ELSA LANCOM™ Business 6000

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. ELSA shall be liable only to the degree specified in the terms of sale and delivery.

ELSA is DIN EN ISO 9001 certified. The accredited TÜV CERT certification authority has confirmed ELSA conformity to the worldwide ISO 9001 standard in certificate number 09 100 5069, issued on June 15, 1998.

You can find all declarations and approvals for the products, as long as they were available at the time of publication, in the appendix of this documentation.

Trademarks

Subject to change without notice. No liability for technical errors or omissions.

ELSA AG
Sonnenweg 11
52070 Aachen
Germany

www.elsa.com

Aachen, January 2001

100177/0101

Preface

Thank you for placing your trust in this ELSA product.

By selecting the *ELSA LANCOM Business* you have chosen a router which you can use to connect local area networks via an 2 Mbit connection.

Model varieties

This documentation describes various model varieties belonging to the *ELSA LANCOM Business* series, which differ in their hardware and software configurations:

- *ELSA LANCOM Business 6001*
- *ELSA LANCOM Business 6011*
- *ELSA LANCOM Business 6021*

Model restrictions

The sections of the documentation that refer only to a range of models are marked either in the corresponding text itself or with appropriate comments placed beside the text.

Our online services (www.elsa.com) are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. In the Support file section, you can find answers to frequently asked questions (FAQs). The KnowledgeBase also contains a large pool of information. Current drivers, firmware, tools and manuals can be downloaded at any time.

Contents

1 Introduction

The use of router solutions is constantly increasing in the construction of corporate-wide infrastructures. Bandwidth requirements—especially for Internet access or the interconnection of branch-office networks—is growing steadily. Today, 2-Mbit fixed connections are taken for granted in small to mid-sized businesses. Local-area networks (LANs) that have evolved at various locations as well as individual PCs can be connected inexpensively by routers. Corporate branches and offices can be linked to the central network transparently, making a single, central database available to all systems.

See the following sections for a detailed description of the functions of the *ELSA LANCOM Business*, the software and how to use it and an introduction to the technical basics.

1.1 What does the *ELSA LANCOM Business* offer?

The following is an outline of the principal features of the device giving you a quick overview of its capabilities. A detailed description can be found in chapter 5.

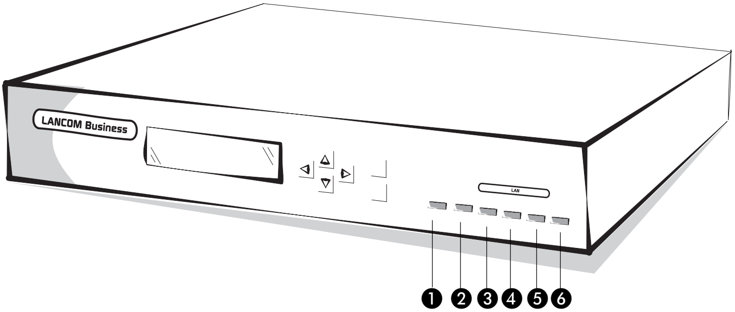
- Operation on 2-Mbit fixed connections
- Connection to the local network (LAN)
- Simple installation with software wizards
- Convenient administration with *ELSA LANconfig* and *WEBconfig*
- Professional device monitoring with *ELSA LANmonitor*
- Simple and reliable software updates with ELSA FirmSafe
- Comprehensive security and firewall functions
- Flexible ISDN connection including dial-up backup
- Network-enabled *ELSA LANCAPI*
- Optional support for *ELSA Dynamic VPN*

2 Description of the device

This section will introduce the interfaces and display elements of the *ELSA LANCOM Business*.

2.1 Front side

The display and operating elements can be found on the front: a display, several buttons and light-emitting diodes (LEDs).



The display indicates the various operating states and messages issued by the unit. Operating states and messages can be displayed in three different modes.

Use the keys to select the display mode, confirm messages and scroll through the multi-line display.

❶ Power/Msg

This LED flashes once when the power supply is switched on. After the self-test, either an error is output by a flashing light code or the device starts and the LED remains lit.

off		Device off
red	1 x short	Boot procedure (test and load) started
red	flashing	Display of a boot error (flashing light code)
red		Device ready for use
red	interrupt	Error message or a charge block prevents outgoing calls

❷ **Rx