Reference). For Windows computers, the Syslog Demon included in DIME Tools can record the data and distribute to various files depending on the contents (see Brickware for Windows).

Settings for syslog messages are made in:

- ***SYSTEM***,
- ***SYSTEM*** ➧ ***EXTERNAL SYSTEM LOGGING*** and

■ ***WAN PARTNER*** ➧ **Edit** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***:

Field	Meaning
Syslog output on serial console	Displays syslog messages on the computer connected to **BinGO!**'s serial interface. Possible values: ■ *yes* ■ *no.*
Message level for the syslog table	Specifies the priority of the syslog messages to be displayed. Possible values: ■ *emerg*: emergency messages (highest priority) ■ *alert*: alert messages ■ *crit*: critical messages ■ *err*: error messages ■ *warning*: warning messages ■ *notice*: notice message ■ *info*: info messages ■ *debug*: debug messages (lowest priority) Syslog messages are only displayed if they have a lower priority than or one identical to the priority indicated.
Maximum Number of Syslog Entries	Maximum number of syslog messages saved in **BinGO!**.

Table 8-1: ***SYSTEM***

Field	Meaning
Log host	➤➤ **IP address** of the host to which syslog messages are passed.

Field	Meaning
Level	Priority of the syslog messages to be sent to *Log Host*. Corresponds to *Message level for the syslog table* in ***SYSTEM***.
Facility	Syslog facility at *Log Host*. Only required if the *Log Host* is a Unix computer.
Type	Message type. Possible values: ■ all: all messages. ■ system: syslog messages except accounting messages. ■ accounting: accounting messages.

Table 8-2: ***SYSTEM*** ➧ ***EXTERNAL SYSTEM LOGGING***

Field	Meaning
IP Accounting	For saving accounting messages for ➤➤ **TCP**, ➤➤ **UDP** and ICMP sessions. Possible values: *on*, *off*.

Table 8-3: ***WAN PARTNER*** ➧ **ADD** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***

Make the desired settings for syslog messages as follows:

➤ Go to ***SYSTEM***.

➤ Select *Syslog output on serial console*.

➤ Select *Message level for the syslog table*.

➤ Enter *Maximum Number of Syslog Entries*.

➤ Go to ***SYSTEM*** ➧ ***EXTERNAL SYSTEM LOGGING*** to pass syslog messages to external hosts.

➤ Select an existing entry and confirm it with **Return** or add a new entry with **ADD**.

➤ Enter *Log Host*.

➤ Select *Level*.

➤ Select *Facility*.

➤ Select *Type*.

Extended IP accounting

Proceed as follows to activate extended IP accounting. **BinGO!** then saves accounting messages from TCP, UDP and ICMP sessions:

➤ Go to ***WAN PARTNER*** ➧ **Edit** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.

➤ Activate *IP Accounting* with *on*.

Displaying syslog messages

Proceed as follows to display syslog messages:

➤ Go to ***MONITORING AND DEBUGGING*** ➧ ***MESSAGES***.

This displays the syslog messages saved in **BinGO!**:

```
BinGO! Setup Tool                                BinTec Communications AG
[MONITOR][MESSAGE]: Syslog Messages                              MyBinGO!

Subj    Lev Message

SNMP    DEB sent TRAP (linkUp,0) 115 bytes to circindex 1001 Port36880
SNMP    DEB sent TRAP (linkUp,0) 115 bytes to 199.1.1.13 Port 162


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

Deleting syslog messages

➤ Select **RESET** to delete the syslog messages in **BinGO!**.

For interpretation of syslog messages: see the Software Reference.

8.1.2 Monitoring Functions in the Setup Tool

You can also use the Setup Tool to display other data in addition to syslog messages. The current status of certain subsystems is updated periodically and displayed. Display modules are available for the following functional areas:

- ISDN connections
- Credits
- Interface statistics (comparative display of several interfaces)
- ➤➤ **TCP/IP** statistics
- Syslog messages (see chapter 8.1.1, page 228)
- ISDN connections

ISDN connections

Proceed as follows to display ISDN connections:

➤ Go to ***MONITORING AND DEBUGGING*** ➧ ***ISDN MONITOR***.

A list of the existing ISDN connections (incoming and outgoing calls) is displayed.

```
BinGO! Setup Tool                                BinTec Communications AG
[MONITOR][ISDN CALLS]: ISDN Monitor - Calls                      MyBinGO!

Dir Remote Name/Number   Charge   DurationeStack   Channel  State

in  2                             2910        0       B1       active
out 3                             106         0       B2
disc_req


(c)alls        (h)istory        (d)etails        (s)tatistics
(r)elease
```

This menu also offers you other options:

➤ Select **h** to display a list of the last 20 completed ISDN calls (incoming and outgoing) since the last system start.

➤ Select **d** to display detailed information on existing and completed ISDN calls.

➤ Select **s** to display statistics on the activity of the existing ISDN calls.

➤ Select **c** to display the list of existing ISDN calls again.

➤ Select **r** to close ISDN connections.

Credits Proceed as follows to display the status of the credits:

➤ Go to ***MONITORING AND DEBUGGING*** ➧ ***ISDN CREDITS***.

➤ Select a subsystem and confirm with **Return**.

The current credits status of the selected subsystem is displayed.

```
BinGO! Setup Tool                                BinTec Communications AG
[MONITOR][CREDITS][STAT]: Monitor isdnlogin Credits              MyBinGO!


                                        Total    Maximum       % reached
Time till end of measure interval (sec)7794    86400         91

Number of Incoming Connections                0           2   0
Number of Outgoing Connections                0          20   0

Time of Incoming Connections                     428800       0
Time of Outgoing Connections                    1328800       0

Charge                                        0

EXIT
```

Interface statistics Proceed as follows to display the current values and activities of the **BinGO!** interfaces:

➤ Go to ***MONITORING AND DEBUGGING*** ➧ ***INTERFACES***.

The values for two interfaces are displayed side by side.

```
BinGO! Setup Tool                                  BinTec Communications AG
[MONITOR][INTERFACE]: Interface Monitoring                        MyBinGO!

Interface Name        en1                          PROVIDER
Operational Status    up                           dormant

                      total    per second          total    per second

Received Packets      5512     0                   0        0
Received Octets       920664   0                   0        0
Received Errors       0                            0

Transmit Packets      9        0                   0        0
Transmit Octets       1193     0                   0        0
Transmit Errors       0                            0

Active Connections    N/A                          0
Duration              N/A                          0

EXIT                  EXTENDED                     EXTENDED

Use <Space> to select
```

➤ Select the interface to be displayed under *Interface Name*.

➤ Select **EXTENDED** to display additional information. You can then change the status of the interface under *Operation* and confirm the entry with **START OPERATION**.

TCP/IP statistics

Proceed as follows to display the statistics for connections with the ICMP, ➤➤ **IP**, UDP and TCP ➤➤ **protocol**:

➤ Go to ***MONITORING AND DEBUGGING*** ➧ ***TCP/IP***.

The statistics for IP connections are displayed. You can find the meaning of the MIB variables in the MIB Reference.

```
BinGO! Setup Tool                                BinTec Communications AG
[MONITOR][IP]: IP Statistics                                     MyBinGO!

InReceives          3912        OutNoRoutes          0
InHdrErrors         0           ReasmTimeout         500
InAddrErrors        0           ReasmReqds           0
ForwDatagrams       0           ReasmOKs             0
InUnknownProtos     0           ReasmFails           0
InDiscards          0           FragOKs              0
InDelivers          3321        FragFails            0
OutRequests         9           FragCreates          0
OutDiscards         0           RoutingDiscards      0

EXIT

        I(C)MP              (I)P              (U)DP              (T)CP
```

- Select **c** to display the statistics for ICMP connections.
- Select **i** to display the statistics for IP connections.
- Select **u** to display the statistics for UDP connections.
- Select **t** to display the statistics for ICMP connections.

8.1.3 HTTP Status Page

Every BinTec router has a homepage, the so-called HTTP status page. You can use this with the aid of an Internet browser (e.g. Netscape Navigator, Internet Explorer) to display the status of **BinGO!**. All users of the **BinGO!** LAN can then view the router status, provided they know the password for the user name `http`.

Do bear in mind HTTP pages are usually stored in the cache memory of the browser, so that they can be read by other users at the same workplace and viewed on the proxy ➤➤ **servers** concerned.

- Enter the URL `http://<System Name>:80` in your browser.

  The HTTP status page of the BinTec router with the system name <System Name> is displayed.

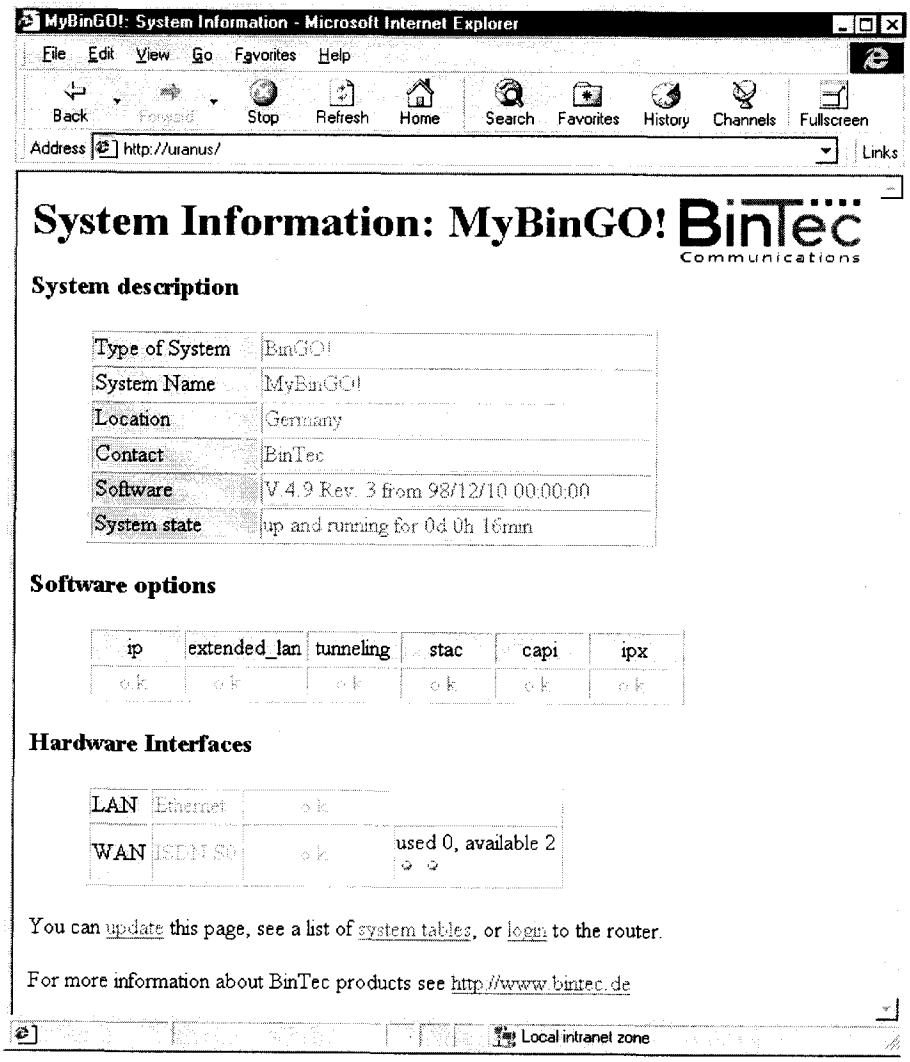


Figure 8-1: HTTP status page

The HTTP status page contains three tables:

- System description:
  This table lists information from the MIB **admin** table such as **System Name** and **Contact**. If a valid e-mail address is given under **Contact,** this is shown underlined.
- Software options:
  This table lists information from the MIB table **biboAdmLicInfoTable** and displays the status of **BinGO!**'s subsystems.
- Hardware interfaces:
  This table displays the LAN and WAN interface of **BinGO!**. The third column of the table provides information on the current status of the physical interfaces, which can have the following values:

Interface	Status	Possible cause
LAN	o.k.	Normal operation.
	inactive	LAN cable is not connected.
WAN	o.k.	Normal operation.
	inactive	None of the B-channels is in use at present.
	unconfigured	ISDN cable is not connected or a wrong ➤➤ **D-channel** protocol is entered.

Table 8-4: Status of the interfaces

The HTTP status page contains a number of links:

- `update`
  Click `update` to update the status page.
- `login`
  Click `login` to log in to the associated BinTec router via ➤➤ **telnet**.
- `http://www.bintec.de`
  Use this link to access BinTec's WWW server with the latest information on products and the current system software and documentation for **BinGO!**.

- `system tables`
  Click `system tables` to display a list with all the **BinGO!** MIB tables. Clicking a table name lists the variables contained in the table.

If you do not want to display your HTTP status page, enter 0 as the port number of the http port:

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

➤ Enter *HTTP TCP port: 0.*

➤ Confirm with **SAVE**.

8.1.4 Java Status Monitor

The Java status monitor offers you another facility for displaying information about **BinGO!** using an Internet browser. You can call up the following information with the Java status monitor:

- Static information such as the system name of the BinTec router and the software version.
- Data flow via the individual interfaces.
- Connections to WAN partners.

If you have installed the Java status monitor together with BRICKware (see chapter 3.3, page 43), you can start as follows:

➤ Select **Program** ➧ **BRICKware** ➧ **Java Status Monitor** in the Windows start menu.

The Java status monitor opens with your standard browser.

You can find out how to use the individual functions of the Java status monitor in Brickware for Windows.

8.2 Access Security

There are several ways of restricting logging in and access to **BinGO!** to authorized users only.

8.2.1 Logging In

Password

You can log in to **BinGO!** in several different ways as described in chapter 5, page 97, but logging in is always protected by a password. Every failed attempt is logged by a syslog message indicating the source and creates a relevant SNMP trap. Pauses are introduced after several failed attempts in order to make automatic attempts to log in more difficult.

Caution!

All BinTec routers are supplied with the same user names and passwords and are consequently not protected against unauthorized access.

- You must change the passwords as described in Chap. chapter 6.1.2, page 122.
- Make sure that **BinGO!** is installed in a room inaccessible to the unauthorized.

Until you have changed the default password for the user name `admin`, **BinGO!** always gives you a warning after logging in.

Auto logout

To make unauthorized access difficult, the connection to **BinGO!** is disconnected if no keyboard entry is made for a period of 15 minutes. You can change this time using the command `t<time in seconds>` (see chapter 12.1, page 308).

If you are updating your software (see chapter 9.2, page 279), you should disable autologout, to do so, enter `t 0` in the SNMP shell.

You can create additional user accounts with the aid of SNMP commands (see the Software Reference). A certain password and a certain action can be assigned to a user.

8.2.2 Checking the Calling Party's Number

CLID

BinGO! uses Calling Line Identification (➤➤ **CLID**) to check the calling party's number of an incoming call. If the calling party's number has been entered for all the configured WAN partners, **BinGO!** generally accepts calls from known telephone numbers only.

Screening indicator

You can also determine whether calling party numbers have been modified by the calling parties. For some connections, it is possible that another number (e.g. 5678) is displayed at the called party instead of the calling party's own number (e.g. 1234). **BinGO!** can detect this from the screening indicator in the setup message of the ISDN ➤➤ **D-channel.** The screening indicator has four possible values:

- *user*: The calling party's number indicated originates from the far end and has not been checked by the network.
- *user_verified*: The calling party's number has been checked by the exchange and is correct.
- *user_failed*: The calling party's number has been checked by the exchange and is incorrect.
- *network*: The calling party's number indicated originates directly from the exchange (normal case).

If you want **BinGO!** to check the screen indicator for incoming calls, you must enter one of the values stated in the following MIB tables or variables (only incoming calls with the appropriate screening indicator are accepted)

- ➤ For incoming PPP connections: **Screening** variable in **biboDialTable**.
- ➤ For incoming isdnlogin connections: **Screening** variable in **isdnloginAllowTable**.

8.2.3 Authentication of PPP Connections with PAP, CHAP or MS-CHAP

➤➤ **PAP**, ➤➤ **CHAP** and MS-CHAP are the common procedures used for authentication of ➤➤ **PPP** connections. These use a standard procedure to exchange a user ID and a password for checking the identity of the far end. You can find further information in chapter 6.2.1, page 144 and chapter 7.1.4, page 190.

8.2.4 Callback

The callback mechanism can be used for each WAN partner to achieve additional security regarding the connection partner or to clearly distribute the costs of connections. A connection is then not set up until the calling party has been clearly identified by calling back. **BinGO!** can answer an incoming call with a callback or dial into a WAN partner and then wait for a callback:

Identification can be based on the calling party's number or PAP/CHAP/MS-CHAP authentication. Identification is made in the first case without call acceptance, as the calling party's number is transferred over the ISDN D-channel, and in the second case with call acceptance.

You can find a detailed description of the callback mechanism in the Software Reference.

Callback is configured in ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***:

Field	Meaning
Callback	Activates the callback function.

Table 8-5: ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***

Callback offers the following selection options:

Possible Values	Meaning
no	**BinGO!** does not call back.
expected (awaiting callback)	**BinGO!** calls the WAN partner, ends the connection and awaits a callback.
yes (PPP negotiation)	**BinGO!** calls back with the number entered for the WAN partner. If no number is entered, the required number can be reported by the caller in a PPP negotiation. You should avoid this setting if possible for security reasons, but no alternative is currently available for connecting Microsoft ➤➤ **Clients** over the data communications network.
yes (delayed)	**BinGO!** calls back after four seconds, if requested to by the WAN partner.
yes	**BinGO!** calls back immediately, if requested to by the WAN partner.

Table 8-6: *Callback*

Proceed as follows to activate callback for a WAN partner:

➤ Go to ***WAN Partner*** ➧ ***Edit*** ➧ ***Advanced Settings***.

➤ Select *Callback*.

➤ Confirm with **OK**.

8.2.5 Closed User Group

BinGO! supports the use of the Closed User Group service feature, which you can request for your ISDN line from your telephone company. The external/internal reachability is monitored and controlled by the exchanges if this feature is selected.

Proceed as follows to activate a Closed User Group for a WAN partner:

➤ Go to ***WAN Partner*** ➧ ***Edit*** ➧ ***WAN Numbers*** ➧ ***Edit*** ➧ ***Advanced Settings***.

➤ Select *Closed User Group*: *specify*.

➤ Enter the CUG index.

➤ Confirm with **OK**.

8.2.6 Access to Remote CAPI

The special features offered by BinTec routers include implementation of the ➤➤ **Remote CAPI** and Remote TAPI programming interfaces (only for PABX devices). This enables applications on computers in the LAN to use the resources of the router as if these components were installed directly in the computer.

By using BinTec's ➤➤ **CAPI** user concept, you can make sure that only users authenticated by user name and password can access **BinGO!**'s Remote CAPI interface (see chapter 7.1.2, page 184).

You can also prevent unauthorized access by defining filters (see chapter 8.2.8, page 250) and local filters (see chapter 8.2.9, page 262).

8.2.7 NAT (Network Address Translation)

➤➤ **NAT** is a simple-to-operate procedure that can be used for four purposes in the BinTec implementation:

- Hiding the internal host addresses of a LAN by remapping to one or more external addresses. The external addresses remain unchanged.
- Controlling the external to internal access. Externally the router forwards all ➤➤ **data packets**, internally it only forwards what has been explicitly enabled (Forward NAT).

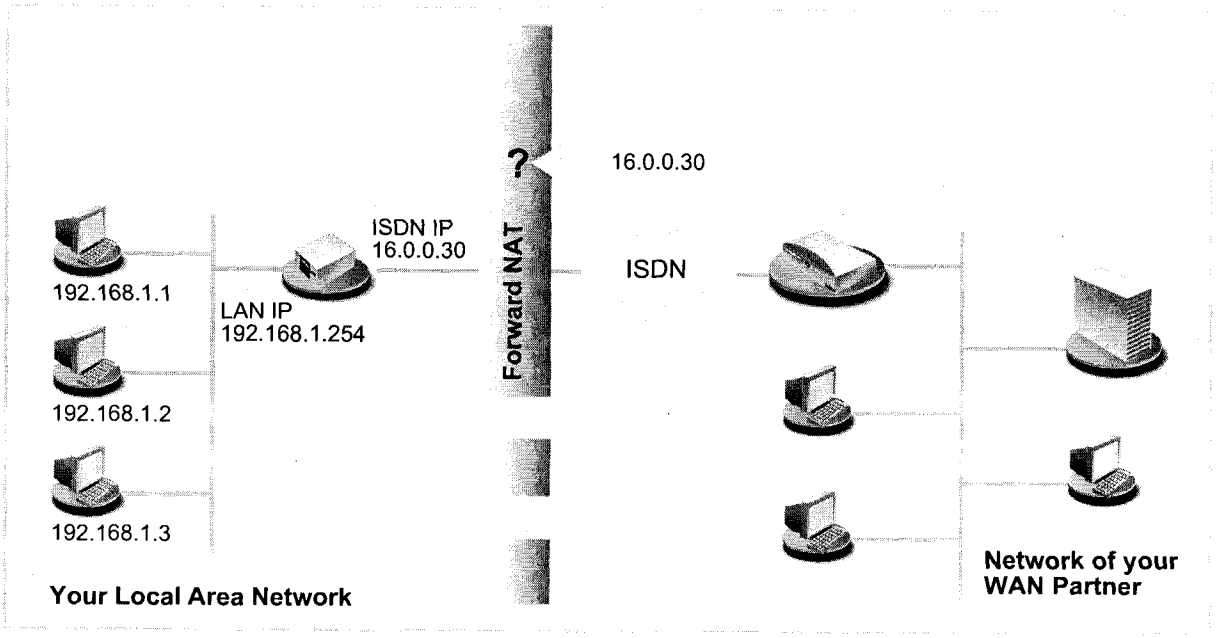


Figure 8-2: Forward NAT

- Reverse NAT ensures that a connection partner uses only a single ➤➤ **IP address**. Only incoming connections are allowed from the partner, e.g. as a service from Internet Service Providers (ISP).

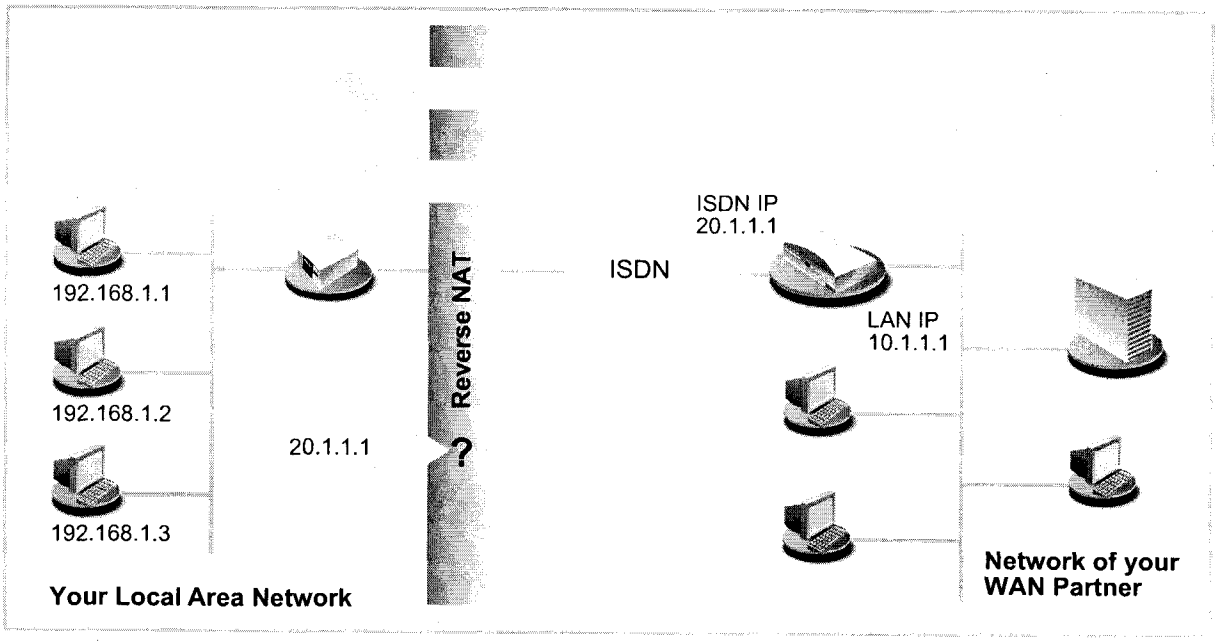


Figure 8-3: Reverse NAT

- Permanent monitoring of the connections into and out of a network via the router with indication of the source and destination addresses and ➤➤ **ports**.

NAT always refers to an interface. The LAN to which **BinGO!** is connected is always referred to as "inside", the WAN partner as "outside".

You will find more on NAT in the Software Reference.

Configuration is made in ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.

Activate NAT for a **BinGO!** interface in ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Return**:

Field	Meaning
Network Address Translation	Defines the type of NAT for the selected interface. Possible values: ■ *off*: do not execute NAT. ■ *on*: execute Forward NAT. ■ *reverse*: execute Reverse NAT.

Table 8-7: ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Return**

You can explicitly allow a NAT interface certain IP connections to a certain internal host in ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Return** ➧ **ADD**:

Field	Meaning
Service	Service that is allowed for connections of the host defined under *Destination*. Possible values: ■ *ftp* ■ *telnet* ■ *smtp* ■ *domain/udp* ■ *domain/tcp* ■ *http* ■ *nntp* ■ *user defined*: if you do not use any of the predefined services. Enter the required values under *Protocol* and *Port* to define a service.
Protocol	Only for *Service = user defined.* Defines the permitted protocol. Possible values: ■ *icmp* ■ *tcp* ■ *udp*
Port (-1 for any)	Only for *Service = user defined.* Defines the permitted port. Entering -1 permits any port for the protocol. If you specify the port, the entry must agree with the internal port number of **BinGO!**.

Field	Meaning
Destination	IP address of the host in the LAN. If you do not make an entry here, **BinGO!** is assumed as the destination.

Table 8-8: ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Return** ➧ **ADD**

Proceed as follows to activate NAT:

- Go to ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION***.
- Select the interface for which you want to activate NAT and confirm with **Return**.
- Select *Network Address Translation*, e.g. *on*.
  This activates NAT for the selected interface.
- Confirm with **SAVE**.

An entry takes effect as soon as you confirm it with **SAVE**. Never forget this, especially if you are configuring NAT from a remote host (e.g. with telnet)!

Proceed as follows to enable certain connections for a NAT interface to a certain host in the LAN:

- Go to ***IP*** ➧ ***NETWORK ADDRESS TRANSLATION*** ➧ **Return**.
- Add an entry with **ADD** or select an existing entry and confirm with **Return**.
- Select *Service*.
- Select *Protocol* if necessary.
- Enter *Port (-1 for any)* if necessary.
- Enter *Destination*.
- Confirm with **SAVE**.
- Repeat these steps to define several session profiles for the selected NAT interface.

8.2.8 Filters

➤➤ **Filters** in **BinGO!** are based on a concept of filters, rules and so-called chains. Filters respond to incoming data packets, which means they can allow or deny the passage of certain data through **BinGO!**.

Filter A filter describes a part of the IP data traffic based on the IP address, network ➤➤ **netmask**, protocol and source and/or destination port. If you define a filter, you are telling **BinGO!**: "Watch out for all incoming data packets that match the following: ...".

Rule You use a rule to tell **BinGO!** what to do with the data packets it has filtered out, i.e. whether or not it should allow them to pass through. You can also define several rules, which you arrange in the form of a chain to obtain a certain order.

Chain In principle, there are two options for defining rules and rule chains:

- Allows all packets that are not explicitly prohibited, i.e.
  - Deny all packets that match Filter 1.
  - Deny all packets that match Filter 2.
  - ...
  - ...
  - Allow the rest.
- Allow only what is explicitly permitted, i.e.
  - Allow all packets that match Filter 1.
  - Allow all packets that match Filter 2.
  - ...
  - ...

Interface Finally, you can also individually specify the order of the rules for each **BinGO!** interface.

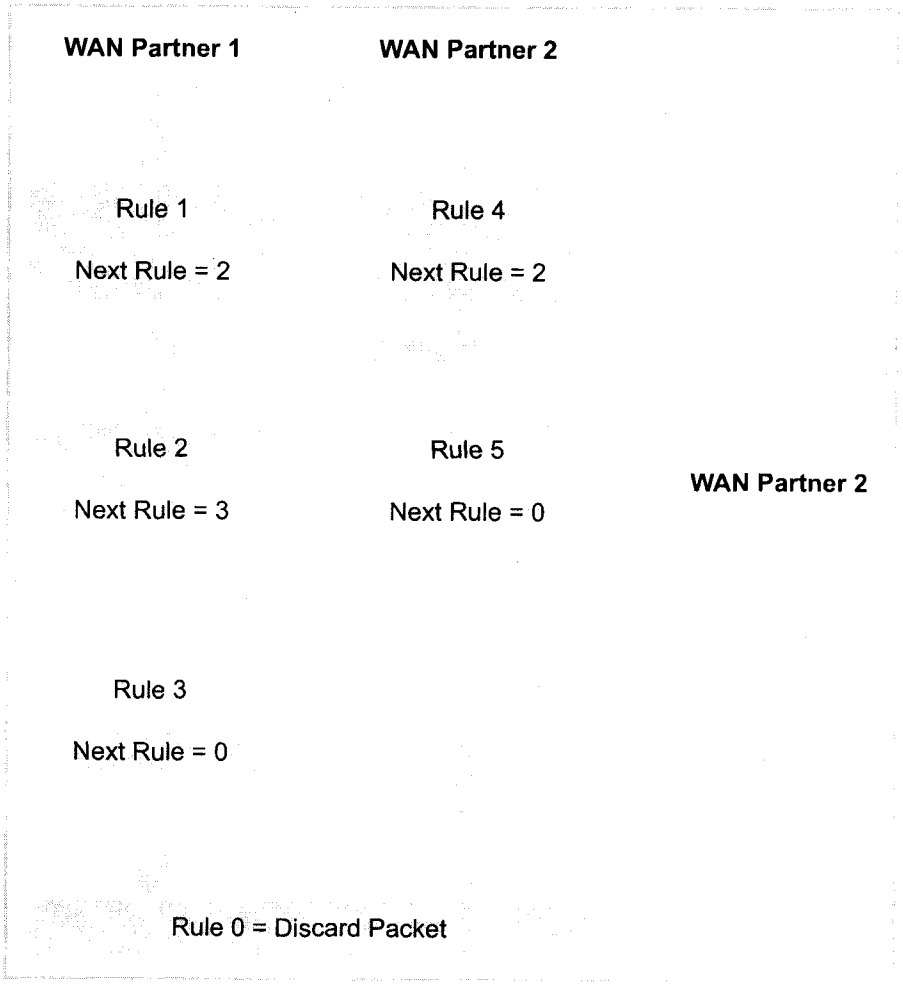


Figure 8-4: Rule chains for various interfaces

Configuration is made in:

- ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER***,
- ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES***,
- ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **REORG** and
- ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES***.

You can define filters in ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTER***:

Field	Meaning
Description	Designation of the filter. Note that possibly only the first 15 characters are displayed in other menus.
Index	Cannot be changed. **BinGO!** issues a number to newly defined filters automatically.
Protocol	Defines a protocol. Possible values: *any, icmp, ggp, tcp, egp, pup, udp, hmp, xns_idp, rdp, rsvp, gre, esp, ah, igrp, ospf, l2tp.* *any* is suitable for any protocol, *tcp* is suitable only for TCP data packets, etc.
Connection State	If *Protocol = tcp*, you can define a filter based on the TCP connection state. Possible values: *established*: The filter is suitable for all TCP packets that would not open any new connection on routing over **BinGO!**. *any*: The filter is suitable for all TCP packets.
Type	Only if *Protocol = icmp*. Possible values: *any, echo reply, destination unreachable, source quench, redirect, echo, time exceeded, param problem, timestamp, timestamp reply, address mask, address mask reply.* See RFC 792.
Source / Destination Address	(Optional) source and destination IP address of the data packets that match the filter.
Source / Destination Mask	(Optional) source and destination network mask. The combination of *Address* and *Mask* describes a range of IP addresses that match the filter.
Source / Destination Port	Port number or range of port numbers that match the filter.

Field	Meaning
Specify Port	Only if *Source / Destination Port* = *specify* or *specify range*: Enter range of port numbers.

Table 8-9: ***IP ➧ ACCESS LISTS ➧ FILTER***

The *Source Port* and *Destination Port* fields contain the following selection options:

Possible Values	Meaning
any	The filter matches all ➤➤ **port numbers**.
specify	Permits the entry of a port number under *Specify Port*.
specify range	Permits the entry of a range of port numbers under *Specify Port*.
priv (0..1023)	Port numbers: 0 ... 1023.
server (5000..32767)	Port numbers: 5000 ... 32767.
clients 1 (1024..4999)	Port numbers: 1024 ... 4999.
clients 2 (32768..65535)	Port numbers: 32768 ... 65535.
unpriv (1024..65535)	Port numbers: 1024 ... 65535.

Table 8-10: *Source Port* and *Destination Port*

Port numbers The port numbers are distributed as follows:

0 ... 1023	1024 ... 4999	5000 ... 32767	32768 ... 65535
Well-known ports, i.e. permanently assigned.	The ports are created dynamically by ➤➤ **clients** and ➤➤ **servers** and have no permanent meaning (with the exception of special agreements): *unpriv (1024..65535)*		
priv (0..1023)	*clients 1 (1024..4999)*	*server (5000..32767)*	*clients 2 (32768..65535)*

Table 8-11: Ranges of port numbers

The following table contains an overview of some frequently used port numbers with the services assigned to them:

Service	Protocol	Port number
File Transfer Protocol (➤➤ **FTP**) (data)	TCP	20
File Transfer Protocol (FTP) (commands)	TCP	21
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (➤➤ **DNS**)	TCP, UDP	53
Trivial File Transfer Protocol (TFTP)	UDP	69
http / WWW	TCP	80
POP3 (E-mail query)	TCP	110
Network Time Protocol	TCP, UDP	119
➤➤ **NetBIOS** Name (NBNAME)	UDP	137
NetBIOS Datagram (NBDATA)	UDP	138
NetBIOS Session (NBSESSION)	TCP	139
Simple Management Network Protocol (SNMP)	UDP	161
SNMP (traps)	UDP	162
Syslog Service (SYSLOG)	UDP	514
Network File System	UDP	2049
Remote CAPI	TCP	2662
Remote TAPI	TCP	2663

Table 8-12: Services and port numbers

Example A simplified FTP connection is used as an example to illustrate how to use source and destination ports: in addition to source and destination IP addresses, the IP protocol also uses source and destination port numbers to uniquely identify data connections. The FTP client creates a number, e.g. xyz, which is

used as source port number. As destination port number, the client uses the number under which the FTP server offers the FTP service, e.g. 21. The FTP server then sends IP packets that use 21 as source port number and xyz as destination port number:

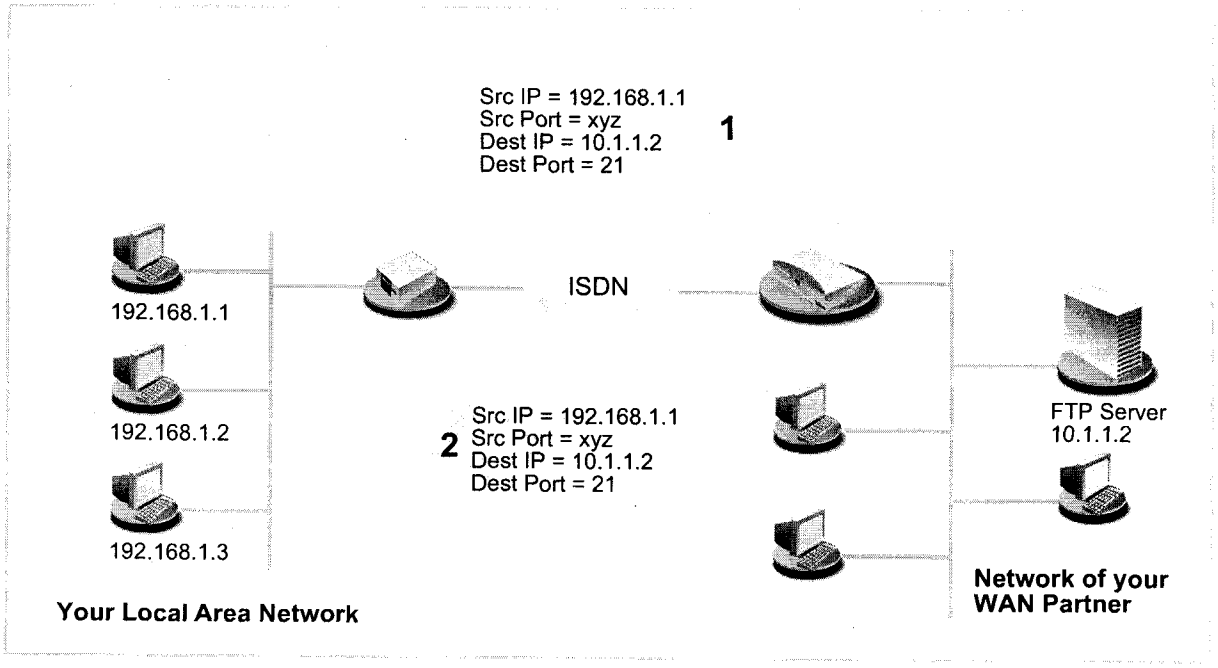


Figure 8-5: Example: FTP connection

You can define rules in ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES***:

Field	Meaning
Index	Cannot be changed. **BinGO!** issues a number to newly defined rules automatically or displays the *Index* of existing rules.
Insert behind Rule	Appears only if a new rule is defined. Defines the rule behind which the new rule is inserted. You can start a new independent chain with *none*.
Action	Defines the action to be taken for a filtered data packet.
Filter	Filter used.
Next Rule	Appears only if an existing rule is edited. Defines the next rule to be used.

Table 8-13: ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES***

The *Action* field contains the following selection options:

Possible Values	Meaning
allow M	Allow packet if the filter matches.
allow !M	Allow packet if the filter does not match,
deny M	Deny packet if the filter matches.
deny !M	Deny packet if the filter does not match.
ignore	Use next rule.

Table 8-14: *Action*

You can change the order of the rules in a chain using the submenu ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **REORG**:

Field	Meaning
Index of Rule that gets Index 1	Defines the first rule in the chain.

Table 8-15: ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **REORG**

If you reorganize such a chain, **BinGO!** rearranges the remaining rules according to the selection in *Index of Rule that gets Index 1*:

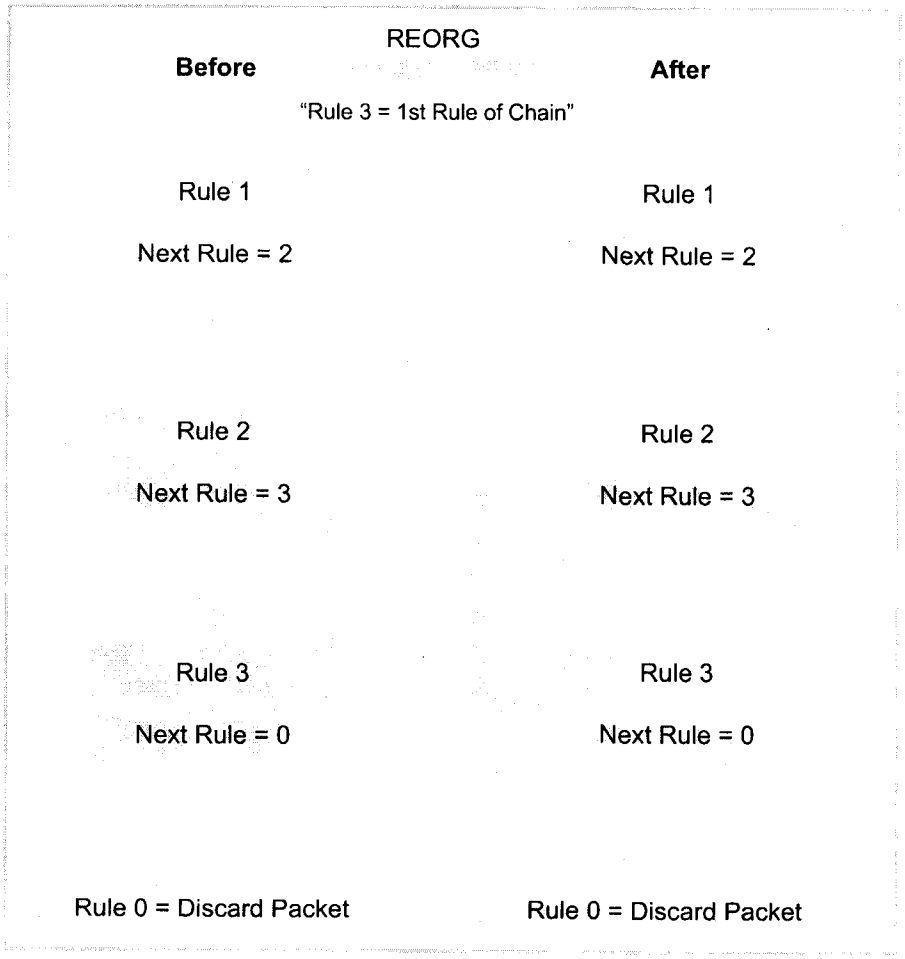


Figure 8-6: Example of a reorganization of a chain

You can define which interface starts and with which rule in ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES***:

The rule with *Index = 1* is normally always used as the first rule for a newly created interface (e.g. to a WAN partner).

Field	Meaning
Interface	**BinGO!** interface
First Rule	Defines which rule is used first for data packets that reach **BinGO!** via the *Interface*. If you enter *none*, you specify that no filters are used for the *Interface*.

Table 8-16: ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES***

To do Proceed as follows to define filters and rules:

Ensure that you don't lock yourself out when configuring the filters. For example, if you link the first filter to a rule which executes *Action* = *Allow M*, only that which you have expressly allowed with the filter actually gets through. It can easily occur that your telnet access to **BinGO!** is no longer allowed as soon as you enter the filter and confirm with save.

- Do not use any filters on the LAN interface (*First Rule* = *none*), if you access **BinGO!** via telnet.
- If you access **BinGO!** via the serial interface or isdnlogin, at least nothing can happen to you during configuration.

Filter

➤ Go to ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTERS***.

➤ Add a new entry with **ADD** or select an existing entry and confirm with **Return** to change it.

➤ Enter *Description*.

➤ Select *Protocol*.

➤ Enter *Source Address* if necessary.

➤ Enter *Source Mask* if necessary.

➤ Select *Source Port*.

➤ Enter *Specify Port* if necessary.

➤ Enter *Destination Address* if necessary.

➤ Enter *Destination Mask* if necessary.

- Select *Destination Port*.
- Enter *Specify Port* if necessary.
- Confirm with **SAVE**.
- Repeat these steps until you have defined all the desired filters.

Do not forget to define a filter if necessary for enabling the remaining data packets (*Protocol = any, Source Port = any, Destination Port = any*).

- Leave ***IP*** ➧ ***ACCESS LISTS*** ➧ ***FILTERS*** with **EXIT**.

Rules

- Go to ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** to interlink the filters with rule chains.
- Add a new entry with **ADD** or select an existing entry and confirm with **Return** to change it.
- Select *Insert behind Rule* if you create a new rule.
- Select *Action*.
- Select *Filter*.
- Select *Next Rule* if you change an existing rule.
- Confirm with **SAVE**.
- Repeat these steps until you have defined all the desired rules.

Do not forget to define the last rule in the chain as a rule for enabling the remaining data packets (*Action = allow M*).

You can open a new rule chain with *Insert behind Rule = none*.

- Leave ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** with **EXIT**.

Interface

- Go to ***IP*** ➧ ***ACCESS LISTS*** ➧ ***INTERFACES***.

- Select an interface and confirm with **Return** if you wish to use a rule as the first rule for this interface that is not the rule displayed.
- Select *First Rule*.
- Confirm with **SAVE**.

Reorganize chain Proceed as follows to reorganize an existing chain of rules:

- Go to ***IP*** ➧ ***ACCESS LISTS*** ➧ ***RULES*** ➧ **REORG**.
- Select *Index of Rule that gets Index 1*.
- Confirm with **REORG**.

If you work with Windows in your network, it is usually advisable to define a NetBIOS filter. An example of this configuration is explained step by step in chapter 6.1.6, page 138.

8.2.9 Local Filters

Access to the local services in **BinGO!** (telnet, ➤➤ **CAPI**, trace, etc.) can be controlled via a separate MIB table. As long as this is empty, access to local services is possible via all interfaces, provided it is not prohibited by the use of NAT (see chapter 8.2.7, page 244) or global filters (see chapter 8.2.8, page 250).

Local filters, therefore, provide an additional instrument that is easier to handle than global filters and also does not adversely affect performance in normal routing.

Activate local filters by entries in the MIB tables **localTcpAllowTable** and **localUdpAllowTable**.

8.2.10 Back Route Verify

This term conceals a simple but very effective **BinGO!** function. If Back Route Verify is activated at a WAN partner's, only those data packets are transported via the interface to the WAN partner that would be routed over the same interface on the back route. You can therefore prevent packets with fake IP address-

es being fed to your LAN – even without filters. This means you can easily prevent known and as yet unknown Denial-of-Service and IP Spoofing Attacks.

Proceed as follows to activate Back Route Verify for a WAN partner:

➤ Go to ***WAN PARTNER*** ➧ ***Edit*** ➧ ***IP*** ➧ ***ADVANCED SETTINGS***.

➤ Activate *Back Route Verify* with *on*.

➤ Confirm with **OK**.

8.2.11 TAF Client

Personalized authentication

The Token Authentication Firewall (TAF) function permits personal authentication of IP connection partners. BinTec's solution integrates the token authentication mechanisms of Security Dynamics and allows data packets to pass through the router only after successful authentication of the associated source address.

You can enable this function on BinTec's Corporate Access Routers and set up the router as TAF server. You can configure the **BinGO!** Personal Access Router as TAF ➤➤ **client** to obtain access on a TAF server and the connected LAN (if the TAF server has been set up appropriately). A detailed description of operation and the necessary configuration steps is contained in BRICKware for Windows.

8.2.12 Extended IP Routing XIPR

In addition to the normal routing table, **BinGO!** can also make routing decisions based on an additional table called the Extended Routing Table. Apart from the destination address, it can also include the protocol, source and destination port, type of service (TOS) and the status of the destination interface in the decision. If there are entries in the Extended Routing Table, these are preferentially treated compared with entries in the normal routing tables.

XIPR is useful, for example, if two networks are connected via ISDN with a LAN-LAN connection, but where services (e.g. telnet) should be routed not over an ISDN switched connection but over an X.25 link. By making entries in the Extended Routing Table, you can allow a part of the IP traffic to run over the ISDN

switched connection and a part of the IP traffic (e.g. for telnet) to run over an X.25 link (see also the Software Reference).

Configuration is made in the MIB table **ipExtRtTable** and a detailed description is contained in the Software Reference.

8.3 Line Tapping Security

You can use an encryption mechanism to obtain data security for PPP connections on connections with critical security, provided both connection partners support this mechanism.

8.3.1 Encryption

BinGO! supports the encryption of PPP connections to WAN partners. Encryption is based on the ➤➤ **MPPE** (Microsoft Point to Point ➤➤ **Encryption**) procedure with code lengths of 40 bits and 128 bits.

Configuration is made in ***WAN PARTNER*** ➧ **ADD**:

Field	Meaning
Encryption	Defines the type of encryption. Possible values: ■ *MPPE 40*: code length 40 bits. ■ *MPPE 128*: code length 128bits. ■ *none*: no encryption.

Table 8-17: ***WAN PARTNER*** ➧ ***Edit***

Proceed as follows to activate encryption:

➤ Go to ***WAN PARTNER***.

➤ Select a WAN partner and confirm with **Return** to encrypt the PPP connections to this partner.

➤ Select *Encryption*, e.g. *MPPE 40*.

➤ Confirm with **SAVE**.

8.3.2 VPN (with extra license)

BinGO! can set up a VPN (Virtual Private Network) using the PPTP (Point to Point Tunneling Protocol). This provides safe (encrypted) transmission of data over WAN connections, e.g. over Internet. It can be used, for example, by field service staff to obtain low-cost access to data in the company network via Internet and laptop (dial-in via a local Internet Service Provider).

You can find detailed information and configuration instructions (with examples) in Extended Features Reference.

8.4 Special Features

8.4.1 Startup Procedure

BinGO! does not start its routing activities until the complete configuration is loaded, especially the defined filters. This means it is not possible to provoke a system start to make use of an intermediate system state in which perhaps routing takes place before the filters are active.

8.4.2 Auto Logout

Connections to **BinGO!** via telnet, ➤➤ **isdnlogin** or serial interface are disconnected automatically if no entry is made on the keyboard for a period of 15 minutes. This makes it difficult to read out or change the system configuration on "forgotten" connections. You can change the time with the command `t <time in seconds>` (see chapter 12.1, page 308).

8.4.3 Prevention of Denial-of-Service Attacks

A Denial-of-Service (DoS) attack is an attempt to flood a router or a host in a LAN with forged requests and thereby to fully overload it. Thus, authorized access to the LAN is rendered impossible. A local address taken from the local LAN is used as the source address of the attacker.

Some Denial-of-Services attacks on the router itself are already prevented by the internal coding.

For example, all **BinGO!** interfaces for which you activate Network Address Translation (NAT) protect the connected computers against some DoS attacks with fragmented packets. The packet fragments are assembled again on passing through NAT, before the packet can pass the router.

You can prevent some DoS attacks that operate with fake source IP addresses by using the Back Route Verify function (see chapter 8.2.10, page 262).

You can counter DoS attacks that speculate on destroying the system by causing the log files to overflow (syslog messages) by suitably positioning and limiting the size of these files.

8.5 Checklist

The following list indicates the most important critical security points that you should observe when configuring **BinGO!**:

- Have you changed all four passwords for system access (admin, read, write, http)? See chapter 6.1.2, page 122.
- Are the activities of your **BinGO!** sufficiently accurately logged on at least one external computer and do you check the syslog messages regularly? See chapter 8.1.1, page 228.
- Have you restricted access to the local services and resources to known computers or networks? In particular, you should only allow accesses via CAPI, SNMP, HTTP, Trace and Telnet to known computers.
- Are configuration files saved by TFTP kept in a safe place?
- Have you protected all PPP accesses with a password?
- Have you activated Network Address Translation (NAT) for the connection to the Internet Service Provider (ISP)? See chapter 8.2.7, page 244.
- Have you controlled the IP data traffic at critical interfaces, if necessary with the aid of filters, and prevented IP Address Spoofing? You should pay special attention to the interfaces you have not protected with NAT! See chapter 8.2.8, page 250.
- Have you restricted remote maintenance access via isdnlogin? Have you made an entry under ***CM-1 BRI, ISDN S0 ➧ INCOMING CALL ANSWERING*** See chapter 6.1.4, page 126.

You should also observe the following additional points:

- Do you use the Microsoft callback procedure for PPP connections? See chapter 8.2.4, page 242.
- Do you use an encryption protocol for line tapping security on connections with critical security? See chapter 8.3.1, page 265.
- Do you use personal authentication on connections with critical security?

- Do you allow the influence of routing protocols (e.g. RIP) only on trustworthy networks? See chapter 7.2.6, page 202.
- Do you check what computers have access to the Remote CAPI interface, what applications are used on them and whether the connections used with these applications are desired? Do you use the CAPI user concept?
- Are any additional user accounts created trouble-free?
- Have you prevented the interception of connections on the Ethernet by a suitable LAN infrastructure?

9 Configuration Management

In this chapter, you will find instructions about the administration of your configuration files and about the updating of **BinGO!** software. The following areas are covered:

- Administration of Configuration Files:
  - Where are the configuration files?
  - What is Flash?
  - How do I save configuration files?
- Updating Software:
  - How do I keep in touch with the latest developments?
  - How do I load a new Boot Image?

9.1 Managing Configuration Files

Flash **BinGO!** reads its configuration information from configuration files. These configuration files are stored in Flash EEPROM (electronically eraseable, programmable read-only memory) from **BinGO!**. Several different configuration files can be stored in the Flash memory. The data also remains stored in the Flash when **BinGO!** is turned off.

Memory The current configuration and all changes you set during the operation of **BinGO!** are stored in the working memory (RAM). The contents of the RAM are lost when **BinGO!** is switched off. So if you modify your configuration and want to retain these changes for the next time you start **BinGO!**, you have to save the modified configuration to the Flash: **Exit ➧ save as boot configuration and exit** (see chapter 6.3, page 179). This file is thus saved as a boot configuration file under the name "boot". When **BinGO!** is started again, this very file, the configuration file with the name "boot", is loaded in the RAM and becomes operative.

Imagine the Flash memory as a directory of configuration files. The files in this directory can be copied, moved, erased and newly filed. It is also possible to transfer configuration files between **BinGO!** and a remote host by TFTP.

Windows Under Windows, you can use the TFTP server of **DIME Tools** (see BRICKware for Windows). You would thus be able to save a configuration file from **BinGO!** to your local PC.

The files to be transferred with the TFTP server of DIME Tools may only consist of a maximum of 8 characters (and a maximum of 3 characters as suffix), e. g. bingo.cf.

Unix Under Unix, a TFTP server is part of the system, please bear in mind the instructions included in the Software Reference.

With the help of Setup Tool, you can perform various functions:

➤ Go to the menu ***CONFIGURATION MANAGEMENT***.

```
BinGO! Setup Tool                                   BinTec Communications AG
                                                                    MyBinGO!

    Operation                       get  (TFTP --> FLASH)

    TFTP Server IP Address          192.168.1.1
    TFTP File Name                  brick.cf

    Name in Flash                   boot

    Type of last operation          get (TFTP --> FLASH)
    State of last operation         done

        START OPERATION                          EXIT

Use <Space> to select
```

The menu contains the following fields:

Field	Meaning
Operation	Operation you want to perform
TFTP Server IP Address	The IP address or host name (if the host name can be resolved) of the TFTP server from or to which you want to transfer a configuration file.
TFTP File Name	Name of the configuration file on the TFTP server (without path data).
Name in Flash	Name of the configuration file in the Flash.
New Name in Flash	Name of the configuration file to be newly created in Flash.
Type of last operation	Previous operation (since the last **BinGO!** start).
State of last operation	Status of the last operation.

Table 9-1: ***CONFIGURATION MANAGEMENT***

The field *Operation* contains the following selection:

Possible Values	Meaning
save (MEMORY --> FLASH)	Save all current settings from Memory to Flash as configuration file <Name in Flash>. <Name in Flash> is thus overwritten or recreated.
load (FLASH --> MEMORY)	Loading the configuration file <Name in Flash> from Flash to Memory. The settings in <Name in Flash> take immediate effect.
move (FLASH --> FLASH)	Rename configuration file <Name in Flash> to <New Name in Flash>.
copy (FLASH --> FLASH)	Copy configuration file <Name in Flash> as <New Name in Flash>.
delete (FLASH)	Delete configuration file <Name in Flash>.
put (FLASH --> TFTP)	Transfer configuration file <Name in Flash> from Flash to TFTP host with the IP address <TFTP Server IP Address>. <TFTP File Name> is then overwritten or reproduced on the TFTP host with the contents of <Name in Flash>. <TFTP File Name> is saved in the ASCII format and can be edited.
get (TFTP --> FLASH)	Transfer configuration file <TFTP File Name> from TFTP host with the IP address <TFTP Server IP Address> to Flash. <Name in Flash> is then overwritten and reproduced with the contents of <TFTP File Name>. As the configuration file is transferred to Flash and not to Memory, the file must be then loaded from FLASH to MEMORY, so that the settings can take effect on **BinGO!**.
state (MEMORY --> TFTP)	Save all current settings in Memory as <TFTP File Name> on TFTP host with the IP address <TFTP Server IP Address>. <TFTP File Name> is then overwritten or reproduced.

Possible Values	Meaning
reboot	Restart **BinGO!**. All settings in Memory are replaced by boot settings from Flash.

Table 9-2: *Operation*

The field *State of last operation* can display the following:

Possible Values	Meaning
to do	The operation has not yet been started.
running	The operation is being executed.
done	The operation was successfully executed.
error	The operation could not be fully executed (see syslog message).

Table 9-3: *State of last operation*

If an error should occur while running *get (TFTP --> FLASH)* and the operation is aborted, the file to be overwritten in the Flash is deleted. So if you transfer a "boot" file, **BinGO!**s boot file will be deleted, on restarting, **BinGO!** can not load a configuration. If necessary, rename the file to be transferred!

To run *put (Flash --> TFTP)*, *get (TFTP --> Flash)* and *state (MEMORY --> TFTP)*, you need a TFTP server on the host, to or from which you want to transfer a configuration file.

If the TFTP host is a Windows PC, click **Program ➧ BRICKware ➧ DIME Tools** in the Windows Start menu to open **DIME Tools** and activate the TFTP server with **File ➧ TFTP Server** before you run the operation in question.

If you want to use your Windows PC as a TFTP host, but are not sure what the IP address of the PC is, proceed as follows:

For Windows 95:

➤ In the Windows Start menu, click **Run**.

➤ Type in `winipcfg`.

A window opens where you can see the IP address of your PC and other network information.

For Windows NT:

➤ In the Windows Start menu, point to **Program ➧Command Prompt**.

➤ Type in `ipconfig` or `ipconfig/all` to request the IP address of your PC and other network information.

Running an operation

To run an operation, proceed as follows:

➤ Select *Operation*.

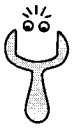
➤ Activate a TFTP server if you have selected *put*, *get* or *state* as the *Operation*.

➤ Select or type in the necessary settings in ***CONFIGURATION MANAGEMENT***.

➤ Select **START OPERATION** and press **Return**.

As long as the operation is being carried out, *OPERATING* appears in the help line of Setup Tool; *State of last operation* displays *running*.

When the operation has been successfuly executed, whichever operation you have chosen is displayed under *Type of last operation*, *State of last operation* assumes the word *done*.



If *error* is displayed next to *State of last operation*, check your settings:

- Have you entered an incorrect IP address next to TFTP Server IP Address?
- Does the name of the configuration file consist of more than 8 characters and the extension of more than 3 (when using DIME Tools)?
- Does the host not support TFTP (did you forget before starting the operation to start the TFTP server of DIME Tools)?
- Is the source file not in the configured directory of the TFTP path of DIME Tools (when *Operation* = *get*)? To change the TFTP path, refer to BRICKware for Windows.
- If none of these points applies, proceed as follows to find the cause of the problem:

➤ Leave Setup Tool.

➤ In the SNMP shell, type in: `debug config &`

➤ Reopen the Setup Tool with `setup`.

➤ Carry out the desired operation ***CONFIGURATION MANAGEMENT***.

In the help line of Setup Tool, an error message with the cause of the error appears on the occurrence of an error.

➤ Solve the problem and carry out the operation again.

➤ Leave ***CONFIGURATION MANAGEMENT*** by **EXIT**.

Example You have created the configuration file brick.cf, e. g. with the help of the Configuration Wizard. You have not transferred the file to **BinGO!** over serial interface; brick.cf can be found in the directory C:\BRICK on your PC. Your PC has the IP address 192.168.1.1. If you want to transfer brick.cf from your PC to **BinGO!**, proceed as follows:

➤ Windows PC: click the Windows Start button then point to **Program** ➧ **BRICKware** ➧ **DIME Tools** to start **DIME Tools**.

The TFTP server must be active

➤ To activate a TFTP server running Unix, see the Software Reference.

➤ Go to ***CONFIGURATION MANGAGEMENT***.

TFTP host --> Flash

➤ Select *Operation*: *get (TFTP --> FLASH)*.

➤ Type in *TFTP Server IP Address*, e. g. *192.168.1.1*.

➤ Type in *TFTP File Name*: *brick.cf*.

➤ Type in *Name in Flash*, e. g. *boot*.

➤ Select **START OPERATION** and press **Return**.

As long as the operation is being carried out, *State of last operation* displays *running*; the help line of Setup Tool displays *OPERATING*.

When the operation has been successfully executed, *get (TFTP --> FLASH)* is displayed next to *Type of last operation*; *State of last operation* assumes the value *done*.

The configuration file brick.cf is saved in **BinGO!**´s Flash under the name boot, for example.

➤ To make the settings of brick.cf take immediate effect on **BinGO!**, proceed as follows:

Flash --> Memory

➤ Reselect *Operation*: *load (FLASH --> MEMORY)*.

➤ Select *Name in Flash*, e. g. *boot*.

➤ Select **START OPERATION** and press **Return**.

As long as the operation is being carried out, *State of last operation* displays *running*; the help line of Setup Tool displays *OPERATING*.

When the operation has been successfully executed, *load (FLASH --> MEMORY)* is displayed under *Type of last operation*; *State of last operation* assumes the value *done*.

The configuration file boot has been loaded to **BinGO!**´s Memory, the settings have been activated.

➤ Leave ***CONFIGURATION MANAGEMENT*** with **EXIT**.

You have returned to the main menu.

There is another way to transfer configuration files with the XMODEM protocol over the serial interface. The procedure for this is explained in the Software Reference.

9.2 Updating Software

As BinTec Communications AG is constantly redeveloping the software for all its products and you certainly want to avail of the latest functions of **BinGO!**, here you will find out how to update your software.

www.bintec.de

If you want to update your software, get a new software image running on **BinGO!** (boot image). Every boot image includes new functions, better performance and several bugfixes from the previous version. You can find the most up-to-date software images made available by BinTec Communications AG free of charge on the World Wide Web at http://www.bintec.de. Here you can also find current product-specific documentation (Release Notes, handbooks, quick installation guides) and general product information (Software Reference, Extended Features Reference, BRICKware for Windows).

If you want to update some software, make sure to consider the corresponding Release Note. Here the changes are described that are made available on the new software image.

Update

There are various ways to update software. This chapter will show how to update with the help of the update command of the SNMP shell and is described step for step. The alternatives to this method can be found in the Software Reference and in chapter 11.5, page 304.

An additional update of the BOOTmonitor and or Firmware Logic is recommended in some few cases. If this should be the case with a new release, it is clearly noted in the corresponding Release Note. The procedure and recommendation can then be found in the Release Notes BOOTmonitor and Firmware Logic Update.

As long as BinTec Communications AG does not expressly recommend updating BOOTmonitor or Firmware Logic, you should not do it!

To Do

To update software (boot image), proceed as follows:

Do not turn **BinGO!** off during the update!

Before starting the update, deactivate autologout by entering `t 0` in the SNMP shell.

- Type in the URL `www.bintec.de` in your browser (e. g. Internet Explorer or Netscape Navigator).
  The BinTec home page opens.
- Click FTP server.
  There you will find the latest software and documentation for BinTec products.
- Click BinGO!.
  There you will also find the latest software and documentation for **BinGO!**.
- With the right mouse button, click the current boot image, e. g. boot image Rel. 5.1 Rev.1.
- In the context menu, click **Save link as...**
- Type in the directory and name under which the boot image should be saved on your PC. Normally, with Windows PCs the directory is C:\BRICK and /tftpboot for Unix work stations. Use a clearly recognizable name, such as bgo511.bg.
- Press **SAVE**.
  The boot image has been saved on your PC.
- Activate a TFTP server on your PC.
  For PCs running Windows: click the Windows Start menu, point to **Program** ➧ **BRICKware** ➧ **DIME Tools**, to start **DIME Tools** (for installation of **DIME Tools**, see chapter 3.3, page 43). Activate the TFTP server.
  For computers running Unix: follow the instructions in the Software Reference.
- Log on to **BinGO!**, in case you have not already done so.
- *Deactivate autologout with* `t 0`.
- In the SNMP shell, type in `update <IP Address> <file name>`.
  The `<IP address>` is the IP address of the TFTP server, e. g. the IP address of your Windows PC under which the TFTP server of DIME Tools is

running and on which you have saved the new boot image (e. g. 192.168.1.1).
<file name> is the name of the boot image as it was saved on your PC (e. g. bgo511.bg).

The file <file name> is firstly transferred to and checked by the working memory of **BinGO!**.

The query will appear in the SNMP shell: Perform update (y or n)?

➤ Enter `y` and press **Return**.

The software update process begins; the new boot image is loaded to the Flash memory.

BinGO! requires a connected block of working memory that is somewhat larger than the software image. If insufficient working memory is available on **BinGO!**, **BinGO!** offers an incremental update, although the image is loaded directly and without checking in "chunks" to the Flash memory. Proceed as follows:

If insufficient working memory is available, a query will appear in the SNMP shell:
Do you want to perform an incremental update (y or n)?

➤ First, enter `n`.

➤ Type in `update -v <IP address> <file name>`.

The image is checked, but not yet loaded.

➤ Type in `update <IP address> <file name>`.
In the SNMP shell appears the query: Perform update (y or n)?

➤ Affirm then press **Return**.

BinGO! performs an incremental update, the image is saved to the Flash memory. This procedure takes longer than a normal update!

An enquiry will appear in the SNMP shell: Reboot now (y or n)?

➤ Affirm then press **Return**.

BinGO! starts with the new boot image. The previous configuration is overwritten.

10 Troubleshooting

Tips If you are having problems with **BinGO!**, the following tips should help you to overcome some of the more usual stumbling blocks:

- Log in to **BinGO!** and type in to the SNMP shell:
  `debug all`
  This makes available all debugging information in the SNMP shell.
- Check the syslog messages created by **BinGO!** (see chapter 8.1.1, page 228). It is wise to forward and save syslog messages to an external host to be able to evaluate the output of a longer period of time.

To interpret debugging information and syslog messages, see the Software Reference.

This chapter shows you what the causes of particular problems can be and how to determine those causes. It is structured as follows:

- Aids to Troubleshooting
- Typical Errors

10.1 Aids to Troubleshooting

Here you can find methods to help narrow down the possible causes of your problem:

- Local SNMP shell commands
- External aids

10.1.1 Local SNMP shell commands

These commands are to be directly typed in to **BinGO!**'s SNMP shell:

debug

The `debug` command can be used to operate an error search for one or more **BinGO!** subsystems. An exact explanation of the syntax and options can be found in chapter 12.1, page 308.

Examples:

➤ Type in `debug all` to display debugging information for all subsystems.

➤ Type in `debug config &` to track down problems with configuration management (see chapter 9, page 271).

If you attach an `&` to an SNMP shell command, the command will be executed in the background.

isdnlogin

To verify that an `ISDN` connection can be made, you can use `isdnlogin`. This is explained in chapter 12.1, page 308.

Example:

➤ Type in `isdnlogin 1234 telephony` to establish a connection with the telephone in your local office with the number 1234.

If a connection is made, the telephone will ring.

trace

The `trace` command can be used to display and interpret sent or received data packets over ISDN (D and B-channels) and over the LAN. An explanation of the syntax can be found in chapter 12.1, page 308.

Examples:

- Type in `trace -ip next` to display ISDN messages that are to run over the next B-channel to be opened.
- Type in `trace -x -s me -d 0:a0:f9:d:5:a 0 0 1` to give out data packets sent from **BinGO!**'s MAC address to the host with the MAC address 0:a0:f9:d:5:a.

10.1.2 External aids

Running Windows or Unix, you can analyse connections with **BinGO!** using the following utility programs.

DIME Tracer (Windows)

From a Windows PC, the DIME Tracer allows you to trace ISDN and CAPI data traffic. DIME Tracer is a part of DIME Tools. A detailed explanation can be found in BRICKware for Windows.

bricktrace (Unix)

From a Unix work station, the bricktrace program can be used to inspect data being sent over **BinGO!**´s ISDN channels. Bricktrace is part of BRICKtools for UNIX on your BinTec Companion CD. A detailed explanation can be found in chapter 12.2, page 314.

10.2 Typical Errors

The following is a compilation of typical error situations, including instructions for error detection and solution. Try to narrow down the causes of the problem. These situations are broken down into the following categories:

- System errors
- IPX routing
- ISDN connections

10.2.1 System Errors

I have forgotten my password.

You must return **BinGO!** to the original configuration state in which it was shipped:

➤ Connect your router over the serial interface with **BinGO!** as explained in chapter 5.1.3, page 101.

➤ Switch **BinGO!** off, wait a moment, then switch it on again.

You see diverse self tests and then "Press <sp> for BOOTmonitor or any other key to boot system".

➤ Now press the **SPACE BAR**.

The BOOTmonitor menu is displayed.

➤ Select (4) Delete Configuration and respond to the following security checks.

The password as well as the complete configuration of **BinGO!** are deleted.

➤ Select (1) Boot System.

➤ Reconfigure **BinGO!**.

I can´t reach BinGO! in the network.

Try to establish a serial connection:

➤ Connect your PC with **BinGO!** over the serial interface.

- Log in as the user `admin` with the corresponding password.
- Start the Setup Tool with `setup`.
- Check if a configuration error is the cause: Have you entered the IP address under ***CM-BNC/TP, ETHERNET***? Have you entered a filter under ***IP*** ➧ ***ACCESS LISTS*** that is locking you out? If so, make the required corrections.

If a serial connection does not work:

- Check the settings of the terminal program (see chapter 5.1.1, page 99). If you have changed the standard settings in BOOTmonitor, adjust your terminal settings accordingly.
- If you have no success, proceed as explained under "I have forgotten my password".

10.2.2 ISDN Connections

Here you will find possible causes of errors for failed or faulty ISDN connections.

The telephone bill is unusually high.

Use the credits based accounting system (see chapter 7.1.3, page 188). You can thus set a limit for connections with **BinGO!** to prevent unnecessary charges from accumulating as a result of mistakes made during configuration.

In case of **BinGO!** ISDN connections that remain open or unwanted ISDN connections being established:

- Using `debug all` or `trace`, check if a PC in the LAN is using a different netmask from the one entered on **BinGO!**.
- Using `debug all` or `trace`, check if a PC in the LAN is configured for Remote CAPI with an incorrect IP address (destination port 2662).
- Check in ***SYSTEM*** ➧ ***EXTERNAL SYSTEM LOGGING*** if **BinGO!** is configured to send syslog messages to a host outside the LAN (destination port 514).

- Check in the MIB table **biboAdmTrapHostTable** if **BinGO!** is configured to send SNMP traps to a host outside the LAN (destination ports 161, 162).
- Check if, due to different loads of traffic, frequent opening and closing of a B-channel is occurring for connections with dynamic channel bundling.
- Using `debug all` or `trace`, check if a PC in the LAN is configured with an incorrect IP address for the WINS server (destination ports 137-139). If necessary, configure the PC properly or enter the corresponding filters.
- Using `debug all` or `trace`, check if a PC in the LAN is configured for the resolution of NetBIOS names with the help of DNS (it is accessed from a client port to destination port). Do not try to resolve NetBIOS names with DNS!
- Using `debug all` or `trace`, check if an application on a PC in the LAN is trying to resolve names that the name server at the Internet provider does not know (it is accessed from a client port to destination port 53). Install a local HOSTS file in the Windows directory that can facilitate name resolution (see chapter 4.5, page 87).
- Using `debug all` or `trace`, check if NetBIOS over IP is configured on a PC in the LAN (it is accessed from source port 137 to destination port 53). The attempt is thus made to resolve NetBIOS names over DNS. Disable NetBIOS over IP or insert filters (configuration of the corresponding filters can be found in chapter 6.1.6, page 138 or use the simple NetBIOS filter of the Configuration Wizard, see chapter 3.4.1, page 48).
- Check if you have configured Callback (see chapter 8.2.4, page 242) and in doing so entered an incorrect dial number (*Number* under ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***WAN NUMBERS*** ➧ ***EDIT***).
- Check if you left running a trace program over an ISDN-PPP connection. That would cause the constant sending of packets over ISDN, the connection would remain permanently open.

Outgoing calls can not be made.

- By looking at the LEDs on the front side of **BinGO!**, check (see chapter 11.2, page 297) if a connection is made.
- Using `isdnlogin`, check if outgoing calls are possible.

- Check in ***MONITORING AND DEBUGGING*** ➧ ***ISDN MONITOR*** if any outgoing calls have been recorded, if the number dialed is correct and if the call was connected.
- Check if ISDN syslog messages with "disconnect cause" were recorded.
- Check if *Encapsulation* in ***WAN PARTNER*** ➧ ***EDIT*** is identical for the connection partners.
- Check if *Authentication* in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***PPP*** is identical for the connection partners.
- Using `trace`, check what is being sent over the ISDN channels.
- Check in the MIB table **isdnStkTable** if the MIB variable **Status** has the value *loaded.*
- In ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING,*** check if your own dial number is entered correctly. It is also valid for outgoing calls.

Incoming calls can not be made.

- By looking at the LEDs on the front side of **BinGO!** (see chapter 11.2, page 297), check if an incoming call is being received.
- In ***MONITORING AND DEBUGGING*** ➧ ***ISDN MONITOR***, check if an incoming call has been recorded.
- In ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***WAN NUMBERS***, check if a suitable number for incoming calls has been entered.
- Check in the MIB tables **isdnCallHistoryTable** the MIB variables **DSS1Cause**, **1TR6Cause** and **LocalCause**. To interpret the entries, see the Software Reference.
- In ***CM-1BRI, ISDN S0*** ➧ ***INCOMING CALL ANSWERING,*** check if the necessary entries have been made for incoming calls.
- Check if *Encapsulation* in ***WAN PARTNER*** ➧ ***EDIT*** is identical for the connection partners.
- Check if *Authentication* in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***PPP*** is identical for the connection partners.

10.2.3 IPX routing

Here you will find some problems that could crop up with IPX routing, and suggestions of how they can be solved.

Using the Setup Tool, check:

- have you made the correct entries under ***LICENSES***?
- in ***IPX,*** is the entry under *Internal Network Number* unique in the LAN?

A server exists in a Remote LAN (LAN-LAN connection over ISDN), but is "invisible" for clients in the local LAN.

The server could be invisible for the clients because SAP packets are not received by **BinGO!**:

- Check the entries of *Update Time* and *Age Multiplier* in ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IPX***. The settings must be compatible with the settings on the servers in the **BinGO!** LAN.
- Check if an intermediate router is filtering out the SAP packets.
- Using isdnlogin, check if an ISDN connection between client and server can be made.
- Check if you have entered correctly *local IPX-NetNumber* and *Encapsulation* under ***CM-BNC/TP, ETHERNET*** and if the server can receive them.

When the client tries to reach a server in a remote network via a PPP connection, he must wait a long time and the connection could be terminated.

In some cases, the local router erroneously tells the client that a server can be reached.

- Check if the server has crashed and the aging interval has not expired. If necessary, change the setting of *Send RIP/SAP Updates* under ***WAN PARTNER*** ➧ ***EDIT*** ➧ ***IPX***.
- Check if the server and the router in the remote network are simultaneously inactive (e. g. because of a power cut). Briefly set the WAN interface of the corresponding WAN partner with the command `ifconfig` to *down* and

then back to *dialup,* in order to delete the routes and services learned from the WAN partner.

I can´t change to a network drive on the client station.

- The file server may be "invisible" to the client, see "A server exists in a remote LAN".
- Check if there are any user licenses available on the server.

ISDN connections constantly reconnecting.

In general, RIP/SAP packets do not cause ISDN connections.

- Check if there is an entry in the MIB table **ipxDenyTable** that is preventing Novell serialization packets from being sent over the dialup interface.
- Check in the main menu of Setup Tool if SPX spoofing is enabled and if IPX spoofing is enabled.
- Check if somebody is using NetBIOS over IPX (Windows for Workgroups, NT, Win95/98). You may need to set NetBIOS Broadcast replication to *"no"* or *"on LAN_only"*.
- Check if RCONSOLE is running somewhere with a constantly changing screen (e. g. MONITOR, IPXCON, TCPCON, a screensaver, etc.).
- Check if NDS Replica Synchronization is active (for Netware 4.1 servers and higher).
- Check the list in **Monitoring and Debugging ➧ Messages**. The IPX messages included in this list will tell you why (by packet type and socket) a connection is being established. It may be possible to filter these packets.

The MIB variable ipxAdmSpxConns shows more connections than are actually present.

BinGO! 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 **BinGO!** 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 **ipxAdmSpx-**

Conns. Once the connection does close, SPX sends a message to the server informing it that the connection is closed

11 Technical Data

In this chapter, you can find **BinGO!**'s technical data, the following points will be covered:

- General Product Features
- **BinGO!** – Front Side and LED Displays
- **BinGO!** – Rear Side and Connections
- Pin Assignments
- BOOTmonitor

11.1 General Product Features

The general product features cover **BinGO!**'s performance features and the technical prerequisites for installation and operation.

Description	Value
Product name:	**BinGO!**
Dimensions and weight (B x H x D): Dimensions of device without cable Placement size and maintenance surface Weight Transport weight (incl. documentation, cabling, packaging)	 141 mm x 50 mm x 145 mm 150 mm x 60 mm x 210 mm 420 g 2 kg
Memory:	4 MB / 32 bit DRAM, 1 MB / 8 bit flash-ROM
LEDs:	6 (1 power, 4 function, 1 error)
Power consumption:	2 W (typical)
Voltage supply:	AC/DC adaptor Input: 230V~50Hz / 70mA Output: 5V-800mA 4VA
Ambient requirements: Storage temperature Operating temperature Relative humidity Room classification	 -20° - + 85°C 50°C 20 - 90% non-condensing in operation 5 - 95% non-condensing in storage operate only in dry rooms
MTBF value	100 000 hours

Description	Value
Available interfaces: Serial interface V.24 Ethernet IEEE802.3 LAN ISDN-WAN S_0	 built-in, supports the Baud rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud built-in (only twisted-pair), node/hub-switch built-in
Plug used: Serial interface Ethernet interface ISDN interface	 Sub9 male (PC) RJ-45 RJ-45
Applications interface:	Dual Remote CAPI (v1.1 and 2.0), R-CAPI driver for Windows 3.11/95/NT and Novell Netware. Source Code Library for other systems (e. g. Unix, AS400).
Data compression:	PPP LZS STAC compression rate up to 4:1
SAFERNET™ security technology:	Community passwords, PAP, CHAP, MS-CHAP, Callback, Access Control Lists, Allow Lists, CLID, RADIUS, NAT, TAF, MPPE Encryption
Required licenses:	Licenses included for CAPI, IP, IPX, STAC. Additional licenses for VPN, unlimited number of LAN or WAN users possible.
Software included:	RVS-COM Lite (communication program) BRICKware for Windows BRICKtools for Unix
Included printed documentation:	User's Guide (Eng.) Quick Install Guide (Eng. and Ger.)

Description	Value
Online documentation:	BRICKware for Windows (Eng.) Software Reference (Eng.) Extended Features Reference (Eng.) User´s guide (Ger.)

11.2 Front Side - LEDs

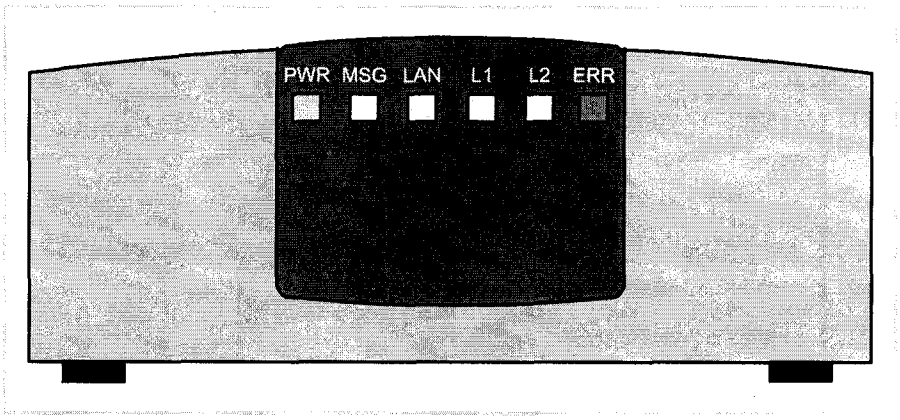


Figure 11-1: **BinGO!** front side

There are 6 LED displays on the front side that indicate the current status of your device. Each LED can convey different information, according to which mode is in operation. When **BinGO!** is starting up, it changes between different function states:

- Start mode
- BOOTmonitor mode (see chapter 11.5, page 304)
- Normal operation mode

The significance of the LEDs in their different states is described in the following tables.

Start mode

LED	State	Meaning
PWR	On	Power supply connected.
MSG	Blinking	DRAM test being carried out.
LAN	Off	Not being used.
L1	Blinking	Flash ROM test being carried out.
L2	Blinking	CHIP test being carried out.
ERR	Off	Not being used.

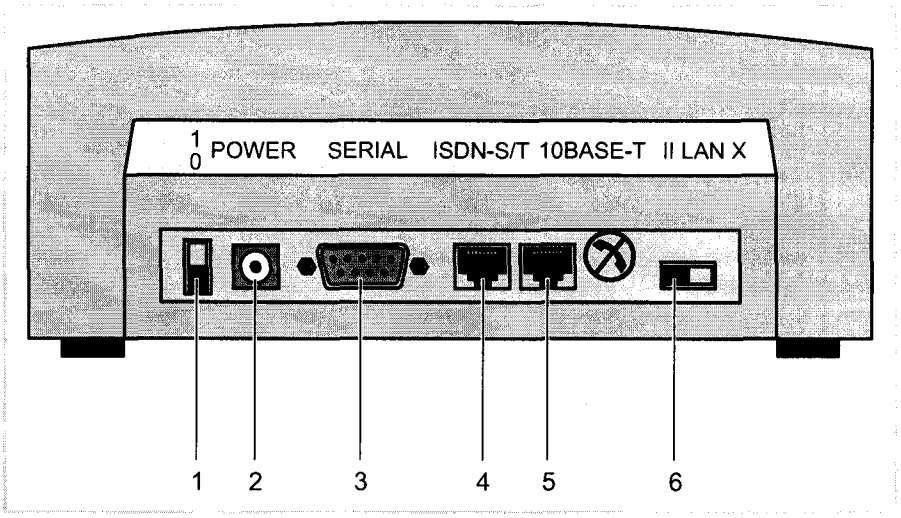
BOOTmonitor mode

LED	State	Meaning
PWR	On	Power supply connected.
MSG	Off	Not being used.
LAN	Blinking	TFTP transfer being carried out.
L1, L2, ERR	On	BOOTmonitor is active (or waiting for a keyboard entry).
L1, L2, ERR	Blinking	BOOTmonitor decompressed boot image.

Normal operation mode

LED	State	Meaning
PWR	On	Power supply connected.
MSG	–	Reserved for future use.
LAN	On	Data packet passing the LAN interface.
L1, L2	On	Data traffic over ISDN B-channel 1 or 2.
ERR	On (occasionally)	Collision in LAN detected (every lighting display indicates a collision)
ERR	On (constant)	The LAN connection was not made (no 10Base-T cable connected) or the LAN switch is in the wrong position.

11.3 Rear Side - Connections



1	On/off switch	4	S_0-interface (ISDN)
2	Power supply connection	5	10Base-T interface (LAN)
3	Serial port	6	LAN switch

Figure 11-2: **BinGO!** rear side

BinGO!'s main board contains a LAN and an ISDN interface. These interfaces are reached via the connections on the rear side. (chapter 11.4, page 300).

Caution!

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

- Only use the mains unit included (5 VDC).
- Make sure that the rated voltage marked on the mains unit conforms with the local voltage supply.
- Never exchange the mains adaptors from **BinGO!** and **BinGO! Plus/Professional**.

11.4 Pin Assignment

Serial port:

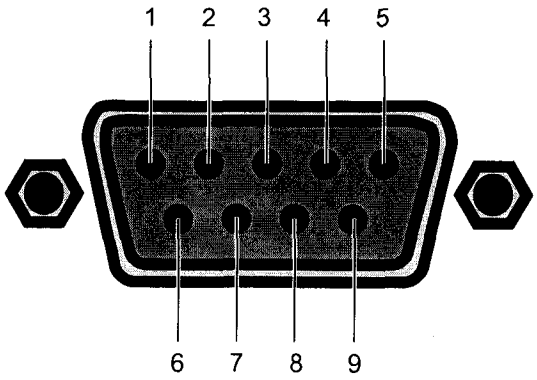


Figure 11-3: 9-pin serial port

As console port, **BinGO!** has a serial port with a 9-pin sub-D port. Baud rates supported between 1200 and 115200. The pin assignment was modified to be compatible for a greater selection of terminals.

The pin assignments for the 9-pin sub-D port (3) are as follows:

Pin	Function
1	DCD (not connected)
2	Receive
3	Send
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

ISDN S_0 Port

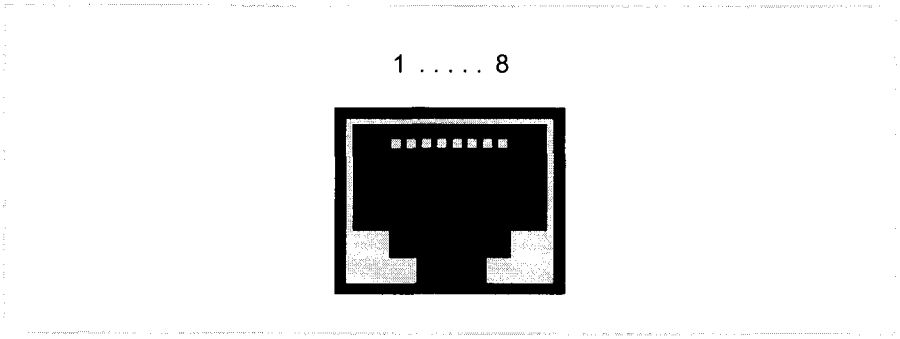


Figure 11-4: ISDN S_0 BRI port (RJ-45 port)

The pin assignments for the ISDN S_0 BRI interface (RJ-45 port) (4) are as follows:

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

LAN interface

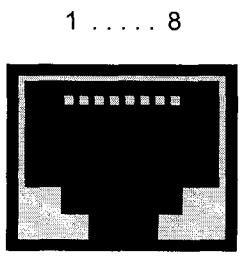


Figure 11-5: Ethernet 10Base-T interface (RJ-45 port)

The pin assignments for the Ethernet 10Base-T interface (RJ-45 port) are as follows:

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

If you want to connect **BinGO!**'s LAN interface directly to the Ethernet card of your PC and not to an external hub, you must flick the LAN switch to ⋈ on the rear side of the device. This setting allows you to use the 1 to 1 wired LAN cable and saves you having to buy a crossover cable.

11.5 BOOT Sequence

On starting **BinGO!**, various states are passed through (see also chapter 11.2, page 297):

- Start Mode
- BOOTmonitor Mode
- Normal Operation Mode

After several self-tests have been successfully performed, **BinGO!** arrives at the BOOTmonitor mode. The BOOTmonitor prompt is displayed if you are connected over a terminal program with **BinGO!**.

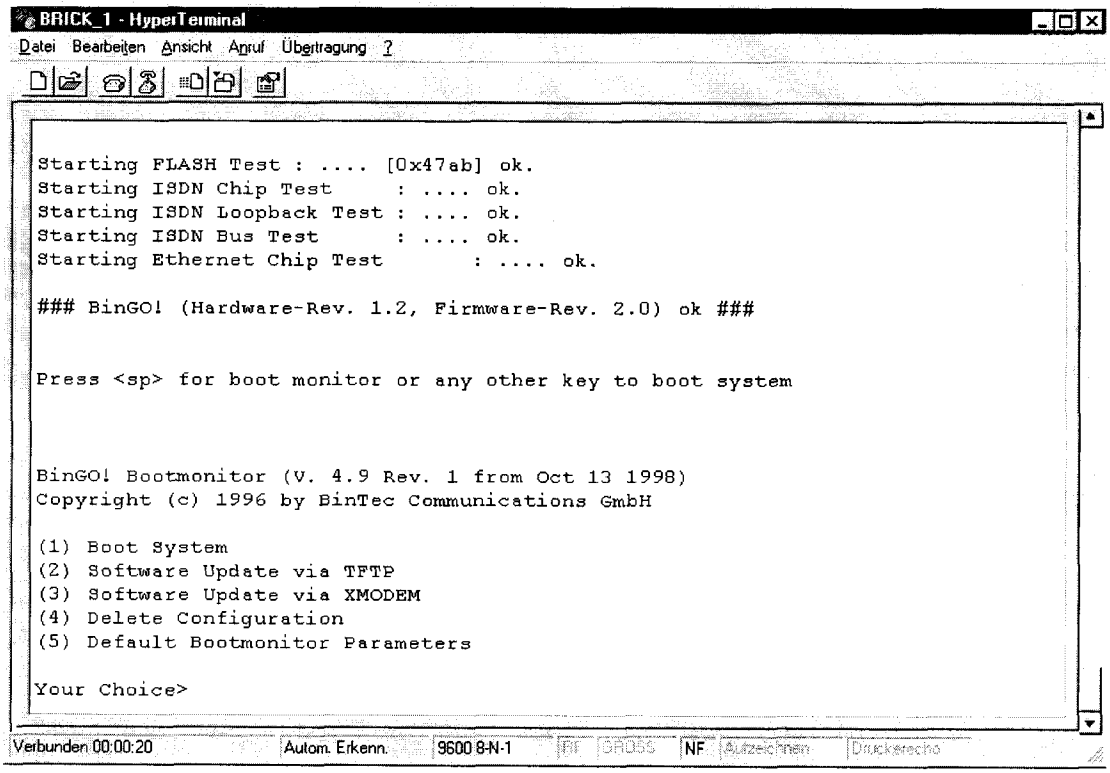


Figure 11-6: BOOTmonitor

BOOTmonitor Within 4 seconds of the display of the BOOTmonitor prompt, press the **SPACE BAR** (figure 11-6, page 304) to use the functions of the BOOTmonitor. If you do not make an entry within the 4 seconds, **BinGO!** changes back to normal operation mode.

Functions The BOOTmonitor makes available the following functions you select by entering the relevant digit (for more detailed information, refer to the Software Reference):

- (1) Boot System:
  BinGO! loads the compressed boot file from the Flash memory to the working memory. This happens automatically when started.
- (2) Software Update via TFTP:
  BinGO! performs a software update via a TFTP server.
- (3) Software Update via XMODEM:
  BinGO! performs a software update over a serial interface with XMODEM.
- (4) Delete Configuration:
  BinGO! is returned to the state in which it is shipped. All configuration files are deleted, the BOOTmonitor settings are set to the standard values.
- (5) Default BOOTmonitor Parameters:
  You can change the standard settings of **BinGO!**s BOOTmonitor, e. g. the Baud rate for serial connections.

If you change the Baud rate (the pre-setting is 9600 Baud), make sure the terminal program used uses this Baud rate. If this is not the case, you will not be able to establish a serial connection with **BinGO!**

12 Important Commands

This chapter describes the following commands:

- SNMP shell commands
  - telnet
  - ping
  - trace
  - isdnlogin
  - debug
  - ifconfig
  - ifstat
  - netstat
  - date
  - t
- BRICKtools for Unix commands
  - bricktrace
  - capitrace

12.1 SNMP Shell Commands

BinGO! contains several pre-installed programs that can be used directly from the SNMP shell of the client. This chapter includes a short description of these programs, their usage and the necessary command lines to start the respective programs in the SNMP shell.

Please be aware that parameters of the command lines contained within corner brackets [ ] represent optional values. Terms within angle brackets < > can take several values.
Do not enter the brackets!

telnet

```
telnet [-f] <host> [<port>]
```

Is used to communicate with another host.

- `-f`: specifies that the telnet connection should be transparent. This option is especially useful for establishing connections to non-telnet ports (e. g. uucp or smtp).
- `host`: IP address or name of host.
- `port`: port number.

ping

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

Is used to test the communication with another host.

- `-c <count>`: limits the number of packets to be sent, `count` sets the number of packets.
- `host`: IP address or name of host to which the echo_request packet is sent.
- `size`: sets the length of the packets to use.

If you do not specify `-c <count>`, ping will continue to send packets until you stop it, e. g. by pressing `Ctrl-C`.

trace

For WAN interfaces:

```
trace [-h23aFAtpiNxX] [next] [-T <tei>] [-c <cref>]
<channel> <unit> <slot>
```

For LAN interfaces:

```
trace [-h23iNxXl] [-d <destination MAC filter>] [-o]
[-s <source MAC filter>]0 0 <slot>
```

Is used to trace and interpret ISDN messages (D and B-channels) or LAN packets sent or received via **BinGO!**'s interfaces.

- `-h`: hexadecimal output
- `-2`: layer 2 output
- `-3`: layer 3 output
- `-a`: asynchronous HDLC (B-channel only)
- `-F`: FAX (B-channel only)
- `-A`: FAX and AT commands (B-channel only)
- `-t`: output in ASCII-text (B-channel only)
- `-p`: PPP (B-channel only)
- `-i`: IP output (B-channel only)
- `-N`: Novell IPX output (B-channel only)
- `-x`: raw dump mode
- `-X`: asynchronous PPP over X.75 (B-channel)
- `next`: only display information for the next B-channel that is opened (B-channel only).
- `-T <tei>`: set TEI filter (D-channel only)
- `-c <cref>`: set callref filter (D-channel only)
- `channel`: 0 = D-channel or X.21 interface, 1 ... 31 = Bx-channel
- `unit`: 0 ... 1. Selection of the physical interface for modules with two interfaces (e. g. CM-2BRI).
- `slot`: 1 ... 2. Entry of slot in which the module is installed.
- `-d <destination MAC filter>`: set destination MAC address filter (LAN only).
- `-s <source MAC filter>`: set source MAC address filter (LAN only).
- `-o`: combines two or more -d- or -s filters with a logical OR operation.

- `MAC filter`: `me` = **BinGO!**'s MAC address, `bc` = broadcast packets

You can combine a -d MAC filter and an -s MAC filter with a logical AND operation by simply specifying them both.

To combine two or more -d and -s MAC filters with a logical OR operation, specify the first filter, followed by -o, then specify the next filter, and so on.

isdnlogin

```
isdnlogin [-c <stknumber>] [-C] [-s <service>]
[-a <addinfo>] [-b <bits>] isdn-number [isdn-service]|
layer1-protocol]
```

Is used to open a remote login shell on **BinGO!** over ISDN.

- `-c <stknumber>`: selects the ISDN stack to use for this login.
- `-C`: tries 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. `use -b 7` for 7bit ASCII transmissions).
- `isdn-number`: isdn-number of the ISDN partner you want to login to.
- `isdn-service`: the ISDN service you want to use (data, telephony, faxg3, faxg4, btx).
- `layer1-protocol`: possible values: v110_1200, v110_2400, v110_4800, v110_9600, v110_19200, v110_38400, modem, dovb56k, telephony.

debug

```
debug [show]|[[-t] all|acct|system|<subs> [<subs> ...]]
```

Is used to selectively display debugging information originating from one or more of **BinGO!**'s subsystems.

- `show`: displays all possible subsystems that can be debugged.
- `-t`: prints a timestamp before each debugging message.
- `all`: displays debugging information for all subsystems.
- `acct`: displays debugging information for the accounting subsystem.

- `system`: debugging information for all subsystems except for the accounting system.
- `subs`: one or more subsystems separated by whitespace can be entered to display only debugging information from these subsystems.

ifconfig

```
ifconfig <interface> [destination <destaddrs>] [<address>]
[netmask <mask>] [up | down | dialup] [-] [metric <n>]
```

Is 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.

- `interface`: name of the interface (**ifDescr**)
- `destination <destaddrs>`: destination IP address of a host. This adds a host route to the routing table (**ipRouteDest**).
- `address`: **BinGO!**s IP address for the interface (**ipRouteNextHop**).
- `netmask <mask>`: netmask of the interface (**ipRouteMask**).
- `up`: sets the interface to the state: up.
- `down`: sets the interface to the state: down.
- `dialup`: sets the interface to the state: dialup.
- `-`: does not define its own IP address (**ipRouteNextHop** = *0.0.0.0*).
- `metric <n>`: sets route metric to n (**ipRouteMetric1**).

ifstat

```
ifstat [-lur] [<ifcname>]
```

Is used to display status information for the system´s interfaces, based on the contents of the **ifTable**.

- `-l`: displays the full length of the interface descriptions (normally the description is only displayed up to the twelfth character).
- `-u`: only displays information on interfaces which are in the **up** status.
- `-r`: displays the access rules that apply to the specified interface.

- `ifcname`: only displays information on interfaces whose description starts with the given characters (e. g. `ifstat en1` will display information on the interfaces en1, en1-llc and en1-snap an).

netstat

```
netstat [[-i | -r | -p [<interface>]] | -d <dest. IP addr.>]
```

Is used to display a quick list of interfaces, routing table entries or ISDN partners.

- `-i`: displays a list of the interfaces.
- `-r`: displays a list of routing table entries.
- `-p`: displays a list of WAN partners.
- `interface`: details about displayed information can be limited to a selected interface.
- `-d <dest. IP addr.>`: displays routes to a destination IP address.

date

```
date [YYMMDDHHMMSS]
```

BinGO! has a software clock. By entering `date`, the set time is displayed.

Using `date` followed by a date string `YYMMDDHHMMSS`, set the clock to the corresponding value (year, month, day, hour, minute, second).

t

```
t [<seconds>]
```

Is used to define the number of seconds to wait before closing the current login session once there is no more terminal input (autologout timer). The timeout is set to 900 seconds or 15 minutes by default. By entering `t 0`, you deactivate autologout.

By entering `-?` , you will generally receive help with the syntax.

The `update` command can be found in chapter 9.2, page 279.

Further SNMP commands can be found in the Software Reference.

12.2 BRICKtools for Unix Commands

The bricktrace and capitrace programs are included in BRICKtools for UNIX on the BinTec companion CD. They are started on a Unix workstation by entering the following commands.

bricktrace

```
bricktrace [-h23aeFpiNtxs] [-T <tei>] [-c <cref>]
[-r <cnt>] [-H <host>] [-P <port>] <channel> <unit> <slot>
```

Is used to trace and interpret ISDN messages (D and B-channels).

- `-h`: hexadecimal output
- `-2`: layer 2 output
- `-3`: layer 3 output
- `-a`: asynchronous HDLC (only B-channel)
- `-e`: ETS300075 (EuroFileTransfer) output
- `-F`: Fax (only B-channel)
- `-p`: PPP (only B-channel)
- `-i`: IP output (only B-channel)
- `-N`: Novell IPX output (only B-channel)
- `-t`: output in ASCII text (only B-channel)
- `-x`: Raw dump mode
- `-s`: scan **BinGO!** for available trace channels
- `-T` <tei>: set TEI filter (only D-channel)
- `-c` <cref>: set Callref filter (only D-channel)
- `-r` <cnt>: receive only cnt bytes
- `-H` <host>: IP address or name of the IP hosts
- `-p` <port>: specify trace TCP port (default: 7000)
- `channel`: `0` = D-channel or X.21 interface, `1` ... `31` Bx-channel
- `unit`: 0 ... 1. selection of the physical interface for modules with two interfaces (e. g. CM-2BRI).
- `slot`: 1 ... 2. entry of the slot in which the module is installed.

capitrace

```
capitrace [-h] [-s] [-l]
```

Is used to trace and interpret CAPI messages. All CAPI messages sent or received by **BinGO!** are displayed. The IP address of **BinGO!** must be entered as the environment variable CAPI_HOST.

- -h: hexadecimal output (is set by default if no options are specified).
- -s: short output. At the end of the information line, only the application ID and a connection identifier in the form (application / identifier) and the name of the CAPI message are displayed.
- -l: long output (default). A detailed interpretation of each parameter included in the CAPI message is given.

Each CAPI message is preceded by a line containing the following information:

- Timestamp ("seconds.milliseconds" local time)
- Sent/Received flag (X = sent, R = received)
- Name of the CAPI message (ASCII string)
- Command of the CAPI message (0xABXY, AB = <subcommand> XY = <command>)
- Number of the tracer message (#<decimal>)
- Length of the CAPI message (len = <decimal>)
- Application ID (appl = <decimal>)
- Number of the CAPI message (messno = 0x<hexadecimal>)
- Short output only: connection identifier (ident = 0x<hexadecimal>)

13 General Safety Precautions in 15 Different Languages

Allgemeine Sicherheitshinweise in deutsch

In den nachfolgenden Abschnitten finden Sie Sicherheitshinweise, die Sie beim Umgang mit Ihrem Router unbedingt beachten müssen.

Transport und Lagerung

- Transportieren und lagern Sie **BinGO!** nur in der Originalverpackung oder in einer anderen geeigneten Verpackung, die Schutz gegen Stoß und Schlag gewährt.

Aufstellen und in Betrieb nehmen

- Beachten Sie vor dem Aufstellen und Betrieb von **BinGO!** die Hinweise für die Umgebungsbedingungen (vgl. Technische Daten). Verwenden Sie eine feste und ebene Unterlage.
- Wenn das Gerät aus kalter Umgebung in den Betriebsraum gebracht wird, kann Betauung sowohl am Geräteäußeren als auch im Geräteinneren auftreten. Warten Sie, bis Ihr Router temperaturangeglichen und absolut trokken ist, bevor Sie ihn in Betrieb nehmen.
- Überprüfen Sie, ob die auf dem Typenschild des Netzteils angegebene Nennspannung mit der örtlichen Netzspannung übereinstimmt. **BinGO!** darf nur mit dem original BinTec Communications-Steckernetzteil (5 V DC) betrieben werden. BinTec Communications AG haftet nicht für Schäden, die durch die Verwendung eines anderen Steckernetzteils hervorgerufen werden.
- Beachten Sie beim Verkabeln die Reihenfolge, wie im Handbuch beschrieben. Verkabeln Sie zuerst LAN-, ISDN- und serielle Anschlüsse, schließen Sie dann die Stromversorgung an, und schalten Sie zum Schluß **BinGO!** ein.
- Überprüfen Sie, ob Sie die Verkabelung – insbesondere die ISDN- und LAN-Verkabelung – richtig durchgeführt haben, bevor Sie **BinGO!** in Betrieb nehmen. Der ISDN-Anschluß von **BinGO!** darf nicht mit dem Ethernet-Anschluß Ihres Rechners oder Hubs verbunden werden, der LAN-Anschluß von **BinGO!** nicht mit Ihrem ISDN-Anschluß.

- Verwenden Sie für die Verkabelung nur die beigelegten Kabel. Falls Sie andere Kabel verwenden, übernimmt BinTec Communications AG für auftretende Schäden keine Haftung.
- Verlegen Sie Leitungen so, daß sie keine Gefahrenquelle (Stolpergefahr) bilden und nicht beschädigt werden.
- Schließen Sie Datenübertragungsleitungen während eines Gewitters weder an noch ziehen Sie sie ab.

Bestimmungsgemäße Verwendung, Betrieb

- **BinGO!** ist für den Einsatz in einer Büroumgebung bestimmt. Als ISDN-Multi-Protokoll-Router baut **BinGO!** in Abhängigkeit von der Systemkonfiguration ISDN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen.
- **BinGO!** entspricht den einschlägigen Sicherheitsbestimmungen für Einrichtungen der Informationstechnik für den Einsatz in einer Büroumgebung.
- Der bestimmungsgemäße Betrieb gemäß IEC 950/EN 60950 des Systems ist nur bei montiertem Gehäusedeckel gewährleistet (Kühlung, Brandschutz, Funkentstörung)
- Die Umgebungstemperatur sollte 50°C nicht übersteigen. Vermeiden Sie direkte Sonneneinstrahlung.
- Achten Sie darauf, daß keine Gegenstände (z. B. Büroklammern) oder Flüssigkeiten ins Innere des Geräts gelangen (elektrischer Schlag, Kurzschluß). Achten Sie auf ausreichende Kühlung.
- Unterbrechen Sie in Notfällen (z. B. geschädigtes Gehäuse oder Bedienelement, Eindringen von Flüssigkeit oder Fremdkörpern) sofort die Stromversorgung und verständigen Sie den Service.

Reinigung und Reparatur

- Das Gerät darf nur durch geschultes Fachpersonal geöffnet werden. Lassen Sie daher Reparaturen am Gerät nur von einer BinTec-autorisierten Servicestelle durchführen. Wo sich die Servicestelle befindet, erfahren Sie von Ihrem Händler. Durch unbefugtes Öffnen und unsachgemäße Reparaturen können erhebliche Gefahren für den Benutzer entstehen (z. B. Stromschlag). Unerlaubtes Öffnen der Geräte hat den Garantie- und Haftungsausschluß der BinTec Communications AG zur Folge.

- Das Gerät darf auf keinen Fall naß gereinigt werden. Durch eindringendes Wasser können erhebliche Gefahren für den Benutzer (z. B. Stromschlag) und erhebliche Schäden am Gerät entstehen.
- Niemals Scheuermittel, alkalische Reinigungsmittel, scharfe oder scheuernde Hilfsmittel benutzen.

Almindelige sikkerhedsforskrifter på dansk

Efterfølgende afsnit indeholder sikkerhedsforskrifter, som skal overholdes, når Deres router benyttes.

Transport og opbevaring

- Transportér og opbevar kun **BinGO!** i originalemballage eller i anden egnet emballage, der beskytter mod stød og slag.

Opstilling og ibrugtagning

- Læs og overhold forskrifterne for de omkringliggende betingelser, før **BinGO!** opstilles og tages i brug (se Tekniske data). Benyt et fast og jævnt underlag.
- Hvis apparatet er koldt, når det bringes ind i brugsrummet, kan der opstå dug i og uden på apparatet. Sørg for at Deres router har rumtemperatur og er absolut tør, før den tages i brug.
- Kontrollér om spændingen på typeskiltet stemmer overens med spændingen på brugsstedet. **BinGO!** må kun arbejde med den originale stiknetdel fra BinTec Communications (5 V DC). BinTec Communications AG fraskriver sig ansvaret for skader, som måtte opstå som følge af brug af en anden stiknetdel.
- Sørg for at kablerne forbindes i den rigtige rækkefølge (se beskrivelsen i manualen). Forbind først LAN-, ISDN- og serielle tilslutninger, tilslut derefter strømforsyningen og tænd til sidst for **BinGO!**.
- Kontrollér om kablerne - især ISDN- og LAN-kablerne - er forbundet rigtigt, før **BinGO!** tages i brug. ISDN-tilslutningen på **BinGO!** må ikke forbindes med Ethernet-tilslutningen på Deres computer eller hub og LAN-tilslutningen på **BinGO!** må ikke forbindes med Deres ISDN-tilslutning.
- Apparatet må kun forbindes med vedlagte kabler. Hvis De benytter andre kabler, fraskriver BinTec Communications AG sig ansvaret for evt. skader.
- Ledningerne skal trækkes på en sådan måde, at de ikke beskadiges og at de ikke er til fare for omgivelserne (fare for at snuble).
- Tilslut ikke datatransmissionsledninger og træk dem ikke ud af apparatet, når det er tordenvejr.

Beregnet anvendelse-område, brug

- **BinGO!** er beregnet til at blive brugt på kontorer. **BinGO!** opbygger som ISDN-multi-protokol-router ISDN-forbindelser afhængigt af systemkonfigurationen. De bør overvåge produktet for at undgå uønskede gebyrer.
- **BinGO!** overholder gældende sikkerhedsbestemmelser mht. indretning af informationsteknik til kontorer.
- Den beregnede brug af systemet (iht. IEC 950/EN 60950) er kun sikret, når låget er monteret på huset (køling, brandbeskyttelse, radiostøjdæmpning)
- Omgivelsestemperaturen må ikke overstige 50°C. Undgå direkte solstråler.
- Vær opmærksom på, at genstande (f.eks. klips) eller væske ikke trænger ind i apparatet (elektrisk stød, kortslutning). Sørg for tilstrækkelig køling.
- Afbryd straks strømforsyningen og kontakt serviceafdelingen i nødstilfælde (f.eks. beskadiget hus eller betjeningselement, indtrængning af væske eller fremmede genstande).

Rengøring og reparation

- Apparatet må kun åbnes af skolet fagligt personale. Reparationer på apparatet skal derfor altid udføres på et autoriseret BinTec serviceværksted. Deres forhandler kan oplyse om det nærmeste serviceværksted. Ubeføjet åbning og ukorrekte reparationer kan udsætte brugeren for stor fare. BinTec Communications AG fraskriver sig ethvert ansvar og garantien bortfalder, hvis apparatet åbnes uden tilladelse.
- Apparatet må under ingen omstændigheder rengøres med væske. Indtrængende vand kan udsætte brugeren for alvorlige farer (f.eks. elektrisk stød) og alvorlige skader på apparatet.
- Benyt aldrig skuremidler, alkaliske rengøringsmidler, skrappe eller skurende hjælpemidler.

Yleiset turvallisuusmääräykset

Seuraavista kappaleista löydät turvallisuusmääräykset, joita on ehdottomasti noudatettava reittivalitsinta käytettäessä.

Kuljetus ja varastointi

- Kuljeta ja varastoi **BinGO!** vain alkuperäispakkauksessaan tai muussa sopivassa pakkauksessa, joka suojaa töytäisyiltä ja iskuilta.

Asennus ja käyttöönotto

- Tarkista ennen **BinGO!** -laitteen asennusta ja käyttöä, että ympäristöolosuhteista annettuja ohjeita (kts. lukua Tekniset tiedot) on noudatettu. Aseta laite tukevalle, tasaiselle alustalle.
- Kun laite tuodaan kylmästä tilasta käyttötiloihin, voi sekä laitteen ulkopinnalla että sen sisäpuolella esiintyä tiivistynyttä vettä. Odota siksi, kunnes reittivalitsimen lämpötila on noussut huonelämpöön ja se on ehdottoman kuiva, ennen kuin otat sen käyttöön.
- Tarkasta, että verkkolaitteen tyyppikilvessä annettu verkkojännite on sama kuin paikallinen verkkojännite. **BinGO!** -laitetta saa käyttää vain alkuperäisen BinTec Communications-pistokeverkkolaitteen (5 V DC) kanssa. BinTec Communications AG ei vastaa vahingoista, jotka ovat aiheutuneet muun pistokeverkkolaitteen käytöstä.
- Käsikirjassa kuvattua kaapelien liitäntäjärjestystä on ehdottomasti noudatettava. Yhdistä ensin LAN-, ISDN- ja sarjaliitännät, liitä laite sitten virtaverkkoon ja kytke lopuksi **BinGO!** päälle.
- Tarkasta, että olet liittänyt kaapelit oikein, erityisesti ISDN- ja LAN-kaapelit, ennen kuin käynnistät **BinGO!** -laitteen. **BinGO!** -laitteen ISDN-liitäntää ei saa liittää laskimen tai jakajan Ethernet-liitäntään eikä **BinGO!** -laitteen LAN -liitäntää saa yhdistää ISDN-liitäntääsi.
- Käytä laitteiden yhdistämiseen vain mukanatoimitettuja kaapeleita. Jos käytät muita kaapeleita, ei BinTec Communications AG vastaa tästä aiheutuvista vahingoista.
- Vedä kaapelit sellaisiin paikkoihin, että ne eivät aiheuta vaaratilanteita (kompastumisia) eivätkä vahingoitu.
- Ukkosen aikana ei tietoliikennekaapeleita tule liittää eikä myöskään irroittaa.

Määräystenmukainen käyttö, käyttö

- **BinGO!** on suunniteltu käytettäväksi toimistotiloissa. **BinGO!** toimii ISDN-monikäytäntö-reittiohjaimena ja luo järjestelmän konfiguraation mukaisesti ISDN-yhteyksiä. Epätoivottujen maksujen välttämiseksi on tuotteen toimintaa välttämättä valvottava.
- **BinGO!** vastaa toimistotiloissa käytettäville tietotekniikan laitteistoille asetettuja asiaankuuluvia turvallisuusmääräyksiä.
- Järjestelmän määräystenmukainen käyttö standardin IEC 950/EN 60950 mukaan on mahdollista vain kun kotelon kansi on asennettu paikalleen (jäähdytys, palosuojelu, häirintäsuojaus)
- Ympäristön lämpötila ei saisi nousta yli 50°C. Älä aseta laitetta alttiiksi suoralle auringonpaisteelle.
- Varo, ettei mitään vieraita esineitä (esim. paperiliittimiä) tai nesteitä pääse laitteen sisäpuolelle (sähköisku, lyhytsulku). Huolehdi siitä, että laitteen jäähdytys on riittävä.
- Keskeytä hätätilanteessa (esim. särkynyt kotelo tai käyttölaite, nesteen tai vieraiden esineiden joutuminen laitteen sisään) virransyöttö välittömästi ja ota yhteyttä huoltopalveluun.

Puhdistus ja korjaus

- Vain koulutettu ammattihenkilöstö saa avata laitteen. Anna sen vuoksi kaikki korjaustyöt vain BinTec-valtuutetun huoltokorjaamon tehtäväksi. Kauppiaasi voi kertoa, missä on lähin valtuutettu huoltokorjaamo. Luvaton aukaiseminen ja asiantuntemattomat korjaukset saatttavat aiheuttaa käyttäjälle vakavia vaaratilanteita (esim. sähköisku). Laitteiden luvaton aukaiseminen aiheuttaa BinTec Communications AG -takuun raukeamisen sekä kaikkinaisen vastuun epäämisen.
- Älä missään tapauksessa puhdista laitetta runsaalla vedellä. Sen sisään tunkeutunut vesi saattaisi aiheuttaa vakavia vaaroja (sim. sähköisku) käyttäjälle ja vaurioittaa laitetta pahasti.
- Älä koskaan käytä puhdistamiseen hankausaineita, alkalisia puhdistusaineita taikka syövyttäviä tai hankaavia tehoaineita.

Consignes de sécurité générales en français

Vous trouverez, dans les paragraphes suivants, les consignes de sécurité que vous devez absolument respecter lors de l'utilisation de votre router.

Transport et entreposage

- Transportez et entreposez **BinGO!** uniquement dans son emballage d'origine ou dans un autre emballage approprié lui garantissant une bonne protection contre les chocs et les coups.

Installation et mise en service

- Avant de procéder à l'installation et à la mise en service de **BinGO!** , veillez aux indications concernant les conditions d'environnement (cf. Caractéristiques techniques). Utilisez un support stable et plan.
- Lorsque vous transportez l'appareil d'un environnement froid jusqu'à la salle dans laquelle il fonctionnera, une rosée peut se former aussi bien sur la paroi extérieure de l'appareil qu'à l'intérieur de ce dernier. Attendez jusqu'à ce que votre Router ait atteint la température ambiante et jusqu'à ce qu'il soit absolument sec avant de le mettre en service.
- Vérifiez si la tension nominale indiquée sur la plaque signalétique du bloc d'alimentation correspond bien à la tension de l'endroit en question. **BinGO!** doit uniquement fonctionner avec la fiche du bloc d'alimentation BinTec Communications originale (5 V DC). BinTec Communications AG décline toute responsabilité pour les dommages dus à l'utilisation d'une autre fiche de bloc d'alimentation.
- Lors du câblage, respectez l'ordre tel qu'il est indiqué dans le manuel. Câblez tout d'abord les raccordements LAN, ISDN et sériels, établissez ensuite la connexion avec le courant et mettez finalement **BinGO!** en service.
- Vérifiez si vous avez bien effectué le câblage, en particulier celui de ISDN et LAN, avant de mettre **BinGO!** en service. Le raccordement ISDN de **BinGO!** ne doit pas être relié au raccordement Ethernet de votre ordinateur ou de votre borne, le raccordement LAN de **BinGO!** ne doit pas être relié à votre raccordement ISDN.
- Utilisez uniquement les câbles joints à la livraison pour effectuer le câblage. Dans le cas où vous utilisez d'autres câbles que ces derniers, BinTec Communications AG décline toute responsabilité pour tout dommage qui pourrait en découler.

- Posez les câbles de telle sorte qu'ils ne puissent pas être à l'origine de risques (risques de trébuchement) ni ne puissent être endommagés.
- Ne connectez pas ni ne déconnectez les câbles de transmission de données pendant un orage.

Utilisation conforme à l'affectation prévue, fonctionnement

- **BinGO!** est prévu pour être employé dans les bureaux. **BinGO!** établit des connexions ISDN qui dépendent de la configuration du système en tant que routeur ISDN Multi à procès-verbal. Pour éviter de payer des taxes inconsidérément, vous devriez absolument surveiller ce produit.
- **BinGO!** est conforme aux prescriptions de sécurité correspondantes relatives aux équipements de la technique de l'information pour l'emploi en bureau.
- L'emploi de ce système conforme à l'affectation prévue, conformément à la norme IEC 950/EN 60950 n'est garantit que si le couvercle du boîtier est monté (refroidissement, protection anti-incendie, étincelles)
- La température ambiante ne doit pas dépasser 50°C. Evitez le rayonnement direct du soleil sur l'appareil.
- Veillez à ce qu'aucun objet (par ex. des agrafes) ni aucun liquide ne s'introduise à l'intérieur de l'appareil (électrocution, court-circuit). veillez à ce que l'appareil soit suffisamment refroidi.
- Dans les cas d'urgence extrême (par ex. si le boîtier ou des éléments de commande sont endommagés, si du liquide ou des corps étrangers se sont introduits dans l'appareil), déconnectez immédiatement l'alimentation en courant et prévenez le service.

Nettoyage et Réparation

- L'appareil doit être ouvert uniquement par un personnel spécialisé dûment instruit. Ne faites donc réaliser les réparations de l'appareil que par un poste de service autorisé BinTec. Votre concessionnaire vous fera part de l'adresse à laquelle vous pourrez contacter ce service. Des risques très importants pour l'opérateur (par ex. électrocution) peuvent naître à cause d'une ouverture non autorisée et de réparations non conformes aux règles de l'art. Le fait d'ouvrir l'appareil sans autorisation rend caduque toute clause de garantie et de responsabilité de la part de la BinTec Communications AG.

- L'appareil ne doit être en aucun cas nettoyé à l'eau. Une introduction de l'eau dans l'appareil pourrait entraîner des risques énormes pour l'opérateur (par ex. électrocution) et des dommages importants de l'appareil pourraient en être la conséquence.
- Ne jamais utiliser de produits récurants, de produits de nettoyage alcalins, ni de produits auxiliaires tranchants ou grattants.

2 Γενικές οδηγίες ασφαλείας στα Ελληνικά

Στις ακόλουθες παραγράφους θα βρείτε τις οδηγίες ασφαλείας, τις οποίες θα πρέπει να λάβετε οπωσδήποτε υπ' όψιν σας κατά τη χρήση του Router.

Μεταφορά και αποθήκευση

- Να μεταφέρετε και να αποθηκεύετε το BinGO! μόνο στη γνήσια συσκευασία ή σε μία άλλη κατάλληλη συσκευασία, η οποία να εξασφαλίζει προστασία κατά των κρούσεων και χτυπημάτων.

Στήσιμο και έναρξη της λειτουργίας

- Πριν το στήσιμο και την έναρξη της λειτουργίας του BinGO! να λάβετε υπ' όψιν σας τις οδηγίες σχετικά με τις περιβαλλοντολογικές συνθήκες (βλέπε Τεχνικά στοιχεία). Χρησιμοποιήστε ένα σταθερό και επίπεδο υπόβαθρο.
- Όταν η συσκευή μεταφέρεται από ψυχρό περιβάλλον στο χώρο λειτουργίας, μπορεί να κατακαθίσει υγρασία στο εξωτερικό της συσκευής καθώς και στο εσωτερικό της ίδιας. Να κάνετε υπομονή, μέχρι που η θερμοκρασία του Router να έχει προσαρμοστεί και η συσκευή να είναι τελείως στεγνή, προτού να τη θέσετε εκ νέου σε λειτουργία.
- Επανελέγξτε εάν η ονομαστική τάση που αναφέρεται στην πλακέτα τύπου του φις αντιστοιχεί στην κατά τόπους τάση του δικτύου. Το BinGO! επιτρέπεται να λειτουργεί μόνο με το γνήσιο φις BinTec Communications (5 V DC). Η BinTec Communications AG δεν ευθύνεται για ζημιές που ενδέχεται να προκληθούν από τη χρήση ενός άλλου φις.
- Προσέξτε κατή την καλωδίωση, ώστε να τηρηθεί η σωστή σειρά που περιγράφεται στο εγχειρίδιο. Καλωδιώστε κατ' αρχήν το LAN, το ISDN και τη σειριακή διεπαφή. Στη συνέχεια να γίνεται η σύνδεση με το ηλεκτρικό ρεύμα και στο τέλος θέστε το BinGO! σε λειτουργία.
- Επανελέγξτε εάν καλωδιώσατε κατά τον προβλεπόμενο τρόπο ιδίως το ISDN και το LAN, προτού να θέσετε το BinGO! σε λειτουργία. Η σύνδεση ISDN του BinGO! δεν επιτρέπεται να συνδεθεί με τη σύνδεση Ethernet του υπολογιστή ή της υποδοχής σας, και η

σύνδεση LAN του **BinGO!** δεν επιτρέπεται να συνδεθεί με τη σύνδεση ISDN.

- Χρησιμοποιήστε για την καλωδίωση μόνον τα συνημμένα καλώδια. Σε περίπτωση που χρησιμοποιήσετε άλλα καλώδια, η BinTec Communications AG δεν αναλαμβάνει καμία ευθύνη για ενδεχόμενες προκληθείσες ζημιές.
- Διαστρώστε το δίκτυο κατά τέτοιον τρόπο, ώστε να μην προκύψουν σημεία κινδύνου (κίνδυνος παραπατήματος) και ώστε να μη μπορεί να υποστεί ζημιά.
- Μη συνδέετε και μην αποχωρίζετε κατά τη διάρκεια μιας καταιγίδας αγωγούς μεταφοράς δεδομένων.

Προβλεπόμενη χρήση, λειτουργία

- Το **BinGO!** προβλέπεται για τη χρήση σε περιβάλλον γραφείου. Ως Router ποικίλων προτοκόλλων ISDN το **BinGO!** εγκαθιστά συνδέσεις σε συνάρτηση με τη σύνθεση του συστήματος ISDN. Για να αποφύγετε την κατάπτωση ακούσιων τελών, θα έπρεπε το προϊόν οπωσδήποτε να επιβλέπεται.
- Το **BinGO!** ανταποκρίνεται στις σχετικές διατάξεις ασφαλείας για εγκαταστάσεις της τεχνολογίας πληροφοριών κατά τη χρήση σε περιβάλλον γραφείου.
- Η προβλεπόμενη λειτουργία του συστήματος σύμφωνα με την IEC 950/EN 60950 διασφαλίζεται μόνον, όταν το καπάκι του κελύφους είναι μονταρισμένο (ψύξη, αντιπυρική προστασία, παρεμβολή σπινθήρων).
- Η περιβαλλοντολογική θερμοκρασία δε θα έπρεπε να υπερβαίνει τους 50°C. Αποφύγετε την έκθεση σε άμεση ηλιακή ακτινοβολία.
- Να προσέχετε, ώστε να μην εισέλθουν αντικείμενα (π.χ. συνδετήρες) ή υγρά στο εσωτερικό της συσκευής (κίνδυνος ηλεκτροπληξίας, βραχυκυκλώματος). Θα πρέπει να εξασφαλίζεται η επαρκής ψύξη.
- Να διακόπτετε σε έκτακτες περιπτώσεις (π.χ. όταν έχει προκληθεί βλάβη στο κέλυφος ή στη μονάδα χειρισμού ή όταν έχουν εισέλθει υγρά ή αντικείμενα) αμέσως την παροχή ρεύματος και να έρχεστε σε επαφή με το κατάλληλο συνεργείο.

Καθαρισμός και επισκευή

- Η συσκευή επιτρέπεται να ανοίγεται μόνον από ειδικά εκπαιδευμένο τεχνικό προσωπικό. Γι' αυτόν το λόγο να επιτρέπεται τη διεξαγωγή εργασιών επισκευής μόνο σε συνεργεία που έχου εξουσιοδοτηθεί από την BinTec. Σχετικά με την έδρα των σχετικών συνεργείων μπορείτε να ζητήσετε πληροφορίες από τον εμπορικό σας αντιπρόσωπο. Το άνοιγμα της συσκευής από αναρμόδια άτομα καθώς και ακατάλληλες εργασίες επισκευής μπουρούν να θέσουν το χρήστη σε σοβαρούς κινδύνους (π.χ. ηλεκτροπληξία). Το ανεπίτρεπτο άνοιγμα της συσκευής έχει σαν αποτέλεσμα την αποποίηση κάθε εγγύησης και ευθύνης από μέρους της BinTec Communications AG.
- Η συσκευή δεν επιτρέπεται σε καμία περίπτωση να καθαριστεί. Από την ενδεχόμενη είσοδο νερού μπορεί να προκύψουν σημαντικοί κίνδυνοι για το χρήστη (π.χ. ηλεκτροπληξία) και σοβαρές ζημιές στη συσκευή.
- Να μη χρησιμοποιείτε ποτέ μέσα που προβλέπονται για το τρίψιμο, αλκαλικά απορρυπαντικά μέσα και αιχμηρά ή αδρά βοηθητικά μέσα καθαρισμού.

Istruzioni generali di sicurezza

Nei seguenti paragrafi si trovano elencate le istruzioni generali di sicurezza da osservare rigorosamente nell'uso del Suo Router.

Trasporto e magazzinaggio

- Trasporti ed immagazzini **BinGO!** soltanto nell'imballaggio originale o in altro imballaggio adeguato a garantire protezione da urti e scotimenti.

Installazione e azionamento

- Prima di installare ed azionare **BinGO!** faccia attenzione alle istruzioni sulle condizioni ambientali (cfr. Dati tecnici). Utilizzi un ripiano stabile e piano.
- Se l'apparecchio viene introdotto nel locale di funzionamento da un ambiente freddo può verificarsi una condensa sia all'interno che all'esterno dell'apparecchio. Aspetti che il Suo Router si sia adeguato alla temperatura e che sia perfettamente asciutto prima di azionarlo.
- Controlli che la tensione indicata sulla targhetta della sezione di rete corrisponda alla tensione di rete locale. **BinGO!** può essere azionato soltanto con la spina di sezione di rete originale BinTec Communications (5 V DC) La BinTec Communications AG non risponde dei danni causati dall'utilizzo di una spina di sezione di rete diversa.
- Nel cablare osservi l'ordine di successione descritto nel manuale. Cabli prima i collegamenti LAN-, ISDN- e quelli seriali, colleghi poi al distributore di corrente ed alla fine azioni **BinGO!** .
- Controlli di aver eseguito il cablaggio correttamente – in particolare quello ISDN- e LAN- prima di azionare **BinGO!** . Il collegamento ISDN di **BinGO!** non deve essere collegato al collegamento Ethernet del Suo computer o dell'Hub, il collegamento LAN-di **BinGO!** non deve essere collegato al Suo collegamento ISDN.
- Utilizzi per il cablaggio soltanto i cavi allegati.. Nel caso in cui si utilizzino cavi diversi, la BinTec Communications AG non risponde per i danni che ne derivino.
- Disponga i collegamenti in modo che non costituiscano fonte di pericolo (pericolo d'inciampo) e che non possano essere danneggiati.
- Non colleghi nè scolleghi i collegamenti di trasmissione dati durante un temporale.

Utilizzazione conforme a destinazione, funzionamento

- **BinGO!** *è destinato ad essere impiegato in ambiente d'ufficio.* Quale ISDN-Multi-Protokoll-Router istituisce **BinGO!** collegamenti ISDN in dipendenza della configurazione di sistema. Onde evitare conteggi indesiderati dovrebbe assolutamente sorvegliare il prodotto.
- **BinGO!** è conforme alle relative disposizioni di sicurezza per impianti della tecnica informatica impiegati in ambiente d'ufficio.
- Il funzionamento conforme a destinazione secondo IEC 950/EN 60950 del *sistema è garantito soltanto a coperchio montato sulla cassetta (raffreddamento, protezione antincendio, schermatura contro radio disturbi)*
- La temperatura ambientale non dovrebbe superare i 50°C. Eviti l'esposizione diretta alla luce solare.
- Faccia attenzione che nessun oggetto (p.es. fermagli) o liquido si insinui all'interno dell'apparecchio (scossa elettrica, corto circuito). Faccia attenzione ad un sufficiente raffreddamento.
- In casi d'emergenza (p.es. danneggiamento della scatola o dell'elemento servente/manovrante, infiltrazione di liquido o di corpi estranei) stacchi immediatamente la corrente ed informi il servizio assistenza.

Pulizia e riparazione

- *L'apparecchio può essere aperto soltanto da personale competente ed addestrato.* Si consiglia pertanto di far riparare l'apparecchio soltanto presso un centro assistenza autorizzato BinTec. Gli indirizzi dei servizi assistenza sono a disposizione presso il Suo rivenditore. Apertura non autorizzata e *riparazioni inappropriate possono essere fonte di gravi pericoli per l'utente* (p.es. scossa elettrica). Un'apertura non autorizzata degli apparecchi comporta l'esclusione della garanzia e della responsabilità della BinTec Communications AG .
- L'apparecchio non deve assolutamente essere pulito con acqua. L'infiltrazione di acqua può causare gravi pericoli per l'utente (p.es. scossa elettrica) nonché gravi danni all'apparecchio.
- Non utilizzi in nessun caso abrasivi, detersivi a base alcalina, detersivi corrosivi o abrasivi.

Algemene veiligheidsinstructies in het Nederlands

In de volgende paragrafen vindt u veiligheidsinstructies, die u bij de omgang met uw router absoluut moet in acht nemen.

Transport en bewaring

- Transporteert en bewaart u **BinGO!** alleen in de originele verpakking of in een andere geschikte verpakking, die bescherming biedt tegen schokken en stoten.

Opstellen en in bedrijf nemen

- Let voor het opstellen en het bedrijf van **BinGO!** op de instructies voor de omgevingsvoorwaarden (vergelijk technische gegevens). Gebruikt u een harde en vlakke ondergrond.
- Wanneer het apparaat uit een koude omgeving in de werkruimte wordt gebracht, kan er zowel uitwendig op als inwendig in het apparaat condensatie optreden. Wacht u tot uw router is aangepast aan de temperatuur en tot hij volledig droog is, voordat u hem in bedrijf neemt.
- Controleert u, of de op het typeplaatje aangegeven nominale spanning overeenstemt met de plaatselijke netspanning. **BinGO!** mag alleen met de originele BinTec Communications elektrische stekkervoeding (5 V DC) worden gebruikt. BinTec Communications AG is niet aansprakelijk voor beschadigingen, die ontstaan door gebruik van een andere elektrische voeding.
- Let bij de aansluiting van de kabels op de volgorde, zoals in het handboek wordt beschreven. Eerst sluit u de LAN-, ISDN- en de seriële aansluitingen aan, sluit daarna de stroomverzorging aan, en tenslotte schakelt u **BinGO!** in.
- Controleert u, of u de aansluiting - in het bijzonder de ISDN- en LAN-aansluiting correct heeft uitgevoerd, alvorens u **BinGO!** in bedrijf neemt. De ISDN-aansluiting van **BinGO!** mag niet met de ethernet-aansluiting van uw computer of hub go-ahead worden verbonden, de LAN-aansluiting van **BinGO!** niet met uw ISDN-aansluiting.
- Gebruikt u voor de aansluiting slechts de bijgevoegde kabels. Indien u andere kabels gebruikt, is BinTec Communications AG niet aansprakelijk voor optredende schade.

- Leg de kabels zodanig, dat zij geen gevaarsbron (struikelgevaar) vormen en niet worden beschadigd.
- Koppel de datatransfertkabels nooit aan of af tijdens een onweer.

Doelmatig gebruik, bedrijf

- **BinGO!** is bestemd voor toepassing in een kantooromgeving. Als ISDN-Multi-Protocol-Router maakt **BinGO!** afhankelijk van de systeemconfiguratie ISDN-verbindingen. Om ongewenste kosten te vermijden, dient u het product absoluut te bewaken.
- **BinGO!** voldoet aan de gebruikelijke veiligheidsbepalingen voor inrichtingen van informatietechniek voor toepassing in een kantooromgeving.
- Het doelmatig bedrijf, overeenkomstig IEC 950/EN 60950 van het systeem, is alleen bij gemonteerd huisdeksel gewaarborgd (koeling, brandveiligheid, vonkontstoring)
- De omgevingstemperatuur mag niet hoger zijn dan 50°C. Vermijdt u direct zonlicht.
- Let erop, dat er geen voorwerpen (bijv. paperclips) of vloeistoffen in het inwendige van het apparaat geraken (elektrische schok, kortsluiting). Let u op voldoende koeling.
- Onderbreekt u in noodgevallen (bijv. beschadigd huis, of bedienelement, binnendringen van vloeistof of vreemde voorwerpen) onmiddellijk de stroomverzorging en neemt u contact op met de service-dienst.

Reiniging en reparatie

- Het apparaat mag alleen door geschoold vakpersoneel worden geopend. Laat u daarom reparaties aan het apparaat alleen uitvoeren door een door BinTec-geautoriseerde service-dienst. Waar zich deze service-dienst bevindt, ervaart u bij uw handelaar. Door het onbevoegde openen en ondeskundige reparaties kunnen aanzienlijke gevaren ontstaan voor de gebruiker (bijv. elektrische schok). Onbevoegd openen van de apparaten heeft verval van de garantie en uitsluiting van de aansprakelijkheid van de BinTec Communications AG tot gevolg.
- Het apparaat mag in geen geval nat worden gereinigd. Door binnendringend water kunnen er aanzienlijke gevaren ontstaan voor de gebruiker (bijv. elektrische schok) en kan er aanzienlijke schade ontstaan aan het apparaat.

- Gebruikt u nooit schuurmiddelen, alkalische reinigingsmiddelen, scherpe of schurende hulpmiddelen.

Generelle sikkerhetshenvisninger på norsk

I de følgende avsnittene finner du sikkerhetshenvisninger som du absolutt må ta hensyn til ved omgangen med din Router.

Transport og lagring

- Du må kun transportere og lagre **BinGO!** i originalemballasjen eller i en annen egnet emballasje som beskytter mot støt og slag.

Oppstilling og ibruktaking

- Før oppstilling og drift av **BinGO!** må du ta hensyn til henvisningene når det gjelder omgivelsesbetingelsene (sml. tekniske data). Bruk et fast og jevnt underlag.
- WDersom apparatet blir tatt fra en kald omgivelse og inn i rommet der det skal brukes, kan det oppstå kondens både på utsiden og på innsiden av apparatet. Vent til Router har tilpasset seg temperaturen og er helt tørr før du tar den i bruk.
- ÜKontroller om den spenningen som er oppgitt på typeskiltet på nettdelen stemmer overens med spenningen på stedet. **BinGO!** må kun brukes sammen det originale BinTec kommunikasjons-støpselet (5 V DC). BinTec Communications AG er ikke ansvarlig for skader som måtte oppstå på grunn av at det er blitt brukt en annen støpsel-nettdel.
- Ved sammenkopling av kablene, må det tas hensyn til rekkefølgen som er beskrevet i håndboken. Sammenkople først kablene LAN-, ISDN- og serielle tilkoplinger, tilkople så strømforsyningen, og slå deretter til slutt på **BinGO!** .
- Kontroller om du har foretatt sammenkoplingen av kablene skikkelig– i særdeleshet ISDN- og LAN-sammenkoplingen, før du tar **BinGO!** i drift. ISDN-tilkoplingen fra **BinGO!** må ikke forbindes med Ethernet-tilkoplingene på datamaskinen eller med Hubs, og LAN-tilkoplingen må ikke forbindes med **BinGO!** ISDN-tilkoplingen.
- Bruk kun de vedlagte kablene for sammenkabling. Dersom du bruker andre kabler, overtar BinTec Communications AG intet ansvar for skader som måtte oppstå av den grunn.
- Legg opp ledningene slik at de ikke kan bli skadet og at de ikke danner farekilder (fare for å snuble) .

- Under tordenvær må du hverken tilkople eller trekke av noen av dataoverføringsledningene.

Forskriftsmessig bruk, drift

- **BinGO!** er beregnet for innsats på kontoromgivelser. Som ISDN-Multi-Protokoll-Router bygger **BinGO!** opp ISDN-forbindelser i avhengighet av systemkonfigurasjonen. For å unngå uønskede gebyrer, bør produktet absolutt overvåkes.
- **BinGO!** tilsvarer de gyldige sikkerhetsbestemmelsene for innretninger innenfor informasjonsteknikken for innsats i en kontoromgivelse.
- Den forskriftsmessige bruken i henhold til IEC 950/EN 60950 for systemet er kun garantert ved montert maskinkasse (Kjøling, brannbeskyttelse, fjerning av radiostøy)
- Omgivelsestemperaturen bør ikke overstige 50°C. Unngå direkte sollys.
- Pass på at ingen gjenstander (f. eks. binders) eller væsker kan komme inn i apparatet (fare for elektrisk støt, kortslutning). Pass på tilstrekkelig avkjøling.
- I nødstilfeller (z. B. skadet kasse eller betjenings-elementer, når væske eller fremmedlegemer er kommet inn) må du straks avbryte strømforsyningen og tilkalle service.

Rengjøring og reparasjon

- Apparatet må kun åpnes av opplært fagpersonell. La derfor alltid reparasjoner på apparatet gjennomføres av et BinTec-autorisert serviceverksted.. Din forhandler informerer det om hvor du finner serviceverksteder. Dersom uvedkommende åpner eller reparerer apparatet, kan det oppstå stor skade for brukeren (f. eks. strømstøt). Dersom apparatet blir ulovlig åpnet, kan ha til følge at garantien mistes, og at ethvert ansvar blir utelukket fra BinTec Communications AG .
- Apparatet må under ingen omstendigheter rengjøres med vann. Dersom vannet trenger inn, kan det oppstå alvorlige skader for brukeren (f. eks. strømstøt) og også på apparatet.
- Bruk aldri skuremidler, alkaliske rengjøringsmidler, skarpe eller skurende hjelpemidler.

2 Ogólne zasady bezpieczeństwa w języku polskim

Poniżej podano zasady bezpieczeństwa, których należy bezwzględnie przestrzegać przy obchodzeniu się z routerem.

Transport i magazynowanie

- Urządzenie **BinGO!** należy transportować i magazynować wyłącznie w opakowaniu oryginalnym lub innym nadającym się do tego celu opakowaniu, zapewniającym ochronę przed obiciami i uderzeniami.

Ustawianie i uruchamianie

- Przed ustawieniem i uruchomieniem urządzenia **BinGO!** należy zastosować się do wskazówek dotyczących warunków otoczenia (por. Parametry techniczne). Urządzenie należy ustawić na trwałym i równym podłożu.
- Po przeniesieniu urządzenia z zimnego otoczenia do pomieszczenia roboczego zarówno we wnętrzu, jak i na częściach zewnętrznych urządzenia może się tworzyć rosa. Przed uruchomieniem routera należy odczekać na zrównanie się jego temperatury z temperaturą pomieszczenia i jego całkowite wyschnięcie.
- Należy sprawdzić, czy podane na tabliczce typologicznej zasilacza napięcie znamionowe jest zgodne z lokalnym napięciem sieciowym. Urządzenie **BinGO!** można eksploatować wyłącznie w połączeniu z oryginalnym zasilaczem wtykowym produkcji firmy BinTec Communications (5 V DC). Firma BinTec Communications AG nie odpowiada za szkody wywołane stosowaniem zasilacza innego typu.
- Przy przyłączaniu przewodów należy przestrzegać kolejności opisanej w instrukcji obsługi. W pierwszej kolejności należy przyłączyć złącza LAN, ISDN oraz złącza seryjne, następnie włączyć zasilanie prądem elektrycznym, na koniec zaś włączyć router **BinGO!**.
- Przed uruchomieniem urządzenia **BinGO!** należy sprawdzić, czy przyłączenie przewodów - a w szczególności przewodów ISDN i LAN - jest prawidłowe. Złącze ISDN urządzenia **BinGO!** nie może być połączone ze złączem eternetowym komputera lub koncentratora, zaś złącze LANurządzenia **BinGO!** ze złączem ISDN.

- Do przyłączenia produktu należy zastosować wyłącznie dostarczone wraz z nim przewody. W przypadku zastosowania innych przewodów firma BinTec Communications AG nie ponosi odpowiedzialności za powstałe szkody.
- Przewody należy ułożyć tak, aby nie występowało niebezpieczeństwo potykania się o nie oraz ich uszkadzania.
- Podczas burzy nie należy przyłączać ani odłączać przewodów transmisji danych.

Zgodne z przeznaczeniem stosowanie, eksploatacja

- Urządzenie **BinGO!** jest przeznaczone do stosowania w otoczeniach biurowych. Jako router multiprotokołowy ISDN urządzenie **BinGO!** wykonuje połączenia typu ISDN w zależności od konfiguracji systemu. W celu unikania niepożądanych opłat należy koniecznie nadzorować produkt.
- Urządzenie **BinGO!** spełnia obowiązujące zasady bezpieczeństwa dla urządzeń informatycznych przeznaczonych do stosowania w otoczeniu biurowym.
- Zgodne z przeznaczeniem użytkowanie systemu według wymogów norm IEC 950/EN 60950 jest zagwarantowane tylko przy zamontowanej pokrywie obudowy (chłodzenie, zabezpieczenie przeciwpożarowe, eliminacja zakłóceń)
- Temperatura otoczenia nie powinna przekraczać 50°C. Należy unikać bezpośredniego działania promieni słonecznych.
- Należy uważać, aby do wnętrza urządzenia nie wnikały żadnego rodzaju przedmioty (np. spinacze biurowe) bądź ciecze (udar prądowy, zwarcia). Zapewnić wystarczające chłodzenia urządzenia.
- W sytuacjach awaryjnych (np. uszkodzona obudowa lub elementobsługi, wniknięcie cieczy bądź ciał obcych) należy natychmiast przerwać zasilanie urządzenia prądem elektrycznym i zawiadomić serwis.

Oczyszczanie i naprawa

- Urządzenie może być otwierane tylko przez odpowiednio przeszkolony personel. Naprawy urządzenia należy w związku z tym zlecać wyłącznie autoryzowanym przez firmę BinTec punktom serwisowym. Informacji na temat lokalizacji tych punktów można zasięgnąć w punkcie sprzedaży. Otwieranie obudowy urządzenia bez upoważnienia lub jego niefachowe naprawy mogą wywoływać poważne zagrożenia dla użytkownika (np.

porażenie prądem). Niedozwolone otwieranie urządzeń pociąga za sobą utratę gwarancji udzielanej przez firmę BinTec Communications AG oraz jej odpowiedzialności cywilnej za skutki użytkowania produktu.

- Urządzenia pod żadnym pozorem nie wolno czyścić na mokro. Dostanie się wody do wnętrza urządzenia może wywoływać poważne zagrożenia dla użytkownika (np. porażenie prądem) oraz poważne uszkodzenia produktu.
- Nigdy nie stosować środków do szorowania, zasadowych środków czyszczących, ostrych lub szorujących środków pomocniczych.

Considerações genéricas em matéria de segurança em português

Nos parágrafos que se seguem, encontra considerações em matéria de segurança que terá de respeitar estritamente ao lidar com o Router.

Transporte e armazenamento

- Transporte e armazene o **BinGO!** apenas na embalagem original ou noutra adequada para o efeito que o proteja contra embates fortes e pancadas.

Instalação e colocação em funcionamento

- Antes de proceder à instalação e à colocação em funcionamento do **BinGO!** tenha em conta as indicações relativas às condições ambientais (cf. Dados técnicos). Utilize uma base consistente e lisa.
- Ao trazer o aparelho de um ambiente frio para a sala de trabalho, podem formar-se gotículas tanto no exterior, como no interior do aparelho. Espere até que o Router fique à temperatura da sala e absolutamente seco, antes de o pôr a funcionar.
- Verifique se a tensão nominal constante da placa de características da fonte de alimentação é a mesma da do local. O **BinGO!** só pode ser colocado em funcionamento com a ficha da fonte de alimentação BinTec Communications (5 V DC) original. A BinTec Communications AG não se responsabiliza por danos decorrentes da utilização de outra ficha de fonte de alimentação.
- Ao proceder à cablagem, respeite a sequência, tal como descrito no manual. Proceda primeiro à distribuição das ligações LAN, RDIS e em série, conecte depois a alimentação de corrente e, para terminar, ligue o **BinGO!**.
- Verifique se a cablagem, em especial da RDIS e da LAN, ficou bem feita, antes de pôr o **BinGO!** em funcionamento. A ligação RDIS do **BinGO!** não pode ser conectada à Ethernet do seu computador ou Hubs, a ligação LANdo **BinGO!** não pode ser conectada à sua ligação RDIS.
- Para o cableamento, utilize unicamente o cabo fornecido juntamente. Se usar outro cabo, a BinTec Communications AG não se responsabiliza por danos daí decorrentes.
- Instale os cabos de maneira a não constituírem uma fonte de perigo (perigo de tropeçar) nem se danificarem.

- Não conecte nem desconecte os cabos de transmissão de dados se estiver a trovejar.

Utilização conforme com as especificações, Operação

- O**BinGO!** destina-se à utilização em escritórios. Enquanto Router multiprotocolo RDIS, o **BinGO!** estabelece as ligações RDIS em função da configuração do sistema. Para evitar taxas adicionais deve vigiar sempre o produto.
- O**BinGO!** corresponde às normas de segurança habituais relativas a dispositivos de informática para utilização em escritórios.
- O funcionamento conforme com as especificações IEC 950/EN 60950 do sistema só é garantido com a tampa da caixa montada (refrigeração, protecção contra incêndios, desparasitagem)
- A temperatura ambiente não pode ultrapassar 50°C. Evite expor o aparelho à luz solar directa.
- Tenha o cuidado de não deixar entrar objectos (por ex. clipes) ou líquidos para o interior do aparelho (choque eléctrico, curto-circuito). Verifique se a refrigeração é suficiente.
- Em caso de emergência (por ex. caixa ou elemento de comando danificado, entrada de líquido ou de corpos estranhos), interrompa imediatamente a alimentação de corrente e recorra ao serviço de assistência técnica.

Limpeza e reparação

- O aparelho só pode ser aberto por pessoal especializado. Por isso, deixe as reparações do aparelho exclusivamente a cargo de um serviço de assistência técnica BinTec autorizado. Informe-se junto do seu agente para saber onde encontrar um ponto de assistência técnica. O utilizador pode colocar-se a si próprio em perigo caso abra o dispositivo sem qualquer autorização ou proceda a uma reparação imprópria (por ex. choque eléctrico). A abertura não autorizada do aparelho tem como consequência a perda da garantia e da responsabilidade daBinTec Communications AG.
- O aparelho nunca pode ser limpo a húmido. A infiltração de água pode constituir perigo para o utilizador (por ex. choque eléctrico) e danos de monta no aparelho.
- Nunca utilizar abrasivos, produtos de limpeza alcalinos, objectos afiados ou que risquem.

Instrucciones generales de seguridad

En los párrafos siguientes encontrará unas instrucciones de seguridad. Es imprescindible tener las mismas en cuenta a la hora de manejar su router.

Transporte y almacenamiento

- Transporte y almacene su **BinGO!** únicamente en su embalaje original o en otro embalaje adecuado que garantice su protección contra golpes y choques.

Colocación y puesta en servicio

- Antes de la colocación y puesta en servicio de **BinGO!**, observe las instrucciones acerca de las condiciones ambientales (ver "Datos técnicos"). Utilice una superficie firme y plana.
- Al trasladar el aparato desde un ambiente frío a la habitación prevista para su puesta en servicio puede formarse rocío tanto en el exterior como en el interior del aparato. Antes de ponerlo en marcha, espere hasta que su router se haya adaptado a la temperatura y esté absolutamente seco.
- Asegúrese de que la tensión nominal indicada en la placa de características coincide con la tensión de la red local. **BinGO!** únicamente debe ponerse en funcionamiento con el bloque de alimentación original de BinTec Communications (5 V DC). BinTec Communications AG no se hace responsable de los daños y perjuicios causados por el uso de otro tipo de bloque de alimentación.
- A la hora de cablear, respete el orden descrito en el manual. Cablee primero las conexiones LAN, RSDI y de serie, conecte la alimentación de energía eléctrica y encienda finalmente el **BinGO!**.
- Asegúrese del cableado correcto -y sobre todo del cableado de las conexiones LAN y RSDI- antes de poner **BinGO!** en servicio. La conexión RSDI de **BinGO!** no debe conectarse a la conexión Ethernet de su ordenador o hub, ni la conexión LAN de **BinGO!** a su conexión RSDI.
- Realice el cableado únicamente con los cables suministrados. Si utiliza cables distintos, BinTec Communications AG no asumirá la responsabilidad de los daños y perjuicios que puedan producirse.
- Coloque los cables de manera que no constituyan un peligro (tropezones) y no puedan ser deteriorados.

- No conecte ni desconecte líneas de transmisión de datos durante una tormenta

Utilización prevista, servicio

- **BinGO!** está previsto para su utilización en oficinas y despachos. Como router RSDI multiprotocolo, **BinGO!** crea conexiones RSDI en función a la configuración del sistema. Para evitar gastos telefónicos no deseados es imprescindible controlar el aparato
- **BinGO!** corresponde a las disposiciones de seguridad pertinentes para equipos informáticos utilizados en oficinas y despachos.
- El servicio previsto del sistema de acuerdo con IEC 950/EN 60950 queda únicamente garantizado si la tapa permanece montada en la caja (refrigeración, prevención de incendios, supresión de interferencias)
- La temperatura ambiental no debe superar los 50°C. No exponga el aparato a la luz solar directa.
- Procure que ningún objeto (p. ej. clips) o líquido entre en el interior del aparato (descargas eléctricas , cortocircuitos) y que exista una refrigeración suficiente.
- En casos de emergencia (p. ej. caja o elemento de mando deteriorados, penetración de líquidos o de cuerpos extraños), interrumpa inmediatamente la alimentación de energía y avise al servicio técnico.

Limpieza y reparación

- El aparato debe ser abierto únicamente por personal técnico cualificado. Por lo tanto, realice las posibles reparaciones del aparato sólamente a través de un servicio técnico autorizado por BinTec. Su vendedor le informará de la dirección del servicio técnico. El abrir y reparar el aparato sin autorización puede conllevar un peligro considerable para el usuario (descargas eléctricas). El abrir de los aparatos sin autorización tiene como consecuencia la exoneración de la responsabilidad y de la garantía de BinTec Communications AG.
- En ningún caso, el aparato debe limpiarse en húmedo. Al penetrar agua, puede existir un peligro considerable para el usuario (p. ej., descargas eléctricas) y pueden producirse daños considerables en el aparato.
- No utilizar jamás productos abrasivos, detergentes alcalinos, ni instrumentos afilados o abrasivos.

Allmänna säkerhetsanvisningar på tyska

Nedan följer säkerhetsanvisningar som du måste ta hänsyn till när du använder din Router.

Transport och förvaring

- **BinGO!** får endast transporteras och förvaras i originalförpackningen eller i en annan lämplig förpackning som skyddar mot stötar och slag.

Installation och start

- Innan du installerar och börjar använda **BinGO!** bör du först läsa specifikationerna om miljökraven (se Tekniska Data). Använd ett fast och jämnt underlag.
- Om apparaten kommer utifrån och skall ställas upp inomhus kan det börja imma båda utvändigt och inuti apparaten. Vänta därför tills din nya Router har antagit rumstemperatur och är absolut torr innan du börjar använda den.
- Kontrollera att märkspänningen på typskylten stämmer överens med den lokala nätspänningen. **BinGO!** får endast användas tillsammans med original BinTec Communication nätenhet (5 V DC). BinTec Communications AG ansvarar inte för skador som kan hänföras till att en annan nätenhet har använts.
- Kablarna skall dras i den ordning som anges i handboken. Börja med kablarna till LAN-, ISDN- und de seriella anslutningarna, anslut sedan strömmen och starta **BinGO!**.
- Kontrollera att kabeldragningen har genomförts riktigt - särskilt ISDN- und LAN-kablarna - innan du börjar använda **BinGO!**. ISDN-anslutningen till **BinGO!** får inte anslutas till Ethernet-anslutningen på din dator eller på hubben och LAN-anslutningen till **BinGO!** får inte anslutas till din ISDN-anslutning.
- Använd endast bifogade kablar. Om du använder andra kablar kan BinTec Communications AG inte påta sig något ansvar för eventuella skador.
- Ledningarna skall dras så att de inte utgör någon risk (de får inte ligga så att man kan snubbla över dem) och inte kan skadas.
- Dataledningarna får varken anslutas eller lossas under ett oväder.

Normal användning, drift

- **BinGO!** är avsedd för att användas i kontorsmiljö. I egenskap av ISDN-multi-protokoll-router bygger **BinGO!** upp ISDN-linjer beroende på systemuppbyggnaden. För att undvika ofrivilliga avgifter bör du absolut övervaka produkten.
- **BinGO!** uppfyller kraven i gällande säkerhetsbestämmelser för IT-utrustning för kontor.
- För normal användning av systemet enligt IEC 950/EN 60950 måste locket vara monterat (kylning, brandskydd, gnistavstörning)
- Omgivningstemperaturen får inte vara högre än 50°C. Undvik direkt solljus.
- Kontrollera att det inte kan hamna några föremål (t ex häftklammer) eller vätskor i apparaten (risk för kortslutning). Sörj för fullgod kylning.
- Bryt genast strömmen i nödsituationer (t ex om apparaten eller manöverelementen är trasiga eller om vätska eller främmande föremål har trängt in i den) och kontakta serviceavdelningen.

Rengöring och reparation

- Apparaten får endast öppnas av fackpersonal med motsvarande kompetens. Reparationer på apparaten får därför endast utföras av en av BinTec auktoriserad serviceverkstad. Var närmaste serviceverkstad finns kan du få reda på om du vänder dig till den affär där du köpt apparaten. Om apparaten öppnas av obehöriga eller repareras på felaktigt sätt kan allvarliga skador drabba den som använder apparaten (elektriska stötar). Om apparaten öppnas utan tillstånd gäller inte garanti- och ansvarsvillkoren för BinTec Communications AG längre.
- Apparaten får absolut inte våtrengöras. Om vatten tränger kan allvarliga skador drabba den som använder apparaten (t ex elektriska stötar) samt allvarliga maskinskador uppkomma.
- Apparaten får inte rengöras med skurpulver, alkaliska rengöringsmedel, skarpa medel eller medel som ger repor.

2 Všeobecné bezpečnostní pokyny

V následujících odstavcích najdete bezpečnostní pokyny, kterých musíte bezpodmínečně dbát při práci se svým routerem.

Doprava a uskladnění

- Dopravujte a skladujte **BinGO!** jen v originálním obalu nebo v jiném vhodném obalu, který zaručuje ochranu proti nárazu.

Postavení a uvedení do provozu

- Před postavením a uvedením **BinGO!** do provozu si povšimněte pokynů týkajících se podmínek prostředí (viz technické údaje). Pouijte pevnou a rovnou podloku.
- Je-li přístroj přenesen ze studeného prostředí do provozní místnosti, opotí se jak vnějšek přístroje, tak jeho vnitřek. Počkejte, ne váš router bude mít teplotu okolí a bude absolutně suchý, ne jej uvedete do provozu.
- Zkontrolujte, zda jmenovité napětí na typovém štítku síové části souhlasí s napětím v místní elektrické síti. **BinGO!** se smí provozovat jen s originální síovou přípojkou BinTec Communication. (5 V DC). BinTec Communications AG neručí za škody, které vzniknou pouitím jiného dílu pro napájení ze sítě.
- Při propojování kabelů dbejte na pořadí, jak je popsáno v příručce. Spojte nejprve LAN, ISDN a seriové přípojky, pak teprve zapojte napájení ze sítě a nakonec zapněte **BinGO!** .
- Zkontrolujte, jestli propojení, zvláště propojení ISDN a LAN, bylo provedeno správně, ne uvedete do provozu **BinGO!** Přípojka ISDN **BinGO!** nesmí být spojena s ethernetovou přípojkou vašeho počítače, přípojka LAN od - **BinGO!** s vaší přípojkou ISDN.
- Pro spojení pouijte výhradně přiloené kabely. V případě, e pouijete jiné kabely, nepřejímáBinTec Communications AG za nastalé škody ádnou zodpovědnost.
- Polote kabely tak, abyste se vyhnuli nebezpečí (např. zakopnutí) a aby se nepoškodily.
- Během bouřky nepřipojujte vedení přenosu dat ani je nevytahujte.

Uití k účelu, provoz

- **BinGO!** je určeno pro pouití v kancelářském prostředí. Jako multiprotokolový router ISDN buduje **BinGO!** v závislosti na systémové konfiiguraci spojení ISDN. Abyste se vyhnuli neádoucím poplatkům, měli byste mít výrobek bezpodmínečně pod dohledem.
- **BinGO!** odpovídá bezpečnostním předpisům pro zařízení informační techniky pro práci v kancelářském prostředí.
- Uití k patřičnému účelu podle IEC 950/EN 60950 systému je zaručeno pouze při nasazeném krytu skříně (chlazení, ochrana před poárem, odjiskření).
- Teplota prostředí by neměla překročit 50 °C. Vyhněte se přímému slunečnímu záření.
- Dbejte na to, aby se do vnitřku přístroje nedostaly ádné předměty (např. kancelářské svorky) nebo tekutiny (nebezpečí elektrického výboje, krátkého spojení). Dbejte na dostatečné chlazení.
- V případě tísně (např. poškozená skříň nebo ovládací prvek, vniknutí tekutiny nebo cizích těles) okamitě přerušte přívod proudu a zavolejte servis.

Čištění a opravy

- Přístroj smí otvírat jen školený odborný personál. Dávejte proto provádět opravy přístroje jen do autorizovaného servisu firmy BinTec. Kde tento servis je, se dozvíte od svého obchodníka. Při neoprávněném otevření a neodborných opravách se uivatel může vystavit značným nebezpečím (např. úderu proudu). Nedovolené otevření přístroje má za následek zánik záruky a ručení firmy BinTec Communications AG .
- Přístroj se v ádném případě nesmí čistit mokrým předmětem. Vniknoucí voda vystavuje uivatele vánému nebezpečí (např. úderu proudu) a způsobí váné poškození přístroje.
- Nikdy nepouívejte čisticí prášky, alkalická čistidla, ostré předměty nebo prostředky k drhnutí.

Genel güvenlik bilgileri türkçe

Müteakip bölümlerde router'inizin kullanýrken mutlaka dikkat etmeniz gereken genel güvenlik bilgilerini bulabilirsiniz.

Transport ve Depolama

- **BinGO!** yalnýzca orijinal ambalajý içinde veya çarpmaya ve darbeye karþý koruma saðlayan diðer bir ambalaj içinde taþýnmalý ve depolanmalýdýr.

Kurulmasý ve Çalýþtýrýlmasý

- **BinGO!** kurulup ve çalýþtýrýlmadan önce çevre koþullarý hakkýndaki bilgiler dikkate alýnmalýdýr (Teknik özellikler). Saðlam duran ve düz bir altlýk kullanýnýz.
- Eðer cihaz soðuk bir ortamdan ýþletim odasýna getirilirse cihazýn dýþýnda ve içinde nem oluþabilir. Bu durumda router'inizi çalýþtýrmadan önce bulunduðu ortamdaki ýsýya adapte olmasýný ve tamamen kurumasýný bekleyiniz.
- Trafonun tip etiketindeki anma gerilimin yerel þebeke gerilimi ile eþit deðerde olup olmadýðýný kontrol edin. **BinGO!** yalnýzca orijinal BinTec Communications fiþli trafo (5 V DC) ile iþletilmelidir. BinTec Communications AG baþka bir trafo ile kullanýmdan kaynaklanan hasarlar için sorumluluk üstlenmez.
- Kablo baðlantýlarýný yaparken el kitabinda açýklanan sýralamaya göre çalýþýn. Ýlkönce LAN-, ISDN- ve seri baðlantý yuvalarýna olan kablo baglantýsýný tamamlayýn, sonra elektrik beslemesini baðlayýn, ve son olarak **BinGO!** 'yu çalýþtýrýn.
- **BinGO!** çalýþtýrmadan önce kablo baðlantýlarýnýn – özellikle ISDN- ve LAN kablo baðlantýlarý – doðru olup olmadýðýný kontrol edin. **BinGO!** 'nun ISDN baðlantý yuvasý bilgisayarýnýzýn ve hub'ýnýzýn Ethernet baðlantýsý ile, **BinGO!** 'nun LAN-baðlantýsý sizin ISDN baðlantýnýz ile birleþtirilmemelidir.
- Kablo baðlantýlarý için yalnýzca cihazla beraber gönderilen kablolarý kullanýn. Eðer baþka kablo kullanýrsanýz BinTec Communications AG meydana gelen hasarlar için sorumluluk üstlenmez.
- Kablolarý döþerken tehlike kaynaðý (tökezleme tehlikesi) yaratmamaya özen gösterin ve kablolarý hasar görmeyecek þekilde döþeyin.

- Veri aktarým kablolarýnýý kötü hava esnasýnda (yaðmur, þimþek vs.) baðlamayýn veya çýkarmayýn.

Amacýna uygun kullaným, Ýþletim

- **BinGO!** yalnýzca büro ortamýnda kulanýlmak üzere tasarlanmýþtýr. ISDN-Multi-Protokoll-Router'i olarak **BinGO!** sistem konfigürasyonuna baðýmlý olarak ISDN-baðlantýlarýnýý kurar. Ýstekdýþý ücretlerin önlenmesi için ürün mutlaka kontrol edilmelidir.
- **BinGO!** büro ortamýnda kullanýlan bilgi teknolojisi donanýmlarý ile ilgili güvenlik yönetmeliklerine uygundur.
- Sistemin IEC 950/EN 60950'ye göre kurallara uygun iþletimi, yalnýzca cihaz kasasýnýn kapaðý monte edili ise saðlanýr (soðutma, yangýn koruma, parazit giderme)
- Çevre ýsýsý 50°C üstüne çýkmamalýdýr. Cihazý güneþ ýþýnlarýndan koruyun.
- Cihazýn içine yabancý cisimlerin (örnegýn ataç) veya sývýlarýn girmesini önleyin (elektrik çarpmasý, kýsa devre). Cihazýn yeterli derecede soðutulmasýna dikkat edin.
- Acil durumlarda (örneðin hasar görmüþ cihaz kasasý veya kumandaelemaný, sývý veya yabancý cisimlerin cihaz içine girmesi) derhal elektrik beslemesini kapatýn ve servise haber verin.

Temizlik ve Tamir

- Cihazýn yalnýzca eðitilmiþ kalifiye personel tarafýndan açýlmasýna izin verilmiþtir. Bu nedenle cihazdaki tamir iþlerinin yalnýzca BinTec yetkili servisi tarafýndan yapýlmasýný saðlayýn. Servisin adresini cihazý satýn aldýgýnýz satýcýdan öðrenebilirsiniz. Cihazýn izinsiz açýlmasýndan ve bilgisizce yapýlan tamirlerden dolayý kullanýcý için ciddi tehlikeler oluþabilir (örneðin elektrik çarpmasý). Cihazlarýn izin olmadan açýlmasý sonucunda BinTec Communications AG firmasýnýn garanti ve sorumluluk yükümlülüðü ortadan kalkar.
- Cihazýn suyla temizlenmesi kesinlikle yasaktýr. Cihazýn içine su girmesi sayesinde kullanýcý için ciddi tehlikeler oluþabilir (örneðin elektrik çarpmasý) ve cihazda ciddi hasarlar meydana gelebilir.
- Kesinlikle alkalik temizlik maddesi, keskin veya aþýndýrýcý yardýmcý madde kullanmayýnýz.

Általános biztonsági útmutató

A következõ fejezetekben olyan biztonsági útmutatásokat talál, amelyeket routere használata során feltétlenül figyelembe kell vegyen.

Szállítás és tárolás

- A **BinGO!** csak az eredeti csomagolásban szállítandó és tárolandó, vagy egy másik arra alkalmas csomagolásban, amely lökések és ütések ellen védelmet biztosít.

Felállítás és üzembehelyezés

- A **BinGO!** felállítása és üzemeltetése elõtt vegye figyelembe a környezeti feltételekre vonatkozó útmutatásokat (lásd a mûszaki adatoknál). Használjon szilárd és sík alapot.
- Amennyiben a berendezést hideg környezetbõl szállítják be az üzemi helyiségbe, akkor fennáll a harmatképzõdés lehetõsége úgy a készülék külsején, mint pedig annak belsejében. Mielõtt üzembe helyezné várjon addig, amíg routere hõmérséklete alkalmazkodott a környezetéhez és teljesen kiszáradt.
- Ellenõrizze, hogy a tápegység típustábláján megadott névleges feszültség megegyezik-e a helyi hálózati feszültséggel. A **BinGO!** csak az eredeti BinTec Communications dugaszolható tápegységgel (5 V DC) üzemeltethetõ. A BinTec Communications AG nem felel olyan károkért, amelyek egy más típusú dugaszolható tápegység használata révén keletkeztek.
- A kábelezéskor vegye figyelembe a kézikönyvben megadott sorrendet. Elõször kábelezze be a LAN-, ISDN- és soros csatlakozásokat, ezek után csatlakoztassa az áramellátást, végezetül pedig kapcsolja be a **BinGO!** -t.
- Ellenõrizze, hogy a kábelezés - különösen az ISDN- és LAN-kábelezés - helyesen lett-e kivitelezve, mielõtt a **BinGO!** üzembehelyezése megtörténne. A **BinGO!** ISDN csatlakozóját nem szabad az Ön számítógépének vagy hálózati meghajtójának Ethernet csatlakozójával, a **BinGO!** LAN-csatlakozását pedig tilos az Ön ISDN-csatlakozójával összekötni.
- A kábelezéshez csak a mellékelt kábeleket szabad felhasználni. Amennyiben más kábeleket alkalmaz, úgy a BinTec Communications AG az esetlegesen keletkezõ károkért a felelõsséget nem vállalja.

- Fektesse le úgy a kábeleket, hogy azok ne lehessenek veszélyek forrásai (botlásveszély) és azokban kár sem keletkezhessen.
- Viharos idõben ne csatlakoztasson adatátviteli kábeleket és ne is húzza ki azokat.

Rendeltetés szerinti használat, üzemeltetés

- **BinGO!** irodai jellegû környezetben történõ használatra készült. Mint ISDN-multi-protokoll-router **BinGO!** a rendszer konfigurációjától függõen ISDN-kapcsolatokat épít fel. Az akaratlan költségek elkerülése végett a termék feltétlenül felügyeletre szorul.
- **BinGO!** megfelel az idevágó - irodai környezetben való használatra alkalmas információtechnikai berendezésekre vonatkozó - biztonsági elõírásoknak.
- A rendszer rendeltetésszerû használata IEC 950/EN 60950 szerint csak a készülék házának felszerelt tetõzete esetében biztosított (hûtés, tûzvédelem, zavarmentesítés).
- A környezeti hõmérséklet az 50°C értéket ne haladja meg. A közvetlen napsugárzás elkerülendõ.
- Legyen figyelemmel arra, hogy a készülék belsejébe ne kerülhessenek be tárgyak (pld. gémkapocs) vagy folyadékok (áramütés, rövidzárlat). Figyeljen oda a kielégítõ hûtésre.
- Vészhelyzetben (pld. sérült készülékház vagy kezelõelem esetében, vagy amennyiben folyadék vagy idegen test kerülne bele) azonnal szakítsa meg az áramellátást és értesítse a szervízt.

Tisztítás és javítás

- A készüléket csak arra kioktatott szakszemélyzet nyithatja fel. Ezért a készüléken esedékes javításokat csak egy a BinTec által erre feljogosított szervízzel végeztesse el. Hogy ezen szervíz hol található, azt Ön a kereskedõjétõl tudhatja meg. A készülék jogtalan felnyitása és a helytelen javítás révén a felhasználó számára jelentõs veszélyforrások keletkezhetnek (pld. áramütés). A készülékek engedély nélkül történõ felnyitása a BinTec Communications AG garanciális és felelõsségvállalási kötelezettségének megszûnését vonja maga után.

- A készüléket semmi esetre sem szabad nedvesen tisztítani. A víz behatolása a felhasználó számára jelentõs veszélyt jelent (pld. áramütés) és a készülékben is komoly károk keletkezhetnek.
- Sohasem szabad súrolószereket, lúgos tisztítószereket, éles vagy karcoló segédeszközöket alkalmazni.

100Base-T Twisted pair connection, Fast Ethernet. Network connection for 100-MBit networks.

10Base-T Twisted pair connection. Network connection for 10-MBit networks with the connector ➤➤ **RJ45**.

1TR6 D-channel protocol used in the German ISDN. Today the more common protocol is the ➤➤ **DSS1**.

a/b Standard interface for analog terminals (telephone, telefax group 2/3, analog modems). Only for BinTec routers with integrated ➤➤ **PABX**.

ARP Address Resolution Protocol

ARP belongs to the ➤➤ **TCP/IP protocol family**. ARP translates IP addresses into their corresponding ➤➤ **MAC addresses** .

Asynchronous transmission A method of data transmission by which time intervals between transmitted signals can vary in length. This allows computers and peripheral devices to communicate together without being synchronized by clock signals. Start and stop bits are encapsulated at the beginning and end of the transmitted character. – In contrast to ➤➤ **synchronous transmission**.

B-channel A bearer channel of an ➤➤ **ISDN Basic Rate Interface** or a ➤➤ **Primary Rate Interface** for the transmission of user data (voice, data). An ISDN basic connection consists of two B-channels and one ➤➤ **D-channel**. A B-channel has a data transmission rate of 64 kbps.

With **BinGO!**, ➤➤ **Channel bundling** can increase the data transmission rate of an ISDN basic connection up to 128 kbps.

BootP Bootstrap Protocol

Based on ➤➤ **UDP** or ➤➤ **IP protocol**. Automatically assigns an ➤➤ **IP-address**. A BootP server that you can start on your PC in order to assign the as yet unconfigured router an IP address is contained in Dime Tools.

Bridge Network components to connect homogenous networks. As opposed to a ➤➤ **Router** Bridges operate at layer 2 (data link layer) of the ➤➤ **OSI model**, are independent of higher protocols and transmit data packages by means of ➤➤ **MAC addresses**. Data transmission is transparent, which means the information contained in the data packages is not interpreted.

Bridges are used to connect LANs across a physical link. They reduce network data traffic as they can be configured to accept and forward only certain types of frames or only frames whose source is a particular network.

Some BinTec routers can be operated in bridging mode.

Broadcast Broadcasts (data packages) are sent to all stations in a network in order to exchange information. Generally, there is a certain address (broadcast address) that allows all stations to interpret a message as a broadcast.

Bus A set of leads or wires for the data transmission of all connected devices on a network. Data is forwarded over the entire bus and received by devices from the bus.

CAPI Common ISDN Application Programming Interface

A software interface standardised in 1989 that allows applications programs to access ISDN hardware from the PC. Most ISDN-specific software solutions (communications programs such as RVS-COM Lite) work with the CAPI interface. Over such communications applications, you can, for example, send and receive ISDN faxes or transfer data. See also ➤➤ **Remote CAPI**.

CCITT Consultative Committee for International Telegraph and Telephone

A predecessor organization of the ➤➤ **ITU**, it passed recommendations for the development of communications standards, public telephone/data networks and interfaces for data transmission.

Channel bundling One of **BinGO!'s** features. Channel bundling is a method by which the throughput rate is increased. This is achieved by switching a second ➤➤ **B-channel** (dynamically=on demand or statically=always) to data transmission, thereby doubling the throughput.

CHAP Challenge Handshake Authentication Protocol

A security mechanism during the establishment of a connection with a ➤➤ **WAN-Partner** using ➤➤ **PPP**. This protocol serves to prevent unauthorized access by identifying the partner name and password of the remote end, If the partner name and password do not conform, no connection is established. The user name and password are encoded by CHAP before they are sent to the partner – as opposed to ➤➤ **PAP**.

CLID Calling Line Identification

A security mechanism during the establishment of a connection with a ➤➤ **WAN-Partner**. Before the connection is established, a caller is identified by means of his ISDN calling number. If the calling number does not conform with the calling number you have fixed for a WAN partner, no connection is established.

Client A Client uses the services provided by a ➤➤ **Server**. Clients are usually workstations.

Data compression A process by which amounts of transmitted data are reduced. Higher throughput rates can thus be achieved in similar amounts of transmission time. Examples of this technique include: ➤➤ **V.42bis**, ➤➤ **STAC**, ➤➤ **VJHC**, ➤➤ **MPPC**.

Datagram A self-contained ➤➤ **Data Packet** that contains enough information to be routed from the source to the destination terminal in the network with a minimum of protocol overhead – there is, however, no acknowledgement mechanism, which means no protection against loss or misdelivery.

Data packet A data packet is a unit of data that includes a header containing control information and is sent across a network.

D-channel Control and signalling channel of the ➤➤ **ISDN Basic Rate Interface** or of the. ➤➤ **Primary Rate Interface**. In addition to the D-channel, each ISDN BRI connection has two ➤➤ **B-channels**.

DHCP Dynamic Host Configuration Protocol

A Microsoft protocol that provides a mechanism to dynamically assign ➤➤ **IP Addresses**. A DHCP server allocates to each ➤➤ **Client** in a network an IP address from an address pool compiled by a systems administrator. The prerequisite is that ➤➤ **TCP/IP** is configured by the clients so that they can request their IP addresses from the server. The addresses can be reused when the client no longer needs them. **BinGO!** can be used as a DHCP server.

DIME Desktop Internetworking Management Environment

DIME Tools is a collection of tools for the configuration and monitoring of routers over Windows applications. Included with all BinTec routers free of charge.

DIME browser Windows application (similar to the Windows Explorer), which uses the SNMP-commands in order to request and carry out the configuration of **BinGO!**.

DNS Domain Name Service, Domain Name Server

All hosts in a ➤➤ **TCP/IP Network** are usually located by their ➤➤ **IP Addresses**. Because ➤➤ **Host Names** are often used in networks to reach different network nodes, it is necessary for these names to be translated into their corresponding IP addresses. This service is performed by a DNS server. Alternatively, name resolution can take place over the HOSTS file, available on all PCs.

Domain A domain refers to a group of computers whose host names share a common suffix, the domain name. Thus, in the ➤➤ **Internet**, a part of a naming hierarchy (e. g. bintec.de).

DSS1 Digital Subscriber Signalling System.

A common D-channel protocol used in the Euro-ISDN.

EAZ Endgeräteauswahlziffer

Only exists in German ISDN. The last digit of the ISDN telephone number. Used in the ➤➤ **1TR6** protocol to identify a specific end station (e. g. fax), which is connected to the ISDN basic connection. This occurs by attaching one digit between 0 and 9 to the actual ISDN telephone number. In Euro-ISDN, EAZ corresponds to ➤➤ **MSN**.

Encapsulation Encapsulation of ➤➤ **Data packets** in a certain protocol to transmit the packet over a network that the original protocol does not directly support (e. g. NetBIOS over TCP/IP).

Encryption Refers to the encoding of data, e. g. ➤➤ **MPPE**.

Ethernet A local network that connects all addressable devices in the network (PC, printers, etc.) via a twisted pair or a coaxial cable.

Filter A rule that defines a set of packets that should or should not be transmitted from the router.

Firewall A protective mechanism or set of mechanisms to ensure the protection of a private network from unauthorized access from outside. **BinGO!** includes a range of such mechanisms ➤➤ **NAT**, ➤➤ **CLID**, ➤➤ **PAP/CHAP**, access lists etc.

FTP File Transfer Protocol

A TCP/IP protocol used to transfer files between different hosts.

Gateway The original Internet term for what is now known as a router. That means a node in a network that offers access to different networks, e.g. ➤➤ **LAN** and ➤➤ **WAN**.

Host name In ➤➤ **IP networks**, refers to a name used as a replacement for the corresponding ➤➤ **IP address**. A host name consists of an ASCII string that is unique to the host computer

Hub A device used to connect several computers together into a local network. (star-shaped).

Internet The Internet consists of a range of regional, local and university networks. The ➤➤ **IP Protocol** is used for data transmission in the Internet.

Internet Service Provider Allows companies or private individuals access to the Internet.

IP Internet Protocol

Belongs to the protocol suite ➤➤ **TCP/IP** and is used for the connection of Wide Area Networks (➤➤ **WANs**).

IP address The address by which a device is identified in an IP network, e. g. 192.168.1.254. See also ➤➤ **Netmask**.

IPX/SPX Internet Packet Exchange/Sequenced Packet Exchange

Protocol suite from Novell for the transmission of data in a network. The two parts of this protocol suite are IPX (layer 3 of the OSI model) and SPX (layer 4 of the OSI model).

ISDN Integrated Services Digital Network

The ISDN is a digital network that allows the transmission of voice and data. There are two possible user connections for ISDN, the ➤➤ **ISDN Basic Rate Interface** and the ➤➤ **Primary Rate Interface**. ISDN is an international standard. For ISDN protocols, however, there is a range of variations.

ISDN Basic Rate Interface (BRI) An ISDN user interface. The Basic Rate Interface consists of two ➤➤ **B-channels** and a ➤➤ **D-channel**. Compare ➤➤ **Primary Rate Interface**.

The interface to the user is over an ➤➤ **S_0-Bus**.

isdnlogin One of **BinGO!´s** features. Using isdnlogin, **BinGO!** can be remotely configured and administrated. isdnlogin is already functional for routers in their shipped state, as long as you have an ISDN connection.

ISO International Standardization Organization

An international standards organisation that comprises national standards bodies; ANSI, for example, is the US representative to ISO.

ITU International Telecommunication Union

International organisation that coordinates the construction and operation of telecommunications networks / services.

LAN Local Area Network

A network covering a small geographic area. Usually within the confines of a building or corporate center.

Leased line Fixed connection to a user. As opposed to a ➤➤ **Switched connection**, neither a call number nor the establishing or cutting of the connection is required.

MAC address Every device in the network has a fixed hardware address (MAC address). The network card of the device defines this internationally unique address.

MIB Management Information Base

MIB is a databank that accesses and describes all manageable devices and functions connected to a network. All MIBs (including the BinTec MIB) contain objects specific to the manufacturer. ➤➤ **SNMP** is placed on top of MIB.

Modem Modulator/Demodulator

An electronic device used to convert digital information to analog by MODulating it on the sending end, so that the data can be transmitted in an analog medium. The analog information is then DEModulated back to digital data at the receiving end.

MPPC Microsoft Point-to-Point Compression

Data compression process.

MPPE Data encryption process.

MSN Multiple Subscriber Number

For a BRI in Euro-ISDN. The MSN is a complete telephone number that can be used to establish a connection with a single endpoint on an ➤➤ **S_0-Bus**. An MSN has up to eight digits, e. g. 49 911 7654321, where the 7654321 refers to the MSN.

Usually three call numbers are assigned to each ISDN-BRI.

Multiprotocol router A ➤➤ **Router** that can route several protocols, e. g. ➤➤ **IP**, ➤➤ **IPX** etc.

NAT Network Address Translation

Intended to reduce the need for globally unique IP addresses. Used as a security mechanism in **BinGO!**. A complete network is concealed to the outside. The IP addresses of all devices in ones own network remain confidential, only one IP address is made known to the outside.

NetBIOS Network Basic Input Output System

An applications programming interface (API) which activates network operations on a PC running under Microsoft´s DOS. It is a set of commands that is issued by the applications program to transmit and receive data to another host on the network.

Netmask The second part of an address in an IP network which leads to the identification of the host, e. g. 255.255.255.0. See also ➤➤ **IP address**.

Network address A network address is the network part of an IP address, the latter part of the IP address refers specifically to the host.

NTBA Network Termination for Basic Access.

An NTBA adaptor of an ➤➤ **ISDN Basic Rate Interface** is a device that provides the interface between the private network (➤➤ **S_0-Bus**) and the public ISDN network. In Germany, this can be ordered from Deutsche Telekom AG.

OSI model OSI=Open System Interconnection

Reference model of the ➤➤ **ISO** for networks. Defines a network model to help manufacturers of computer software and hardware create interoperable network implementations..

OSPF Open Shortest Path First

Routing protocol used in networks to exchange information (routing tables) between ➤➤ **Routers**.

PABX Private Automatic Branch Exchange

A telephone exchange operated in an organization with ➤➤ **S_0 interface** and ➤➤ **1TR6** or other manufacturer-specific ➤➤ **D-channel protocols** on the user side.

An ISDN PABX system allows the setting up of an internal telephone infrastructure where both analog and digital terminals can be connected. Each terminal receives its own extension number. Extension systems allow internal connections without connecting with the telephone service provider. Not all BinTec routers include an extension system.

PAP Password Authentication Protocol

Authentication process for connecting over ➤➤ **PPP**. Functions like ➤➤ **CHAP** except that the user name and password are not encoded before being transmitted to the partner.

Ping Packet Internet Groper

A program used to test reachability of destinations by sending them an echo request and waiting for a reply.

Point-to-multipoint A connection in which a single-source end-system connects with multiple destination end-systems.

Point-to-point A dedicated data link between two end-systems.

Port In/output.

By means of the port number, it is decided to which service (telnet, WWW) an incoming data packet should be sent.

PPP Point-to-Point Protocol

A protocol suite for transmitting datagrams over serial ➤➤ **Point-to-Point links**. PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits. Multiprotocol packets are uniformly encapsulated (➤➤ **Encapsulation**) before transmission. Establishing a connection involves a range of components and protocols, such as the authentication mechanisms ➤➤ **PAP/CHAP**.

PPP Authentication Security mechanism. A method of authentication using passwords in ➤➤ **PPP**.

Primary Rate Interface (PRI) An ISDN user interface. The PRI consists of a D-channel and 30 B-channels (Europe). (In America: 23 B-channels and a D-channel.) Compare ➤➤ **ISDN Basic Rate Interface**.

Protocol Protocols are used to define the manner and means of information exchange between two systems. Protocols control and rule the course of data communication on several levels (decoding, addressing, network routing, control procedures etc.).

Proxy ARP ARP=Address Resolution Protocol

A procedure of finding out the ➤➤ **MAC-Adresse** of a host whose ➤➤ **IP-Adresse** is known.

Remote access When an opposite station is not in your own local network and is acccessed over a WAN connection (via **BinGO!**).

Remote CAPI BinTec´s own ➤➤ **CAPI** interface.

The Remote CAPI interface allows all users of a network to use CAPI services, while only one ISDN connection is required (over **BinGO!**), providing all users have installed the necessary software that supports the CAPI interface. This standard interface is used by most communications applications. **BinGO!** is shipped with a suitable software package (RVS-COM Lite).

The CAPI interface from BinTec is implemented as a dual mode CAPI. Parallel to one another, CAPI 1.1 and 2.0 applications can use ISDN resources. Thus, in addition to old programs based on CAPI 1.1, it is possible to operate new CAPI 2.0 programs parallel in the network or on the same PC.

RIP Routing Information Protocol

Routing protocol used in networks to exchange information (routing tables) between ➤➤ **Routers**.

RJ45 Connector for a maximum of eight wires. Connection for a digital terminal.

Router A device which makes decisions about which of several paths network (or Internet) traffic will follow. Routers operate on layer 3 of the ➤➤ **OSI Model**.

Routers are able to recognise blocks of information and evaluate addresses (as opposed to a ➤➤ **Bridge**). By using routing tables, the best paths are chosen. In order to keep the routing tables up to date, routers exchange information between themselves about routing protocols, (e.g. ➤➤ **OSPF**, ➤➤ **RIP**).

Modern routers, such as **BinGO!**, are ➤➤ **Multiprotocol routers** and thus capable of routing several protocols (e g. IP and IPX).

S_0 bus All ISDN leads and wires and the ➤➤ **NTBA**. All S_0 buses consist of a four-wire telephone cable. The lines transmit digital ISDN signals. The S_0 begins at the NTBA and can be up to 150m long. Any ISDN devices can be operated on it. However, only two devices can use the S_0 at any one time as only two ➤➤ **B-channels** are available.

S_0 connection see ➤➤ **ISDN Basic Rate Interface**

S_2M connection see ➤➤ **Primary Rate Interface**

Server A server offers services that ➤➤ **Clients** avail of. Often refers to a certain computer that provides a function to a network, e. g. DHCP server.

In client-server architecture, a server is the software part that provides functions in the service of clients, e. g. ➤➤ **TFTP server**. In such a case, the server is not necessarily a computer server.

Setup Tool Menu-driven tool for the configuration of **BinGO!**. The Setup Tool can be used as soon as the router has been accessed (serial, ➤➤ **isdnlogin**, ➤➤ **LAN**).

Short hold Refers to the cutting of a connection after a predefined amount of time has elapsed subsequent to the last exchange of data. Short hold can be set statically (fixed amount of time) and dynamically (according to the charging unit).

SNMP Simple Network Management Protocol

A protocol in the ➤➤ **TCP/IP Protocol suite** used to send and retrieve management-related information across a TCP/IP network. One component of the SNMP management system is ➤➤ **MIB**. Different network components can be configured, controlled and administrated from one system over SNMP. Such an SNMP tool is included in your router: the ➤➤ **DIME Browser**. As SNMP is a standard protocol, you can use any other SNMP managers, such as HP-OpenView.

SNMP shell Input level for SNMP commands.

SOHO Small Offices and Home Offices

STAC Data compression procedure

Subnet A working scheme that divides a single logical network into smaller physical networks to simplify routing.

Switch LAN switches are network components similar in function to ➤➤ **Bridges** or even ➤➤ **Routers**. They exchange data packets between input and output ports. In contrast to bridges, switches have several input and output ports. Thereby, the bandwidth in the network increases. Switches can also be used to translate between different fast networks (e. g. 100MBit and 10MBit networks.

Switched line A connection is *established on demand* by dialing the number, as opposed to a ➤➤ **Fixed line**.

Synchronous transmission A method of data transmission by which time intervals between transmitted signals are exactly the same in length. As opposed to ➤➤ **asynchron**.

TAPI Telephony Application Program Interface

Standardised software interface used by many telephony programs. Telephony programs enable databank-supported telephoning on the PC. An example is the program orgAnice that can be found on the BinTec Companion CD. TAPI-services are only supported by routers with integrated ➤➤ **PABX**.

All users of a network can use TAPI services via BinTec´s Remote TAPI.

TCP Transmission Control Protocol

Belongs to the ➤➤ **TCP/IP** protocol suite for the connection of Wide Area Networks (➤➤ **WANs**).

TCP/IP Transmission Control Protocol/Internet Protocol

A protocol suite for the connection of Wide Area Networks (➤➤ **WANs**). The two parts of this protocol suite are ➤➤ **IP** (layer 3 of the OSI model) and ➤➤ **TCP** (layer 4 of the OSI model).

Telematics Telematics refers to a combination of telecommunication and computer technology and describes data communication between systems and devices.

Telnet Protocol from the ➤➤ **TCP/IP protocol suite**. Telnet enables communication with a distant terminal in the network.

TFTP Trivial File Transfer Protocol

TFTP server software is a part of ➤➤ **DIME Tools**. It is used for the transfer of configuration files and software to and from the router.

UDP User Datagram Protocol

A transport protocol similar to ➤➤ **TCP**. Unlike TCP, UDP provides no acknowledgements or guaranteed delivery for datagram exchange, but is, however, faster than TCP.

V.42bis Data compression procedure.

VJHC Data compression procedure. IP header compression.

WAN Wide Area Network

WAN interface WAN interfaces connect the local network with the (➤➤ **WAN**). Usually by means of analog or digital telephone lines (➤➤ **Switched** or ➤➤ **Fixed lines**).

WAN partner Remote station that is reached over a ➤➤ **WAN**.

X.21 The X.21 recommendation describes the physical interface between two DTEs in circuit-switched data networks (e. g. Datex-P).

X.25 An internationally agreed standard protocol defined for the interface of a data terminal device, such as a computer, to a packet-switched data network.

Extended Feature Reference

Version 1.2
Document #71050A

February 1999

NOTE

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

This manual provides a complete description of all the complex, separately licensable features available for the BinTec BIANCA/BRICK and BinGO! routers. The information included in this manual is compatible with software version 4.9.

While every effort has been made to ensure the accuracy of all information in this document, BinTec Communications AG assumes no liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document.

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

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

- lb -am

BinTec Communications AG February 1999

CONTENTS

Contents

Introduction

OSPF

RADIUS

Token Authentication Firewall

Virtual Private Networking

X.25

Frame Relay

1

INTRODUCTION

What's covered

How to contact BinTec Communications

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

How to get the latest software and documentation

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

- User documentation for your BinTec software/hardware.
- System software for you BRICK or BinGO router.
- Release notes for upgrading your system software.
- Windows software and UNIXTools applications.

About your User Documentation

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

This document describes extended features available on BIANCA/BRICK and BinGO! routers that require a separate software license. Depending on your particular product some of the features described in this document may not be available on your system. For information regarding which supplemental features can be licensed for your product consult your local BinTec product distributor.

What's covered in this guide

Chapter 1 Introduction is this chapter.

Chapter 2 OSPF describes using the Open Shortest Path First interior routing protocol on your BinTec router.

Chapter 3 RADIUS descirbes using your BinTec router as a RADIUS Client.

Chapter 4 Token Authentication Firewall describes Token Authentication Firewall support on your BinTec router.

Chapter 5 Virtual Private Networking describes using your BinTec router to implement Virtual Private Networking.

Chapter 6 X.25 describes operating your BinTec router in an X.25 environment.

Chapter 7 Frame Relay describes using your BinTec router as Frame Relay router.

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.

Visual Clues	
	Marks the beginning of a list of steps required to configure a 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.
Bold italic type represents special system table names.
Text enclosed in a box like this SYSTEM represents a submenu or menu command found in Setup Tool.

2

OSPF

What's covered

In this chapter we'll describe the Setup Tool menus and settings you'll see while using Setup Tool to configure the OSPF protocol on your router.

After that, we've included an overview of the OPSPF protocol as well as an example OSPF installation using different BinTec routers.

Setup Tool Menus

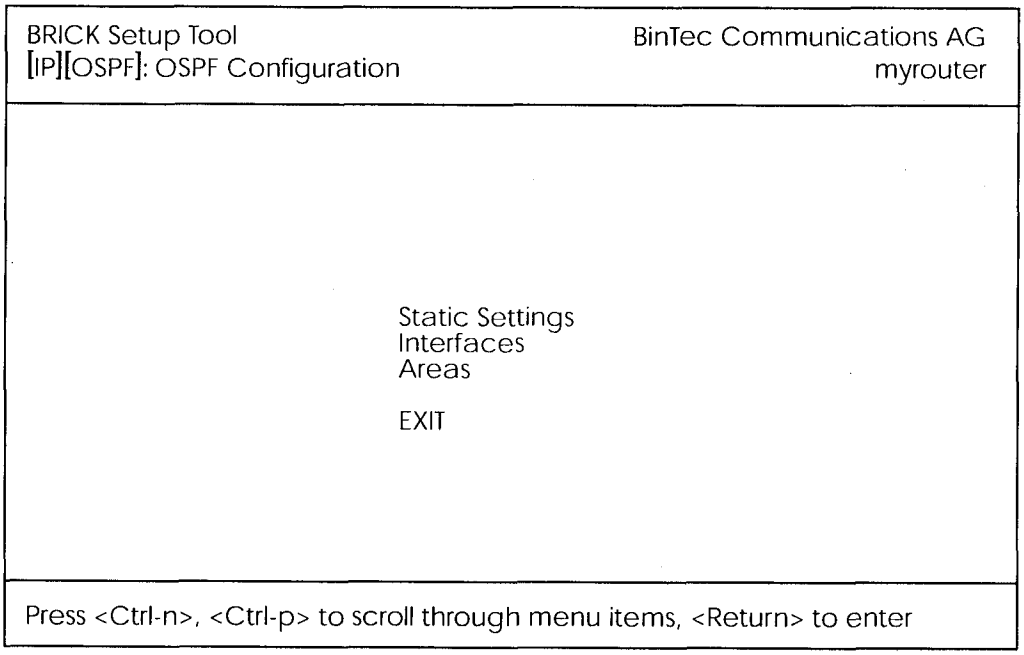
After entering **setup** from the shell prompt Setup Tool's Main Menu is displayed as below. Depending on your hardware setup and software configuration your router's menu may differ slightly.

```
BRICK Setup Tool                                BinTec Communications AG
                                                              myrouter


Licenses                    System

Slot1:          CM-BNC/TP, Ethernet
Slot2:          CM-2XBRI, ISDN S0, Unit 0
                CM-2XBRI, ISDN S0, Unit 1
Slot3:          CM-1BRI, ISDN S0

WAN Partner
IP      IPX     X.25

Configuration Management
Monitoring and Debugging
Exit

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

This is the starting point for all OSPF settings.

IP → OSPF →

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



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

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

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

IP → OSPF → STATIC SETTINGS

This menu contains global settings for the OSPF protocol.

```
BRICK Setup Tool                              BinTec Communications AG
[IP][OSPF][STATIC]: OSPF Static Settings                      myrouter

OSPF                                          disabled
Generate Default Route for the AS             no

                        SAVE                  CANCEL

Use <Space> to select
```

OSPF = Used to enable or disable OSPF. A valid license is also required before OSPF can be used on the router.

Generate Default Route for the AS = When set to yes the router advertises a default route over all active OSPF interfaces (See the "Admin Status" field in the IP → OSPF → INTERFACES menu.).

Note: Special consideration should be made when deciding which router is to provide a default route. This router should have the appropriate routes so that it can properly handle traffic for the AS.

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

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

IP → OSPF → INTERFACES

This menu lists the router interfaces OSPF can be configured for. By default, all IP compatible interfaces (present at the
time OSPF was enabled) are added to this list and are placed in the passive state.

To configure an interface, scroll to the appropriate entry and hit enter. The fields shown in the resulting EDIT menu shown below can be configured separately for each interface.

```
BRICK Setup Tool                                BinTec Communications AG
[IP][OSPF][INTERFACE][EDIT]: Configure Interface en1                myrouter

        Admin Status                    active (propagate routes + run OSPF)
        Area ID                         0.0.0.0

        Metric Determination            auto (ifSpeed)
        Metric (direct routes)          10

        Authentication Type             none
        Authentication Key

        Import indirect static routes   no

                    SAVE                        CANCEL

Use <Space> to select
```

Admin Status = The status of an OSPF interface defines whether routes and/or OSPF protocol packets are propagated over the interface.

If OSPF hasn't been enabled yet only the Admin Status field is displayed (in which case changes are irrelevant).

OSPF routers propagate a Router Link (RL), one per Area, which identifies the router's interfaces in that Area. Both active and passive interfaces are identified in the RL. Status may be active, passive, or off with the following results:

Active OSPF is running over this interface.

Passive OSPF is not running over this interface. OSPF protocol packets are neither sent or received over the interface, however this interface may be included in other Router Links.

Off OSPF is not running over this interface and this interface is not included in Router Links.

Note:  Once an interface is placed in the active state (and saved to memory), OSPF connections may be established over the interface resulting in appropriate costs for dial-up interfaces.

Area ID = Identifies the Area this interface is assigned to.

Metric Determination = Determines how the metric for this interface is calculated. This is the cost of the link that is propagated via link state advertisements.

Determination	Meaning
auto	The metric = the value of the base metric which is based on the bandwidth (***ifSpeed***) of the interface.
fixed	The metric defined (configurable) in the following field is always used (no adjustment).
auto + adjust[1]	When the dial-up interface is in the up state, the metric = <*base metric value*> – 10. Otherwise, metric = <*base metric value*>.
fixed + adjust[a]	When the dial-up interface is in the up state the metric = <*base metric value*> – 10. Otherwise metric = <*base metric value*>.

1. Only valid for Dial-up interfaces.

Metric = Identifies the base metric value, or cost of this interface. For auto determination values (see above) the actual metric used is adjusted starting a base metric value which is a simple function of the band-

width of the physical medium. All interfaces (except leased line interfaces) use the function.

$$\text{Base Metric Value} = \frac{\mathbf{1000{,}000{,}000}}{\textit{<bandwidth in bps>}}$$

This results in 10 for ethernet, 6 for token ring, and 1562 for dialup ISDN interfaces (1 B-Channel). Note that for dialup interfaces the Base Metric Value changes dynamically as ISDN channels are added/removed while the link is up. For leased line interfaces the base metric is equivalent to the result of the same function less 20 (i.e., 1542 for one leased B-Channel, 781 for two B-channels).

For **fixed determination** values (see previous field) the base metric value can be configured here.

Authentication Type = The type of authentication to use when sending (or verifying incoming) OSPF packets via this OSPF interface. This determines how the key in the Authentication Key field is used.

By default this is set to none. With simple, Key is transmitted as a text string in each packet. With md5, Key is used to create (verify) an encrypted digest which is sent with each packet.

Authentication Key = A text string to use in connection with the Authentication Type set above.

Import indirect static routes = If set to no (default) only direct routes for this interface are propagated over active OSPF interfaces (See the Admin Status field). When set to yes, indirect static routes are also propagated over active interfaces and are contained in external advertisements.

Note: 
Although practical for sites using WAN interfaces without transfer networks caution should be made to avoid routing loops when importing indirect static routes.

IP → OSPF → AREAS

This menu lists the OSPF Areas known to the router. Before a router interface can be assigned to an Area, the Area ID must first be added here.

The exception is the backbone area which is automatically generated at boot time if no other area is configured and which all interface assignments default to if not explicitly assigned. To edit area-specific settings select the Area ID and hit enter.

```
BRICK Setup Tool                              BinTec Communications AG
[IP][OSPF][AREA][EDIT]: Area Configuration                    myrouter

        Area ID                                 0.0.0.0

        Import external routes                  no
        Import summary routes                   no
        Create area default route (only ABR)    no

        Area Ranges >

                        SAVE                CANCEL

Enter IP address (a.b.c.d or resolvable hostname)
```

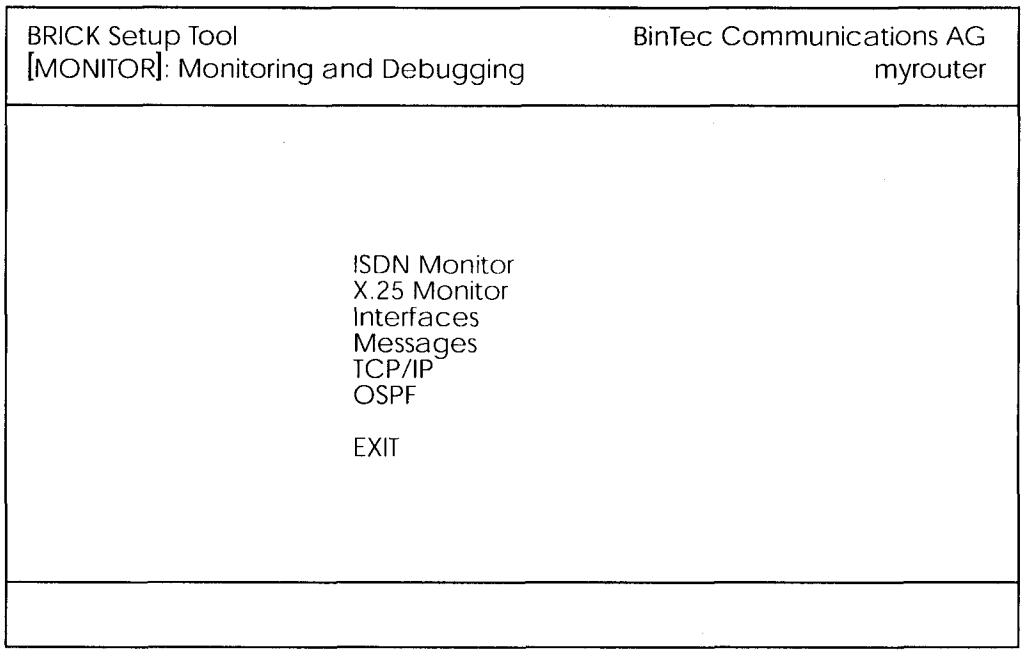
Area ID = Identifies the OSPF Area this entry corresponds to. The backbone area is 0.0.0.0.

Import external routes = Specifies whether external routes should be imported for this area. When set to no, this Area is defined as an OSPF Stub Area.

Area Ranges = This submenu specifies IP Address ranges for route condensation among areas.

MONITORING AND DEBUGGING →

This menu consists of several submenus which allow you to monitor the router's 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 router's 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.

MONITORING AND DEBUGGING → OSPF

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

```
BRICK Setup Tool                                  BinTec Communications AG
[MONITOR][OSPF]: OSPF Monitor                                     myrouter

Interface       DR              BDR             Admin Status    State
en1             192.168.30.1    192.168.30.0    active          BDR
brickxs         0.0.0.0         0.0.0.0         active          PTP

Neighbor        Router ID       Interface       Retx Queue      State

192.168.30.1    10.0.1.1        en1             0               full
12.0.0.2        11.0.0.2        brickxs         0               full

Area        Type          Link State ID   Router ID       Sequence     Age
0.0.0.0     Summary Net   10.0.0.0        10.0.1.1        0x80000003   1641 =
0.0.0.0     Network Link  192.168.30.1    10.0.1.1        0x80000001   361  |
11.0.0.0    Router Link   11.0.0.2        11.0.0.2        0x80000009   1    |
11.0.0.0    Summary Net   0.0.0.0         192.168.40.3    0x80000001   2    v
EXIT

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

Interfaces Section

The Interfaces section lists all enabled OSPF interfaces (interfaces that have NOT been turned "off" in the IP-OSPF-INTERFACES menu.)

Interface = The router interface the entry corresponds to.

DR = The Designated Router's IP address on this interface (A DR is not shown for Point-To-Point interfaces).

BDR = The Backup Designated Router's IP address on this interface (A BDR is not shown for Point-To-Point interface.).

Admin Status = Only active and passive interfaces are shown here (See the IP → OSPF → INTERFACES menu on page 9).

State = The OSPF status (***ospfIfState***) of the interface shown here may be:

down	OSPF is not running on this interface.
wait	The initial phase of OSPF where DR and BDR are determined.

PTP	The interface is a Point-To-Point interface. No DR or BDR is shown.
DR	The router is the Designated Router for this interface.
BDR	The router is the Backup Designated Router for this interface.
DRother	Another router is the DR/BDR for this interface.

Neighbour Section

The Neighbour section lists the OSPF neighbour routers that have been identified via the HELLO protocol.

Neighbor = The neighbour router's address on this interface.

Router ID = The neighbour router's system wide Router ID.

Interface = The router interface this router was identified over.

Retx Queue = The size of the retransmission queue for this neighbour. This is the number of advertisements that need to be sent to (and acknowledged from) this neighbour.

State = The state of OSPF with this neighbour router may be:

init	The initial phase. A HELLO packet was received from this neighbour.
twoWay	Bidirectional communication with the neighbour. Transmitted HELLO packets have been accepted by the neighbour router (parameters are correct).
EXstart	The exchange of Database Description Packets between the router and neighbour has begun.
exchange	Actively exchanging Database Description Packets with the neighbour router.
loading	The router and the neighbour router are now exchanging Link State Advertisements.
full	The router and neighbour routers' Link State Database are now synchronized.

LSDB Section

The Link State Database section lists the headers for all Link State Advertisements (LSA).

Area = The Area database to which this LSA belongs.

Type = The type of LSA. Five types of LSAs exist: Router Link, Network Link, Summary Link, Summary ASBR, and AS External.

Link State ID = The LSA's Link State ID. The Link State ID's meaning depends on the Type of advertisement.

Router ID = Identifies the router that generated this LSA.

Sequence = This advertisement's sequence number. Sequence numbers allow routers to determine if their database is current or if needs to request an update.

Age = The age (in seconds) of this LSA.

Overview of the OSPF Protocol

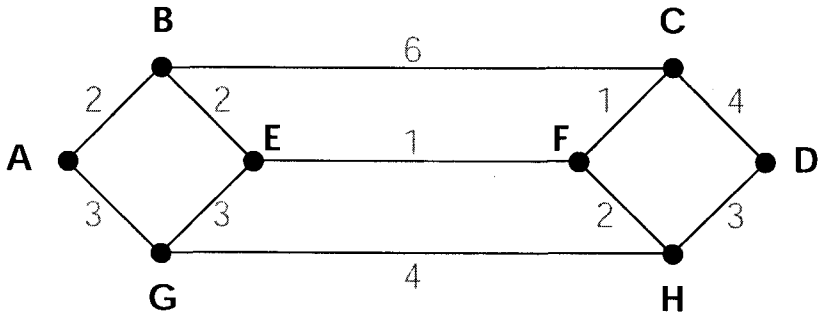
OSPF (Open Shortest Path First), is an interior routing protocol that is often used by larger network installations as an alternative to RIP. It was originally designed to address some of the limitations of RIP (when used in larger networks). Some of the problems (with RIP) that OSPF addresses include:

- **Faster Network Convergence**
  Changes in routing information are propagated immediately when changes occur and not periodically as with RIP.
- **Reduced Network Load**
  After a brief initialisation phase, routing information does not need to be refreshed as in RIP where the entire routing table is broadcast every 30 seconds.
- **Routing Authentication**
  Routers advertising OSPF routes can be authenticated.
- **Routing Traffic Control**
  OSPF areas can be closed to limit the amount of traffic resulting from routing advertisements.
- **Link-Costs**
  When calculating a route's cost OSPF can account for the different transport mediums such as LAN or WAN links.
- **No hop-count limitations**
  In RIP, routes spanning more than 15 hops are unreachable.

Although the OSPF protocol is more complex than RIP the basic concept is the same; the best interface must be calculated for forwarding packets to a particular station.

Shortest Path Routing

With RIP, routes are measured and selected according to number of hops it takes for a packet reach it's destination. In the diagram below, each node represents an IP router. According to RIP, the best route for a packet travelling from A to C will always be ABC.



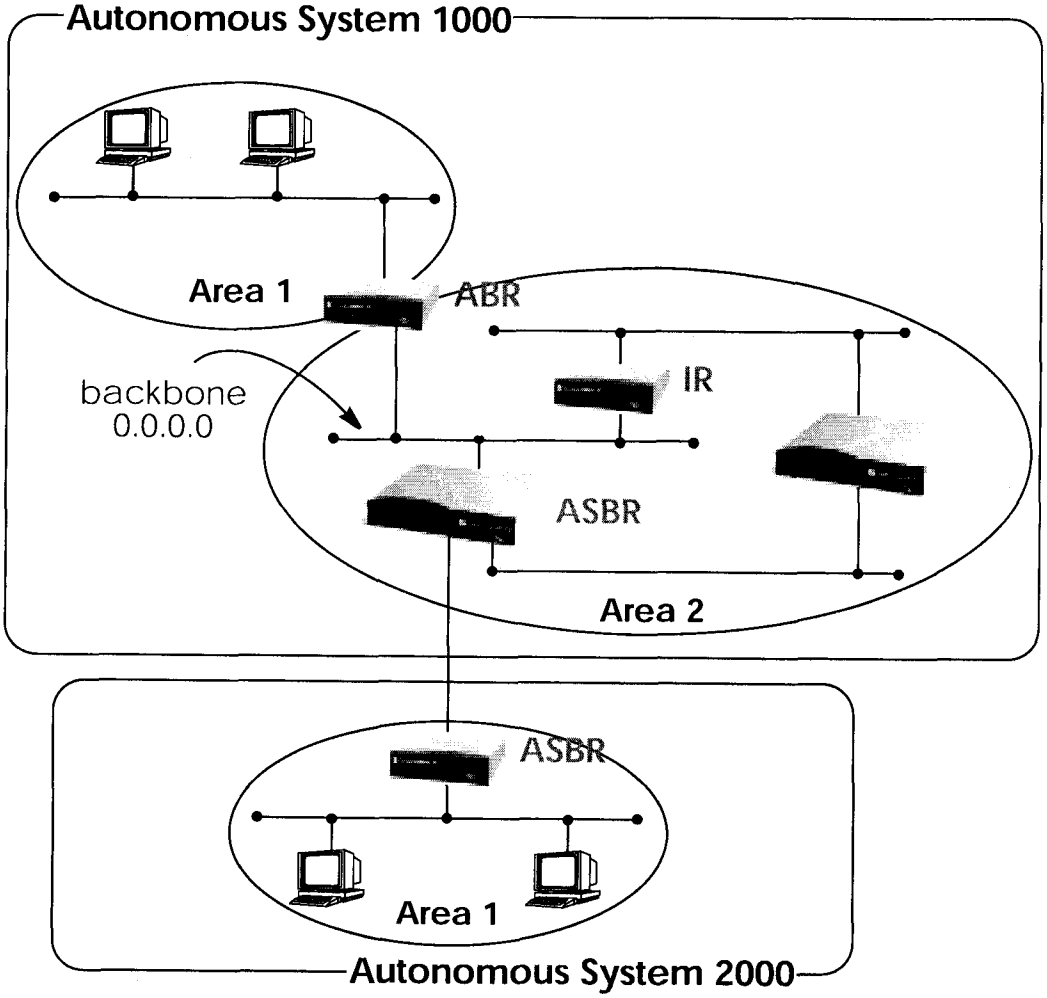
In OSPF each link has a cost associated with it (typically some fixed number divided by the bandwidth of the link). Routes are calculated and selected according to the least cost of the overall path a packet will travel. Thus in shortest-path routing the best path is also the fastest path (theoretically), regardless of the number of stations a packet travels through.

Assuming the relative costs of the links in the diagram above (shown in blue), according to OSPF the best route for a packet travelling from A to C is ABEFC (cost = 6). This route requires 4 hops as opposed to the 2 hop route (ABC) selected.

OSPF Routers and Link State Advertisement

OSPF is based on a concept of Areas. An Autonomous System (AS) consists of one or more Areas defined by network management. An Area may contain of one or more IP networks.

If an AS does contain more than one area one must be designated as the backbone, area: 0.0.0.0. All Area Border Routers (see Router Types) in an AS must have a physical connection to the backbone.

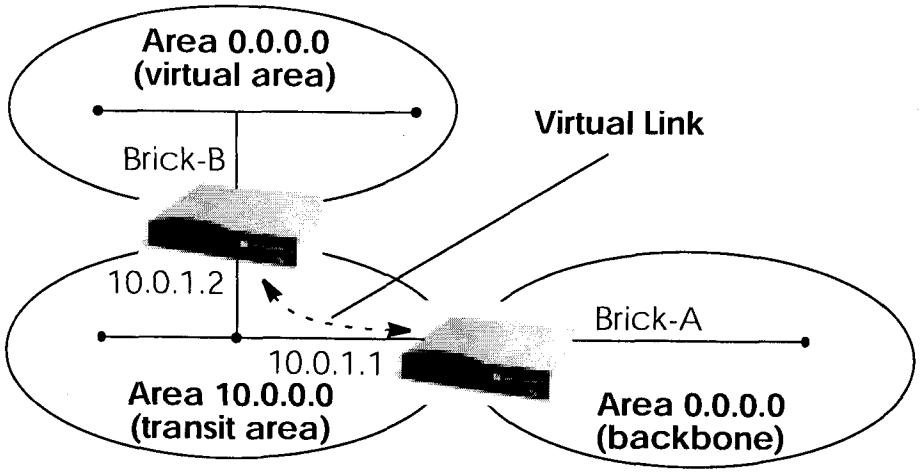


Any of the routers shown above could additionally be the Designated Router or Backup Designated Router for its respective network.

OSPF Virtual Links

Note that in OSPF the backbone, Area 0.0.0.0, is the center for all areas in the Autonomous System. However, sometimes it's not possible to physically connect all areas to the backbone. By configuring a "Virtual Link" between two area border routers a remote area an still be assigned to the backbone.

As shown in the diagram below. a virtual link is established between two Area Border Routers that share a common area; called the "transit area". Both routers must be physically connected to the backbone.



Router Types

The location of a router's interfaces with respect to an area determines the type of router it is and the types of Link State Advertisements it exchanges with other routers in that area.

- **Internal Routers** (IR) – A router whose interfaces are within the same area. All Internal Routers compute the shortest path tree to all destinations within its area.
- **Area Border Router** (ABR) – A router with interfaces in different areas but within the same autonomous system. Topological information is gathered (and stored) for each attached area allowing the ABR to compute the shortest path tree for each area separately.

- **Autonomous System Border Router** (ASBR) – A router that acts as a gateway between OSPF and external routes (i.e., routes provided by other routing protocols, static indirect routes, etc.). These routers propagate routes to external networks.
- **Designated Router** (DR) – On broadcast networks (token ring and ethernet) where more than two routers are present only the DR needs to synchronise its link state database with other routers.
- **Backup Designated Router** (BDR) – A backup router assumes the responsibilities performed by the DR if that system goes down.

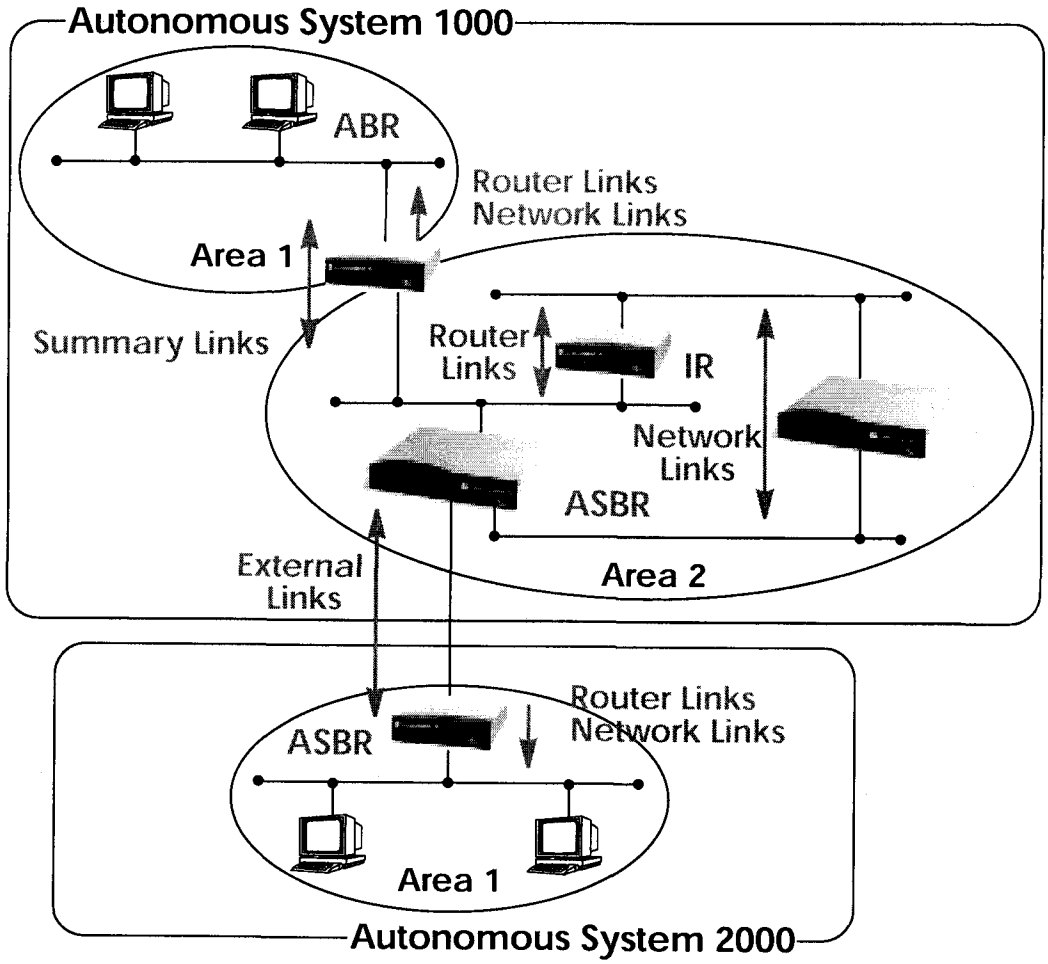
Link State Advertisement Types

OSPF routers exchange routing information via **Link-State Advertisements** (LSAs) that contain information about the networks that can be reached over the router's interfaces.

Link State Advertisements are broken down into five different types shown in the table below. The example network shown on the previous page is redisplayed below and shows where the different types of LSAs would be found in an OSPF network.

LSA Type	Purpose:
Router Links	**Generated by**: ALL OSPF Routers **Purpose**: Contains information regarding the state of a router's interfaces within a particular area. Router Links are only flooded within a single area.
Network Links	**Generated by**: The DR (or BDR). **Purpose**: Identifies all OSPF routers present on the network segment and their state. These links are only flooded within a single area.
Summary Links	**Generated by**: Area Border Routers **Purpose**: Identifies the presence of networks within an AS but outside the (local) area. Provides Inter-Area routes allowing routers to learn of networks in other Areas but within the AS.

LSA Type	Purpose:
ASBR Summary Links	**Generated by**: An Area Border Router. **Purpose**: A special type of summary link that provides routes to Autonomous System Border Routers allowing other routers in the AS to find their way out of the system.
External Links	**Generated by**: An Autonomous System Border Router. **Purpose**: Contains information about other Autonomous Systems and allows routers to learn about routes to networks there. External links are flooded into all areas except stub areas.



Router Identification

All OSPF routers in an Autonomous System must have a unique Router ID that identifies the router with respect to the AS. Generally an OSPF router's Router ID is taken to be the highest IP address for its first LAN interface.

Initialization

OSPF networks are said to be much "quieter" in comparison to RIP based networks. This is because in OSPF once the initialization phase is com-

plete routing information is only exchanged when link state changes occur. This is much different than with RIP where every 30 seconds a router's complete routing table is broadcast and verified over the network.

The initialization phase of OSPF is completed once the Link State Database for the area has stabilized and generally occurs once:

1. The OSPF Neighbors have been identified.
2. The Designated and Backup Designated Routers have been established.

Neighbor Identification

When first coming into service an OSPF router attempts to identify its neighbor OSPF routers using the HELLO protocol. Two router are neighbors if they:

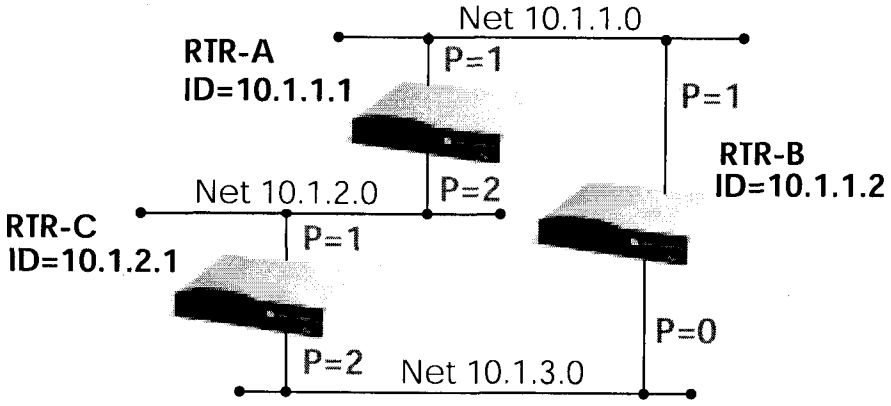
1. Share a common network.
2. Are using the same Area Number for that segment.
3. Are using the same Authentication for the segment.
4. Are using the same parameters (HELLO interval, etc.).

Neighbor routers then decide whether to synchronise their Link State Database (LSDB) with one another. All routers on the segment synchronise their LSDBs with the Designated Router (DR) and the Backup Designated Router (BDR).

Designated/Backup Designated Router Election

When Neighbor routers are identified (via the HELLO protocol) the DR and BDR are also identified. This is sometimes called DR and BDR election and is achieved via IP multicast packets which a router broadcasts via each network segment. For each segment the router with the highest

OSPF priority generally becomes the DR. In case of a tie, the router with the higher Router ID becomes the DR.



The DR and BDRs for the three networks shown above would be elected as follows.

Network	DR	BDR
10.1.1.0	RTR-B	RTR-A
10.1.2.0	RTR-A	RTR-C
10.1.3.0	RTR-C	RTR-B

Building up the LSD and the STP

Link-State Advertisements, contain information about a routers interfaces (i.e.; link's IP address, mask, network type, networks reachable over the link, etc.).

All routers within an area receive all link-state information for all routers in the area. Once synchronized each router has an identical image of the link state database that describes the topological structure of the area.

This database allows each router to separately calculate a **shortest path tree** (SPT), using itself as the root, to any destination in the area. The SPT is used to determine the best interface to route packet. As in RIP the lowest cost route is used however the cost to a destination is calculated differently. In OSPF the cost (or metric) of a link is a function of the bandwidth provided by the link. The higher the bandwidth, the lower the cost.

Authentication

OSPF allows packets containing OSPF routing information to be individually authenticated. Two authentication methods are available which must be configured separately for each network segment.

1. Simple (password) authentication
   A simple text string is sent with each packet. This method is less secure since packet contents can be "sniffed" off the wire using a link analyzer.
2. MD5 (cryptographic) authentication
   When MD5 (Message Digest) is used each packet is appended with a 16 byte encrypted digest. The digest is a function of an authentication key and the contents of the packet. This method is more secure since the key is not sent with the packet.

Note: With MD5 authentication only the digest is encrypted and not the actual contents of the OSPF packet.

OSPF over Demand Circuits

Although OSPF generates less network traffic than RIP, the occasional exchange of routing information (HELLO packets, Link State Database updates or changes, etc.) can lead to increased costs for dial-up interfaces.

To help minimize these costs OSPF on the BRICK has been implemented to include special extensions for Demand Circuits as defined in RFC 1793, *OSPF over Demand Circuits*. These extensions allow for efficient use of dial-up interfaces with OSPF and avoiding excessive ISDN costs. In particular, this means:

1. The exchange of HELLO packets between neighbours is suppressed once the BRICK has synchronized its LSDB with that neighbour (A dial-up connection is initially opened to synchronize the database.).
2. Link State advertisements are only flooded to neighbour routers when an actual change needs to be propagated.
   Each LSA is marked with a special DoNotAge flag (identifiable by the DC-bit of the LSA or OSPF packet).

Note: This feature should only be used if all routers in the AS support this feature (RFC 1793) since some routers don't acknowledge the DC-bit (or use it differently). This could result in unwanted ISDN connections or connections.

Note: If a router without RFC 1793 support is removed from the domain in which this feature has been used it is recommended that all OSPF routers be briefly deactivated and re-activated to ensure that all LSAs generated by the removed router are actually flushed.

Example OSPF Installation

A typical network installation showing how OSPF could be put to use is shown in the diagram on the following page. Highlights for this setup are shown below. Following the diagram is a Configuration Overview and following that a detailed listing of the configuration steps is povided for each router.

Area 11.0.0.0 (stub area)

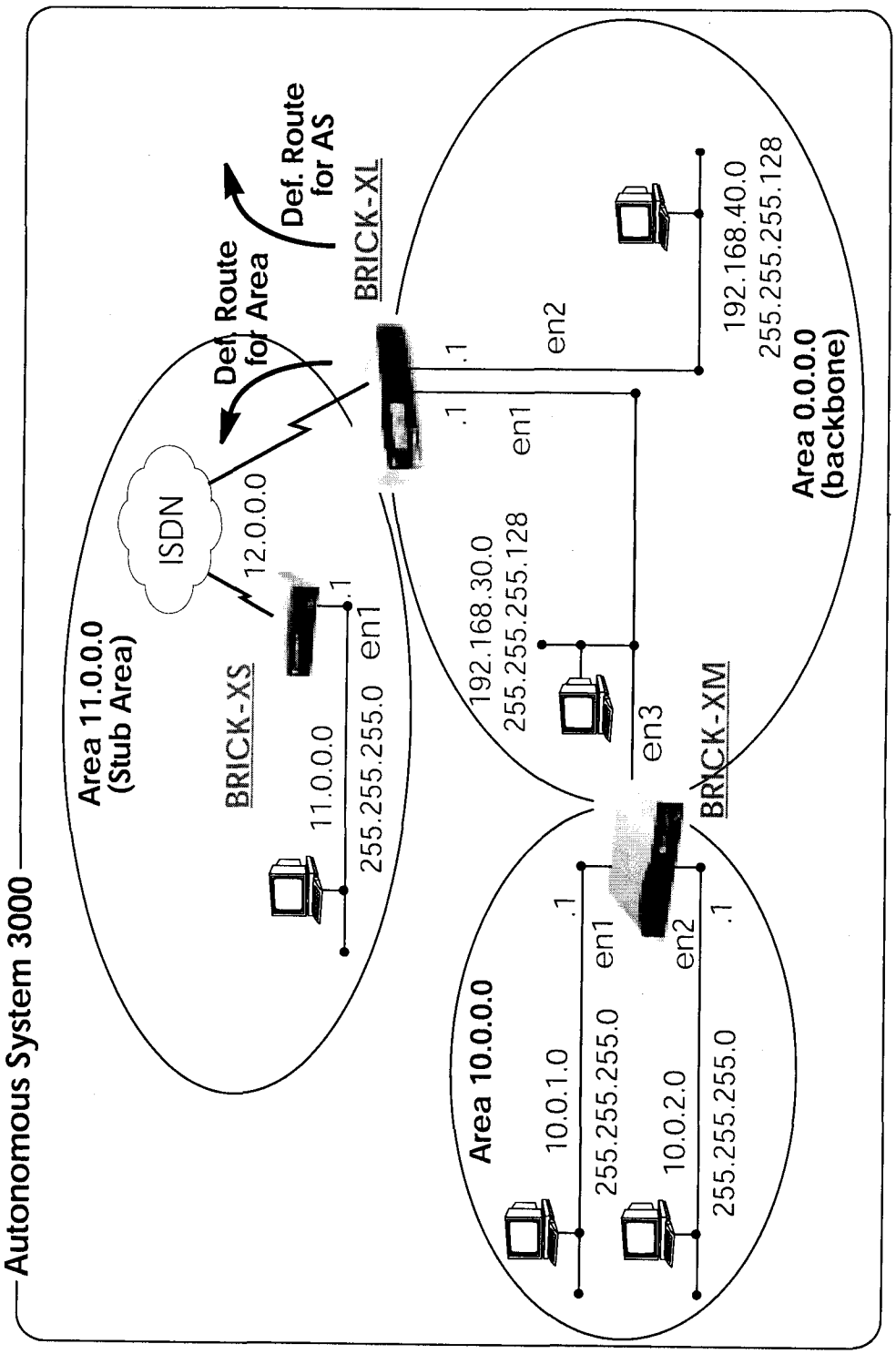
- Since the remote LAN in Area 11.0.0.0 is linked to the backbone via an ISDN dialup link this area is config ured as a stub area. This means that external routing in formation advertisements won't flow into this area. The default route for this area is provided by the router BRICK-XL.
- Because OSPF on the BRICK includes support for Demand Circuits (RFC 1793) the dialup link is only opened when changes in routing information must be propagated.

Area 0.0.0.0 (backbone)

- Area 0.0.0.0 is the backbone of the Autonomous System. The router at BRICK-XL will provide the default route for the entire AS and a default route for Area 11.0.0.0.

Area 10.0.0.0

- Area 10.0.0.0 is connected to the backbone via the border router BRICK-XM. Since this is the only link between networks in this area and any external networks (such as the Internet) BRICK-XM will provide Summary Links to routers in other areas. This means that routing information about networks in Area 10.0.0.0 will be combined (or aggregated) into a single advertisement. This lessens the amount of traffic on the backbone and keeps the size of the link state database for area 0.0.0.0 small.



Configuration Overview

All BRICKs:

1. A valid OSPF license must be installed. This can be added to the *biboAdmLicenseTable* or from Setup Tool's LICENSES → menu.
2. OSPF must be enabled by setting *ospfAdminStat* to **enabled**, or from Setup Tool's IP → OSPF → STATIC SETTINGS → menu.

BRICK-XL Overview (details):

1. Create the dial-up partner interface to BRICK-XS.
2. Have BRICK-XL advertise the default route for the AS.
3. Create the Area entry for Area 11.0.0.0.
4. Assign the new dialup partner interface to Area 11.0.0.0 and set the interface to active.
5. Verify ethernet interfaces en1 and en2 are assigned to Area 0.0.0.0 and set both interfaces to active.

BRICK-XS Overview (details):

1. Create the dial-up partner interface to BRICK-XL.
2. Create the Area entry for Area 11.0.0.0.
3. Assign the ethernet interface (en1) to Area 11.0.0.0 and set the interface to active.
4. Assign the new dial-up interface to Area 0.0.0.0 and set the interface to active.

BRICK-XM Overview (details):

1. Create the Area entry for Area 10.0.0.0.
2. Assign ethernet interfaces en1 and en2 to Area 10.0.0.0 and set both interfaces to active.
3. Verify ethernet interface en3 is assigned to Area 11.0.0.0 and set the interface to active.
4. Create the OSPF aggregate for the LANs attached to en1 and en2 to reduce the routing traffic sent over en3.

Configuration Steps for BRICK-XL

1. Assuming an OSPF license is installed and OSPF has been enabled the partner interface to BRICK-XS should be created. Note that our example uses a transfer network (network 12.0.0.0).
2. Since BRICK-XL should advertise the default route for the AS set this field to yes in IP → OSPF → STATIC SETTINGS →.

```
BIANCA/BRICK-XL Setup Tool                    BinTec Communications AG
[IP][OSPF][STATIC]: OSPF Static Settings                      BRICK-XL

OSPF                                  enabled
Generate Default Route for the AS     yes

                    SAVE                    CANCEL

Enter IP address (a.b.c.d or resolvable hostname)
```

3. In the IP → OSPF → AREAS → menu create an entry for Area 11.0.0.0. Define this area as a Stub Area and have BRICK-XL generate the default route for this area.

```
BIANCA/BRICK-XL Setup Tool                    BinTec Communications AG
[IP][OSPF][AREA][ADD]: Area Configuration                     BRICK-XL

Area ID                               11.0.0.0

Import external routes                no
Import summary routes                 no
Create area default route (only ABR)  yes

Area Ranges >

                    SAVE                    CANCEL

Enter IP address (a.b.c.d or resolvable hostname)
```

4. In the IP → OSPF → INTERFACES → menu locate the dialup interface entry created in step 1 and hit enter to edit the settings.

   Set the Admin Status to active and assign it to Area 11.0.0.0 (or the area created in step 3) and select SAVE.

```
BIANCA/BRICK-XL Setup Tool                    BinTec Communications AG
[IP][OSPF][INTERFACE]: Configure Interface BRICK-XS              BRICK-XL

      Admin Status                  active (propagate routes + run OSPF)
      Area ID                       11.0.0.0

      Metric Determination          auto (ifSpeed)
      Metric (direct routes)        1562

      Authentication Type           none
      Authentication Key

      Import indirect static routes no

                    SAVE                CANCEL

Use (Space) to select
```

   By default, dial-up interfaces are set to passive in the Admin Status field.

5. In IP → OSPF → INTERFACES → menu verify the ethernet interfaces en1 and en2 are assigned to the backbone, (Area 0.0.0.0 which is the default area).

   Set the Admin Status to active and assign it to Area 11.0.0.0 (or the value from step 2) and select SAVE.

Configuration Steps for BRICK-XS

1. Assuming an OSPF license is installed and OSPF has been enabled the dial-up partner interface to BRICK-XL should be created. In our example a transfer network (12.0.0.0) is used.
2. In the IP → OSPF → AREAS → menu create Area 11.0.0.0. and define it as a Stub Area.

```
BIANCA/BRICK-XS Setup Tool                    BinTec Communications AG
[IP][OSPF][AREA][ADD]: Area Configuration                    BRICK-XS

    Area ID                                   11.0.0.0

    Import external routes                    no
    Import summary routes                     no
    Create area default route (only ABR)      no

    Area Ranges >

                        SAVE                  CANCEL

Enter IP address (a.b.c.d or resolvable hostname)
```

3. In the IP → OSPF → INTERFACES → menu assign the ethernet interface (en1) to Area 11.0.0.0 and make sure the Admin Status is set to active.

```
BIANCA/BRICK-XS Setup Tool                    BinTec Communications AG
[IP][OSPF][INTERFACES] Configure Interface en1               BRICK-XS

    Admin Status                              active (propagate routes + run OSPF)
    Area ID                                   11.0.0.0

    Metric Determination                      auto (ifSpeed)
    Metric (direct routes)                    10

    Authentication Type                       none
    Authentication Key

    Import indirect static routes             no

                        SAVE                  CANCEL

Use (Space) to select
```

4. In IP → OSPF → INTERFACES → menu locate the dialup interface (created in step 1) and assign the interface to Area 11.0.0.0 (or the value used in step 2).

   Set the Admin Status for the dialup interface to active and select SAVE.

```
BIANCA/BRICK-XS Setup Tool                          BinTec Communications AG
[IP][OSPF][INTERFACES] Configure Interface dialup                   BRICK-XS

                    Admin Status          active (propagate routes + run OSPF)
                    Area ID               11.0.0.0

                    Metric Determination  auto (ifSpeed)
                    Metric (direct routes) 1562

                    Authentication Type   none
                    Authentication Key

                              SAVE              CANCEL

Use (Space) to select
```

Configuration Steps for BRICK-XM

1. An OSPF license must already be installed and OSPF should been enabled IP → OSPF → STATIC SETTINGS → menu.

   Then create an area entry for Area 10.0.0.0 in the IP → OSPF → AREAS → menu.

```
BIANCA/BRICK-XM Setup Tool                    BinTec Communications AG
[IP][OSPF][AREA][ADD]: Area Configuration                    BRICK-XM

    Area ID                          10.0.0.0
    Import external routes           yes

    Area Ranges >

                      SAVE                CANCEL

Enter IP address (a.b.c.d or resolvable hostname)
```

2. In the IP → OSPF → INTERFACES → menu assign ethernet interfaces en1 and en2 to Area 10.0.0.0 (or the value from the previous step) and set the Admin Status for each interface to active.

```
BIANCA/BRICK-XM Setup Tool                    BinTec Communications AG
[IP][OSPF][INTERFACES] Configure Interface en1              BRICK-XM

    Admin Status                     active (propagate routes + run OSPF)
    Area ID                          10.0.0.0

    Metric Determination             auto (ifSpeed)
    Metric (direct routes)           10

    Authentication Type              none
    Authentication Key

    Import indirect static routes    no

                      SAVE                CANCEL

Use (Space) to select
```

3. Ethernet interface en3 should already be assigned to the backbone, Area 0.0.0.0 which is the default.

   In the IP → OSPF → INTERFACES → menu verify this setting and change the Admin Status to active.

4. Return to the IP → OSPF → AREA → menu and scroll to the Area ID entry for the backbone and hit enter.

   Move to the AREA RANGES → submenu to add an OSPF aggregate for the LANs attached to en1 and en2. The Address and Mask entries shown below will match any routes with a destinations starting with 10, or 10.*.*.*.

```
BIANCA/BRICK-XM Setup Tool                    BinTec Communications AG
[IP][OSPF][AREA][RANGE][ADD]: Configure Address range for Area  BRICK-XM

Address                    10.0.0.0
Mask                       255.0.0.0

Advertise Matching         yes

        SAVE                    CANCEL

Enter IP address (a.b.c.d or resolvable hostname)
```

   This entry means that BRICK-XM will consolidate multiple routes (routes for destinations in Area 10.0.0.0) into a single link state advertisement.

   This will effectively reduce the amount of traffic sent over the backbone as will help keep the size of the link state database and routing tables for routers in other areas to a minimum.

Configuring OSPF Virtual Links

A virtual interface must be defined on each of the ABRs by creating an entry in the ***ospfVirtIfTable***. This is done by setting the ***ospfVirtIfNeighbor*** and ***ospfVirtIfAreaID*** objects.

ospfVirtIfNeighbor should be set to the Router ID of the Area Border Router at the oher end of the virtual link.

ospfVirtIfAreaID should be set to the area ID of the transit area.

The virtual link in the diagram here would be configured on Brick-A as follows.

```
BRICK-A:system> ospfVirtIfTable

inx AreaId(*rw)          Neighbor(*rw)       TransitDelay(rw)
    RetransInterval(rw)  HelloInterval(rw)   RtrDeadInterval(rw)
    State(ro)            Events(ro)          AuthKey(rw)
    Status(-rw)          AuthType(rw)

BRICK-A:ospdVirtIfTable> AreaID=10.0.0.0 Neighbor=10.0.1.2
```

This creates a new OSPF virtual interface (on BRICK-A) that links two parts of the backbone via the transit area 10.0.0.0. The respective interface would be created on BRICK-B using almost the same command (***ospfVirtIfAreaID***=10.0.0.0 ***ospfVirtIfNeighbor***=10.0.1.1)

Remember that the area being used as the transit area must already be defined in the ***ospfAreaTable***.

Controlling Link State Database Overflow

Sites with large (or complicated) network installations that are running OSPF may notice the Link State Database (LSDB) becoming large. Most often this is the case where external routes are being imported as external advertisements.

One way to minimize the size of the LSDB (on the BRICK) is to use the ***ospfExtLsdbLimit*** variable. This object defines the maximum number of external LSAs to store in the database (the local copy).

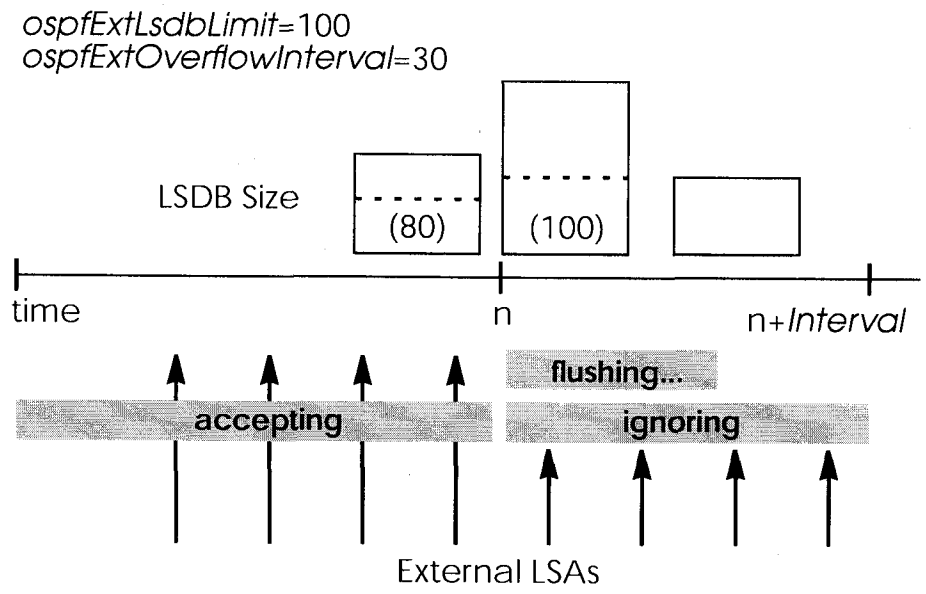
Once the limit is reached the BRICK goes into Overflow State. In Overflow State two things happen:

1. The BRICK begins to flush all external advertisements generated locally.
2. The BRICK ignores all new external advertisements.

NOTE: The maximum size of the LSDB must be the same for all OSPF routers in the domain for this feature to perform efficiently.

By default the BRICK remains in overflow state but can optionally be configured to leave overflow state (and continue to process new external LSAs) automatically after a time period. The ***ospfExtOverflowInterval*** variable defines the number of seconds to wait before leaving overflow state automatically. The default is 0 seconds (i.e., stay in overflow state). After waiting ***ospfExtOverflowInterval*** seconds the number of external LSAs in the LSDB is compared to the ***ospfExtLsdbLimit***. If there is room in the database for new LSAs the BRICK yc leaves overflow state; otherwise another time interval is waited.

The diagram shown below attempts to illustrate the behavior of database overflow control using the ***ospfExtLsdbLimit*** and ***ospfExtOverflowInterval*** variables.



Enabling Demand Circuit Support

Demand Circuit support for dial-up partner interfaces is enabled by default when an existing interface is enabled for OSPF (AdminStatus is set to active). Support can be manually controlled by setting the interface's ***IfDemand*** object (***ospfIfTable***) to "true" or "false". When set to false, the state of this interface is always up.

Setting this variable to true for one side of the connection is sufficient (that is, as long as OSPF has been enabled on both sides, i.e., ***ipExtIfOspf***=active) if both sides support RFC 1793.

Note: Until a neighbour router has been identified HELLO packets are periodically transmitted (default, ***ospfIfPollInterval*** = 120 seconds) over the interface. This results in the link being opened. Once the LSDB has been synchronised, the HELLO protocol is then suppressed.

Import - Export of Routing Information

When different routing protocols are used within the same domain it is sometimes useful to be able to exchange (import or export) routing information between these protocols.

Using the ***ipImportTable*** routing information generated by one protocol (***ipImportSrcProto***) can be imported or exported to another protocol (***ipImportDstProto***).

Currently the following ***SrcProto***↔***DstProto*** combinations are possible.

	ipImportDstProto	
	rip	ospf

ipImportSrcProto \ ipImportDstProto		
default_route		✓[1]
direct		
static		✓[2]
rip	–	
ospf	✓[3]	–

1. ***ipImportSrcProto***=default_route ***ipImportDstProto***=ospf
   This entry forces an external Link State Advertisement to be generated that defines a default route for the Autonomous System.
2. ***ipImportSrcProto***=static ***ipImportDstProto***=ospf
   With this entry statically configured indirect routes will be propagated via OSPF as external LSAs.
3. ***ipImportSrcProto***=ospf ***ipImportDstProto***=rip
   With this entry, all routes learned via OSPF are imported to RIP. If an OSPF route changes the import to RIP will triggered an immediate broadcast of the entire routing table.

The remaining fields of ***ipImportTable*** allow for further control of how (and what) routing information is imported.

- ***ipImportMetric1***
  The metric in the context of the destination protocol the imported routes should get. If sset to -1 these routes get a protocol specific default metric.
- ***ipImportType***
  This object might define protocol specific properties of the imported routes in the context of the destination protocol.
- ***ipImportAddr***
  Specifies (together with ***ipImportMask***) the range of IP addresses for which the table entry should be valid. The entry is valid if the destination IP address of the route lies in the range specified by both objects. If both objects are set to 0.0.0.0, the table entry will be valid for destination.

- ***ipImportMask***
  Together with ***ipImportAddr*** specifies the range of IP addresses for which the table entry should be valid. For example, if Addr=X.X.0.0 and Mask=255.255.0.0 then addresses X.X.0.0 through X.X.255.255 are valid.
- ***ipImportEffect***
  Defines the effect of this entry. If set to "import", importation from ***SrcProto*** to ***DstProto*** takes place. If set to "doNotImport" importation is prevented.
- ***ipImportIfIndex***
  Specifies the interface index of the interface for which the entry should be valid. If set to 0 the entry is valid for all interfaces.

3

RADIUS

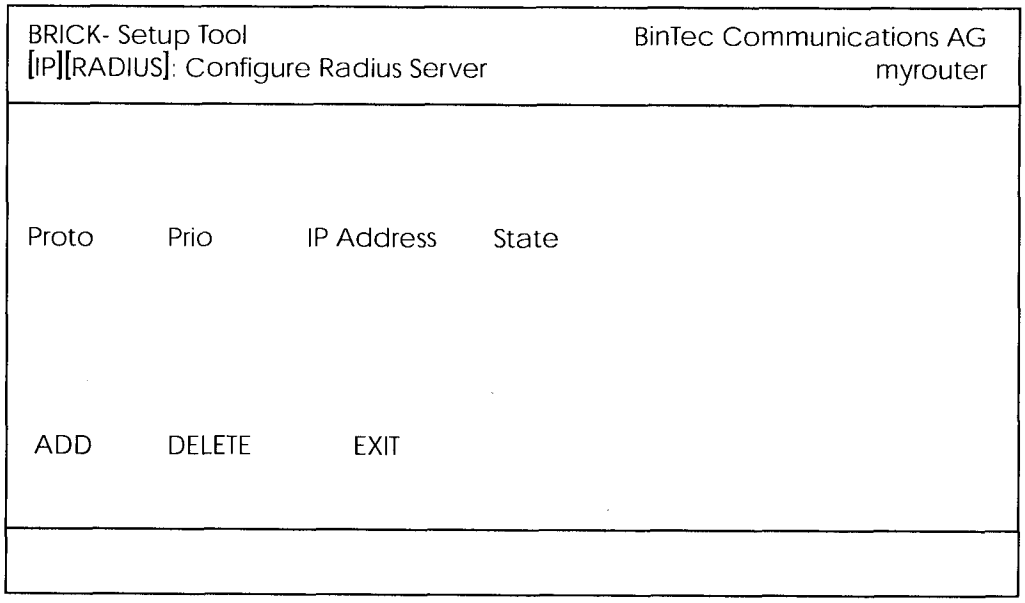
What's covered

In this chapter we'll cover all of the menus and settings you'll see while using Setup Tool to configure your router as a RADIUS Client for authentication and accounting.

Setup Tool Menus

IP → RADIUS SERVER

This menu lists all RADIUS Servers currently configured on the router.



IP → RADIUS SERVER →

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

For each Radius Server you can configure the following parameters:

Protocol = Use this RADIUS Server for authentication purposes (**auth**) or for accounting ISDN connections (**acct**).
When you configure a RADIUS Server for accounting, the BRICK transmits Start and Stop Radius packets for each ISDN connection to this server.
Default value: auth

IP Address = IP Address of the RADIUS Server.

Password = Shared secret between RADIUS Server and BRICK.

Priority = 0 ... 7. When there are several RADIUS Server entries, the server with the lowest priority entry is used first. If there is no reply from this server, the server with the next lowest priority entry is used,

```
BRICK Setup Tool                          BinTec Communications AG
[IP][RADIUS][EDIT]: Configure Radius Server              myrouter

Protocol                auth

IP Address              44.55.66.77
Password                blubb

Priority                0
Policy                  authoritative

Port                    1812
Timeout                 1000
Retries                 1
State                   active

                SAVE                              CANCEL

Use <Space> to select
```

and so forth, i.e. servers with *Priority*=**0** have the highest priority.
Default value: 0

Policy = can be set to **authoritative** or **non-authoritative**. If set to authoritative, a negative answer to a request will be accepted. This is not necessarily true when set to **non-authoritative**, where the next radius server will be asked until there is finally an **authoritative** server configured.
Default value: authoritative

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

Timeout = 50 ... 50000, number of milliseconds to wait for an answer to a request.
Default value: 1000 (1 second)

Retries = number of retries if a request is not answered. If after *Retries* attempts still no answer was received, the server *State* is set to **inactive**. The BRICK then tries to contact the Server every 20 seconds, and once the Server replies, the *State* is changed to **active** again.
Default value: 1

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

RADIUS Overview

RADIUS (Remote Authentication Dial In User Service) is a client/server protocol originally developed by Livingston Enterprises. RADIUS provides a security system that allows you to exchange authentication and configuration information between a Network Access Server, such as the BRICK, and a RADIUS Server, a PC or UNIX machine running a RADIUS daemon process. The RADIUS server maintains a database of user authentication data and configuration information.

RADIUS Packets

Types	Sent from -to	Purpose
ACCESS_REQUEST	Client-Server	When a connection request is received on the BRICK the RADIUS server is polled if a locally defined PPP partner could not be found (i.e., Upon receiving the calling partner's PPP_ID and no local record exists for the PPP partner.).
ACCESS_ACCEPT	Server-Client	If the RADIUS Server authenticates the information contained in the ACCESS_REQUEST packet, it sends an ACCESS_ACCEPT packet to the RADIUS Client that contains the link setup parameters to use.
ACCESS_REJECT	Server-Client	If the information contained in the ACCESS_REQUEST packet doesn't match the information in the RADIUS Server's user database (usually /etc/raddb/users) the Server may deny access to the network.

RADIUS Server Files (UNIX)

File	default location	Remarks
radiusd	/etc/raddb/	The RADIUS daemon on UNIX systems.
dictionary	/etc/raddb/	The dictionary file lists the RADIUS attributes the daemon process supports and defines each attributes default behaviour.
clients	/etc/raddb/	The clients file defines the list of hosts that are allowed to request authentication information from the server. Each entry typically contains the RADIUS client's host name and password, (also called the Client-Key).
users	/etc/raddb/	The users file contains user-authentication information for (dial-in) hosts that will be establishing connections via the RADIUS Clients. The file consists of user-profiles (also referred to as authentication-lines) that 1. define requirements for authenticating callers (password, PPP ID, Calling Line) and, 2. define the type of connections to establish if the user was successfully authenticated.
logfile	/etc/raddb/	The logfile contains error messages from the radiusd process on UNIX hosts.
detail	/usr/adm/radacct/<client>/	The detail file contains RADIUS accounting information records submitted by RADIUS clients. <*client*> in the pathname to this file is usually the host name of the RADIUS client.

Standard RADIUS Attributes

Your router supports the following standard RADIUS attributes. Also a couple of BinTec-specific options have been added, to facilitate using your router in conjunction with RADIUS servers.

Note, however, that the BinTec-specific options are only available if you use the *dictionary* file included on the Companion CD (the file is also available from our WWW server).

The following standard RADIUS attributes are available.

RADIUS Attribute	Type	R / A	Remark
User-Name	string	REQ	User name, mandatory inband: PPP partner name outband: PPP partner telephone number
User-Password	string	REQ	Password for PAP authentication
CHAP-Password	string	REQ	Password for CHAP authentication
NAS-Identifier	string	REQ	sysName of the BRICK
Service-Type	integer	ANS	Framed (for PPP) Callback-Framed (for PPP with Callback)
Framed-Protocol	integer	ANS	inband: PPP outband: PPP, X25, X25-PPP, IP-HDLC, IP-LAPB, MPR-LAPB MPR-HDLC, FRAME-RELAY, X31-BCHAN, X75-PPP, X75BTX-PPP, X25-NOSIG, X25-PPP-OPT
Framed-IP-Address	ipaddr	ANS	Partner IP address
Framed-IP-Netmask	ipaddr	ANS	Partner IP netmask
Framed-Routing	integer	ANS	None, RIPv1-Broadcast, RIPv1-Listen, RIPv1-Broadcast-Listen
Framed-Compression	integer	ANS	None, Van-Jacobson-TCP-IP
Framed-Route	string	ANS	You can create a route of the format ‹ipaddr›[/‹netmask bits›] ‹gateway› [‹metric1›...‹metric5›] e.g.: 192.2.3.4/24 193.141.54.1 1

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

The following RADIUS attributes are *not* yet applicable to your BRICK:

Acct-Authentic	CHAP-Challenge	Login-IP-Host
Acct-Delay-Time	Callback-Id	Login-LAT-Group
Acct-Input-Octets	Called-Station-Id	Login-LAT-Node
Acct-Input-Packets	Calling-Station-Id	Login-LAT-Service
Acct-Output-Octets	Filter-Id	Login-Port
Acct-Output-Packets	Framed-AppleTalk-Link	Login-Service
Acct-Session-Id	Framed-AppleTalk-Network	NAS-Port-Type
Acct-Session-Time	Framed-AppleTalk-Zone	Proxy-State
Acct-Status-Type	Framed-IPX-Network	Session-Timeout
Acct-Terminate-Cause	Framed-MTU	Termination-Action
		Vendor-Specific

BinTec Vendor Extensions

If you use the dictionary file mentioned above you can directly access and configure specific MIB tables via RADIUS.

The following options are available at the moment:

Option	Type	Mode
BinTec-biboPPPTable	string	static
BinTec-ipExtIfTable	string	static
BinTec-ipRouteTable	string	dynamic
BinTec-ipExtRtTable	string	dynamic
BinTec-biboDialTable	string	dynamic
BinTec-ipNatPresetTable	string	dynamic

Each of these options corresponds to a MIB table. You can modify values inside the table by using a syntax similar to the SNMP client shell of your BRICK:

<BinTec-Option> = "variable1=value1 ... variablen=valuen"

A few lines from a RADIUS setup file might look like this:

```
Service-Type = Framed,
BinTec-biboPPPTable = "DynShorthold=50 IpAddress=static",
BinTec-ipNatPresetTable = "Protocol=tcp extport=1050 intport=100"
```

When using these options please note:

- The *ifIndex* is automatically set for each table, you cannot influence it.
  There is, however, one exception to this rule: In the ***IpExtRtTable*** both the *DstIfIndex* and the *SrcIfIndex* are automatically set. You can set one of these to 0 if need be.
- The entries are not case-sensitive.

- You must not use blank spaces before or after »=« signs inside the double quotes.
- There are two different option modes, static, and dynamic.

  Static options modify existing table entries while dynamic options add a new table entry. Therefore all the variables you want to set in a dynamic option have to be included in one single line.

Partner Recognition via CLID

To identify RADIUS partners outband by their CLID (calling line identification, i.e. ISDN telephone number) there has to be a corresponding entry in the RADIUS database, e.g.

9119732123 *Service-Type = Framed,*
Framed-Protocol = IP-HDLC,
Reply-Message = "partner1"

Note that the phone number must be specified here exactly as it is signalled with the incoming call (you can see this in the *RemoteNumber* field of the ***isdnCallTable***).

When a call from this number comes in a new PPP entry is generated with *Encapsulation*=**ip_hdlc** and *ifDescr*=**partner1**.

Please also note that when using RADIUS inband authentication it can take up to 2 seconds to accept an incoming call if the RADIUS server is delayed inactive.

At the moment it is not possible to use both inband and outband RADIUS authentication at the same time for one connection.

Channel Bundling

You can now bundle several B channels to achieve a higher data throughput using the *Port-Limit* option.

Note: 
Certain RADIUS servers handle the setup of further B channels for a connection incorrectly.
This can result in very high charges!
So before using channel bundling for RADIUS make sure your RADIUS server is capable of handling it correctly.

RADIUS Table Entries

The *ifIndexes* of RADIUS PPP entries now start at 15001. They are not stored when saving your configuration.

Default RADIUS UDP Port

The default UDP port used for RADIUS authentication is 1645.

4

TOKEN AUTHENTICATION FIREWALL

What's covered

In this chapter we'll cover the configuration of TAF (Token Authentication Firewall).
We place emphasis on the configuration of the BRICK as ACE/Agent using the Setup Tool, describe the TAF client PC configuration and all related steps in setting up TAF.

Overview

Token Authentication Firewall (TAF) is an advanced feature for controlling access to central site computing resources that goes beyond the theoretical limitations of existing security mechanisms. TAF is a user oriented security system, which affords human interaction and by that grants that an authorized user is sitting in front of the remote host, which is connected to the central site. TAF can only be used to control IP traffic.

TAF login user verification is based on the established and well-respected Token-Card-ACE/Server solution provided by Security Dynamics.

You will need a special TAF license to use TAF on your BRICK. Along with this license you will get 10 *TAF Login* licenses for PCs you wish to use as TAF clients.

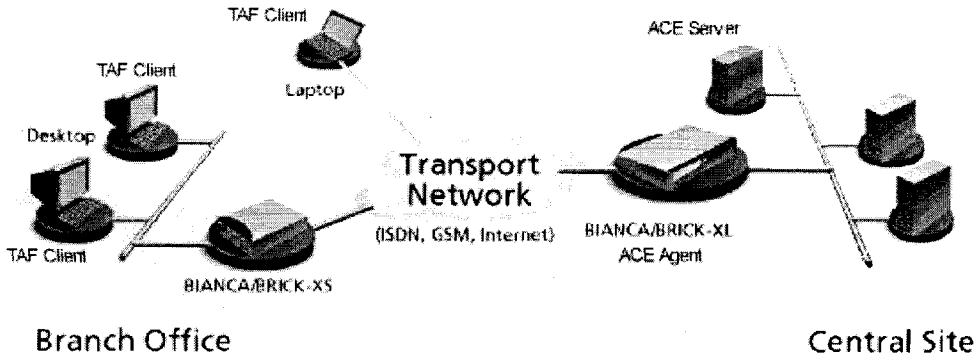


Figure 1: TAF Clients, ACE Agent and ACE Server

A security solution using TAF is made up of four components:

- an ACE/Agent by BinTec (BRICK-XL2, BRICK-XM with 2 MB flash or BRICK-XMP) in the central site
- an ACE/Server by Security Dynamics in the central site
- a Token Card by Security Dynamics for the user of the TAF client PC
- an application for the TAF client PC by BinTec (Windows 3.x, Windows 95/98 and Windows NT)

In this TAF security solution the BRICK as an ACE/Agent answers login attempts from a TAF client with a request for authentification. It then sends the user's response to the ACE/Server for verification. On the other hand the BRICK verifies the authenticity of the ACE/Server so that no other server can masquerade as an ACE/Server with the intention to acquire security data. Above that the BRICK encrypts and decrypts messages between the TAF client and the ACE/Server.

You must bear in mind that TAF can only authenticate IP connections.

Requirements

As a requirement for the TAF authentication procedure the four components (as mentioned above) must be established. Based on an existing WAN partner connection (Remote Client - LAN, LAN - LAN) the following conditions must be provided.

In the central site LAN an ACE Server must be set up and the central site's BRICK must be configured as an ACE/Agent to serve as remote access server to the central site's LAN.

The client side PC must have installed and configured the TAF login program and its user must be in possession of the Token Card, which generates one part of the password for the TAF login.

Figure 2: Token Card

Authentication

User authentication by the ACE/Server uses a "two factor" user authentication, i.e. the password consists of a static PIN, which is secret and

memorized by the user and of a second part, which is generated by the user's token card.

Encryption

Additionally two different encryption methods are used:

For the communication between ACE/Server and ACE/Agent (the BRICK of the central site) Node Secret, a string of pseudorandom data known only to the client (ACE/Agent) and the ACE/Server, is combined with other data to encrypt client/server communications.

For the communication between TAF client and ACE/Agent the BRICK generates a pair of keys (private key and public key), where the private key stays on the BRICK (ACE/Agent) and the public key is sent to the TAF client. By the help of these keys the transmission of authentication data is encrypted and the TAF client also uses them to check the identity of the central site.

Configuration of TAF

Configuring the ACE/Server

The following steps require that you have already installed an ACE/Server in your network. For instructions on how to install and configure the ACE/Server please refer to its manuals.

Please note that the ACE/Server configuration described in this document refers to ACE/Server Version 3.01.

On the ACE/Server you first have to configure the BRICK to act as a gateway for the TAF-protected network, and then you have to configure each user who will be authenticated.

Go to the Client menu of your Server administration tool and select Add Client.

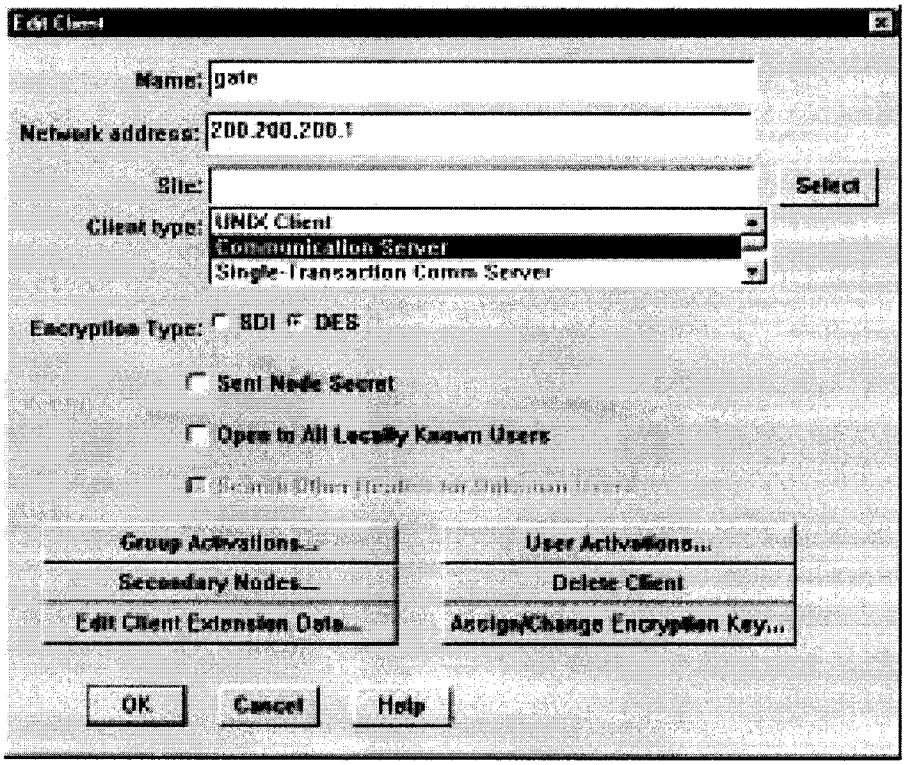


Figure 3: ACE/Server (Windows NT): Add Client

Now enter the name and network (IP) address of the BRICK, select *Communication Server* as the client type, and select the encryption type based on the client device configuration. Please note that the same encryption type must also be configured on the BRICK.

If you want to modify ACE/Server system settings under Unix—e.g. the port to use for communication with the BRICK (default: 5500)—you can use the **sdsetup -config** command. In most cases *no* changes are necessary.

When the server receives the first authentication request from the BRICK it will send a Node Secret, which is subsequently used to encode the messages exchanged between the ACE/Server and the BRICK.

The *Sent Node Secret* checkbox should not be selected. Once the Node Secret has been sent the corresponding check box in the dialog shown above will appear selected (for detailed information see *"Node Secret" on page 65*).

A detailed description of this dialog box and related configuration steps you can find in the ACE/Server Administration Manual.

If you haven't already done so you now have to import the Token Card information into your ACE/Server (see ACE/Server Administration Manual).

You should then enable the Token Cards, and synchronize them with the server.

You can now start adding users (TAF clients). For each user you have to enter his first and last name, login name, whether he will be allowed or required to create his own PIN and some other items. The final step is to assign a Token Card to the user.

After you have entered all users the server configuration is complete (for TAF purposes).

As already mentioned above, we recommend to refer to the ACE/Server's manuals for detailed information on the configuration of the ACE/Server.

Configuring the BRICK (ACE/Agent)

In the following the TAF configuration of the BRICK is described in detail.

The first part introduces the Setup Tool menus dealing with TAF and in a second part the necessary configuration steps are listed.

Setup Tool Menus

IP → **TOKEN AUTHENTICATION FIREWALL**

This menu consists of two submenus where Token Authentication Firewall relevant settings are configured.

```
BRICK- Setup Tool                                BinTec Communications AG
[IP][TAF]: Token Authentication Firewall                        myrouter

                              Interfaces
                              Server

                              EXIT

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

The **INTERFACES** menu is used to enable/disable SecurID support separately for each BRICK interface.

The **SERVER** menu is used for configuring SecurID Server relevant settings on the BRICK. These settings must correspond to the parameters configured on the ACE/Server.

IP → TOKEN AUTH. FIREWALL → INTERFACES

This menu lists the BRICK interfaces that may be configured for Token Authentication Firewall support. TAF can only be used on interfaces which have been explicitly enabled for use with SecurID.

Note: Typically, the SecurID Server (ACE/Server) is accessible via the BRICK's LAN interface. Authentication for this interface should be set to "off". Dial-Up interfaces used for accepting secure connections from TAF clients must be set to "SecurID".

```
BRICK Setup Tool                          BinTec Communications AG
[IP][TAF][INTERFACES]: Interface Configuration          myrouter

     Interfaces      Authentication
     Datex-P         off
     en1             off
     en1-snap        off
     sales-ppp1      SecurID
     sales-ppp2      SecurID

EXIT

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

By default, Authentication is disabled (set to "off") for existing BRICK interfaces.

To enable TAF support for an interface, select the interface and hit the <Enter> key. In the resulting menu ensure that Authentication is set to "SecurID" and select SAVE.

IP → TOKEN AUTH. FIREWALL → INTERFACES → EDIT

This menu is used for configuring interface specific settings for Token Authentication Firewall.

```
BRICK Setup Tool                                BinTec Communications AG
[IP][TAF][INTERFACES][EDIT]: Configure Interface sales-ppp2        myrouter

Authentication Type          SecurID
Life Time (seconds)          3600

Authentication Mode          strict
Keep Alives (seconds)        60

                SAVE                          CANCEL

Use <Space> to select
```

Authentication Type = This field is used to enable/disable TAF for the respective interface. By default Authentication Type is disabled (**off**). Setting to **SecurID** enables TAF for the interface.

Life Time (seconds) = The time in seconds to allow data traffic on this connection. 180 seconds before the Life Time expires a new passcode is requested.
Possible Values: 180 - 3600
Default Value: **3600**

Authentication Mode = The authentication policy used by the ACE/Server. If set to **strict** each source IP address must be authenticated separately. If set to **loose** all source IP addresses are allowed if at least one IP address was successfully authenticated on this interface.
Default value: **strict**

Keep Alives (seconds) = The interval in seconds after which a new keep-alive request is sent to the BRICK by the ACE/Server.
Keep-alive packets will never cause a new connection to be set up, nor will they affect the shorthold mechanism.

IP → TOKEN AUTH. FIREWALL → SERVER

This menu contains a list of the TAF servers currently configured. At the moment up to two active ACE/Servers (Master and Slave server) are supported.

By choosing ADD or EDIT you will get to the following menu, which contains the BRICK settings relevant to the configuration of the SecurID server (ACE/Server). The settings here must correspond to the values used by the ACE/Server.

NOTE: Under Unix the parameters to use here can easily be retrieved from the ACE/Server with the included **`sdinfo`** program. Refer to your ACE/Server documentation for information.

```
BRICK Setup Tool                                BinTec Communications AG
[IP][TAF][SERVER][ADD]: Configure TAF Server                    myrouter

                    Type                    ace
                    IP Address
                    Encryption              des
                    Priority                0
                    State                   active

                    Version                 7
                    Retries                 5
                    Timeout                 5

                    Server Port             5500
                    Client Port             5656
                    Node Secret             empty

                    SAVE        CANCEL      RESET NODE SECRET

Use <Space> to select
```

Type = The type of authentication server. Currently ACE/Server (**ace**) is the only type supported.

IP Address = The IP address of the authentication server.

Encryption = Specifies the type of encryption to use when communicating with the authentication server. For ACE/Servers this can currently be either des (Data Encryption Standard) or sdi (Security Dy-

namics proprietary) encryption.
Default value is **DES**.

Priority = The authentication server with the lowest priority value is the first used for requests. Use the value 0 for the master server and the value 1 for the slave server.

State = Either active or disabled.

Version = The file version number used by the authentication server.
Default value is **7**.

Retries = This is the number of times the BRICK will attempt to connect to the authentication server before reporting a connection failure.
Valid range is 1 - 6.
Default value is **5**.

Timeout = The time in seconds to wait for a reply from the authentication server before retrying. Valid range is 1 -20.
Default value is **5**.

Server Port = The port number to use for communication between the BRICK and the authentication server.
By default port **5500** is used.

Client Port = The port number to use for communication with TAF Clients.
Default port is **5656**.

Node Secret = Indicates whether the Node Secret has already been received by the BRICK (**received**) or not (**empty**).
The node secret is automatically generated by the ACE/Server and then transmitted to the BRICK. It is a password used to encode messages between the BRICK (ACE/Agent) and the ACE/Server). Usually the node secret is initially sent by the ACE/Server and after that the "Sent Node Secret" check box on the ACE/Server is automatically selected. See *"Configuring the ACE/Server" on page 58*.
You can use RESET NODE SECRET to momentarily clear the Node Secret on the BRICK. When the "Sent Node Secret" check box on the ACE/Server is cleared, the ACE/Server will transmit a new Node Secret at the next communication.
Whenever the BRICK receives a new Node Secret form the ACE/Serv-

er the ***tafServerTable***, where the Node Secret is stored, is saved to the flash ROM.

TAF Commands on the BRICK

makekey Command

`makekey [-g]`

The makekey command can be used to show the current public key (stored on the *biboAdmPublicKey* variable), or—when invoked with the **`-g`** option—to generate a new pair of keys (public and private).

You will only need to use **`makekey -g`** once before configuring TAF for a WAN partner for the first time.

shtaf Command

`shtaf`

The **shtaf** command can be used to test the TAF authentication procedure. The BRICK will prompt you for an ACE/Server user name and a passcode (the Token currently displayed on this user's Token Card).

If the authentication was successful, it will give you a normal BRICK login prompt. After logging in to the BRICK you can terminate *shtaf* by typing **exit**.

Configuration of the BRICK (ACE/Agent) via Setup Tool

We will assume that your BRICK is up and running, and that a TAF license is available.

Login to your BRICK as the *admin* user and start the Setup Tool (*setup*). Go to the [*IP*][*TAF*][*SERVER*] menu and [*ADD*] a new Server.

First you have to add a main ACE/Server.

Enter the ACE/Server's name or IP address and select the same encryption as configured on the Server. Make sure to use the correct (Config File) Version, Retries, and Timeout settings (you can obtain a list of the important Server settings under Unix by issuing the *sdinfo* command on your ACE/Server).

For normal applications it is advisable to use the default port setting (5500).

The Node Secret field is filled in automatically (see p. 64).

You can then, if necessary, add one slave server, which must be configured identically to the main server, only its *Priority* value must be set to **1** or higher (i.e. it gets a lower priority than the main server).

Exit the Setup Tool and execute the command **makekey -g** (see page 66). This will generate a pair of keys (public and private) which will be used to encode the authentication messages exchanged between the BRICK and the user's PC.

These steps only have to be taken once.

At this point you should test your configuration by executing the **shtaf** (see page 66) command on your BRICK. The BRICK will then contact the main ACE/Server and request you to enter a user name and passcode for authentication.

When the respective TAF client is part of a LAN, the remote BRICK , the gateway to the TAF client's LAN, must be configured as a WAN Partner. When you have TAF clients, which are single remote PCs (via modem or ISDN), then you have to create a WAN Partner entry for every PC that will be used to authenticate users.

For this WAN Partner only the IP protocol should be configured, because TAF can only authenticate IP packets. If you activate IPX or Bridging simultaneously, this traffic won't be verified by TAF.

After you made sure the connection works go to the [*IP*][*TAF*][*INTERFACES*] menu and select the interface you just created (interface name = WAN partner name). Switch Authentication Type to **SecurID**. Adjust the other three parameters if necessary for your application (for an explanation of the parameters please refer to page 63).

Repeat this procedure until all partners are configured.

System Logging Messages

Syslog messages are created during various events. TAF Syslog messages are reported on the BRICK under the INET subsystem. The following messages may be seen in connection with Token Authentication Firewall and SecurID.

biboAdmSyslogMessage (and Meaning)	***~Level***
TAF: new session for <IP addr> ifc <ifindex>›	Debug
TAF: delete session for ‹IP addr.›	Debug
TAF: set Authlifetime to <seconds> for <IP addr> ifc <ifindex>	Debug
TAF: allow auth packet from if <ifindex> prot <protocol> <IP addr> :<port>-><IP addr> :<port>	Debug
TAF: early request for ‹IP addr.› ifc ‹ifindex›	Info
TAF: life timer expired for ‹IP addr.› ifc ‹ifindex›	Info
Taf: mibio: ACE server ‹IP addr.› ignored - wrong Configuration *(The named server was deactivated, because its configuration was different to the configuration of the Master Server.)*	Err
Taf: mibio: ACE server ‹IP addr.› ignored - too many masters *(Two Master Servers have the same priority; one of them was deactivated.)*	Err
Taf: mibio: ACE server ‹IP addr.› ignored - too many slaves *(Two Slave Servers have the same priority; one of them was deactivated.)*	Err
Taf: mibio: Saving tafServerTable to the flash ROM *(The tafServerTable was automatically saved to flash ROM after the Node Secret had been transmitted. All changes, made to this table are still existent after the next reboot.)*	Notice
Taf: clienudp: Unable to create/bind ACE/Server socket - errno = ...	Err
Taf: clienudp: Unable to locate ACE/Server host - errno = ... *(There are no servers configured in the tafServerTable.)*	Err
Taf: clienudp: Unable to send to the ACE/Server - errno = ... *(Cannot send message to the ACE/Server; internal error.)*	Err
Tafd: PC Message corrupted *(The message from the client was wrong coded.)*	Notice
Tafd: decryption error 0x‹type› *(The message from the client was wrong coded.)*	Err
Tafd: encryption error 0x‹type› *(The message from the client was wrong coded.)*	Err

biboAdmSyslogMessage (and Meaning)	***~Level***
Tafd: no key for encryption *(You have to call "makekey -g" to generate a new key.)*	Err
Tafd: Request for token authentication ignored - no key available *(You have to call "makekey -g" to generate a new key.)*	Err
Tafd: TAF server unreachable *(The ACE/Server is unreachable/does not answer/ is not working.)*	Err
Tafd: No TAF License	Err
Tafd: Authentication result for <IP addr> ifc <ifindex>: <result>	Info
Tafd: Tafd: received <message type> Message from <IP addr> ifc <ifindex>	Debug
Tafd: Tafd: sent <message type> Message to <IP addr> ifc <ifindex>	Debug

Configuring the TAF Client PC

The TAF client application is a component of BinTec's BRICKware, which can be found on the BinTec ISDN Companion CD respectively can be downloaded from BinTec's Web Server at http://www.bintec.de (Section: FTP Server).You can install it together with BRICKware on the TAF client PC.

When you want to use TAF Login from a PC, you must select **TAF Login** in the **Components** list during the installation of BRICKware for Windows. In case you already have installed other components of BRICKware and want to add TAF Login, we recommend to reinstall all components of BRICKware (including TAF).

The TAF Login program will automatically be installed in your Autostart menu (eventually you must select this during installation). When the TAF Login is not automatically started after the installation is complete, you must select TAF Login from the BRICKware group in the Start menu. In the **Login** dialog box you must select **Configuration** to configure the Login program. In this dialog you enter the BRICK's (ACE/Agent of the central site LAN) **IP address** and can modify the **Listen Port** if necessary (the listen port setting on the PC must be identical to the setting on the BRICK). Above that you must initially enter the program's license key for

the TAF client, which is provided together with your BRICK's TAF license.

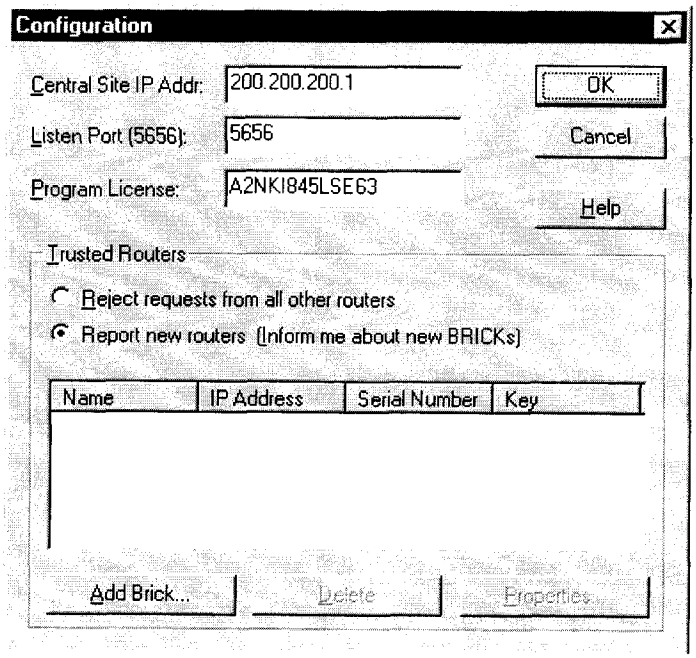


Figure 4: TAF Configuration

Repeat this procedure on each PC you want to use for TAF authentication purposes. Each PC needs his own TAF client license.

In the **Trusted Routers** group you can select, whether only to accept logins from trusted routers or also be notified, when a router not contained in the trusted routers list below, sends a login request. In the notification (shown below), you can then decide, whether to trust the new router. Trusted routers are displayed in the list at the bottom of the Trusted Routers group.

Using TAF Login

The TAF Login program is added to the Autostart menu and will remain in the background until it receives an authentication request from the remote LAN.

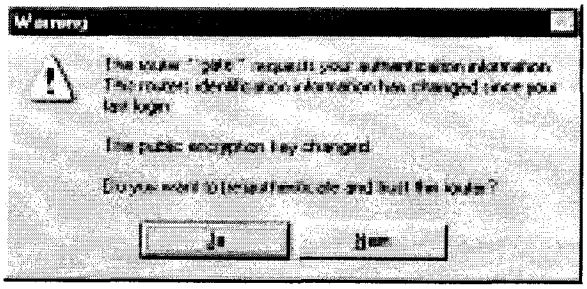


Figure 5: Notification about the login request of a not-trusted routers

You can also activate the program by double-clicking on the TAF icon in the task bar or by starting it from the BRICKware program group to start the authentication procedure from your TAF client PC.

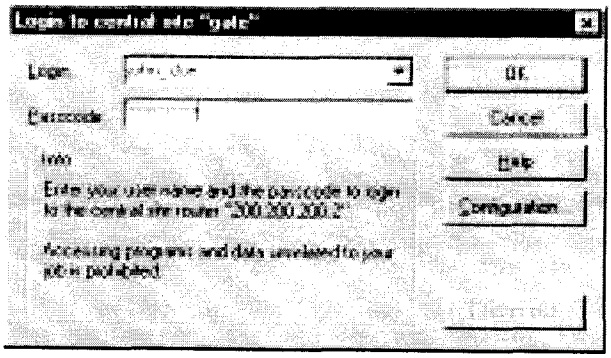


Figure 6: TAF Login

Enter your login name for the ACE/Server and the passcode displayed on your Token Card. Click on the *OK* button.

If the authentication was successful the TAF Login dialog will be closed and the TAF icon in the task bar will change to , if the authentication failed an error message is displayed, and the icon will remain .

TAF Login also includes a monitoring function. If you right-click on the TAF icon you will get a menu from which you can select **Show Monitor Window**.

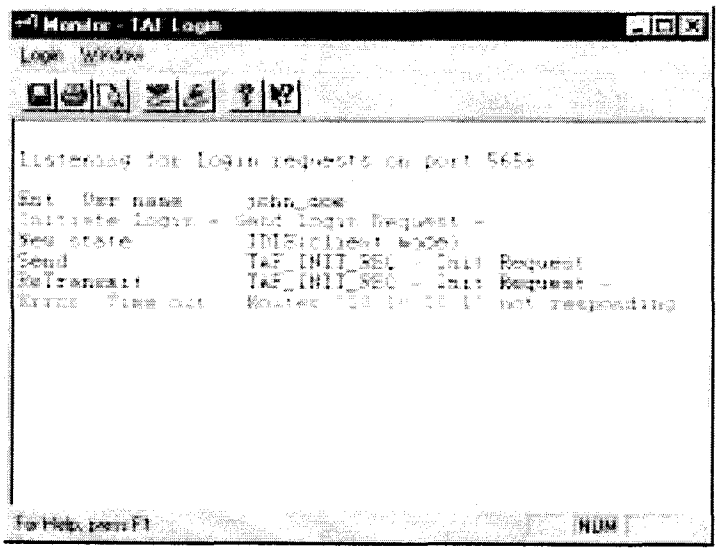


Figure 7: TAF Monitor

All important activities concerning TAF are logged in this window. You can also initiate a login or configure the program from this window.

5

VIRTUAL PRIVATE NETWORKING

What's covered

In this chapter we'll cover the Setup Tool menus and set tings you'll see while using configure the Virtual private networking support on your router.

Following that we'll cover some background information relating to Virtual Private Networking technology.

Then we'll describe a few examples showing you how Virtual Private Networking can be used on your router.

Setup Tool Menus

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 router's menu may differ slightly.

```
BRICK Setup Tool                                BinTec Communications AG
                                                              myrouter

Licenses                    System

Slot1:          CM-BNC/TP, Ethernet
Slot2:          CM-2XBRI, ISDN S0, Unit 0
                CM-2XBRI, ISDN S0, Unit 1
Slot3:          CM-1BRI, ISDN S0

WAN Partner
IP      IPX     X.25        VPN

Configuration Management
Monitoring and Debugging
Exit

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

VPN This is the point where our exploration of Setup Tool begins.

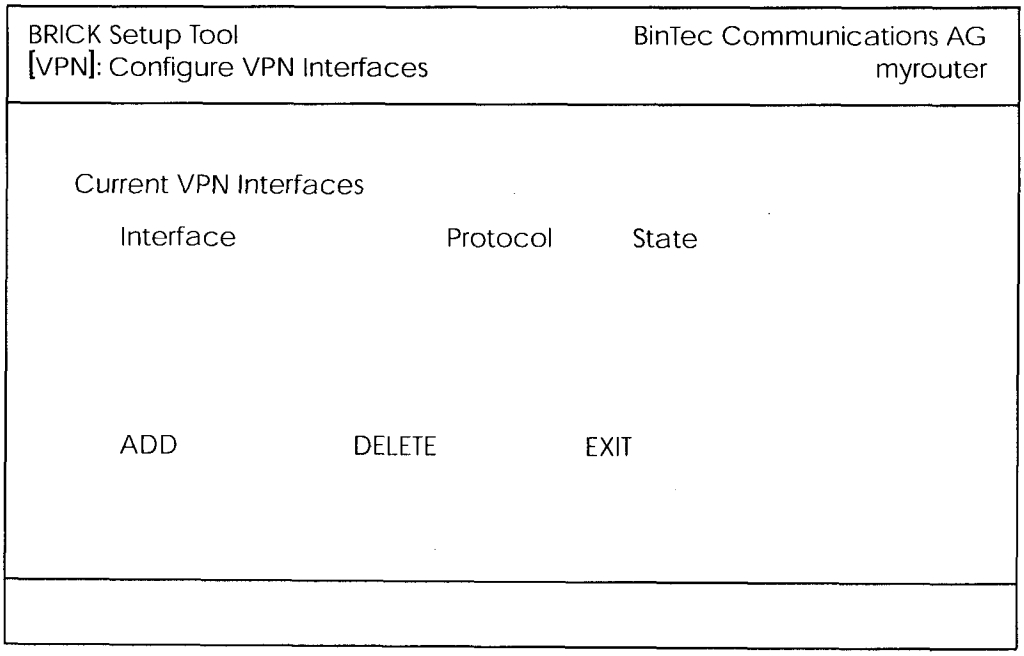
VPN→

The VPN menu lists the current Virtual Private Networking partner interfaces configured on the router.

Select ADD to add a new VPN interface.

Select DELETE to delete a VPN interface that has been marked (using the spacebar) for deletion.

Select EXIT to return to accept the configured list of partners ad return to the main menu.



VPN → ADD →

Use this menu to create Virtual Private Networking interfaces.

```
BRICK Setup Tool                              BinTec Communications AG
[VPN][ADD]: Configure VPN Interface                           myrouter

Partner Name                  tunnel
Enabled Protocols             <X> IP  < > IPX  < > BRIDGE
Encapsulation                 PPP
Encryption                    none
Identify by Calling Address   no
PPP Authentication Protocol   CHAP + PAP + MS-CHAP
Partner PPP ID                tunnel1-ppp-id
Local PPP ID                  brick
PPP Password                  tunnel1-ppp-pwd

IP >
IPX >
Advanced Settings >

                        SAVE                  CANCEL

Enter string, max length = 25 chars
```

Partner Name

= The partner name assigned to this virtual interface.

Enabled Protocols

= The protocols that may be routed over this interface.

Encapsulation

= The type of encapsulation to use; currently PPP must be used.

Identify by Calling Address

= This allows the BRICK to verify this VPN partner by its "calling IP Address". This is the IP address the VPN partner can be reached at on the Internet (i.e., an official IP address).

PPP Authentication Protocol

= The authentication protocol to use when authenticating this partner.

Partner PPP ID

= The PPP ID that the VPN partner must identify itself with during PPP negotiation.

Local PPP ID

= The BRICK's PPP ID which is used during PPP negotiation with this VPN partner.

PPP Password

= The password this VPN partner must use when challenged by the BRICK during PPP negotiation.

VPN → ADD → IP →

The VPN IP submenu defines IP address settings for the VPN partner interace.

Note: VPN partners will have two different IP addresses that define which network the host is on.

1. The Internet. This address must be an official address and defines where the host can be reached on the Internet. For the purposes of VPN, this address must be static (it may not be dynamically assigned by an ISP).
2. The VPN. The host's IP address on the local LAN.

```
BRICK Setup Tool                          BinTec Communications AG
[VPN][ADD][IP]: IP Configurartion (vpn1)          myrouter

VPN Partner's IP Address          192.168.12.99
  via IP Interface                ISP

Partner's LAN IP Address          192.168.13.99
Partner's LAN Netmask             255.255.255.0

                    SAVE                CANCEL

Enter string, max length = 25 chars
```

VPN Partner's IP Address

= The VPN partner's IP address where it can be reached at on the Internet.

via IP Interface

= The IP interface that packets received from this VPN partner will be received on. This will typically be the interface to the Internet Service Provider.

Partner's LAN IP Address

= The VPN partner's LAN address.

Partner's LAN Netmask

= The netmask the partner uses on it's LAN. If left blank, a standard netmask for the respective network class will be used.

VPN → ADD → IPX →

The VPN IPX submenu defines IPX relevant settings for VPN partner interfaces that support IPX.

```
BRICK Setup Tool                                BinTec Communications AG
[VPN][ADD][IP]: IP Configurartion (tunnel)                      myrouter


IPX NetNumber              0
Send RIP/SAP Updates       triggered + piggyback
Update Time                60


                      SAVE                CANCEL

Enter hex number range 0..fffffffe
```

IPX NetNumber

= The IPX network number of the network link (the PPTP link). This is required by some IPX routers.

Send RIP/SAP Updates

= Determines how often RIP and SAP packets are tranmitted to this VPN partner. The possible options are the same as those defined in the menu, see chapter 4 of the *User's Guide* for additional information.

Update Time

= Determines how often (in seconds) periodic updates are sent to this VPN partner.

VPN → ADD → ADVANCED SETTINGS

The settings defined here are similar to the [WAN PARTNERS][ADVANCED SETTINGS] menu but apply specifically to an VPN partner interface.

```
BRICK Setup Tool                                BinTec Communications AG
[VPN][ADD][ADVANCED]: Advanced Settings (tunnel)                myrouter

Dynamic Name Server Negotiation   yes

RIP Send                          none
RIP Receive                       none

IP Accounting                     off
Dynamic IP-Address Server         off
Back Route Verify                 off

                  OK                        CANCEL

Enter string, max length = 25 chars
```

Dynamic Name Server Negotiation
= Defines whether (and how) the name server's address is configured.

RIP Send/Receive
= Defines the which version of RIP packets to exchange with this partner.

IP Accounting
= Enable/disable generation of IP accounting messages for this partner. When enabled, an accounting message is generated (and written in *biboAdmSyslogTable*) which contains detailed information regarding connection activity for this partner.

Dynamic IP-Address Server
= Defines whether or not the BRICK should assign this partner an available IP address from the IP address pool.

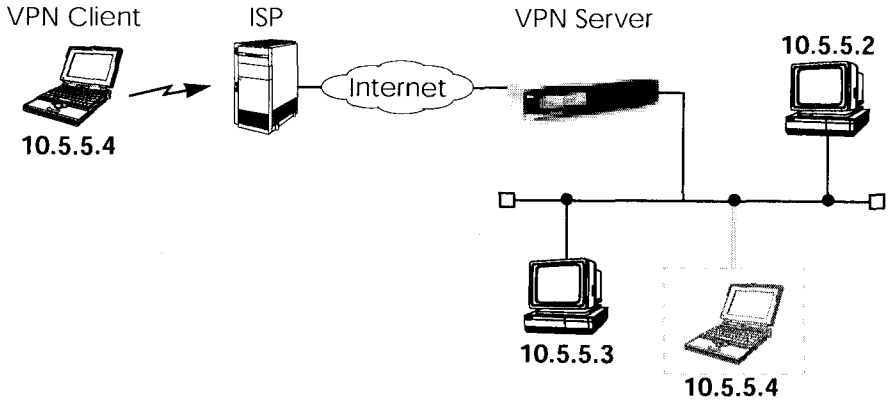
Back Route Verify
= When enabled the BRICK verifies that the return route for all packets received from this partner interface uses the same interface the packet arrived on.

Overview of Virtual Private Networking

Overview

A Virtual Private Network can be considered as a virtual Wide Area Network. It is *Virtual* in the sense that the network is not physical but is established on demand by software that establishes a link between a client and the server. VPNs are typically established over public (TCP/IP-based) data networks such as the Internet.

A VPN is also considered *Private* since user data transmitted over the link is typically encrypted. Windows 95/NT based networks achieve this security via Microsoft's own Point-to-Point Encryption protocol, or MPPE. Since these VPN connections are encrypted (user data portion) network administrators can be assured that the use of the underlying public data network does not compromise data integrity.



The protocol that makes VPN possible is the Point-to-Point Tunnelling Protocol or PPTP. PPTP is an IETF standard described in RFC 1171.

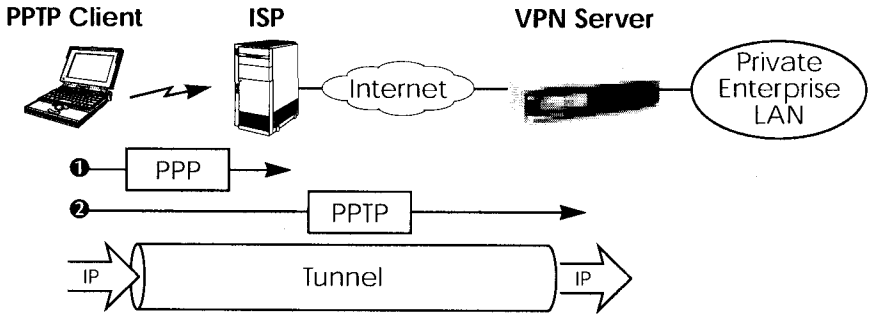
Tunnelling and PPTP

Simplified, tunnelling is a method of encapsulating packets of one high layer protocol within the envelope of another high layer protocol (typically IP), "IP-over-IP" if you will. This technique also allows protocol data such as IPX and NetBEUI to be tunnelled via IP packets.

There are two commonly used scenarios for establishing VPN connections. The difference lies in which hosts involved in establishing the end-

to-end connection support PPTP and which do not. Where PPTP support starts and stops also defines where the "tunnel" begins an ends.

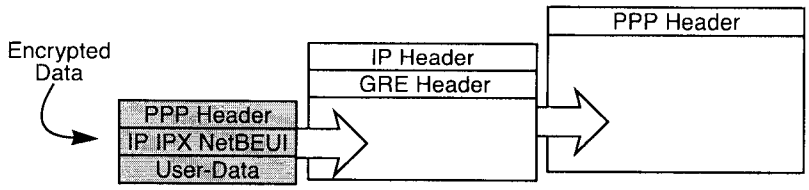
Scenario 1. PPTP Client–to–VPN Server



This is the most common scenario for PPTP. The remote client (mobile Win95 host) first establishes a standard PPP connection to a local ISP. The same client then initiates a second, logical connection, to the VPN Server. The ISP (and all intermediate Internet routers), unaware that it is participating in a VPN, simply routes IP packets from the PPTP Client.

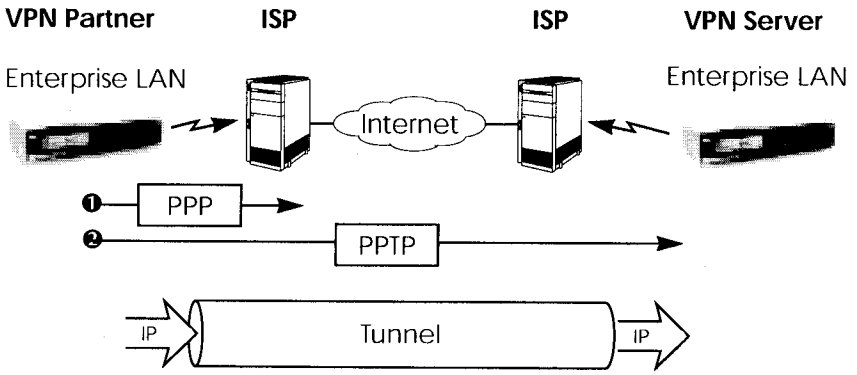
To hosts on the Private Enterprise LAN the remote PPTP Client appears as if it were directly connected to the LAN.

When sending data to the enterprise LAN the PPTP Client encapsulates PPP packets in the user-data field of the IP packet which is later unpacked by the VPN Server.



In the diagram above, GRE refers to the Generic Routing Encapsulation protocol. The GRE header identifies PPTP relevant functions and allows for efficient use of the link.

Scenario 2. LAN–to–LAN VPN



Here a Virtual Private Network that connects two enterprise LANs via the Internet is established via two VPN Servers. Either side may initiate a standard PPP link to a local ISP. Once the link is established the same server establishes a PPTP connection to the remote VPN server. Again, the ISP is unaware of its participation in the VPN.

All traffic routed via the ISP and destined for the remote LAN is encapsulated/unpacked by the respective VPN servers as mentioned in scenario 1.

Authentication – Encryption – Compression

In both scenarios above a second PPTP connection is established over an existing link. This second connection has its own PPP parameters (unique from those of the underlying link) with respect to user authentication, encryption, and compression.

Authentication

Both the ISP and the VPN Server will typically want to verify the initiating partner during connection establishment. Authentication is performed inband using PAP, CHAP, or MS-CHAP.

Data Encryption

Data encryption allows you to be sure that all user data transmitted over public data networks via a VPN is secure. The BRICK supports Microsoft's Point-to-Point Encryption protocol, or MPPE data encryption. Data

encryption/decryption is performed at each end of the tunnel. Each host separately generates a *session-key* (40 or 128 bit key) using the respective partner's PPP password which is known to each host ahead of time.

Note: Since session-key generation is based upon the partner's password, data encryption is only possible if authentication (PAP, CHAP, or MS-CHAP) is enabled. Also, for 128 bit encryption the MS-CHAP authentication protocol is required (i.e., must be successfully negotiated at connect time.)

The Windows PPTP configuration dialoge includes an option for *password encryption*. This option applies to transmittal of the PPP password and does not apply to data encryption.

Compression

Data compression, depending on the data and the compression algorithm used, can increase performance over dial-up links as much as 30 fold (best case scenario using Stacker LZS). In both scenarios shown above, compression can be enabled for the initial PPP connection. Compression can also be enabled for PPTP links between BRICKs (Scenario 2: LAN-to-LAN VPN).

Note: The following limitation currently exists when combining compression + encryption for a PPTP link with Windows based hosts.

When the **Enable software compression** option is enabled in the **Server Types** tab (see Step 5.) Windows PPTP Clients offer EITHER MS-STAC Compression OR MPPE Encryption when tunnel parameters are negotiated. Currently, compression is only possible for the PPTP link if Encryption is set to "none" for the VPN partner interface on the BRICK (see the [VPN][ADD] menu on page 90).

Virtual Private Networking Examples

Example Client-to-LAN Configuration

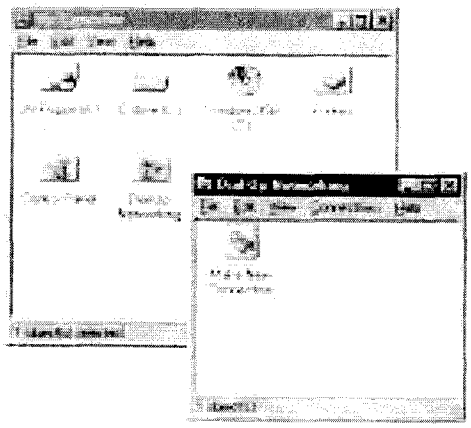
The Virtual Private Network shown in Scenario 1 on page 83 would be configured as follows.

Configure PPTP Client

Requirements: VPN Partners must support the PPTP protocol. For Windows 95 hosts this involves installing Winsock and Dial-Up Networking 1.2 Updates. Software updates and configuration information can be retrieved via Microsoft's web site at:
http://www.microsoft.com/communications/pptpdownnow.htm

Configure PPP Link to the Internet Service Provider.

1. Open the Dial-Up Networking folder by double-clicking **My Computer**, and then **Dial-Up Networking** from the desktop.



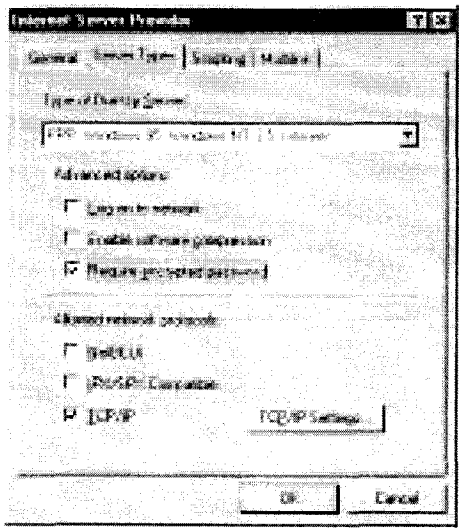
2. Double-click the **Make New Connection** icon. In the resulting dialoge:
   - Specify a name for the ISP this host will be using.
   - Select a modem device to use for the ISP PPP link.
   - Then click the **Next** button.
3. Here you will need to enter the ISP's telephone number.
4. Click **Next>** and then **Finish**. A new icon will be added to the Dial-Up Networking folder. Right-click this icon and select **Properties** to display the properties window.

5.Click the **Server Types** tab.
- In the **Type of Dial-Up Server:** field select: "PPP: Windows 95, Windows NT, Internet"
- In the **Advanced options:** box

Disable "Log on to network"
Disable "Enable software compression"
Enable "Require encrypted password"

- In the **Allowed network protocols:** box

Disable "NetBEUI"
Disable "IPX"
Enable "TCP/IP"



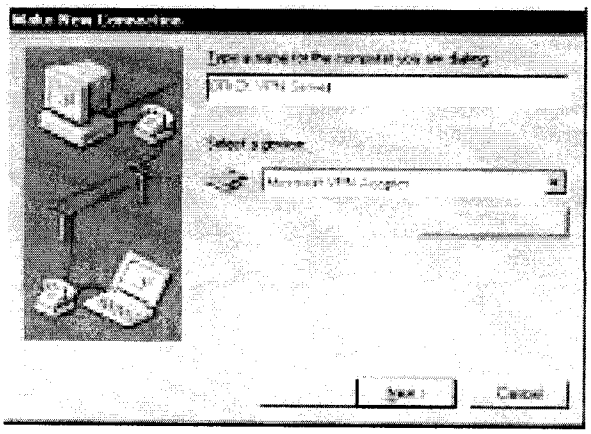
6.Click the **TCP/IP Settings...** button. Verify the IP address, name service, and compression settings are consistent with those required by the ISP and click **OK**.

NOTE: In most cases the default settings in the **Scripting** and the **Multilink** tabs can be left untouched.

7.Click **OK** again. The initial PPP link to the Internet Service Provider is now configured. Proceed to the next section to configure the link to the BRICK VPN Server.

Configure the PPTP Link to the BRICK VPN Server.

1.From the **Dial-Up Networking** folder double-click the **Make New Connection** icon to configure the connection for the BRICK VPN Server.

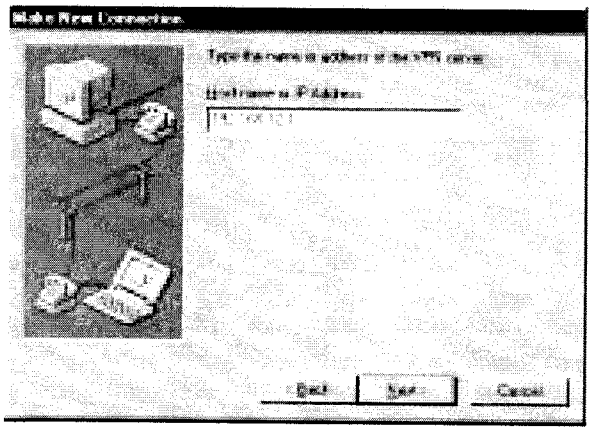


2.In the **Type a name for the computer you are dialing:** field specify a name for your BRICK VPN Server.

3.From the **Select a device:** drop menu select the device "Microsoft VPN Adapter" and click **Next>**.

In the dialogue shown below enter the official IP address of the BRICK VPN Server.

NOTE: If the *Microsoft VPN Adapter* device is not available verify that version 1.2 (or newer) of Microsofts Dial-Up Networking software is installed.



4.Click **Next>** and the **Finish**. A new icon for the BRICK VPN Server will be added to the Dial-Up Networking folder.

5.In the Dial-Up Networking folder right-click the new BRICK VPN Server icon and select **Properties** to verify the connection settings.

6.Click the **Server Types** tab.

– In the **Type of Dial-Up Server:** field select:
"PPP: Windows 95, Windows NT, Internet"

– In the **Advanced options:** box

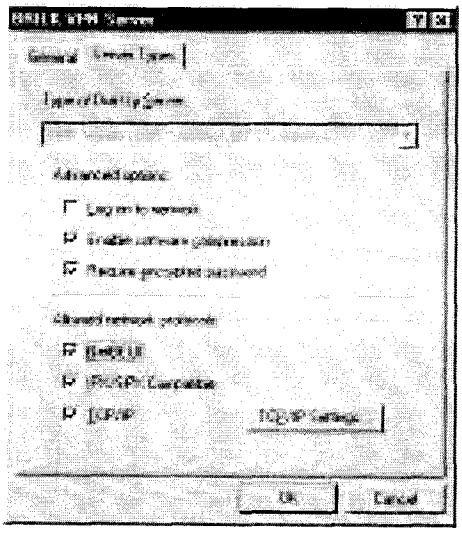
Enable "Log on to network" if hosts are required to register with the network.

Enable "Enable software compression"

Enable "Require encrypted password"

– In the **Allowed network protocols:** box enable only those protocols this host will use to communicate with remote hosts on the central site LAN.

At a minimum "TCP/IP" must be selected.



7.Click the **TCP/IP Settings...** button. Verify the IP address, name service, and compression settings are consistent with those on the BRICK and click **OK**. The settings used here must correspond to the respective BRICK VPN partner interface settings (see page 90).

8.Click **OK** again to accept the settings for the PPTP link. Once the respective BRICK partner interface is configured the Virtual Private Networking connection can be established as described on page 92.

Configure BRICK VPN Server

Requirements: A separate VPN license must be installed before the BRICK will support VPN connections. A VPN license can be purchased from BinTec Communications directly or from your local distributor.

Configure Link to the Internet Service Provider.

1. The link to the BRICK's ISP can be configured as a standard dial-up/ leased PPP interface via Setup Tool's WAN Partners menu.

Configure the VPN Partner Interface

1. VPN partners are configured in the VPN menu. The settings below could be used for the VPN Partner (PPTP client) configured above.

```
BRICK Setup Tool                              BinTec Communications AG
[VPN][ADD]: Configure VPN Interface                          myrouter

Partner Name                  vpn1
Enabled Protocols             <X> IP  < > IPX  < > BRIDGE
Encapsulation                 PPP
Encryption                    MPPE 40
Identify by Calling Address   no
PPP Authentication Protocol   MS-CHAP
Partner PPP ID                vpn1id
Local PPP ID                  mybrick
PPP Password                  vpn1pass

IP >
IPX >
Advanced Settings >

                    SAVE                    CANCEL

Enter string, max length = 25 chars
```

- In the **Encryption** field you may select MPPE encryption (40 bit or 128 bit session-key) or none.
- Disable ("no") the **Identify by Calling Address** option. This option can not be used since the BRICK will assign the PPTP client an IP address at connect time.
- In the **PPP Authentication Protocol** field select which authentication to use.

NOTE: If MPPE 128 encryption was selected the MS-CHAP protocol is required here.

- The **Partner PPP ID** and **PPP Password** fields define the values the VPN Partner must enter in the **User name** and **Password:** fields when establishing the VPN Connection.

2. Because Windows 95 PPTP clients expect the VPN server to assign them an IP address when the "tunnel" is established the **Dynamic IP Address Server** option in the ADVANCED SETTINGS sub menu must be enabled.

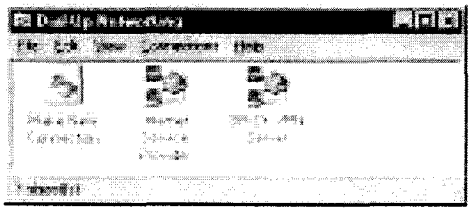
```
BRICK Setup Tool                              BinTec Communications AG
[VPN][ADD][ADVANCED]: Advanced Settings (vpn1)              myrouter

Dynamic Name Server Negotiation   yes

RIP Send                          none
RIP Receive                       none

IP Accounting                     off
Dynamic IP-Address Server         on
Back Route Verify                 off

                    OK                    CANCEL

Enter string, max length = 25 chars
```

For information on the other options available in this menu see the description of the [WAN PARTNERS][ADVANCED SETTINGS] menu your *User's Guide*.

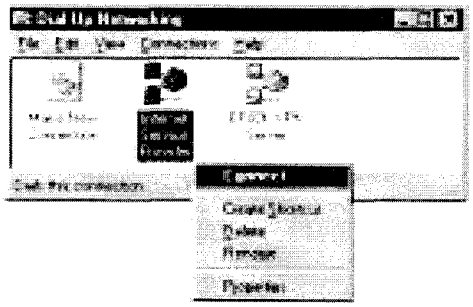
3. So that the BRICK can assign the PPTP client an IP address, make sure there are available IP addresses defined in the IP → Dynamic IP Addresses menu.

Connecting to the BRICK VPN Server

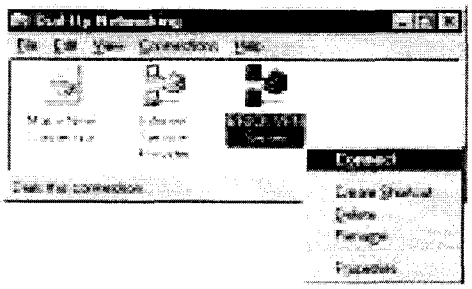
1. Open the Dial-Up Networking folder by double-clicking **My Computer**, and then **Dial-Up Networking**.



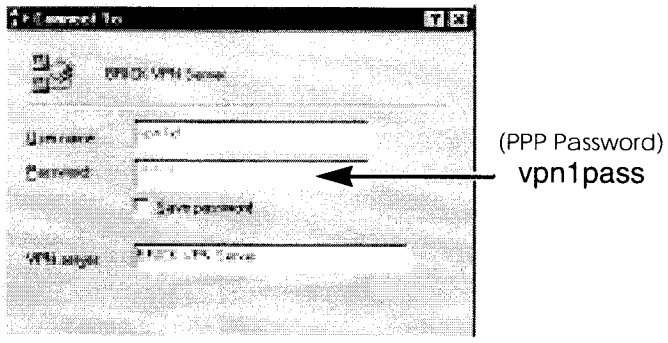
2. Right-click the Internet Server Provider icon, select **Connect** and enter the user/password assigned by the ISP.



3. After connecting to the ISP right-click the BRICK VPN Server icon and select **Connect**.

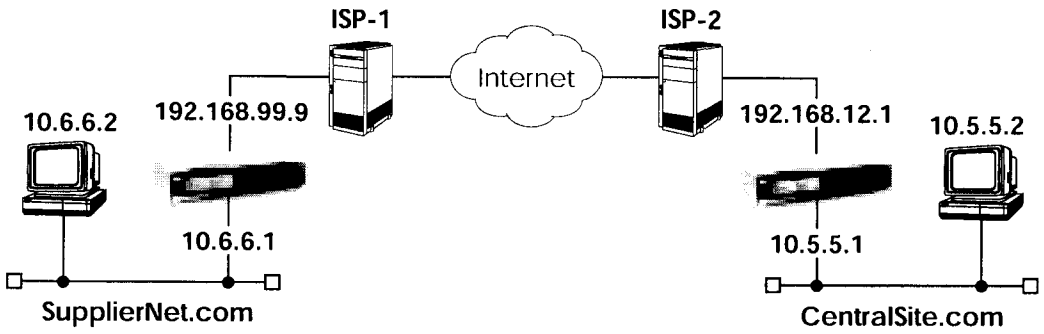


4.In the **Connect To** window shown below enter the PPP ID and PPP Password settings configured on the BRICK (see page 91) in the **User name** and **Password:** fields.



Example LAN-to-LAN Configuration

Two distant networks, a corporate central site LAN and a supplier or partner's network can be connected over the Internet via a Virtual Private Network using two BRICKs as follows.



Once both BRICKs are configured for Virtual Private Networking hosts on either LAN can connect to hosts on the remote LAN. All traffic that is routed between the two networks is encrypted (user-data encryption). Individual hosts are not required to support PPP or PPTP, the VPN remains transparent.

Configuration on SupplierNet BRICK

1. A separate license must be installed before Virtual Private Networking can be used. Verify the license is installed in Setup Tool's LICENSES menu.
   The status for "TUNNEL" must be "valid".
2. The link to the ISP-1 can be setup as a standard dial-up/leased PPP interface in the WAN PARTNER menu.
3. Configure the VPN Partner interface in the VPN menu. The VPN Partner interface for the BRICK-XL on CentralSite.com could be configured as follows.
   - Define a partner name (`csite`) and enable one or more protocols to support on the link.
   - In the **Encryption** field you may select MPPE encryption (40 bit or 128 bit session-key) or none. The options specified here must be the same for each partner.

- Enable ("yes") the **Identify by Calling Address** option. The VPN partner will be identified by the IP address it uses when establishing the PPP link.
- In the **PPP Authentication Protocol** field select which authentication to use.

NOTE: If MPPE 128 encryption was selected the MS-CHAP protocol is required here.

- Set **Partner PPP ID** and **PPP Password** as needed.

```
BRICK Setup Tool                                BinTec Communications AG
[VPN][ADD]: Configure VPN Interface                             Supplier

Partner Name                    csite
Enabled Protocols               <X> IP  < > IPX  < > BRIDGE
Encapsulation                   PPP
Encryption                      MPPE 40
Identify by Calling Address     yes
PPP Authentication Protocol     CHAP
Partner PPP ID                  csiteid
Local PPP ID                    mybrick
PPP Password                    csitepass

IP >
IPX >
Advanced Settings >

                        SAVE                    CANCEL

Enter string, max length = 25 chars
```

4. In the IP menu you will need to define the IP addresses the VPN Partner will be using.
   - The **VPN Partner's IP Address** field for `csite` would be set to 192.168.12.1.
   - Under **via IP Interface** select the PPP interface for the local ISP. VPN connections to CentralSite.com may only be established over this interface.

- Specify `csite`'s LAN address and netmask in the **Partner's LAN IP Address / Netmask** fields.

```
BRICK Setup Tool                                  BinTec Communications AG
[VPN][ADD][IP]: IP Configurartion (csite)                        Supplier

VPN Partner's IP Address                  192.168.12.1
  via IP Interface                        ISP-1

Partner's LAN IP Address                  10.5.5.1
Partner's LAN Netmask                     255.0.0.0

                        SAVE                    CANCEL

Enter string, max length = 25 chars
```

5. In the ADVANCED SETTINGS sub menu the **Dynamic IP Address Server** option must be set to "off". Other options available there apply to the VPN interface and are described in chapter 4 of your *User's Guide* under the [WAN PARTNERS][ADVANCED SETTINGS] section.

Configuration on Central Site BRICK

1. A separate license must be installed before Virtual Private Networking can be used. Verify the license is installed in Setup Tool's LICENSES menu.
   The status for "TUNNEL" must be "valid".
2. The link to the ISP-2 can be setup as a standard dial-up/leased PPP interface in the WAN PARTNER menu.
3. Configure the VPN Partner interface in the VPN menu. The VPN Partner interface for the BRICK-XL on SupplierNet.com could be configured as follows.
   - Define a partner name (`SupplierNet`) and enable one or more protocols to support on the link.

- In the **Encryption** field you may select MPPE encryption (40 bit or 128 bit session-key) or none. The options specified here must be the same for each partner.
- Enable ("yes") the **Identify by Calling Address** option. The VPN partner will be identified by the IP address it uses when establishing the PPP link.
- In the **PPP Authentication Protocol** field select which authentication to use.

NOTE: If MPPE 128 encryption was selected the MS-CHAP protocol is required here.

- Set **Partner PPP ID** and **PPP Password** as needed.

```
BRICK Setup Tool                          BinTec Communications AG
[VPN][ADD]: Configure VPN Interface                          csite

Partner Name                  SupplierNet
Enabled Protocols             <X> IP  < > IPX  < > BRIDGE
Encapsulation                 PPP
Encryption                    MPPE 40
Identify by Calling Address   yes
PPP Authentication Protocol   CHAP
Partner PPP ID                supplierid
Local PPP ID                  mybrick
PPP Password                  supplierpass

IP >
IPX >
Advanced Settings >

                    SAVE                    CANCEL

Enter string, max length = 25 chars
```

4. In the IP menu you will need to define the IP addresses the VPN Partner will be using.
   - The **VPN Partner's IP Address** field for `SupplierNet` would be set to 192.168.99.99.
   - Under **via IP Interface** select the PPP interface for the local ISP. VPN connections to SupplierNet.com may only be established over this interface.

- Specify `SupplierNet`'s LAN address and netmask in the **Partner's LAN IP Address/Netmask** fields.

```
BRICK Setup Tool                                BinTec Communications AG
[VPN][ADD][IP]: IP Configurartion (SupplierNet)                  csite


VPN Partner's IP Address                 192.168.99.99
  via IP Interface                       ISP-2

Partner's LAN IP Address                 10.6.6.1
Partner's LAN Netmask                    255.0.0.0

                    SAVE                 CANCEL

Enter string, max length = 25 chars
```

5. In the ADVANCED SETTINGS sub menu the **Dynamic IP Address Server** option must be set to "off". Other options available there apply to the VPN interface and are described in chapter 4 of your *User's Guide* under the [WAN PARTNERS][ADVANCED SETTINGS] section.

6

X.25

What's covered

We start this chapter with an introduction to X.25 to give you an overview of the X.25 protocol.

Then we'll cover all of the menus and settings you'll see while using Setup Tool to configure the X.25 protocol on your router.

Following that are several brief examples for configuring the available X.25 features on your router.

Under Utilities you find the X.25 PAD and a reference of X.25 relevant SNMP shell commands.

Lastly, hardware specifications for the CM-X21 communications module are covered.

An Introduction to X.25

Packet Switching

X.25 is commonly referred to as being a Connection-Oriented, Reliable, Packet-Switched network. These catchwords describe some of the important characteristics of X.25 networks which are explained briefly here to help you better understand X.25.

Connection-Oriented

X.25 is connection-oriented which means that when data needs to be transferred, a connection must first be established. Communications parameters such as window size and packet sizes are negotiated when the connection is first established.

Multiple connections between two end points can be achieved by multiplexing logical connections onto data links. Different logical connections (or "Virtual Circuits") are identified by assigning a virtual circuit number for each logical connection. This number is included in the header of each X.25 data-packet.

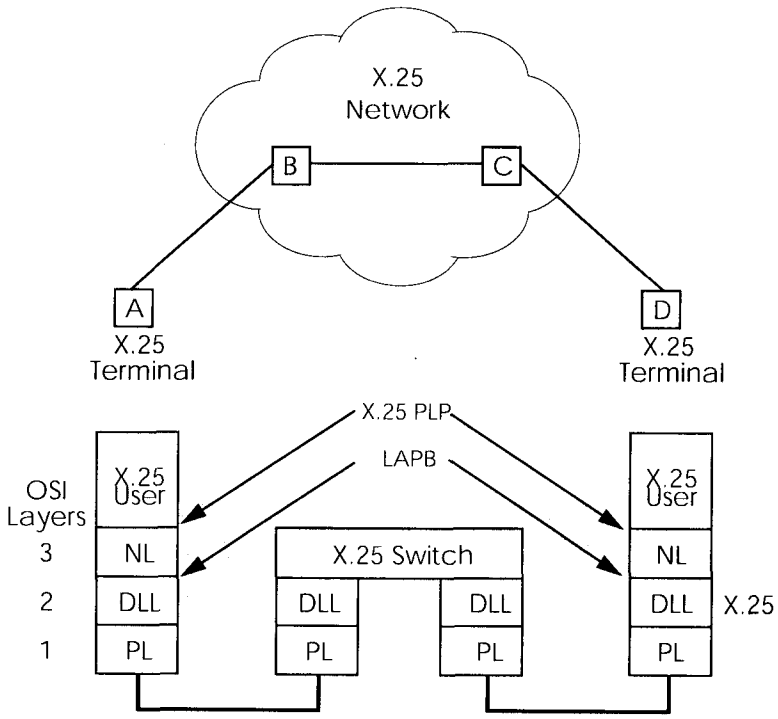
Packet Switched

X.25 is a packet switched network which means that user data is divided up and placed into X.25 packets of a predefined maximum length (usually 128 bytes). Each packet is assigned a virtual circuit number and is transmitted over the data link.

With a 128 byte packet size, user data must normally be fragmented into many packets. The X.25 frame format defines a special field, M-bit (M for more), which is used to allow fragmented packets to be reunited at the receiving station.

Reliable

X.25 connections are reliable connections which means that all data packets sent are confirmed by the receiving station. This is achieved using either special packets (Receiver Ready packets) or by having the receiving station "piggyback" confirmation messages onto other packets. Also, in X.25, packets always arrive in sequence at the receiving station.



Call Setup

Before data can be exchanged among X.25 partners an X.25 call must be setup. An X.25 CALL packet is sent by the calling partner to the called partner who can accept/refuse the connection. Once a call has been established, a unique Virtual Circuit (VC) number is assigned to the connection which is used throughout the duration of the connection.

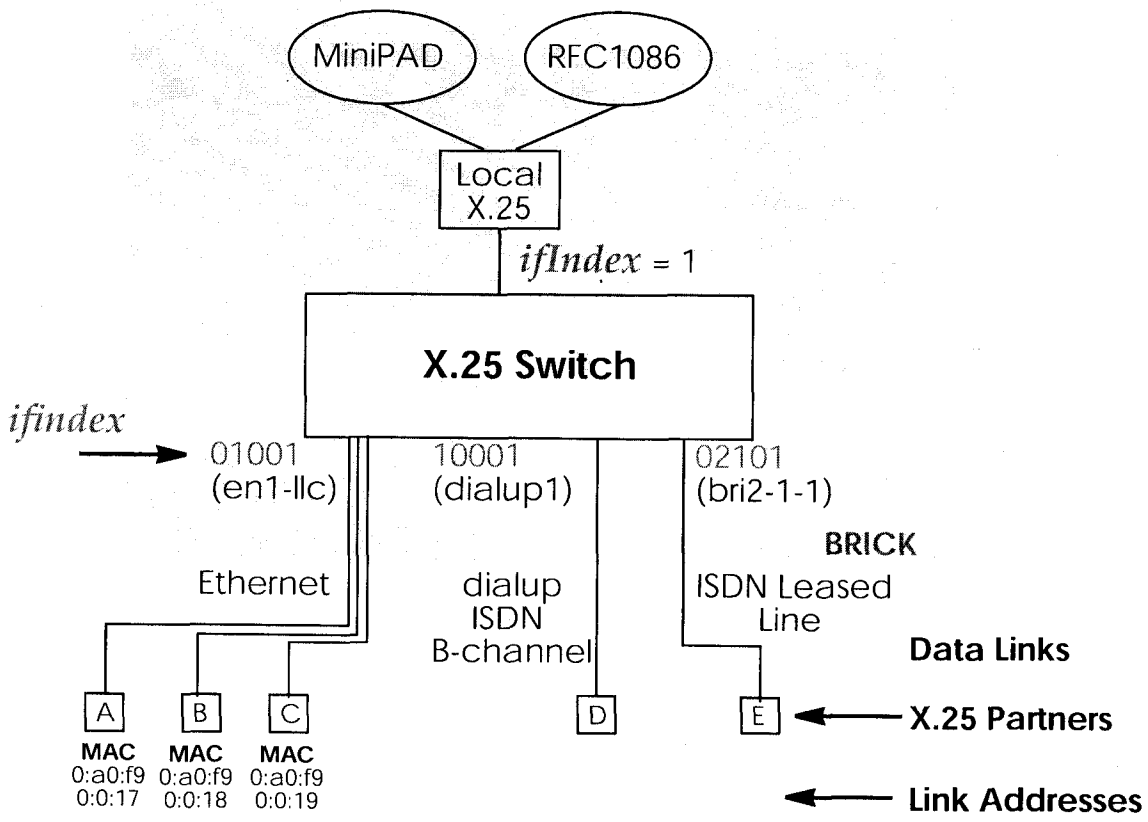
If an X.25 network lies between two end stations, the VC numbers used by each end station may be different. For example, if hosts A and D in the diagram above are communicating, the VC number used for the A–B connection may be different from the one used for C–D.

After the call is initially setup all packets exchanged between the partners follow a fixed path defined during the initial call setup phase. Once the connection is no longer needed, it can be disconnected, and later reused by the same or different communications partners.

Data Links and Virtual Circuits

A **data link** is a direct, point-to-point, connection between two X.25 stations. This physical connection can be via an ISDN B or D channel, an X.21 connection, or an ethernet connection (LLC2). On a point-to-multipoint physical medium (i.e. ethernet), multiple point-to-point data links are multiplexed over the same physical interface.

A **virtual channel** (VC) is a Logical Connection that is multiplexed onto a data link. This means that multiple X.25 connections can exist over the same physical medium, simultaneously



In X.25, each data link uses one interface. The characteristics of each data link are defined in Setup Tool **X.25/Link Configuration** menu resp. in the ***x25LinkPresetTable***. These characteristics, such as window and packet size, can be changed by editing these links.

To display a list of all available interfaces known to the system you can use the **`ifstat`** command.

There are three types of interfaces available on the BRICK; the first of which is always available. The other interface types will depend on your particular configuration.

- **Local Interface**
  The local interface is a special interface and is always available on the BRICK.
- **Point-to-Point Interface**
  This interface is referred to as being Point-to-Point because the two end stations of the connection are determined solely by the ***IfIndex***. These interfaces include: ISDN dialup, ISDN leased lines, and X.31 interfaces.
- **Point-to-Multipoint Interface**
  The Point-to-Multipoint interface is referred to as such because the ***IfIndex*** does not completely specify an end-to-end connection. Additional information is required (such as the end stations MAC address) when creating these interfaces to provide an end-to-end link. These interfaces include: LAN connections over LLC2.

Point-to-Point and Point-to-Multipoint Interfaces

One of the characteristics of an X.25 interface that must be defined is the encapsulation it uses.

When creating X.25 Point-to-Point interfaces in the **WAN Partner/Add** menu in Setup Tool resp. in the ***biboPPPTable***, you can specify either **`x25`** or **`x25_ppp`** encapsulation. By default, **`x25`** encapsulation is used. This allows an interface to be used solely for X.25 traffic. Using **`x25_ppp`** allows PPP and X.25 traffic to be routed over the same interface (i.e. multiplexing IP datagrams and X.25 packets simultaneously over the same ISDN channel).

For X.25 Point-to-Multipoint interfaces such as ethernet, you must use the enx*-llc interfaces, since not all ethernet interfaces on the BRICK support X.25 (i.e. enx, enx-snap, and enx-nov802.3)

X.25 Addressing Schemes

As in TCP/IP networks, each host in an X.25 network must be uniquely identified before communication between them is possible. However, there is one important difference. In TCP/IP, each data packet contains the source/destination addresses and is routed individually (packets can take different paths). In X.25, addresses are only used during call setup and all subsequent data packets follow the same exact route.

In X.25, three different address formats, can be used to identify X.25 hosts.

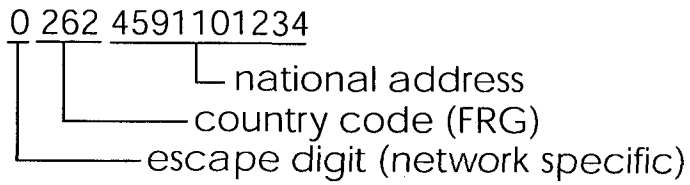
- *Standard X.25 Addressing (X.121)*
- *Extended X.25 Addressing*
- *NSAP Addresses (X.213)*

Standard X.25 Addressing (X.121)

The X.121 addressing scheme is the oldest and most common format used in X.25 networks. X.121 addresses consist of up to 15 digits and may begin with a leading escape digit (normally a 0). If the leading 0 is present, it is assumed to be an international address, otherwise a national address is assumed. For example:[1]

National Address:

International Address:



When working within ISDN, E.164 addresses are used instead of X.121 addresses. E.164 describes the numbering plan of the ISDN network and the commonly known telephone numbering system consisting of country code, area code, and subscriber number. To address other ISDN devices,

1. Note that spaces in the example addresses are used only for added readability.

an international ISDN number (according to E.164) is used which is similar to a national X.121 address. An additional zero following the escape code specifies an ISDN address for internetworking. For example:

ISDN Address: 499114501234
└international E.164 address

Internetworking Address: 0 0 499114501234
└international E.164 address
└E.164 indicator (ISDN)
└escape digit (network specific)

Extended X.25 Addressing

The extended addressing format provides a standardized way for distinguishing different types of addresses in X.25. However, many public networks do not support this addressing format.[1]

When the call is setup, a special bit (the A bit) in the call packet is used to define whether the addresses used are standard or extended. When the A bit is set, an extended address is used which consists of up to 255 digits[2]. The first two digits have special meanings and specify the Type of Address (TOA) and Numbering Plan Identification (NPI) respectively.

TOA and NPI Digits		
First Digit	0	Network dependent number
	1	International number
	2	National number
Second Digit	1	E.164 ISDN numbering plan
	3	X.121 numbering plan

1. The BRICK supports extended addresses and differentiates between standard and extended addresses using a leading @ in the ~Addr field.
2. Most implementations are currently using less than 42 digits.

For example, the following addresses are characterized according to their TOA and NPI digits:[1]

A national X.121 address	@2 3 4591101234
An international X.121 address	@1 3 262 4591101234
National E.164 address	@2 1 9114501234
International E.164 address	@1 1 49 9114501234

NSAP Addresses (X.213)

An alternative to the standard and extended formats is the NSAP (Network Service Access Point) address format. The NSAP format is defined in X.213. Only a few public networks support this format.

The NSAP format is complex. For our purposes it should be sufficient to say that NSAP addresses consist of up to 40 hexadecimal characters. Two types of NSAP addresses also exist, OSI conformant (indicated by a leading X) and Non-OSI conformant (indicated by a leading N).

Some example NSAP addresses are as follows:[2]

OSI compatible address	X 37 262459110123404711 abc
Non-OSI compatible address	N 0123456789abcdef

NSAPS can be used, instead of or in addition to, the other address formats.

X.25 Routing

To give you an overview of X.25 routing we use the ***x25RouteTable*** of the MIB, which shows X.25 routing systematically. To configure routes via the Setup Tool, you must enter the menu **X.25/Routing/Add** as described in the following chapter.

---

1. Spaces in the example addresses are used only for added readability.
2. Note that spaces in the example addresses are used only for added readability.

The routing of X.25 packets is accomplished via a routing table similar to the ***ipRouteTable***. The BRICK uses entries in the ***x25RouteTable*** to determine which link to route X.25 calls it receives. Routing decisions can be made based on the source link and/or different parameters found in the call packet.

The routing table for our example switch (see *Data Links and Virtual Circuits* on page 102) might look as follows:

	SrcIfIndex	SrcLinkAddr	DstAddr	DstIfIndex	DstLinkAddr
00	en1-llc	0:a0:f9:0:0:17		dialup1	
01	dialup1			en1-llc	0:a0:f9:0:0:17
02	en1-llc	0:a0:f9:0:0:18		bri2-1-1	
03	bri2-1-1			en1-llc	0:a0:f9:0:0:18
04	en1-llc	0:a0:f9:0:0:19	[0-4]*	dialup1	
05	en1-llc	0:a0:f9:0:0:19	[5-9]*	bri2-1-1	

Here, the first two entries route all calls between partners A and D. The third and fourth entries provide routes for all calls between partners B and E. The last two entries specify routes for calls originating from partner C. Any calls to an X.25 destination address beginning with 0, 1, 2, 3, or 4 are routed to D. All calls beginning with 5, 6, 7, 8, or 9, originating from C, are routed to E.

Calls with extended addresses are not routed since no routing entry for calls with a leading "@" is present. Therefore, such calls are refused.

Since some calls may match more than one route in the table, a metric can be used to prioritize routes. A route with the lowest metric value always has higher priority.

Setup Tool Menus

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 router's menu may differ slightly.

```
BRICK Setup Tool                          BinTec Communications AG
                                                        myrouter

Licenses                    System

Slot1:                      CM-BNC/TP, Ethernet
Slot2:                      CM-2XBRI, ISDN S0, Unit 0
                            CM-2XBRI, ISDN S0, Unit 1
Slot3:                      CM-1BRI, ISDN S0

WAN Partner
IP      IPX     X.25

Configuration Management
Monitoring and Debugging
Exit

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

X.25 This is the point where our exploration of Setup Tool begins.

X.25 →

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

```
BRICK Setup Tool                          BinTec Communications AG
[X.25]: X.25 Configuration                                myrouter

        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 router's X.25 address.

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

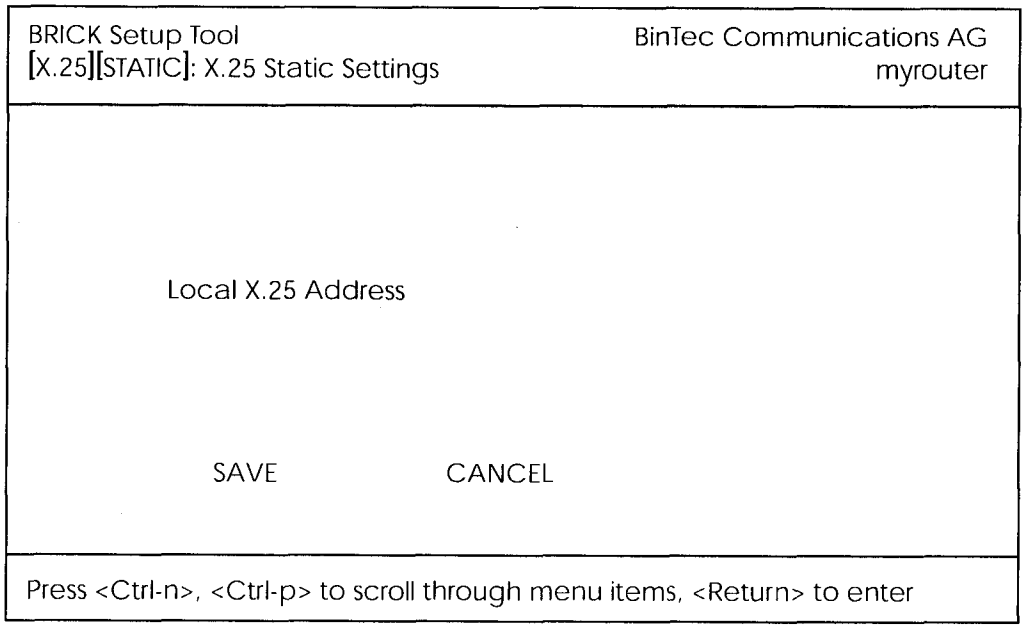
ROUTING contains the router's X.25 routing table.

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

Select EXIT to return to the main menu.

X.25 → STATIC SETTINGS →

The X.25 Static Settings menu contains the router's local X.25 address.



Local X.25 Address = The router's official X.25 address. Setting this variable is only required if the router is not directly connected to an official X.25 data network. When connected directly, the router 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.
- Hardware interfaces — Depending on which slot the X.21 module is installed in (1 - 3 on a BRICK-XM, 1 - 6 on a BRICK-XL), the system creates an initial link using xi1 through xi3 (xi6).
- 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*>

```
BRICK Setup Tool                                BinTec Communications AG
[X.25][LINK]: X.25 Link Configuration                            myrouter

    Select link to configure

    xi3
    en1-llc (create new configuration)

    DELETE CONFIGURATION          EXIT

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

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 .

X.25 → LINK CONFIGURATION → EDIT

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

```
BRICK Setup Tool                              BinTec Communications AG
[X.25][LINK][EDIT]: Change X.25 Link Configuration              myrouter

        Link                                  en1-llc
        L3 Mode                               dte
        L3 Packet Size                        default: 128      max: 128
        L3 Window Size                        default: 2        max: 7
        Windowsize/Packetsize Neg.            when necessary (default)

        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.

L3 Mode = This defines the mode the router operates in at Layer 3 of the X.25 protocol stack. Set to DCE if the router must provide clocking information or DTE if provided by the remote side of link.

L3 Window Size / Packet Size = Defines the *default* and *maximum* values for Packet size (128, ..., 4096 bytes) and Window size (2 - 127).

Windowsize/Packetsize Neg. = Decides whether window/packet-size negotiation is made for this X.25 link. The possible values are ***never, always*** and ***when necessary,*** where ***when necessary*** is the default value. The value ***never*** means no negotiation. When a call arrives that does not correspond to the default size, the call is cleared. ***Always*** means negotiations are always made and when ***when necessary*** is selected, there are only negotiations, when the requested values differ from the default values.

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.

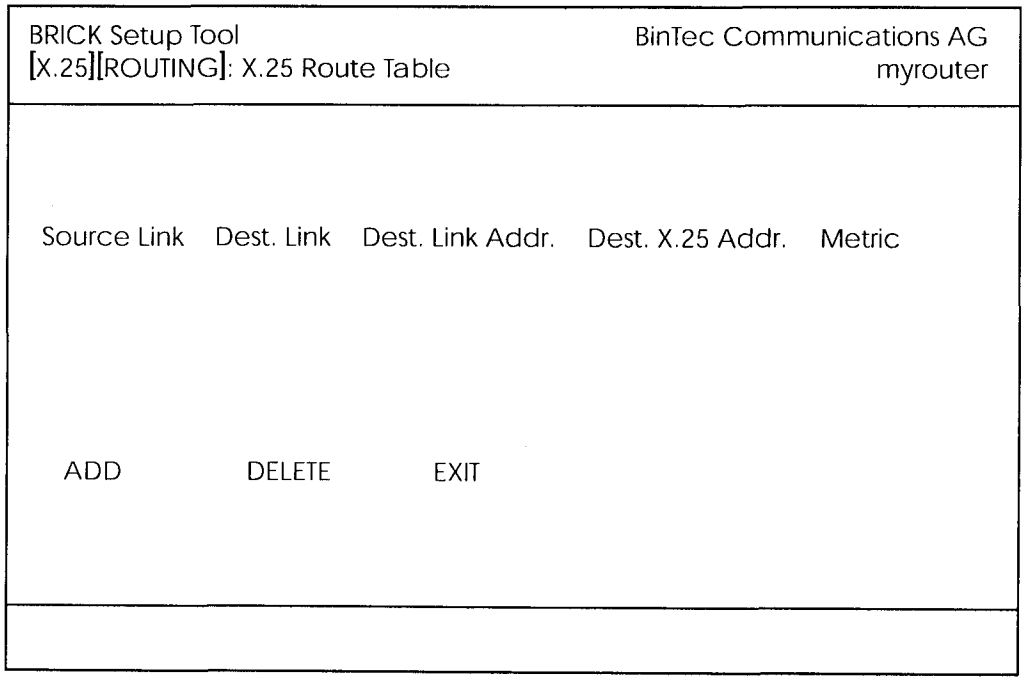
Partner MAC Address (LLC) = Used when configuring a link for a partner on the LAN and specifies the host's MAC or hardware address.

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

Disconnect Timeout = Time in milliseconds 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.



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 → ROUTING → ADD →

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

Since some calls may match more than one route in the table, a metric can be used to prioritize routes. A route with the lowest metric value always has higher priority.

When your destination link is a multipoint interface, you additionally have to adjust the Destination Link Address (LLC).

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 router may differ.

```
BRICK Setup Tool                          BinTec Communications AG
[X.25][ROUTING][EDIT]: Add or Change X.25 Routes          myrouter

Source Link                    any
Destination Link               local

Destination X.25 Address       45*

Metric                         0

        SAVE                                    CANCEL

Use <Space> to select
```

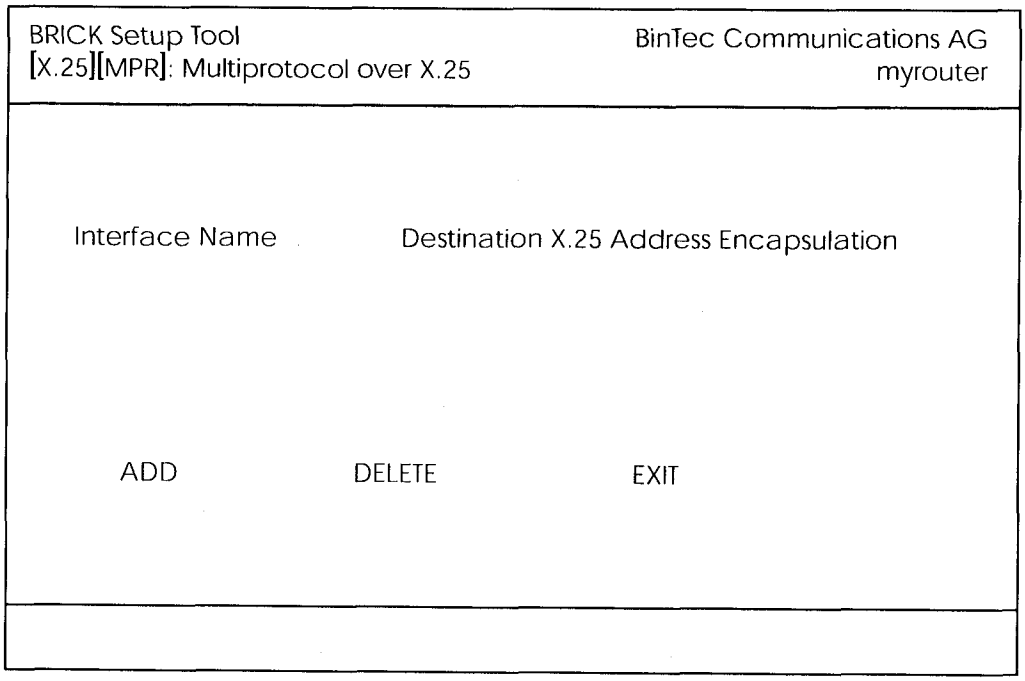
SAVE immediately saves route to memory and returns to the previous menu.

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 router 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 →



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.

X.25 → MULTIPROTOCOL OVER X.25 → ADD →

Use this menu to add or change MPX25 interfaces.

```
BRICK Setup Tool                          BinTec Communications AG
[X.25][MPR][ADD]: Add or change X.25 MPR                  myrouter

    Partner Name                  mpxpartner1

    Encapsulation                 ip_rfc877
    X.25 Destination Address      49911555



Advanced Settings >

IP >
IPX >

                    SAVE                          CANCEL

Enter string, max length = 25 chars
```

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

Encapsulation = Here you select the type of encapsulation/protocol 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			

When selecting *ip_rfc877* or *ip*, you must define the IP settings in the IP Submenu (see below).

When selecting *mpr*, you can enter IP and IPX settings in the respective submenus (see below). When you define the settings for both submen-

us, both will be routed, but you can also decide to configure just one of the protocols or none of it. The Bridge functionality is always available, when *mpr* is selected and needs no configuration.

When selecting *ipx*, you must define the IPX settings in the IP menu (see below).

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.

X.25 → MULTIPROTOCOL OVER X.25 → ADD → IP →

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

Note: The settings used in this menu are the same as those used in the WAN PARTNER → ADD → IP → menu but only apply to this MPX25 partner.

X.25 → MULTIPROTOCOL OVER X.25 → ADD → IPX →

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

Note: The settings used in this menu are the same as those used in the WAN PARTNER → ADD → IPX → menu but only apply to this MPX25 partner.

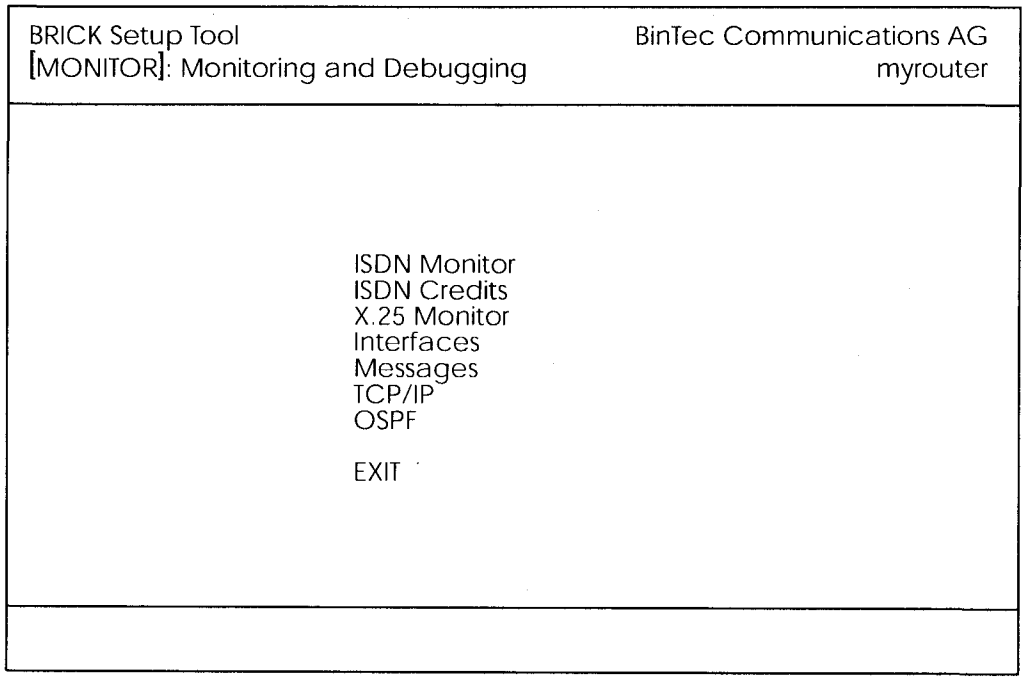
X.25 → MULTIPROTOCOL OVER X.25 → ADD → ADVANCED SETTINGS →

This menu can be used to configure advanced features.

Note: The settings used in this menu are a subset of those used in the WAN PARTNER → ADD → ADVANCED SETTINGS → menu but only apply to this MPX25 partner.

MONITORING AND DEBUGGING →

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



ISDN MONITOR lets you track incoming and outgoing ISDN calls.

ISDN CREDITS lets you track credits based accounting.

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 router's 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.

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, the menu commands (c, h, d, and s) listed at the bottom of the screen list different statistics relating to X.25 calls.

```
BRICK Setup Tool                                  BinTec Communications AG
[MONITOR][X.25 CALLS]: X.25 Monitor                              myrouter

From        To          Calling Addr      Called Addr     Duration
xi3         local       1       0         0               591




EXIT

   (c)alls        (h)istory          (d)etails          (s)tatistics
```

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

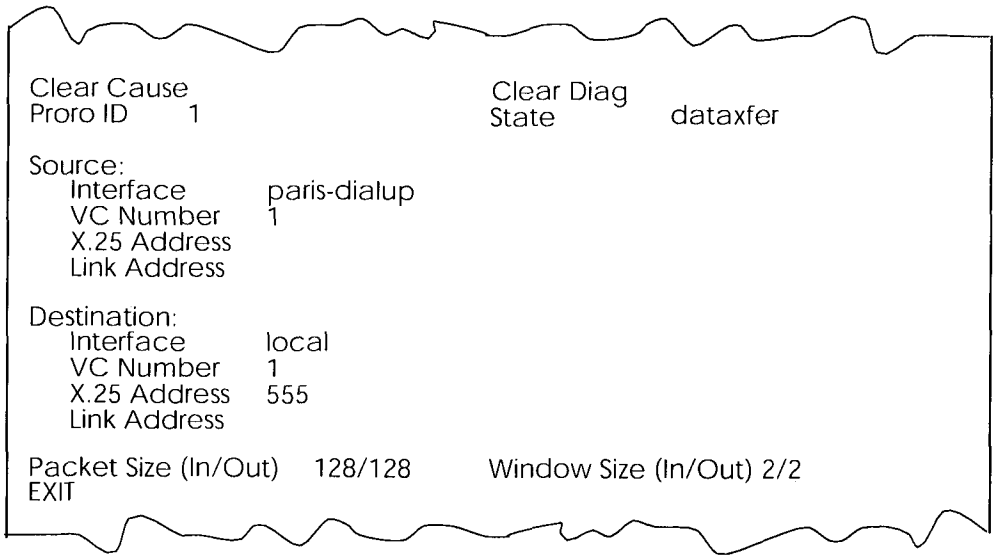
```
From        To          Calling Addr      Called Addr     Duration
xi1         local       1                 0
mpr-1       london2     3                 2               591
                                                          139
```

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
local       london2     19:34:01      2           (0x01) number busy
                                                  (0x03) network congestion
```

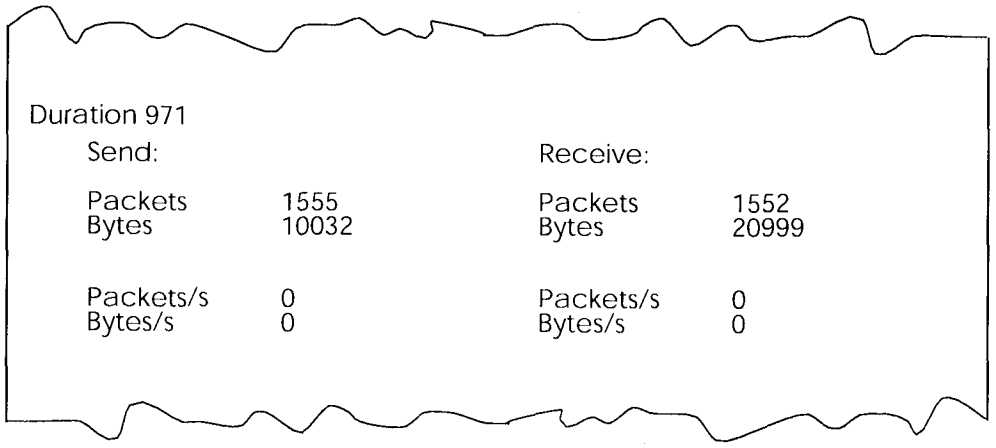
For completed calls, you can display additional information about the call. Select a call from the list, then enter "d" to see a detailed listing.

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:                              Receive:

    Packets          1555              Packets          1552
    Bytes            10032             Bytes            20999

    Packets/s        0                 Packets/s        0
    Bytes/s          0                 Bytes/s          0
```

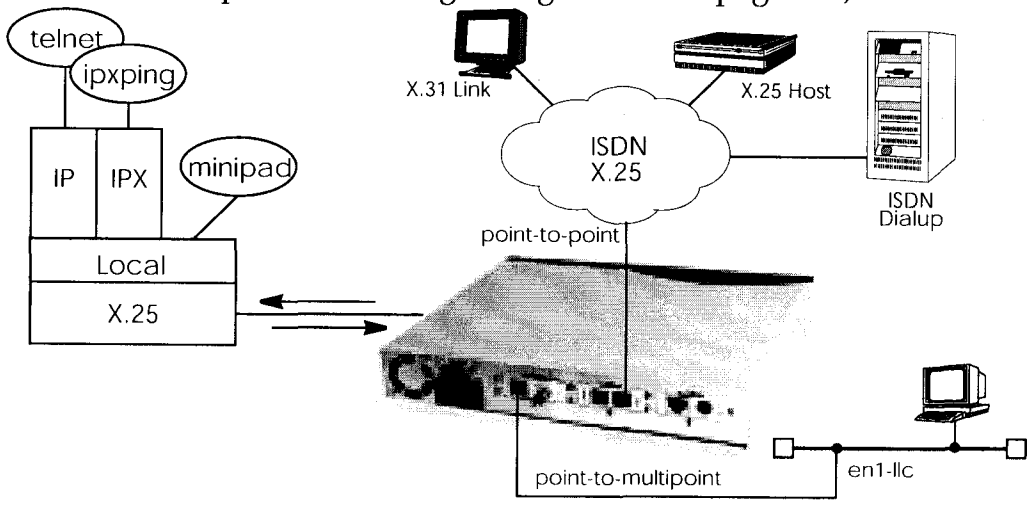
X.25 Features

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

Special Note: The X.25 Local Interface

In X.25 routing the router 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 router's special "local" interface.

This local interface is an internal *virtual* interface. Here, the X.25 packet is given to one of the router's 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 137).



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 router's X.25 address.
- The ISDN telephone number for this subscriber outlet.

Configure it

LICENSES → **Verify License**

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

X.25 → LINK CONFIGURATION → **Configure the X.31 Link**

If the router 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 Packet Size	default:128 max:128
L3 Window Size	default:2 max:7
Windowsize/Packetsize Neg.	when necessary (default)
Lowest Two-Way-Channel	1
Highest Two-Way-Channel	2
Layer 2 Behaviour	always active

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 router's X.25 address to be given to the local[1] 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	<*router's ISDN telno*>

Note:

The router's ISDN telephone number used here should be in the format: <*country code*><*area code*><*local number*>

X.25 → ROUTING → **Create Route for Outgoing Calls**

Create an X.25 route for outgoing calls. This route says that all calls from the local[1] 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 router at it's X.25 address.

In Germany, a special "Echo Port" provided by the Deutsche Telekom can be used to verify your router 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.

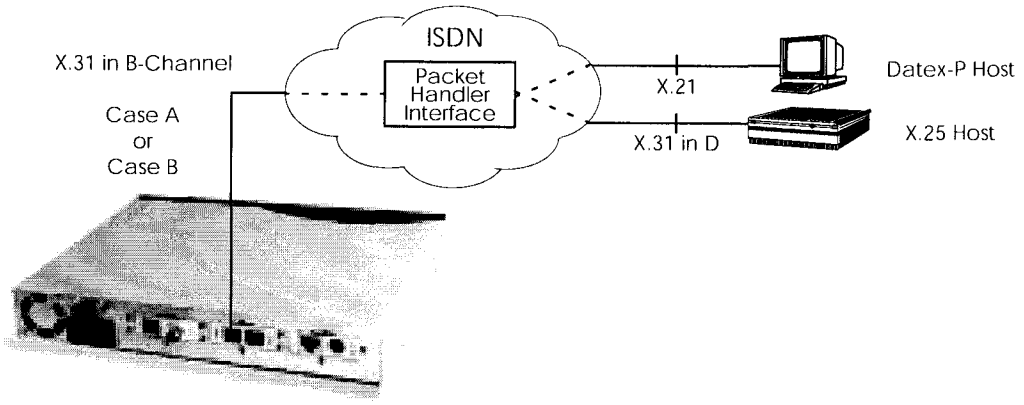
You can also connect to the Deutsche Telekom's Traffic Generator service to verify data transfers are possible over the X.31 link. This can be done with:

minipad 026245911029003

1. See page 123 for information on the router's special local interface.

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

The router 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 S_0 interface. In both scenarios the router 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 router, 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 router's ISDN telephone number.
- (Case A only) The telephone number of your local PHI. Contact your local carrier for this information.

Configure it

WAN PARTNER → ADD → **Configure WAN Partner**

First, configure the PHI as a new WAN partner.

Partner Name	phi
Encapsulation	X31 B-channel

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

Number	*<PHI's telephone number>*
Direction	both

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 Packet Size	default:128 max:128
L3 Window Size	default:2 max:7
Windowsize/Packetsize Neg.	when necessary (default)
Lowest Two-Way-Channel	1
Highest Two-Way-Channel	2
Layer 2 Behaviour	disconnect when idle

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 router's X.25 telephone number to be given to the local[1] interface.

Source Link	*<interface name for PHI>*
Destination Link	local
Destination X.25 Address	*<router's ISDN telephone number>*

X.25 → ROUTING → ADD → **Route for Outgoing Calls**

Create another route for outgoing calls. This route says that all calls from the local[1] 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 123 for information on the router's special local interface.

How do I configure my X.21 module so I can access my X.25 network?

You can use the CM-X21 communications module to connect networks over a public (or private) X.25 data network.

Before you begin

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

- The number of Virtual Channels, and the Window and Packet sizes assigned by your X.25 network service provider.
- Your router's official X.25 address.
- The remote partner's official X.25 address.
- Decide what types of traffic will be routed over this interface.

Configure it

CM-X21, X.21 → **Configure Hardware Interface**

First, we need to configure the hardware interface.

Layer 1 Mode	dte
Layer 2 State	auto

WAN PARTNER → ADD → **Edit WAN Partner**

Locate the appropriate X.21 entry to configure, (X.21 partner entries have the format: xi<*slot number*>) and enable X.25.

Encapsulation	X. 25

X.25 → LINK CONFIGURATION → **Configure Data Link**

Locate the X.21 entry for the WAN partner you just configured. If you didn't change the partner name you should see an xi<*slot number*> link depending on where your X.21 module is installed.

L3 Mode	dte
L3 Packet Size	<*Packet assigned by network*>
L3 Window Size	<*Win Size assigned by network*>
Windowsize / Packetsize Neg.	when necessary (default)
Lowest Two-Way-Channel	<*LTC assigned by network*>
Highest Two-Way-Channel	<*HTC assigned by network*>
Layer 2 Behaviour	always active

X.25 → ROUTING → ADD → **Route for Incoming Calls**

Next, create a route for incoming calls. This will allow calls arriving on the X.21 link that are addressed to the router's X.25 address to be given to the local[1] interface.

Source Link	xi<*slot number*>
Destination Link	local
Destination X.25 Address	<*router's X.25 address*>

X.25 → ROUTING → ADD → **Route for Outgoing Calls**

Create another route for outgoing calls. This route says that all calls from the local[1] interface are routed over the X.21 link.

Source Link	local
Destination Link	xi<*slotnumber*>
Destination X.25 Address	<*leave empty*>

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 170. In Germany, call the local echo port to verify X.25 calls can reach the X.25 network with

minipad 45911029002

Or, if you have more than 1 virtual channels available, you can also place a call to your own router's X.25 address with

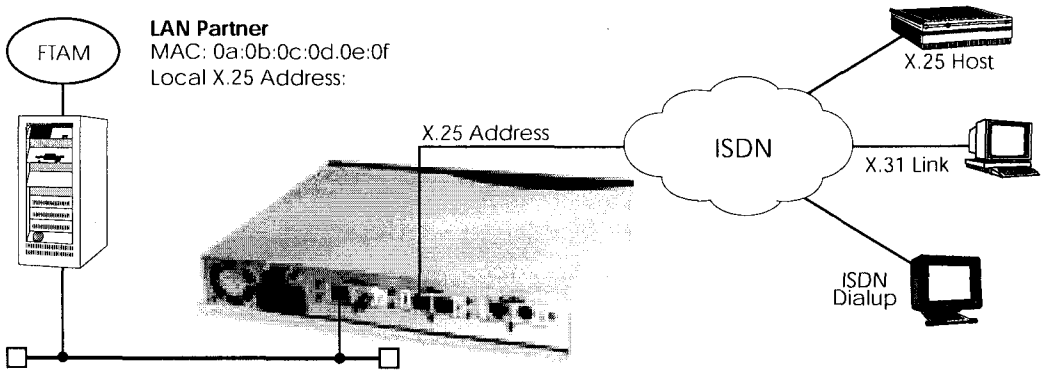
minipad <*your router's X.25 address*>

The call should go out one virtual channel, and come back in on a second virtual channel and you should receive a new login prompt. This can be verified by displaying the x25CallTable from the shell, or in Setup Tool under MONITORING AND DEBUGGING → X.25 MONITOR .

1. See page 123 for information on the router's 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 router 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 router's X.25 address.
- The LAN partner's MAC address.
- A locally assigned X.25 address for the LAN partner.

Configure it

X.25 → STATIC SETTINGS → **Configure X.25 Local Address**

First, verify the router's local X.25 address is configured.

X.25 Local Address *<router's X.25 Address>*

X.25 → LINK CONFIGURATION → **Create LAN Host Link**

We need to create a new link for the host on the router's 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
Windowsize/Packetsize Neg.	when necessary (default)
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.

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 router's X.25 address to the special local[1] interface.

Source Link	en1<*slot*>-llc
Destination Link	local
Destination X.25 Address	*<router's X.25 address>*

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>*

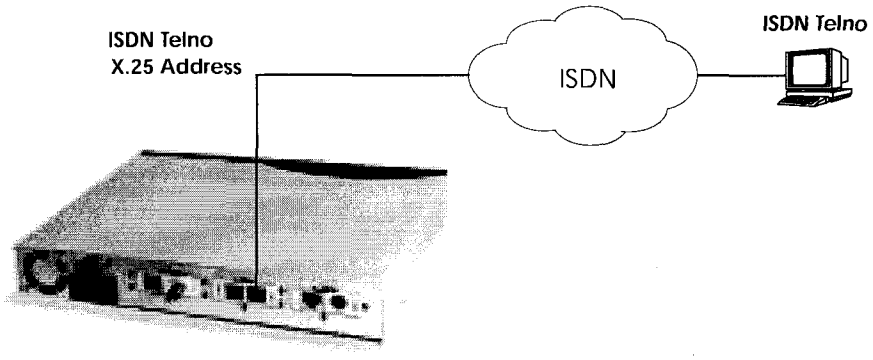
More Info

Depending on how you've set up X.25 routing, you can test your X.25 configurations using minipad. See minipad on page 170.

1. See page 123 for information on the router's 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 router's ISDN telephone number and X.25 address.
- The remote X.25 partner's ISDN telephone number.

Configure it

X.25 → STATIC SETTINGS → **Configure X.25 Local Address**

Verify the router's X.25 address is set here.

WAN PARTNER → ADD → **Edit WAN Partner**

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

Encapsulation	X. 25

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

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

Note: If the remote site is another BinTec router 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 configure X.25 dialout without configuration?

In an X.25 network there is often a large amount of connection partners. Because the number of X.25 partners can theoretically be infinite, there is the possibility to configure dial-out to X.25 partners without configuring the partners individually.

For outgoing X. 25 calls a feature is implemented, which generates a ISDN number out of the destination X.25 address or the destination NSAP.

Before you begin

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

- The router's ISDN telephone number and X.25 address.

Configure it

X.25 → STATIC SETTINGS → **Configure X.25 Local Address**

Verify the router's X.25 address is set here. (optional)

WAN PARTNER → ADD → **Edit WAN Partner**

Create a new WAN partner interface and enable X.25 without configuration.

Encapsulation	X. 25 No Configuration, No Signalling

The now following steps must be configured via the SNMP shell in the MIB, because the necessary variables cannot be configured via the Setup Tool.

x25RouteTable

By adding the new WAN partner like described above a new interface was created.

In the ***x25RouteTable*** now a route for this new interface must be defined.

Example:

inx	SrcIfIndex(*rw) DstLinkAddr(rw) SrcNSAP(rw) ProtocolId(rw) NUI(rw) Cug(rw)	SrcLinkAddr(rw) DstLinkAddrMode(-rw) DstAddr(rw) CallUserData(rw) RewritingRule(rw) CugOutgoing(rw)	DstIfIndex(*rw) SrcAddr(rw) DstNSAP(rw) RPOA(rw) Metric(rw) CugBilateral(rw)
00	1		10008
		rule "*11499119673123"	
	-1		-1
		8	0
	-1	-1	-1

For the variables ***SrcAddr*** and ***DestAddr*** you can use wildcards.

The variable ***DstLinkAddrMode*** can be set to ***auto*** or ***rule***.

When set to ***auto*** the BRICK can generate the destination ISDN number automatically. A requirement for this function is that the X.25 address contains the ISDN number conform to the (extended) X.121 address format.

Note: **X.121 Address Format**

When the extended X.121 address format is used for the destination X.25 address contained in the X.25 call packet, the BRICK assumes that the address starts with an "@" followed by a "0" (TOA) and a "1" (NPI for ISDN). These three digits are deleted and the rest of the X.25 address is taken over as the destination ISDN number.
When the normal X.121 address format is used, the BRICK looks for a "0" (escape character for ISDN) or a "9" (escape character for analog connections) as the first digit of the X.25 address, deletes this first digit and again takes the rest of the X.25 address as the destination ISDN number.
These conventions are the requirement for using the value ***auto*** in the variable ***DstLinkAddrMode***.

In case the ISDN number is not contained in the X.25 address of the call packet the generating of the destination ISDN number must be defined via a rule like explained in the following.

You can set the variable ***DstLinkAddrMode*** to ***rule***. When done so, the variable ***RewritingRule*** must be assigned an integer from 0 to 999999,

which is the number of the rewriting rule used. Then you must generate an entry in the ***x25RewriteTable*** with this rewriting rule number.

x25RewriteTable

The rule for converting the destination X.25 address respectively NSAP into an ISDN number is defined in the variable ***dstLinkAddr*** of the ***x25RewriteTable***. This table contains table entries, which each belong to one rewriting rule number (variable RewritingRule). These numbers are referenced in the ***x25RouteTable*** described above.

Example:

inx	RewritingRule(*rw) NUI(rw) DstAddr(rw) CallUserData(rw) RespDstAddr(rw) RespCallUserData(rw) CugBilateral(rw)	ReverseCharging(-rw) SrcAddr(rw) DstNSAP(rw) RespSrcAddr(rw) RespDstNSAP(rw) Cug(rw) DstLinkAddr(rw)	RPOA(rw) SrcNSAP(rw) ProtocolId(rw) RespSrcNSAP(rw) RespProtocolId(rw) CugOutgoing(rw)
00	8	dont_change	dont_change
			-1
			-1
		-1	-1
	-1	"X%%%%00.....%%%456"	

The format of the variable ***dstLinkAddr*** consists of the following components:

[Layer 1 / Address Type] Input Rule

- Layer 1 / Address Type

  This part of the variable ***dstLinkAddr*** is optional.

  When nothing is defined "data_64k" is used as default.

Part of *dstLinkAddr*	Meaning
1	analog (modem)
2	V110_9600
3	MAC address
4	IP address

- Input

  This part of the variable ***dstLinkAddr*** is mandatory.
  It defines whether the input for the conversion is an X.25 address or a NSAP.

Part of *dstLinkAddr*	Meaning
X	X.25 address
N	NSAP

- Rule

  This part of the variable ***dstLinkAddr*** is mandatory.

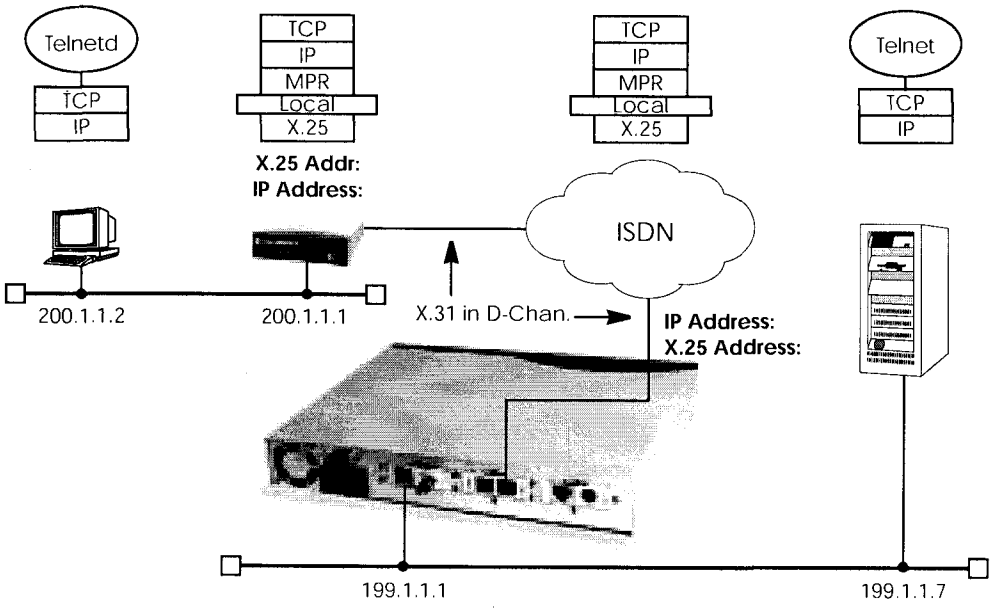
Part of *dstLinkAddr*	Meaning
.	take over one digit
%	delete one digit
*	take over the remaining digits
0-9	insert digits

Examples:

Rule	X.25 Address/NSAP	ISDN Number/MAC Address/IP Address
X%%%%%00.....%%%456	@11499119673123	009119673456
X%%%%%00.....4*	@11499119673123	0091196734123
N%%00.....4*	499119673123	0091196734123
3X%%%*	@5200a0f9000123	00:a0:f9:00:01:23
4X%%%*	@53c03635a0	192.54.53.160

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

The router 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 124.)



Before you begin

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

- The router's X.25 address.
- The remote partner's X.25 address.
- The remote partner's IP address.

Configure it

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.

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 IP → set.

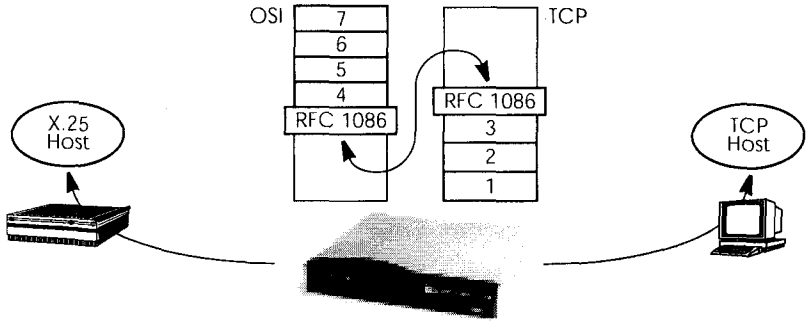
IP Transit Network	yes
Local ISDN IP Address	*<router's IP address>*
Partner's ISDN IP Address	*<MPX25 partner's IP address>*
Partner's LAN IP Address	*<optional>*
Partner's LAN Netmask	*<optional>*

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 170.

How do I use the router as a TCP-X.25 bridge?

The router can be used as a TCP-X.25 bridge as described in RFC 1086. Using this mechanism, the router 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 140) the router performs the appropriate protocol mappings as shown above.

Before you begin

No special information is required to configure the router 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

LICENSES → **Verify License**

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

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 123) 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. By default interfaces for ISDN: x31d-<*slot #*>-<*unit #*>-<*TEI*> and X.21 modules: xi<*slot #*> are available.

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.

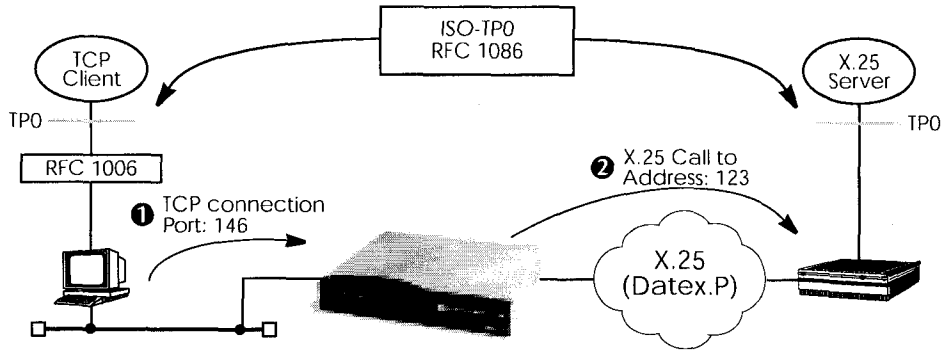
Source Link	*<X.25 interface name>*
Destination Link	local

More Info

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

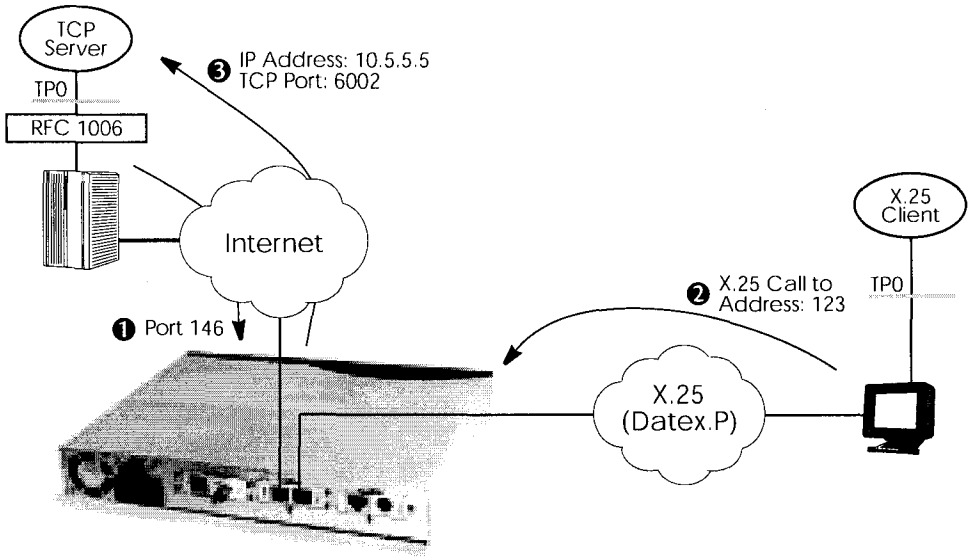
TCP Client requests connection to X.25 Server

Here the TCP-Client initiates a connection (as defined in RFC 1086) with the router using TCP port 146. The router 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 initate a connection with the router at TCP port 146 where it registers its IP address and port number. It instructs the router 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 router will listen for incoming calls to the registered address only as long as the TCP (port 146) connection between the registering host and the router exists.

How do I configure the routing for using an X.25 PAD?

To configure the X.25 PAD utility the ISDN interface configuration must be extended and a new software interface for the X.25 PAD must be created.

Before you begin

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

- The X.25 PAD's unique MSN (Multiple Subscriber Number)
- The remote X.25 network partner's name and possibly X.25 address

Configure it

Configure Hardware Interface

CM-1BRI, ISDN S0 → INCOMING CALL ANSWERING → ADD →

Here you create a new entry for incoming calls on the ISDN interface to be routed to the X.25 PAD.

Item	x25_pad
Number	*<X.25 PAD's MSN>*

Next you must add the X.25 PAD as a new WAN partner.

Edit WAN Partner

Because the X.25 PAD's WAN partners can not be identified by their caller's numbers, you must create one WAN Partner.

WAN PARTNER → ADD →

Create a new WAN partner interface.

Partner Name	*<X.25 PAD's partner name>*
Encapsulation	X.25 PAD

X.25 → LINK CONFIGURATION → **Create X.25 PAD Link**

We need to create a new link for the X.25 PAD's partner. Select the appropriate link template from the list:

<*X.25 PAD's partner name*> (create new configuration)

Highlight the entry and enter <Return> to configure the link.

Now you can edit the items and change them, if necessary. You might e.g. want to configure special values for **L3 Packet Size, L3 Window Size** or **Windowsize/Packetsize Neg.**

In general the default values you will find in this menu do not have to be changed. But even, if you do not make any changes you must leave the menu with **Save** to configure the Link Configuration for the X.25 PAD Partner.

Edit X.25 Routing Table

Depending on whether you want to define a static route from the X.25 PAD's partner interface to a single X.25 host/remote partner or multiple routes between several X.25 partners, the routing information differs.

First the routing configuration for a static routing between two X.25 partners (the X.25 PAD's partner and a remote X.25 host/partner).

X.25 → ROUTING → ADD →

Here we create an X.25 route that routes outgoing calls from the X.25 PAD to the remote X.25 network partner (X.25 host).

Source Link	<*X.25 PAD's partner name*>
Destination Link	<*X.25 network partner name*>

The partner used in the Destination Link must be configured before as an X.25 partner.

This second configuration is an example for connecting three X.25 partners, one of them the X.25 PAD's partner.

X.25 → ROUTING → ADD →

Source Link	<*X.25 PAD's partner name*>
Destination Link	<*X.25 network partner* name A>
Destination X.25 Address	1*

X.25 → ROUTING → ADD →

Source Link	<*X.25 PAD's partner name*>
Destination Link	<*X.25 network partner* name B>
Destination X.25 Address	2*

The partners used in the Destination Links must be configured before as X.25 partners.

More Info

For further information on the X.25 PAD see "X.25 PAD" on page 145.

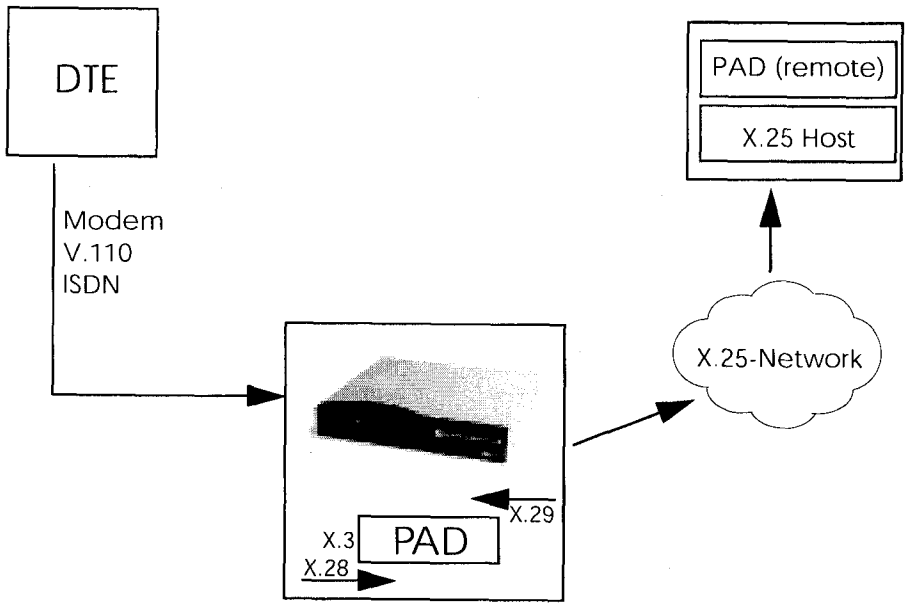
X.25 Utilities

X.25 PAD

General

The PAD is a data assembly / disassembly facility used to connect character-oriented asynchronous data terminal equipment (DTE) to the packet-oriented X.25 network (Datex-P). It is the task of PAD to convert character streams coming from the DTE into data packets and resolve data packets coming from the network into individual character streams that can be displayed on the DTE. In this context the character-oriented data terminal equipment is also called start-stop mode DTE (short: DTE) and a remote X.25 host is defined as packet mode DTE.

Recommendation X.29 defines the procedures between a PAD and a packet-mode DTE or another PAD and recommendation X.28 defines the DTE interface of a start-stop mode DTE accessing the PAD.



The PAD program is an implementation of the X.25 PAD according to the three following ITU-T recommendations:

X.3 Parameter definition

X.28 User interface / commands

X.29 PAD to PAD protocol

In each case, the standard of 1988 is implemented. The implementation should however also be compatible to earlier versions.

PAD features one command mode and one data transfer state. The commands are described below. PAD can manage only exiting calls, it cannot be called itself.

PAD command signals are directed from the DTE to the PAD and are described under "Commands conforming to X.28" on page 159. PAD service signals are directed from the PAD to the DTE and serve for e.g acknowledging PAD commands and or transmitting call progress signals to the DTE.

Additional features

There are two additional features built into the PAD to extend the standard X.25 PAD functionality.

One is the additional variable *AutoCallDstAdr* in the ***x25PadProfileTable***, which can contain an X.25 address, the PAD automatically establishes a connection to. The value of this variable must be defined in the ***x25PadProfileTable*** on the BRICK.

The second item is a timer that determines, when to close down a connection to the remote X.25 station, after the DTE has sent the CLR command to the PAD. This time period is defined by configuring the X.25 PAD's partner. It results from the sum of the values of two items in Setup Tool: **Static Short Hold** in the WAN/EDIT/ADVANCED menu (***Short Hold*** in the ***biboPPPTable*** of the MIB) and **Disconnect Timeout** in the X25/LINK/EDIT menu (***L2IdleTimer*** in the ***X25LinkPresetTable*** of the MIB).

PAD Parameters

All PAD parameters are stored in the variables of the ***x25PadProfileTable*** on the BRICK and can be edited there.

Additional Entries

Number

The value of this parameter defines the unique number of the PAD Profile.

Possible values:

0-99 PadProfileTable numbers

The PadProfileTables 0, 90 and 91 (see below) are implemented in the BRICK.

State

This parameter describes the state of the profile.

Possible Values:

1 The Profile is valid. (**valid**)

2 The Profile is set to delete. (**delete**)

The default value is 1 resp. valid.

AutoCallDstAddr

When this parameter is set to a non-empty string, a call will automatically be established to this PAD address.

By default this variable is empty. To activate the autocall function the user must enter a value (valid X.25 address) for this variable in the ***x25PadProfileTable*** (described below) on the BRICK.

Standard Parameters

The 22 standard PAD parameters defined in X.3 are listed in the table:

Number	Parameter	Description
1	Escape	PAD recall using a character

Number	Parameter	Description
2	Echo	Echo
3	ForwardChar	Selection of the data forwarding character
4	IdleTimer	Selection of idle timer delay
5	DevControl	Ancillary device control
6	SigControl	Control of PAD service control
7	BrkControl	Operation on receipt of the break signal
8	Discard	Discard output
9	CRPadding	Padding after carriage return
10	LineFold	Line Folding
11	Speed	Binary speed (read only)
12	FlowControl	Flow control of the PAD
13	LFInsert	Linefeed insertion after carriage return
14	LFPadding	Padding after linefeed
15	Edit	Editing
16	CharDel	Character delete
17	LineDel	Line delete
18	LineDisp	Line display
19	SigEdit	Editing PAD service signals
20	EchoMask	Echo mask
21	Parity	Parity treatment
22	PageWait	Page wait

The exact meanings of the individual parameters and their possible values are described in the following sections; "^X" stands for the simultaneously pressing the control key (also "Ctrl") and the X key; terms such as BEL or ACK refer to the corresponding characters in the International Alphabet No. 5 (IA5) according to ITU-T T.50.

1 Escape

Definition of a character which causes PAD to switch from the data transfer to the command mode (escape character).

Possible values:

0 It is not possible to leave the data transfer state.

1 Leave the data transfer state with "^P".

32-126 Defines the character of the IA5 with the number specified as escape character

The default value is 0.

If a connection exists, the PAD automatically switches back to the data transfer state after input of a valid command. An ecxception is the clear command.

2 Echo

Defines whether the echo mode is enabled or not.

Possible values:

0 The echo mode is disabled; no echo. (**no_echo**)

1 The echo mode is enabled. (**echo**)

The default value is 0 resp. no_echo.

Specifies whether an echo is to be created by the PAD or not.

Using parameter 20, **EchoMask**, specific characters can be exempted from the echo mode.

3 ForwardChar

Definition of characters upon which the PAD forwards the data entered up to that point as a packet (data forwarding character).

Possible values:

0 No data forwarding character assigned.

1 The characters <A>-<Z>, <a>-<z>, and <0>-<9> serve as data forwarding characters.

2 Data forwarding via activation of the "return" key (IA5 character 0/13, CR).

4 Data forwarding after input of either ESC, BEL, ENQ or ACK.

8 Data forwarding after input of either DEL, CAN or DC2.

16 Data forwarding after input of either EOT or EXT.

32 Data forwarding after input of either HT, LF, VT or FF.

64 All characters in columns 0 and 1 of the IA5 not specified above serve for data forwarding.

The default value is 0.

These values correspond to the individual bits in the 1-byte value that can be assigned to this parameter. The values can also be freely combined, e.g.:

126 All characters of columns 0 and 1 of the IA5 and the character 7/15, DEL serve for data forwarding (combination of the values 2+4+8+16+32+64).

Using the national parameters 121 and 122, another data forwarding character can be defined for each of them. Data forwarding takes place additionally via the BREAK signal and timer delay in the PAD (parameter 4, IdleTimer).

4 IdleTimer

Defines whether after a specific amount of time all data entered up to this point are to be forwarded as a packet.

Possible values:

0 No timer-controlled data forwarding.

1-255 n*50ms after the last input of a character, the data entered up to that point are forwarded as a packet.

The default value is 5 (= 250 ms).

The parameter value n indicates the delay time as a multiple of 50 ms, thus times of up to approx. 12s are possible.

If parameter 15, Edit, is set to 1, timer-controlled data forwarding is disabled.

5 DevControl

Defines use of the characters DC1 and DC3 for the control of ancillary devices.

Possible values:

0 No use of DC1 and DC3. (**no_use**)

DC1 corresponds to X-ON or ^Q, DC3 corresponds to X-OFF or ^S.

6 SigControl

Defines whether, and if so how, PAD service signals are forwarded to the DTE.

Possible values:

0 X.28 mode without PAD service signals.

1 X.28 messages are transmitted to the DTE.

5 X.28 messages are transmitted to the DTE, additionally a prompt ("*") is output in the command mode.

The default value is 1.

7 BrkControl

Defines the reaction of the PAD to the reception of the BREAK signal from the start-stop mode DTE in data transfer state.

Possible values:

0 No reaction.

1 Data forwarding, an interrupt packet is transmitted, the PAD remains in data transfer state.

2 Data forwarding, the virtual connection is reset with possible data loss, the PAD remains in data transfer state.

4 Send an "indication of break" PAD message to the packet-mode DTE (remote PAD).

5 Send an interrupt packet followed by an "indication of break" PAD message to the packet-mode DTE.

8 Data forwarding, switch to command mode

16 Discard output data to the DTE

21 Discard all output data to the DTE, data forwarding, send an interrupt packet and the PAD service signal BREAK indication with parameter field in which parameter 8 is set to 1, the PAD remains in data transfer state.

The default value is 8.

If no connection has been established, the BREAK signal is ignored.

The BREAK signal is not a character of the IA5. It always consists of an approx. 150 ms long continuous string of the level for binary 0.

Receiving a BREAK signal is a requirement for packet forwarding by the PAD except for parameter 7 is set to 0.

8 Discard

Defines whether user sequences in packets are output to the DTE or not.

If parameter 7 is set to 21, parameter 8 is set to 1 when a BREAK signal is received. From now on, all data outputs to the DTE are ignored until parameter 8 is reset to 0.

Possible values:

0 Normal data output to the DTE. (**normal_data_delivery**)

1 Data outputs to the DTE are ignored. (**discard_output**)

The default value is 0 resp. normal_data_delivery.

9 CRPadding

Defines the number of padding characters (NUL) generated after a CR to the DTE.

This parameter has meaning only for purely mechanical DTE (e.g. teletyper - it bridges the time required for the actual carriage return. For modern DTE this parameter is unnecessary, sometimes even interferes (e.g. with direct storing of data in a file).

Possible values:

0 No padding characters

1-255 Number of padding characters (NUL) - only useful for purely mechanical DTE.

The default value is 0.

This parameter is only used upon PAD service signals.

10 LineFold

Defines the number of characters after which automatic line folding (inserting the character CR) is to take place.

Possible values:

0 No automatic line folding

Depending on the settings of parameters 13 or 126, LF is inserted in addition to CR.

11 Speed

Defines the transmission speed of the DTE. This parameter is set automatically by the PAD. The parameter is only used internally and not listed in the ***x25PadProfileTable***. The possible values are described in ITU X.3.

12 FlowControl

Defines whether the user can effect a short-time stop (DC3) and restart (DC1) of the data flow to the DTE via input of the control characters DC1 and DC3.

Possible values:

0 No use of DC1 and DC3 for data flow control. (**no_use_DC1_DC3**)

DC1 corresponds to X-ON or ^Q, DC3 corresponds to X-OFF or ^S.

13 LFInsert

Defines whether the PAD inserts a LF after receiving CR.

Possible values:

0 No LF insertion.

1 LF insertion after each CR in the data stream to the start-stop mode DTE.

2 LF insertion after each CR from the start-stop mode DTE.

4 LF insertion after each CR in the echo stream to the start-stop mode DTE.

5 Combination of 1 and 4.

6 Combination of 2 and 4.

7 Combination of 1, 2 and 4.

The default value is 0.

This parameter is only applied in data transfer mode.

14 LFPadding

Defines the number of padding characters (NUL) which are output after an LF to the DTE.

0 No padding characters

15 Edit

Defines whether editing of user data is possible in data transfer state or not. If parameter 15 is set to 1, parameter 4 is disabled.

Possible values:

0 Editing not possible (**no_editing_user_data**)

1 Editing possible (**editing_user_data**)

The default value is 0 resp. no_editing_user_data

16 CharDel

Defines whether it is possible to delete characters already entered and which character is used for this function.

Possible values:

0-127 Decimal value of the character from the IA5 to be used for character delete.

The default value is 0.

17 LineDel

Defines whether it is possible to delete a line already entered and which character is to be used for this function.

Possible values:

0-127 Decimal value of the character from the IA5 to be used for line delete.

The default value is 0.

With the character defined, all characters entered since data were last forwarded are deleted.

18 LineDisp

Defines whether the characters entered and not yet forwarded can be output again on the DTE and which character is to be used for this function.

Possible values:

0-127 Decimal value of the character from the IA5 that is to be used for output of the last line.

The default value is 0.

19 SigEdit

Defines which PAD service signals are output after editing (character or line delete).

Possible values:

0 No editing PAD service signals.

1 Editing PAD service signals for printer; "XXX" is output to confirm line delete, "\" to confirm character delete.

2 Editing PAD service signals for display units; characters and lines are deleted visibly on the screen.

8, 32-126 Decimal value of the character from the IA5 that is to be output as editing PAD service signal for character delete.

The default value is 0.

20 EchoMask

Defines which characters are to be exempted from the echo function.

Possible values:

0 No echo mask.

1 No echo of character CR.

2 No echo of character LF.

4 No echo of characters VT, HT and FF.

8 No echo of characters BEL and BS.

16 No echo of characters ESC and ENQ.

32 No echo of characters ACK, NAK, STX, SOH, EOT, ETB and ETX.

64 No echo of the editing characters defined in parameters 16, 17 and 18.

128 No echo of DEL and of all characters in columns 0 and 1 of the IA5 not mentioned above.

The default value is 0.

Combinations of the given values are permitted.

The echo mask is effective only if parameter 2 is set to 1.

21 Parity

Defines whether parity bits are checked and/or generated in the PAD.

Possible values:

0 No parity bit checking or generation (**no_parity**)

22 PageWait

Defines the number of lines (or LF characters) after which the PAD is to interrupt output to the DTE.

Possible values:

0 Page wait disabled

National Parameters according to Datex-P

If a national parameter is changed, the respective standard parameter is changed also, and vice versa.

118 XCharDel

This parameter is a repetition of parameter 16.

The default value is 0.

119 XLineDel

This parameter is a repetition of parameter 17.

The default value is 0.

120 XLineDisp

This parameter is a repetition of parameter 18.

The default value is 0.

121 XForwardChar1 and 122 XForwardChar2

Allow the definition of up to two data forwarding characters in addition to parameter 3.

Possible values:

0 No additional data forwarding character

1-126 Decimal value of the character from the IA5 to be used as data forwarding character.

The default value for both parameters is 0.

123 XParity

Corresponds to parameter 21.

Possible values:

0 No parity bit checking or generation (**no_parity**)

125 XDelay

Defines how long data forwarding is to be delayed if it occurs simultaneously with a data input.

Possible values:

0 No delay of data forwarding. Only with full-duplex connections (parameter 2 is set to 1).

1-255 Number of seconds by which data forwarding is to be delayed.

The default value is 0.

If input editing is possible (parameter 15 is set to 1), a sufficiently large value should be selected for parameter 125 (e.g. 60 seconds) so that incoming data are not written into the data to be edited.

Each character entered resets the delay counter to 0. However, after input of an appropriate character, data forwarding starts immediately.

126 XLFInsert

This parameter is a repetition of parameter 13.

The default value is 0.

PAD Commands

Guidelines on Notation

The PAD understands the commands described below.

The character "↵" stands for pressing the "return" key (carriage return).

Alternatives are separated by a " | "; for example, "yes | no" means, that either "yes" or "no" can be entered.

Terms in [square brackets] are optional, terms in {curved brackets} are optional and can be repeated any number of times, terms in <angle brackets> must be replaced by an appropriate character sequence (e.g., <ParNo> stands for a specific parameter number).

Except for the characters {[< | >]} and text in parentheses, all characters of the commands must be entered exactly as indicated in this section.

Upper and lower case letters as well as spaces can be used freely within the commands - internally, lower case letters are converted to upper case letters, spaces are ignored, and the command is executed only after these processes.

The service signals output by the PAD are given here for the standard setting (parameter 6 has the value 1).

Commands conforming to X.28

STAT↵

Queries the status of a connection. In response, one of the following messages is given, depending on whether the connection is free or engaged:

FREE not connected

ENGAGED connected

CLR↵

Disconnects the selected virtual connection. The command is acknowledged with the message:

CLR CONF Disconnect, local cause.

Data that are still in the network when the command is transmitted can be lost.

Within a specified time interval (see page 146) after a CLR command has been sent, another command can be sent or a new connection can be initiated.

ICLR↵

After having received this command the PAD transmits an "Invitation to clear" to the remote partner, i.e. an "invitation" to disconnect the existing connection.

In all the following commands, possible inputs for <ParNo> are the number of the respective parameter (1-22, 118-123, 125-126).

Generally, only the parameter number is indicated in PAD outputs.

PAR? [<ParNo>{,<ParNo>}]↵

Queries the current values of the parameters indicated or of all parameters if no parameter number is given (here the square brackets indicate that the specification of the parameters is optional).

The parameter values are output as follows:

PAR <ParNo>:<value>>{,<ParNo>:<value>}

If an invalid parameter number was entered for <ParNo>, the following message is output:

PAR <ParNo>:INV

RPAR? [<ParNo>{,<ParNo>}]↵

Queries the current values of the parameters indicated or of all parameters if no parameter number is given (here the square brackets indicate that the specification of the parameters is optional) of the remote PAD (= the packet-mode DTE). The local PAD won't put out a message until the remote PAD has answered. When the remote PAD answers with the value(s) of the parameter(s), the local PAD puts them out to the start-stop mode DTE.

The parameter values are output as follows:

PAR <ParNo>:<value>>{,<ParNo>:<value>}

If an invalid parameter number was entered for <ParNo>, the following message is output:

PAR <ParNo>:INV

SET <ParNo>:<value>{,<ParNo>:<value>}↵

Used for setting the parameter values.

The value ranges for the individual parameters are described in detail in the sections "Additional Entries", "PAD Parameters", "National Parameters".

If an invalid parameter number or value was entered for <ParNo>, the following message is output:

PAR <ParNo>:INV

If the parameter number and value entered were valid no confirmation message is put out.

SET? <ParNo>:<value>{,<ParNo>:<value>}↵

Used for setting and querying the parameter values.

The value ranges for the individual parameters are described in detail in the sections "Additional Entries", "PAD Parameters", "National Parameters".

If an invalid parameter number or value was entered for <ParNo>, the following message is output:

PAR <ParNo>:INV

If the parameter number and value entered were valid, the parameters just set are output for checking purposes in the following form:

PAR <ParNo>:<value> {,<ParNo>:<value>}

RSET? <ParNo>:<value>{,<ParNo>:<value>}↵

Used for setting and querying the parameter values of the remote PAD. When the local PAD receives this command, it will send a request to set and put out the specified parameters to the remote PAD. The local PAD won't put out a message until the remote PAD has an-

swered. When the remote PAD answers with the value(s) of the parameter(s), the local PAD puts them out to the start-stop mode DTE.

The value ranges for the individual parameters are described in detail in the sections "Additional Entries", "PAD Parameters", "National Parameters".

If an invalid parameter number or value was entered for <ParNo>, the following message is output:

PAR <ParNo>:INV

If the parameter number and value entered were valid, the parameters just set are output for checking purposes in the following form:

PAR <ParNo>:<value> {,<ParNo>:<value>}

It is possible and permissible to assign the same value (especially the same character) to different parameters (and thus to the functions controlled by them). If the PAD receives such a character assigned to several functions, it executes only the function with the highest priority. The priorities are defined as indicated in the table below.

Priority	PAD Function	ParNo
highest	Recall of the PAD	1
.	Command separating character ("+", "↵")	-
.	DC1, DC3	12, 22
.	Output of last line	18/ 120
.	Delete one character	16/ 118
	Delete one line	17/ 119
lowest	Data forwarding character	3

PROF <ProfileNo>↵

Used for selection of settings for profile <ProfileNo>.

The values 0-99 are possible as <ProfileNo>; the settings of profiles 0, 90 and 91 are summarized in the following table. User-specific settings for profiles 0-89 and 92-99 are possible.

Parameters	Profile		
	0	90	91
Escape	0	1	0
Echo	0	1	0
ForwardChar	0	126	0
IdleTimer	30	0	20
DevControl	0	1	0
SigControl	1	1	0
BrkControl	8	2	2
Discard	0	0	0
CRPadding	0	0	0
LineFold	0	0	0
FlowControl	0	1	0
(X)LFInsert	0	0	0
LFPadding	0	0	0
Edit	0	0	0
(X)CharDel	0	127	127
(X)LineDel	0	24	24
(X)LineDisp	0	18	18
SigEdit	0	1	1
EchoMask	0	0	0
Parity	0	0	0
PageWait	0	0	0

Parameters	Profile		
	0	90	91
XForwardChar1	0	0	0
XForwardChar2	0	0	0
XParity	0	0	0
XDelay	0	0	0

Profile 0 is the initial profile set at the start of PAD (see page 23).
Profile 90 is the simple standard profile according to X.28.
Profile 91 is the standard transparent profile according to X.28.

(The settings for the individual profiles can be queried on the BRICK in the ***x25PadProfileTable***.)

RESET↵
Resets an existing connection to the initial state without disconnecting it, i.e. all data packets sequence numbers are set to 0 and no data packets are on the transfer section.

INT↵
Transmits an interrupt packet. The PAD only sends a line feed (CR LF) as acknowledgement of this command.

<address>↵
Establishes a connection to the <address> (valid X.25 address) indicated after a physical connection has been established.
Also see the parameter "AutoCallDstAddr" on page 147.

^P
After input of this character the PAD switches from the data transfer state to the command mode, if parameter 1 has the value 1. Other char-

acters are also possible instead of ^P (Control-P), please refer to the description of parameter 1 on page 149.

This command is acknowledged by a prompt "*" only if parameter 6 is set to an appropriate value.

The PAD now waits for the input of a PAD command.

In the X.28 mode, the PAD automatically returns to the data transfer state after each command (except the CLR command).

Under certain conditions, it is possible to effect a short-time stop and restart of the output by entering DC1 and DC3, see the description of parameter 12 on page 153.

Further Commands

In addition, the following command is implemented:

BYE↵
Terminates PAD (and disconnects an existing connection)

Validity of PAD Commands

The following matrix shows the validity of PAD command signals in dependence of the state of the DTE (start-stop mode DTE):

PAD command	Valid before virtual call set-up	Valid after escaping from data transfer state
<address>	X	
PROF	X	X
SET	X	X
SET?	X	X

PAD command	Valid before virtual call set-up	Valid after escaping from data transfer state
PAR?	X	X
CLR		X
STAT	X	X
RESET		X
INT		X
RSET?		X
RPAR?		X
ICLR		X

Initial Profile

Whenever a new PAD is created by accepting an ISDN call, the values of the parameters are initialized according to the initial profile, which is always profil 0.

The profiles 0 (initial profile), 90 (simple standard profile) and 91 (transparent standard profile) are by default implemented in the BRICK. These profiles can be selected with the command PROF (see page 162). These three profiles can also be selected, when they are not entered in the *x25PadProfileTable*.

In the following paragraphs, the default settings for all parameters are indicated, with the number (here the PAD parameter number, not the number of the table entry) and name of the parameter followed by a description of the value selected.

1 Escape

0 It is not possible to leave the data transfer state.

2 Echo

0 The echo mode is disabled; no echo. (**no_echo**)

3 ForwardChar

0 No data forwarding character assigned

4 IdleTimer

5 5*50ms= 250 ms

5 DevControl

0 No use of DC1 and DC3 (**no_use**)

6 SigControl

1 X.28 messages are transmitted to the DTE.

7 BrkControl

8 Data forwarding, switch to command mode

8 Discard

0 Normal data output to the DTE (**normal_data_delivery**)

9 CRPadding

0 No padding characters

10 LineFold

0 No automatic line folding

11 Speed

Detected automatically; internal value

12 FlowControl

0 No use of DC1 and DC3 for data flow control. (**no_use_DC1_DC3**)

13 LFInsert

0 No LF insertion

14 LFPadding

0 No padding characters

15 Edit

0 Editing not possible (**no_editing_user_data**)

16 CharDel

0 No editing

17 LineDel

0 No editing

18 LineDisp

0 No display

19 SigEdit

0 No editing PAD service signals

20 EchoMask

0 No echo mask

21 Parity

0 No parity bit checking or generation (**no_parity**)

22 PageWait

0 Page wait disabled

118 XCharDel

Repetition of parameter 16

119 XLineDel

Repetition of parameter 17

120 XLineDisp

Repetition of parameter 18

121 XForwardChar1

0 No additional data forwarding character

122 XForwardChar2

0 No additional data forwarding character

123 XParity

0 No parity bit checking or generation (**no_parity**)

125 XDelay

0 No delay of data forwarding; Only with full-duplex connections (parameter 2 is set to 1)

126 XLFInsert

Repetition of parameter 13

Disconnect by the remote PAD

If a connection is cleared by the remote PAD or by the network, the local PAD returns to the command mode. If parameter 6 (PAD messages) is set to 0, the PAD cannot communicate the disconnect to the user. The PAD is terminated in this case.

Configuration Necessities for the PAD

The configuration of the X.25 PAD is described in the section "How do I configure the routing for using an X.25 PAD?" on page 142.

minipad

minipad [**-7**] [**-p** ‹*pktsz*›] [**-w** ‹*winsz*›] [**-c** ‹*cug*›] [**-o** ‹*outgocug*›] [**-b** ‹*bcug*›] ‹*x25address*›

The minipad program is a basic PAD (Packet Assembler/Disassembler) program that can be used to provide a remote login services for remote X.25 hosts. Minipad takes the following arguments:

-7 Use 7 bit data bytes only.

-p ‹*pktsz*›
Open data connection with packet size ‹*pktsz*›.

-w ‹*winsz*›
Open data connection with window size ‹*winsz*›.

-c ‹*cug*› Closed user group. Possible values for ‹*cug*›: 0-9999.

-o ‹*outgocug*›
Closed user group with outgoing access.
Possible values for ‹*outgocug*›: 0-9999.

-b ‹*bcug*›
Bilateral Closed user group.
Possible values for ‹*bcug*›: 0-9999.

‹*x25address*›
Either a standard X.121 address or an extended address.

Minipad is also useful for testing X.25 routes. To diasble X.25 connections to the minipad, *x25LocalPadCall* must be set to "dont_accept".

X.25 Diagnostic Code

X.25 diagnostic codes are reported in the x25CallHistoryTable. Note that only clear and diagnostic causes reported by the ISDN are stored in this table (via the ClearCause and ClearDiag fields). Restart and Reset causes may be detected when tracing ISDN channels.

The diagnostic codes are devided up in following groups:

- Clear Causes
- Diagnostic Causes
- Restart Causes
- Reset Causes

Clear Causes

Clear causes are reported in the *ClearCause* field of the ***x25CallHistoryTable***

1	0x01	number busy
3	0x03	invalid facility request
5	0x05	network congestion
9	0x09	out of order
11	0x0B	access barred
13	0x0D	not obtainable
17	0x11	remote procedure error
19	0x13	local procedure error
21	0x15	RPOA out of order
25	0x19	reverse charging acceptance not subscribed

33	0x21	incompatible destination
41	0x29	fast select acceptance not subscribed
57	0x39	ship absent

Diagnostic Causes

Diagnostic causes are reported in the *ClearDiag* field of the ***x25CallHistoryTable***

0	0x00	no additional information
1	0x01	invalid P(S)
2	0x02	invalid P(R)
16	0x10	packet type invalid
17	0x11	for state r1
18	0x12	for state r2
19	0x13	for state r3
20	0x14	for state p1
21	0x15	for state p2
22	0x16	for state p3
23	0x17	for state p4
24	0x18	for state p5
25	0x19	for state p6
26	0x1a	for state p7

27	0x1b	for state d1
28	0x1c	for state d2
29	0x1d	for state d3
32	0x20	packet not allowed
33	0x21	unidentifiable packet
34	0x22	call on one-way logical channel
35	0x23	invalid packet type on a PVC
36	0x24	packet on unassigned logical channel
37	0x25	reject not subscribed to
38	0x26	packet too short
39	0x27	packet too long
40	0x28	invalid GFI
41	0x29	restart packet with nonzero logical channel identifier
42	0x2a	packet type not compatible with facility
43	0x2b	unauthorized interrupt confirmation
44	0x2c	unauthorized interrupt
45	0x2d	unauthorized reject
48	0x30	time expired
49	0x31	for incoming call
50	0x32	for clear indication
51	0x33	for reset indication

52	0x34	for restart indication
53	0x35	for call deflection
64	0x40	call set-up, call clearing or registration problem
65	0x41	facility/registration code not allowed
66	0x42	facility parameter not allowed
67	0x43	invalid called DTE address
68	0x44	invalid calling DTE address
69	0x45	invalid facility/registration length
70	0x46	incoming call barred
71	0x47	no logical channel available
72	0x48	call collision
73	0x49	duplicate facility request
74	0x4a	nonzero address length
75	0x4b	nonzero facility length
76	0x4c	facility not provided when expected
77	0x4d	invalid CCITT-specified DTE facility
78	0x4e	max number of call redirections/deflections exceeded
80	0x50	miscellaneous
81	0x51	improper cause code from DTE
82	0x52	non aligned octet
83	0x53	inconsistent Q bit setting

84	0x54	NUI problem
112	0x70	international problem
113	0x71	remote network problem
114	0x72	international protocol problem
115	0x73	international link out of order
116	0x74	international link busy
117	0x75	transit network facility problem
118	0x76	remote network facility problem
119	0x77	international routing problem
120	0x78	temporary routing problem
121	0x79	unknown called DNIC
122	0x7a	maintenance action
144	0x90	timer expired or retransmission count surpassed
145	0x91	for interrupt
146	0x92	for data
147	0x93	for reject
160	0xa0	DTE-specific signals
161	0xa1	DTE operational
162	0xa2	DTE not operational
163	0xa3	DTE resource constraint
164	0xa4	fast select not subscribed

165	0xa5	invalid partially full data packet
166	0xa6	D-bit procedure not supported
167	0xa7	registration/cancellation confirmed
224	0xe0	OSI network service problem
225	0xe1	disconnection (transient condition)
226	0xe2	disconnection (permanent condition)
227	0xe3	connection rejection - reason unspecified (transient condition)
228	0xe4	connection rejection - reason unspecified (permanent condition)
229	0xe5	connection rejection - quality of service not available (transient condition)
230	0xe6	connection rejection - quality of service not available (permanent condition)
231	0xe7	connection rejection - NSAP unreachable (transient condition)
232	0xe8	connection rejection - NSAP unreachable (permanent condition)
233	0xe9	reset - reason unspecified
234	0xea	reset - congestion
235	0xeb	connection rejection - NSAP address unknown (permanent condition)
240	0xf0	higher layer initiated
241	0xf1	disconnection - normal
242	0xf2	disconnection - abnormal

243	0xf3	disconnection - incompatible information in user data
244	0xf4	connection rejection - reason unspecified (transient condition)
245	0xf5	connection rejection - reason unspecified (permanent condition)
246	0xf6	connection rejection - quality of service not available (transient condition)
247	0xf7	connection rejection - quality of service not available (permanent condition)
248	0xf8	connection rejection - incompatible information in user data
249	0xf9	connection rejection - unrecognizable protocol identifier in user data
250	0xfa	reset - user synchronization

Restart Causes

Restart causes are reported by the ISDN and may be detected when tracing ISDN channels.
These causes are not stored on the BRICK.

1	0x01	local procedure error
3	0x03	network congestion
7	0x07	network operational

Reset Causes

Reset causes are reported by the ISDN and may be detected when tracing ISDN channels.
These causes are not stored on the BRICK.

3	0x03	remote procedure error
5	0x05	local procedure error
7	0x07	network congestion
17	0x11	incompatible destination
1	0x01	out of order (PVC)
9	0x09	remote DTE operational (PVC)
15	0x0F	network operational (PVC)
29	0x1D	network out of order (PVC)

X.25 Syslog Messages

(biboAdmSyslogSubject = x25)

Note: The value <fd> used in X.25 system messages is an internal file number to discriminate between the different X.25 and TCP connections.

biboAdmSyslogMessage	***~Level***
ifc 1 vc <*vc*>: receive window exceeded, call cleared Protocol error in X.25 connection directly to BRICK (Interface 1).	err
ifc 1 vc <vc>: N(R) out of range, call cleared Protocol error in X.25 connection directly to BRICK (Interface 1).	err
Cannot rewrite call packet; Rule ... does not exist A rewriting rule has been referenced in ***x25RouteTable***, that is not defined in ***x25RewriteTable.***	err
Unable to route call to IFC ... (X.25 not supported) cannot use ifc ... for routing (ifc does not support X25) The specified target interface in an entry of the ***x25RouteTable*** does not support X.25.	err
source address too long (... bytes) The Link Layer Address (MAC) of a target interface specified in the ***x25RouteTable*** is longer than 20 Octets.	err
cannot use undefined ifc ... for routing The target interface of an entry in the ***x25RouteTable*** does not exist.	err

biboAdmSyslogMessage	***~Level***
channel misconfiguration (HIC) on ifc <*ifc*> channel misconfiguration (LTC) on <*ifc*> channel misconfiguration (HTC) on ifc <*ifc*> channel misconfiguration (LOC) on ifc <*ifc*> channel misconfiguration (HOC) on ifc <*ifc*> The channel specification of a link in the ***x25LinkPresetTable*** does not match the condition: LIC <= HIC < LTC <= HTC < LOC <= HOC	err
ifc=<*ifc*> [addr=...] vc=<*vc*> recv CALL <*SrcAddr*> -> <*DstAddr*> fac=<*fac*> cud=<*user data*> An X.25 CALL-REQUEST/INDICATION has been received. The message contains the interface index, optionally the link-address, the virtual circuit number, source and target address, the call facilities and the call user data.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> send CALL <*SrcAddr*> -> <*DstAddr*> fac=<*fac*> cud=<*user data*> An X.25 CALL-REQUEST/INDICATION is being sent The message contains the interface index, optionally the link-address, the virtual circuit number, source and target address, the call facilities and the call user data.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> recv CALL CONFIRM <*SrcAddr*> -> <*DstAddr*> fac=<*fac*> cud=<*user data*> An X.25 CALL-RESPONSE/CONFIRMATION has been received. The message contains the interface index, optionally the link-address, the virtual circuit number, source and target address, the call facilities and the call user data.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> send CALL CONFIRM <*SrcAddr*> -> <*DstAddr*> fac=<*fac*> cud=<*user data*> An X.25 CALL-RESPONSE/CONFIRMATION is being sent. The message contains, the interface index, optionally the link-address, the virtual circuit number, source and target address, the call facilities and the call user data.	debug

biboAdmSyslogMessage	***~Level***
ifc=<ifc> [addr=...] vc=<*vc*> recv CLEAR cause=<*causecode*> diag=<*diagcode*> A X.25 CLEAR-REQUEST/INDICATION has been received with the given cause and diagnostic codes. The value -1 means, cause or diagnostic not present.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> send CLEAR cause=<*causecode*> diag=<*diagcode*> A X.25 CLEAR-REQUEST/INDICATION is being sent with the given cause and diagnostic codes. The value -1 means, cause or diagnostic not present.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> send CLEAR A X.25 CLEAR-REQUEST/INDICATION is being sent without cause and diagnostic.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> recv CLEAR CONFIRM A X.25 CLEAR-RESPONSE/CONFIRM has been received on the given VC.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> send CLEAR CONFIRM A X.25 CLEAR-RESPONSE/CONFIRM is being sent.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> recv RESET A X.25 RESET-REQUEST/INDICATION has been received on the given VC.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> send RESET A X.25 RESET-REQUEST/INDICATION is being sent.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> recv RESET CONFIRM A X.25 RESET-RESPONSE/CONFIRM has been received on the given VC.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> send RESET CONFIRM A X.25 RESET-RESPONSE/CONFIRM is being sent.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> recv INTERRUPT A X.25 INTERRUPT has been received on the given VC	debug

biboAdmSyslogMessage	***~Level***
ifc=<*ifc*> [addr=...] vc=<*vc*> send INTERRUPT A X.25 INTERRUPT is being sent.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> recv INTERRUPT CONFIRM A X.25 INTERRUPT-CONFIRM has been sent on the given VC	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> send INTERRUPT CONFIRM A X.25 INTERRUPT-CONFIRM is being sent.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> recv DIAG cause=<*causecode*> diag=<*diagcode*> A X.25 DIAG has been received on the given VC. This message is ignored.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> invalid VC number A call on an unassigned VC number was received.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> call collision A call collision occurred on the given VC and will be handled according to X.25.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> TIMEOUT A timeout condition occurred on a VC while waiting for a CALL-RESPONSE/CONFIRMATION, CLEAR-RESPONSE/CONFIRMATION, or a RESET-RESPONSE/CONFIRMATION. The call will be cleared.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> windowsize=<*incoming*>/<*outgoiung*> packetsize=<*incoming*>/<*outgoiung*> The call's incoming/outgoing parameters for windowsize and packetsize will used according to the given values (possibly after negotiation).	debug
ifc=<*ifc*> [addr=...] recv RESTART cause=<*cause*> A restart packet has been received on the given link with the given cause. If the cause value is set to -1, the cause was not present in the message.	debug

biboAdmSyslogMessage	***~Level***
ifc=<*ifc*> [addr=...] send RESTART A RESTART packet is being sent over the given link.	debug
ifc=<*ifc*> [addr=...] recv RESTART CONFIRM A RESTART-CONFIRM packet has been received on the given link.	debug
ifc=<*ifc*> [addr=...] send RESTART CONFIRM A RESTART-CONFIRM packet is being sent over the given link	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> recv ILLEGAL message An unknown message has been received on the given VC.	debug
ifc=<*ifc*> [addr=...] vc=<*vc*> invalid VC number	debug
ifc=<*ifc*> [addr=...] TIMEOUT A timeout occurred on the given link, while waiting for RESTART, RESTART-CONFIRMATION, XID negotiation, link establishment or being idle.	debug
ifc=<*ifc*> [addr=...] restarting The restart procedure starts on the given link and a restart packet is being sent.	debug
ifc=<*ifc*> [addr=...] resetting layer 2 The layer 2 of the given link is being reset due to a timeout while waiting for a RESTART. A SABM[E] will be sent.	debug
ifc=<*ifc*> [addr=...] disconnecting layer 2 The given link will be disconnected, while being idle, i.e. no VCs being established. A DISC will be sent.	debug
ifc=<*ifc*> [addr=...] connecting layer 2 The given link will be established and a SABM[E] will be sent.	debug

biboAdmSyslogMessage	***~Level***
ifc=<*ifc*> [addr=...] layer 2 connected The connect request (SABM[e]) has been accepted by the peer and a UA frame has been received.	debug
ifc=<*ifc*> [addr=...] accept layer 2 connect An incoming connect indication (SABM[E]) on the given link will be accepted and a UA frame being sent.	debug
ifc=<*ifc*> [addr=...] accept layer 2 reset An incoming reset indiaction (SABM[E]) on the given link will be accepted and a UA frame being sent.	debug
ifc=<*ifc*> [addr=...] layer 2 resetted The reset request (SABM[e]) has been accepted by the peer and a UA frame has been received.	debug
ifc=<*ifc*> [addr=...] layer 2 disconnected A disconnect indication (DISC) has been received on the given link and the link is no longer established.	debug
dialup *ifc* ... The given interface is dialed up due to an X.25 call routed to it. The message contains, the interface index, optionally the link-address, the virtual circuit number, source and target address, the call facilities and the call user data.	debug
txd[<*fd*>]: <*tcpaddr*>:<port> New TCP connection A new incoming TCP connection from the specified TCP address via the local port 146 has been established.	debug
txd[<*fd*>]: <*tcpaddr*>:<port> First byte ... - not supported The first byte the TCP host sent to port 146 isn't supported by the Brick. Only the values 1 and 2 are allowed.	debug
txd[<*fd*>]: <*tcpaddr*>:<*port*> Connect to a particular X.25 host The host with the specified TCP address wants to connect to a particular X.25 host.	debug

biboAdmSyslogMessage	***~Level***
txd[<*fd*>]: <*tcpaddr*>:<*port*> Listen for incoming X.25 call on addr=<*address*> The host with the specified TCP address wants to listen for incoming X.25 connections for the specified X.25 listening address.	debug
txd[<*fd*>]: <*tcpaddr*>:<*port*> Timeout while reading X.25 address The specified TCP host didn't send the X.25 address completely within a certain amount of time.	debug
txd[<*fd*>]: <*tcpaddr*>:<*port*> unsupported X.25 address type The address type field entry of the X.25 address, the TCP host sent, isn't supported by the Brick. Only the values 3 and 4 are allowed.	debug
txd[<*fd*>]: <*tcpaddr*>:<*port*> Could not read 16 byte TCP/IP packet The specified TCP host didn't send the complete TCP/IP address of the listening TCP host within a certain amount of time.	debug
txd[<*fd*>]: <*tcpaddr*>:<*port*> IP Address type ... not supported The address type field entry of the TCP/IP address of the listening TCP host, isn't supported by the Brick. Only the value 2 is allowed.	debug
txd[<*fd*>]: <*tcpaddr*>:<*port*> Connection to X.25 host addr=... failed The TCP host wanted to connect to the specified X.25 address but the Brick couldn't reach the X.25 host.	debug
txd[<*fd*>]: X.25 CALL_IND dest_addr=<*address*> An X.25 call indication for the specified X.25 address was received by the Brick.	debug

biboAdmSyslogMessage	***~Level***
txd[<*fd*>]: Connection failed - wrong X.25 address There is currently no TCP host bound to the X.25 address of the previously received X.25 call indication.	debug
txd[<*fd*>]: Connected to X.25 addr=... An incoming X.25 connection was established	debug
txd[<*fd*>]: Connected to TCP <*tcpaddr*>:<*port*> The Brick opened an new TCP connection to the specified listening TCP host.	debug
txd[<*fd*>]: <*tcpaddr*>:<port> TCP <--> txd[<*fd*>] X.25 addr=... connected The Brick connected an incoming X.25 call to the specified TCP host.	debug
txd[<*fd*>]: Disconnect and close connection The Brick disconnects the TCP host and the X.25 host.	debug
txd[<*fd*>]: Received disconnect, cause=<*causecode*> diag=<*diagcode*> The Brick received a disconnect message from the X.25 connection. The cause and diagnostic codes of the X.25 clear indication message are shown.	debug
txd[<*fd*>]: Received disconnect The Brick received a disconnect message from the TCP connection.	debug
No License An attempt has been made to use X.25 without a valid license.	info

X.21 Communications Module

Normal Operation Mode

During normal operation, PWR (power) always displays whether the router is receiving power. ERR (error) is normally off but may blink when an error, such as a cabling problem, has occurred.

Depending on which slots your communications modules are installed the A/B LEDs for slots 1, 2, and 3 are as follows:

CM-X21

LED	State	Meaning
A	On	Currently receiving an X.21 frame.
B	On	Currently sending an X.21 frame.

Depending on which slots your communications modules are installed the LEDs for slots 1 through 6 (S1 ... S6) are as follows:

Modules	State	Meaning
CM-X21	On	Sending or receiving a packet.

CM-X21Adapter

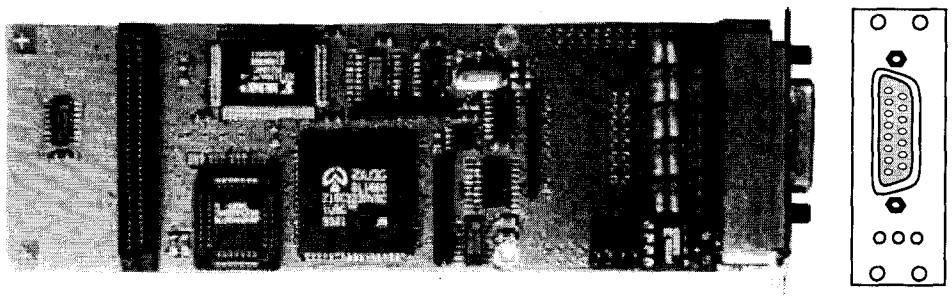


Figure 8: CM-X21 Adapter

The CM-X21 module provides a standard X.21 interface which complies with the V.11 recommendation. The X.21 interface provides a full-duplex synchronous mode and can be configured to operate as either a DTE (pas-

sive mode) or DCE (active mode). When in active mode the X.21 interface can be set to operate at baud rates between 2400 and 2048k.

There are also three status indicators located on the back plane. The LEDs indicate various status conditions, as follows:

CM-X21 back plane LEDs:

Colour	State	Meaning
Red	On	Error transmitting a packet.
Amber	On	Frame being sent/received.
Green	On	Layer 1 is active (i.e., incoming and outgoing calls are possible).

Note: The four jumper settings on the X.21 module are intended for future use. They should remain bridged (or jumpered), these are the default settings and should not be changed.

15 Pin Port for the CM-X21

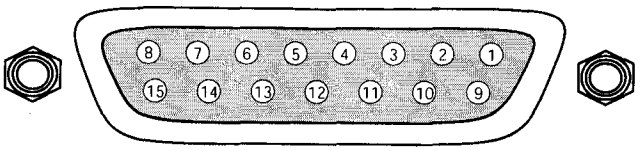


Figure 9: 15 Pin X.21 Port

The pin assignements for the CM-X21 module conform to the V.11 recommendations and are as follows:

Pin	Function	Mnemonic
1	Protection Ground	PG
2	Transmit (A)	T
3	Control (A)	I
4	Receive (A)	R
5	Indicate (A)	I
6	Signal Timing Element (A)	S
7	Not Connected	
8	Signal Ground	SG
9	Transmit (B)	T
10	Control (B)	I
11	Receive (B)	R
12	Indicate (B)	I
13	Signal Timing Element (B)	S
14	Not Connected	
15	Not Connected	

7

FRAME RELAY

What's covered

Frame Relay is officially supported on the BIANCA/BRICK-XL2, BIANCA/BRICK-XMP, BIANCA/BRICK-XM with 2MB flash, BIANCA/BRICK-XS with 2MB flash, and on the BinGO! Plus/Professional. The BRICK (the expression ***BRICK*** in the further text of this Chapter also encloses the BinGO! Plus/Professional) can be used as a Frame Relay Switch or a Frame Relay Router and supports the following official and defacto standards:

RFC 1490 *Multiprotocol Interconnect over Frame Relay*
RFC 1293 *Inverse Address Resolution Protocol*
ITU-T Q933a, Appendix II, X6 *Line Management Extensions*
FRF 1.1 *Congestion Management*

Frame Relay requires a separate license to be installed on the BRICK and may be purchased directly from BinTec Communications or your local distributor.

Frame relay is a connection oriented technology that provides a fast packet-switching service for access to Wide Area Networks. It makes optimum use of available bandwidth using a complex statistical multiplexing algorithm. Due to the ommitance of some layer three network functions, Frame Relay is often thought of as a "streamlined version for X.25".

Frame Relay is a flexible and cost-effective alternative to existing WAN technologies best suited for network installations exemplifying any of the following characteristics:

- Applications generate significant amounts of bursty-traffic
- Network traffic is delay-sensitive
- High network availability is a major priority
- Dispersed enterprise (locations separated by long distances)
- Integration with existing public and/or private packet switched networks is required.

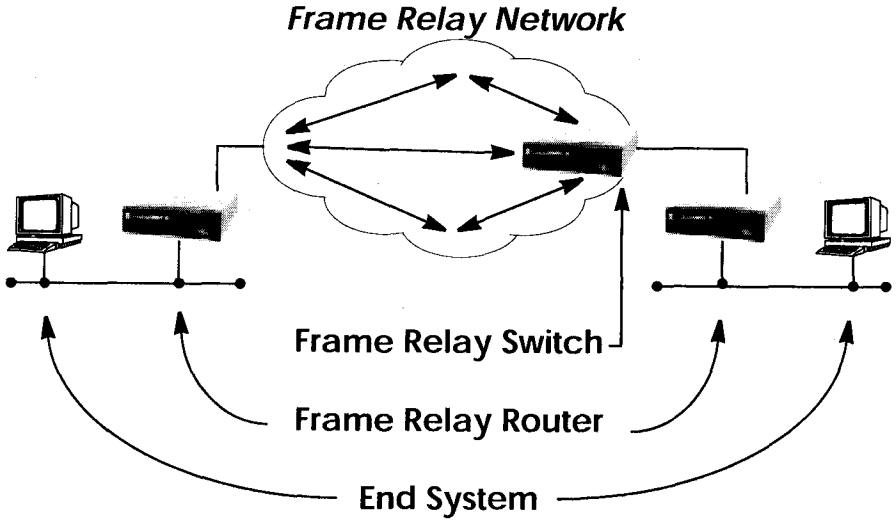
An Overview of Frame Relay Technology

As the name suggests, it works by breaking data streams into variable length frames and forwards (relays) these frames into the network via predetermined logical connections called **Permanent Virtual Circuits**, or PVCs.

Some of the key concepts of Frame Relay are listed below.

- Small, variable length frames are used to transport user data; this makes frame relay well suited for data applications (particularly those generating bursty-traffic) —video and voice transmissions are generally not appropriate.
- Improved overall performance (compared to X.25) —a result of limited error correction and acknowledgement routines.
- Users are guaranteed a minimum amount of bandwidth which is always available (the Committed Information Rate, or CIR).
- High network availability is achieved through statistically multiplexing virtual connections (data streams) onto logical connections, or Permanent Virtual Circuits (PVCs).
- Integrated bandwidth allocation (true bandwidth on demand) allows users to take up additional bandwidth, when available, at no extra charge —based on the user's Committed Burst Rate (CBR) and Excess Burst Rate (EBR).
- Congestion notification allows frame relay device to notify neighbouring devices (in either direction) of bandwidth bottlenecks to help maintain quality of services.

There are different types of equipment found in a typical Frame Relay Networks based on the various tasks they perform.



End Systems

End systems are typically end-user devices that take advantage (make use of) the underlying Frame Relay network. Depending on the application running on the end stations bandwidth requirements of end systems on the LAN can be different. Some applications generate large amounts of intermittent bursty traffic (typical of data applications, telnet, ftp, www) while others (like voice or video) require a constant bitrate.

Frame Relay Routers

Frame Relay Routers are used to connect point-to-multipoint networks (LANs) to a public (or private) Frame Relay network. Its the router's job to encapsulate data into Frame Relay frames for transport over the network link. A Frame Relay Router encapsulates LAN frames in frame relay frames and feeds those frames to a Frame Relay Switch for transmission across the network. A Frame Relay Router also receives frame relay frames from the network, strips the frame relay frame off each frame to product the original LAN frame, and passes the LAN frame on to the end device. A Frame Relay Router communicates directly with one or more Frame Relay Switches to negotiate

the opening/closing of virtual circuits and to control network congestion.

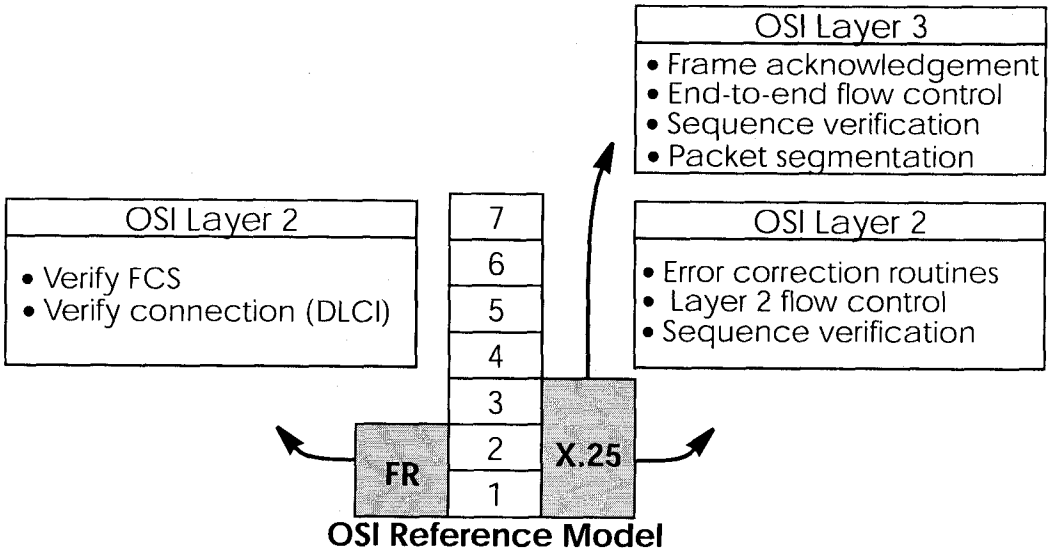
Frame Relay Switches

Switches are typically owned by public network providers but may be owned by private sites implementing private Frame Relay Networks. Aside from the FECN, BECN, and DE frame fields (used for congestion management) the content and final destination of individual frame is of no interest to the switch. Using a simple mapping scheme frames are passed from one interface (DLCI) to another.

Protocol Structure

Frame Relay Protocol Stack

Although similar in concept to X.25, frame relay operates at layer 2 of the OSI reference model. This is where the main differences between the two lie. Frame relay simply leaves out the extensive error detection/correction and end-to-end flow control found in X.25.

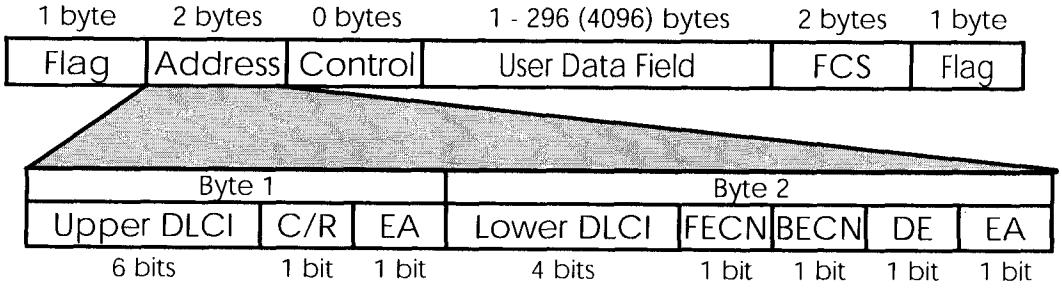


This greatly simplifies the tasks a frame relay switch must perform.

Frame Relay Frame Format

As shown below frame relay is a streamlined protocol that uses HDLC framing. Virtual frame relay connections are routed based on the DLCI field of incoming frames.

Frame Relay Frame



Flag	HDLC Flag (bit sequence: 01111110)
FCS	Frame Checksum Sequence
DLCI	Data Link Connection Identifier
C/R	Command / Response Indicator
EA	Extended Address bit
FECN	Forward Explicit Congestion Notification
BECN	Backward Explicit Congestion Notification
DE	Discard Eligibility Indicator

Frame Relay Addressing

The basic (**unextended**) Frame Relay specification only supports locally significant addressing. These addresses are up to 2 bytes long. Using the EA fields **extended** addresses can be used which may be up to 4 bytes long.

When a frame is read the first EA bit that is set (i.e., it's value = 1) determines the address.

Congestion Notification

The FECN and BECN bits (see above) are used to notify neighbouring frame relay devices of possible congestion.

Virtual Circuits

In Frame Relay multiple connections are mapped to a single physical network connection.

Data Link Connection Identifier

The DLCI field is used to route virtual frame relay connections. A standard DLCI (2 byte address field) consists of 10 bits and is based on the frame's Upper and Lower DLCI fields. These 10 bits establish an upper limit of 1024, 2^{10}, possible simultaneous virtual channels that can be multiplexed on to a PVC.

A DLCI may specify a value between 0 and 1023; however not all values are valid. As shown below some values are reserved for network management or other features such as LAPD in the D-channel.

DLCI	Use (Q.922)	Use (LMI)
0	Signalling	Reserved
1- 15	Reserved	Reserved
16 - 511	Available (except when the D-channel is used)	Available
512 - 991	Available	Available
992 - 1007	Layer 2 management	Available
1008 - 1018	Reserved	Reserved
1019 - 1022	Reserved	Multicasting
1023	Consolidated Link Layer Management	Signalling

NOTE: A DLCI is only significant to the local station. Though it is used locally to identify both directions of a virtual circuit it has no meaning to the next station (or the destination) in the frame relay network.

Frame Relay Services

Frame relay access can be purchased in a variety of configurations depending of your site's needs. Characteristics of the service you will receive include:

1. The type of physical connection you have to the frame relay network, ISDN or X.21.

2. The amount (from 56Kbps up to 2Mbps) and type of bandwidth available via this connection; this will include your guaranteed and excess rates. See CIR, CBR, and EBR below.
3. The number of PVCs you are receiving.

Committed Information Rate

When purchasing frame relay services from your provider, you will be assigned a Committed Information Rate. This defines the minimum amount of bandwidth that your provider guarantees to be available to your site at all times.

Committed Burst Rate

You will also receive a Committed Burst Rate with your service package. This is an additional amount of bandwidth (in excess of your CIR) you may use when network resources are available. The CBR is free of charge, but be aware that all frames that are in excess of your CIR will be DE (Discard Eligible) flagged and may be discarded by intermediate switches if the network becomes congested.

Excess Burst Rate

As Excess Burst Rate is also available; it defines the maximum data rate the service provider's network will attempt to sustain. Also note that all EBR traffic is flagged Discard Eligible.

The Frame Relay Subsystem

Frame Relay on the BRICK consists of 5 SNMP system tables contained in the BRICK's **fr** group. An overview of these tables is shown below. The full description of each SNMP object is contained on the following pages.

frGlobals frDlcmiTablefrCircuitTable
frErrTable frMprTable

Overview: Frame Relay System Tables

- ***frGlobals***
  Global settings for Frame Relay on the BRICK. Currently only contains the frTrapState object which is used to enabled/disable ***frDLCIStatusChange*** traps on the BRICK. (This trap indicates that the state of a particular Virtual Circuit has changed.)
- ***frDlcmiTable***
  Contains parameters for each DLCM (Data Link Connection Management) interface for each instance of frame relay service on the BRICK.
- ***frCircuitTable***
  Contains information for each Data Link Connection Identifiers and corresponding virtual circuits.
- ***frErrTable***
  Used to store important status messages reported for interfaces configured with Local Management Interface.
- ***frMprTable***
  Contains Multiprotocol Routing over Frame Relay interfaces (MPFR) on the BRICK. These interfaces are Virtual interfaces since they do not necessarily map to a single hardware interface. MPFR interfaces may be used by higher level protocols.

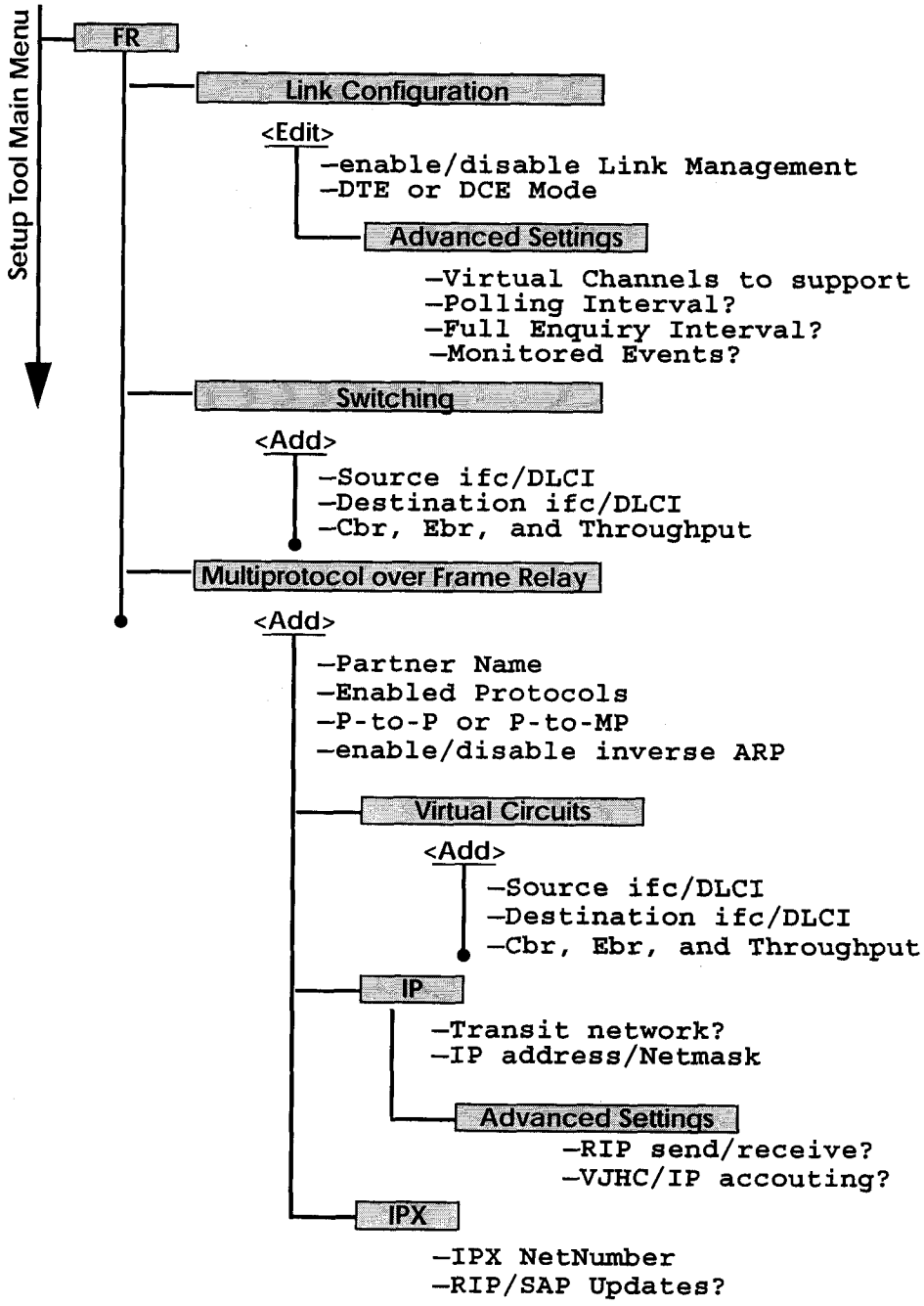
Frame Relay System Messages

biboAdmSyslogMessage	*~Level*
Attach link <*ifindex*> failed	debug
Attach link <*ifindex*>	debug
Bind link <*ifindex*> failed	debug
Link <*ifindex*> bound; starting LMI	debug
Be exceeded - packet discarded	debug
Want open ifc <*ifindex*>.	debug
Unknown ARP protocol <*proto*>	debug
No license	info
DLCI out of range: <*dlci*>	notice
No more than 256 interfaces allowed	error
Create: illegal index <*ifindex*>	error
Create: index <*ifindex*> already exists	error

Frame Relay Setup Tool Menus

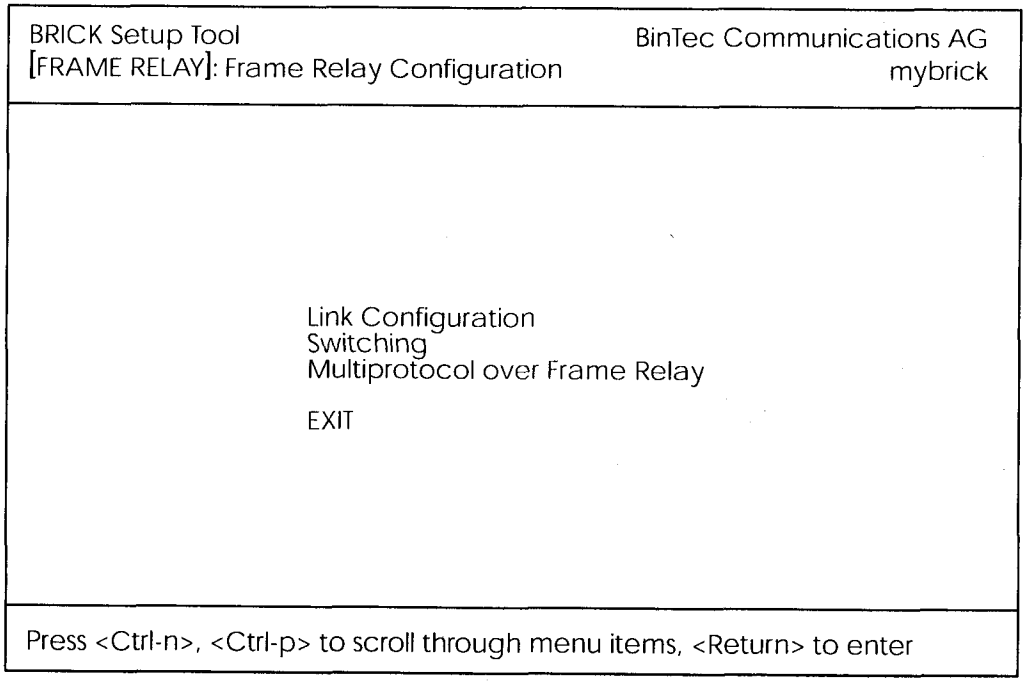
Several menus have been added to Setup Tool to allow for easy configuration of Frame Relay on the BRICK. An overview of the menu struc-

ture is shown below. Individual submenus are described in detail on the following pages.



Setup Tool Menus

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



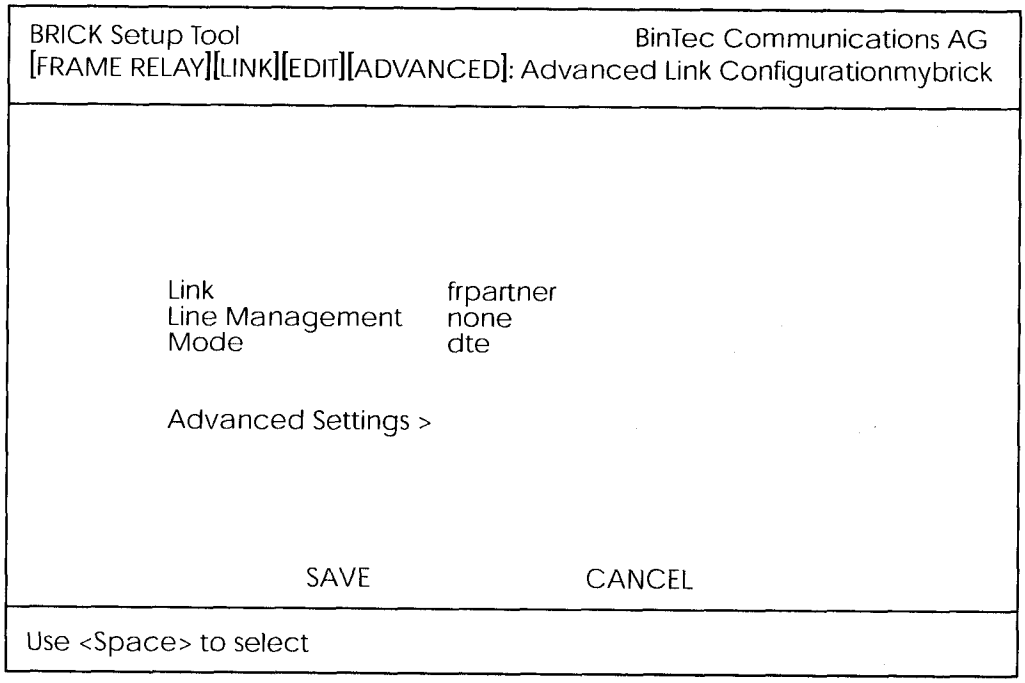
LINK CONFIGURATION contains the settings relative to the layer 2 of Frame Relay interface.

SWITCHING lists settings for each Frame Relay Virtual Circuit.

MULTIPROTOCOL OVER FRAME RELAY lists all existing MPFR interfaces configured on the BRICK.

FR → LINK CONFIGURATION →

This menu lists the available links that may be configured as the transport layer of a Frame Relay interface. Use the menu shown below (First select the link and hit enter) to edit link's settings.



Link = Shows the link that is currently being edited.

Line Management = Determines whether or not link management is being performed on this link. Currently, the method described in Q.933 is supported.

Mode = Defines the mode (DTE or DCE) the BRICK operates at for this connection. Note that one side of the link must operate as DTE and one as DCE.

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

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

FR → LINK CONFIGURATION → ADVANCED SETTINGS →

This menu can be used to configure special settings relating to line management for Frame Relay interfaces on the BRICK . Some options only apply to BRICK operating in DTE or DCE mode.

```
BRICK Setup Tool                                BinTec Communications AG
[FRAME RELAY][LINK][EDIT][ADVANCED]: Advanced Link Configurationmybrick


        Supported Vrtual Channels      250

        Polling Interval               10
        Full Enquiry Interval          6
        Idle Interval                  15
        Error Threshold                3
        Monitored Events               4


                    OK                          CANCEL

Enter integer range 1 ..250
```

Supported Virtual Channels = This field can be used to control how many Virtual Channels this Link supports; a maximum of 250 (default) VCs are possible.

Polling Interval = When set for DTE mode (client) and q933a line management is enabled this field determines the number of seconds between successive status enquiry messages sent out by the BRICK. (default 10 seconds)

Full Enquiry Interval = When set for DTE mode (client) and q933a line management is enabled this field determines the number of status enquiry intervals that pass before issuing a full status enquiry message (default 6 intervals).

Idle Interval = When set for DCE mode (server) and line management is enabled this field defines the number of seconds within a status enquiry messages should be received (default 15 seconds).

Error Threshold = When line management is enabled this field defines the maximum number of unanswered Status Enquiries the BRICK accepts before declaring the interface down (default 3 messages).

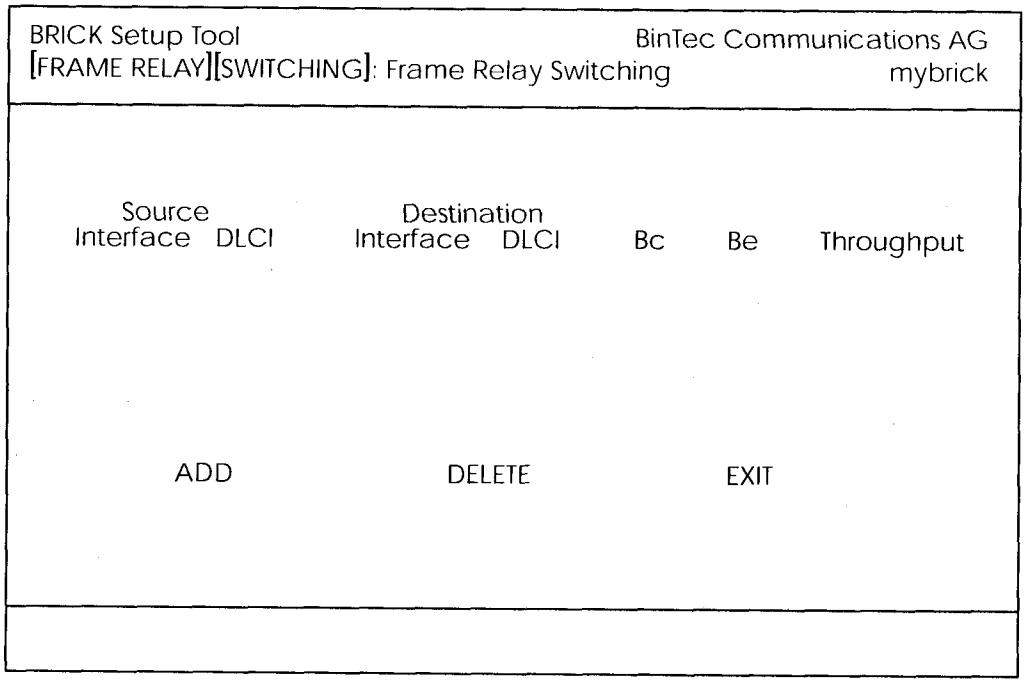
Monitored Events = When line management is enabled this field defines the number of status polling intervals over which the error threshold (previous field) is counted. For example, if within 'MonitoredEvents' number of events the station receives 'ErrorThreshold' number of errors, the interface is marked as down (default 4 intervals).

Select OK to accept the settings and return to the previous menu.

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

FR → SWITCHING →

This menu is used to configure frame relay switching functionality on the BRICK. When used as a Frame Relay switch this menu can be used to configure routes, or mappings (i.e., from incoming interface/DLCI to outgoing interface DLCI).
Frame Relay routes can be added, removed, or changed here.



Select ADD to create a new Frame Relay route.

Select DELETE to remove a Frame Relay route entry that has been tagged (using the spacebar) for deletion.

Select EXIT to accept the list of Frame Relay routes and return to the previous menu.

To edit a Frame Relay route, highlight the entry and then enter <Return>. When adding or changing an entry the following information must be provided.

Source Interface = Use the spacebar and scroll through the list of Frame Relay interfaces to select the source interface for this route.

Source DLCI = Defines the DLCI of the source interface for this route.

Destination Interface = Use the spacebar to scroll through the list of Frame Relay interfaces and select the destination interface.

Destination DLCI = Defines the DLCI on the destination interface to use.

Committed Burst Rate = (Abbreviated Bc) This field defines the maximum amount of data (in bits) to transfer under normal conditions.

Excess Burst Rate = (Abbreviated Be) This field defines the maximum amount of uncommitted data (in bits) to attempt deliver.

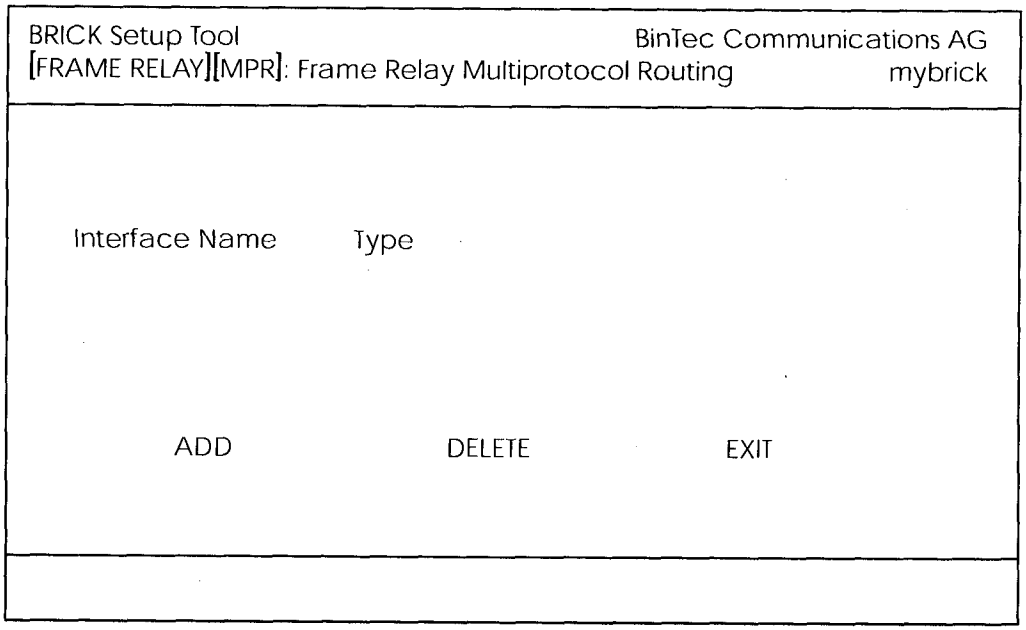
Throughput = This field defines the physical throughput for this interface (and defaults to ifSpeed).

Select OK to accept the settings and return to the previous menu.

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

FR → MULTIPROTOCOL OVER FRAME RELAY

This menu lists Multiprotocol Routing over Frame Relay interfaces on the BRICK. MPFR interfaces can be added, removed, or changed here. .



Interface Name = Identifies the interface name (taken from the *ifDescr* object from the *ifTable*).

Type = Specifies whether the interface is a point-to-point, or point-to-multipoint interface.

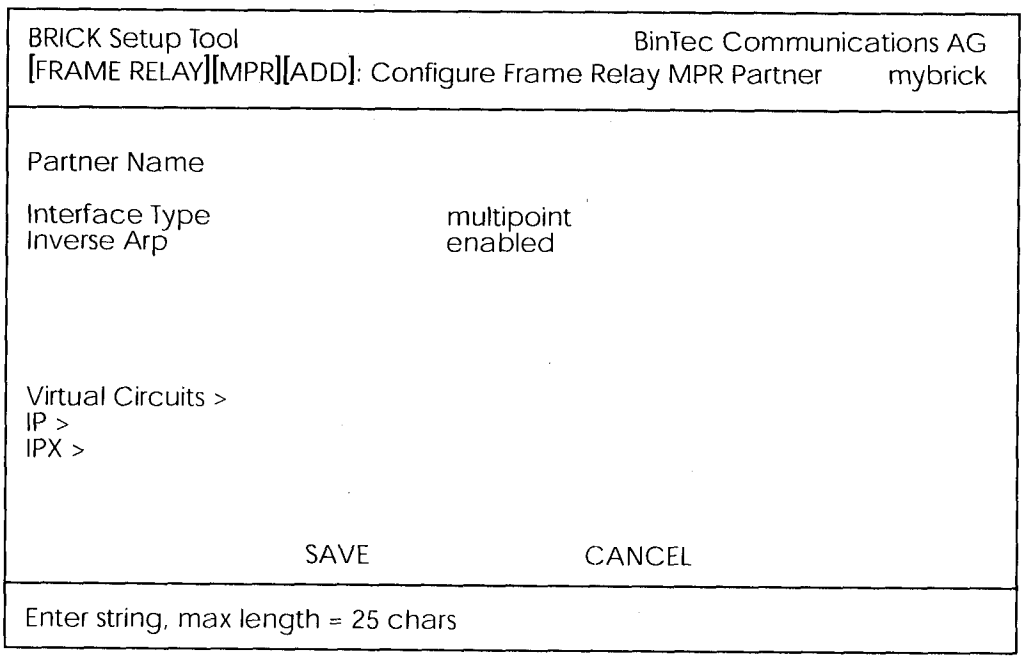
Select ADD to create a new MPFR interface. (See the EDIT/ ADD menu on the following page.)

Select DELETE to remove a MPFR interface that has been tagged (using the spacebar) for deletion.

Select EXIT to accept the interface list and return to the previous menu.

FR → MULTIPROTOCOL OVER FRAME RELAY → ADD

This menu is used to create (or change) MPFR (Multi-Protocol routing over Frame Relay) interfaces on the BRICK.



Partner Name = Define a unique name to identify this MPFR partner.

Interface Type = Determines the interface type as being either "multipoint" or "point to point".

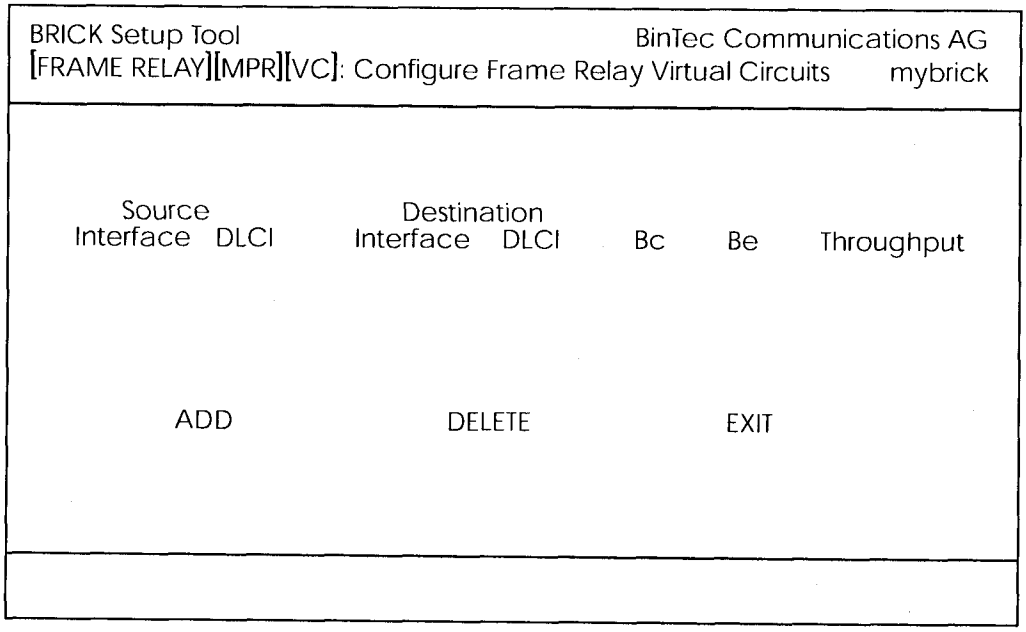
Inverse Arp = Enables/disables inverse ARP over this interface.

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

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

FR → MULTIPROTOCOL OVER FRAME RELAY → VIRTUAL CIRCUITS →

This menu should only be used by sites receiving multiple DLCIs from their Frame Relay service provider. Depending on the number of DLCIs and type of service being received use this menu to define the appropriate data rates.



Source Interface = Using the spacebar scroll through the list of Frame Relay interfaces.

Source DLCI = Defines the DLCI used on this interface.

Committed Burst Rate = The maximum amount of data that is guarenteed to be transferred by the service provider.

Excess Burst Rate = The amount of additional data that is uncommitted by the service provider.

Throughput = The physical throuput of this interface.

Select ADD to create a new Virtual Circuit for this FR interface.

Select DELETE to remove an existing Virtual Circuit that has been tagged (using the spacebar) for deletion.

Select EXIT to accept the list and return to the previous menu.

This is where you configure the IP settings for this remote MPFR partner .

Note: The settings used in this menu are the same as those used in the 

menu described in the *User's Guide* but only apply to this MPFR partner.

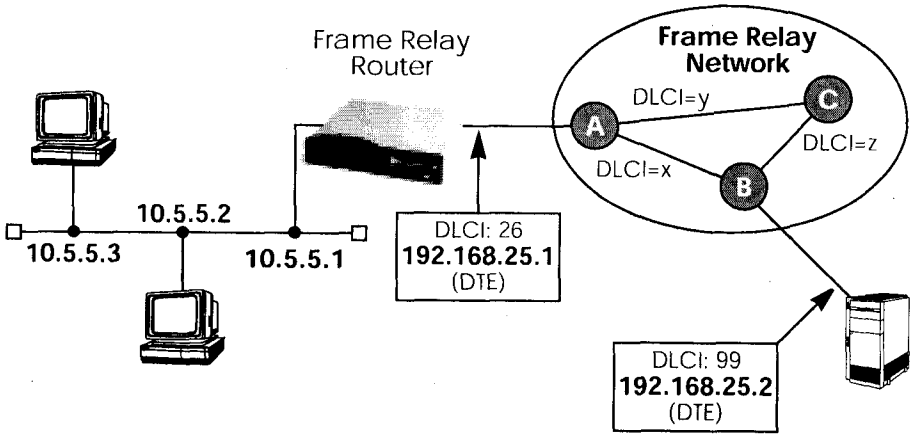
This is where you configure the IPX settings for the remote MPFR partner.

Note: The settings used in this menu are the same as those used in the 

menu described in the *User's Guide* but only apply to this MPFR partner.

Example Configuration using Setup Tool

Frame Relay over ISDN Lines



Requirements: Frame Relay requires a separate license to be installed on the BRICK. After installing your license verify the Frame Relay is listed as "valid" in Setup Tool's License menu (or the Status field for the **frame_relay** entry in the biboAdmLicInfoTable shows **valid_license**).

1.Define the physical interface

In Setup Tool's main menu select the ISDN interface where the Frame Relay service is being received.

```
BRICK Setup Tool                          BinTec Communications AG
[WAN][ADD]: WAN Interface                                 mybrick

Result of autoconfiguration:              Euro ISDN, point to multipoint
ISDN Switch Type                          autodetect on bootup
D-channel                                 dialup
B-channel 1                               dialup
B-channel 2                               dialup

Incoming Call Answering >
Advanced Settings >

                SAVE                                CANCEL

Use <Space> to select
```

You should verify the "Result of autoconfiguration" field is correct. If this interface is a leased line or it was not properly detected set the Switch Type and D/B channel fields appropriately here and [SAVE] the settings.

2. **Configure a new WAN Partner**

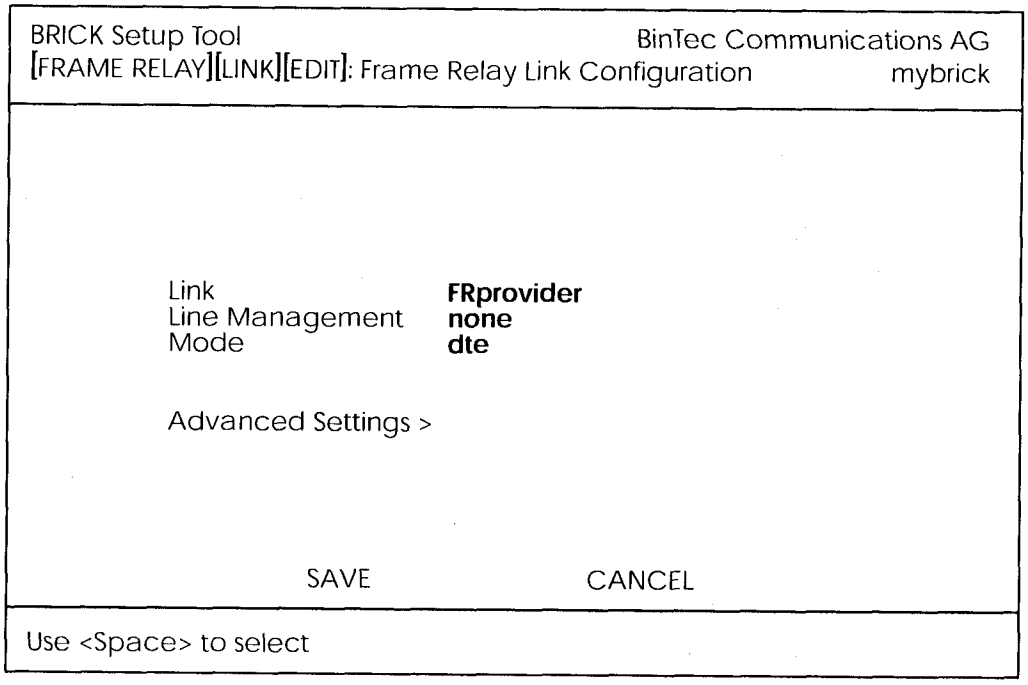
This step defines the (physical) link to the next switch in the Frame Relay network (host A shown above). Create a new interface in the WAN PARTNER → ADD → menu.

```
BRICK Setup Tool                              BinTec Communications AG
[WAN][ADD]: Configure WAN Partner ()                          mybrick

Partner Name                    FRprovider

Encapsulation                   Frame Relay
Encryption                      none
Calling Line Identification     no


WAN Numbers >
PPP >
Advanced Settings >

IP >
IPX >
Bridge >

                SAVE                              CANCEL

Use <Space> to select
```

After defining a partner name select the Encapsulation Frame Relay and configure no other protocol. Under **WAN Numbers** select the ISDN port (from step 1) to use and [SAVE] the settings.

3. **Configure the Frame Relay Link Settings**

Go to the FR → LINK CONFIGURATION → menu and select the physical link (partner name) you configured in the previous step and hit enter to set the desired parameters. It is very important that you set the Mode field to **dte** here if the BRICK is operating as a Frame Relay router.



Optionally, you can define whether Link Management should be performed for this link. If Link management is to be performed on this link, several options are available via the Advanced Settings sub-menu that control how often various LMI packets to send to the server (DCE) and the intervals at which these enquiries are sent.

4. **Configure the Multi-Protocol Routing Interface**

Go to the FR → MULTIPROTOCOL OVER FRAME RELAY → menu and select ADD to create a new MPFR (Multi-Protocol routing over Frame Relay) partner interface. This step will define the virtual interface to the end-system (host at IP address 192.168.25.2 in the diagram above) IP packets will be routed to/from.

Note: When enabling protocols to route over Frame Relay please note that at current, only IP over Frame Relay has been tested on the BRICK.

```
BRICK Setup Tool                                  BinTec Communications AG
[FRAME RELAY][MPR][ADD]: Configure Frame Relay MPR Partner        mybrick

Partner Name                          FRpartner

Interface Type                        point to point
Inverse Arp                           disabled

Virtual Circuits >
IP >
IPX >

                        SAVE                  CANCEL

Enter string, max length = 25 chars
```

5. **Configure IP settings for MPFR Interface**

In the IP submenu configure the IP settings for the remote Frame Relay end station (192.168.25.2 in our example diagram). A transit network is optional. Select [SAVE] to ensure your Frame Relay setup is saved to a configuration file.

```
BRICK Setup Tool                                  BinTec Communications AG
[FRAME RELAY][MPR][IP]: IP Configuration (FRpartner)              mybrick

IP Transit Network                    no

Partner's LAN IP Address >            192.168.25.2
Partner's LAN Netmask >               255.255.255.0

Advanced Setting>

                        SAVE                  CANCEL

Enter string, max length = 25 chars
```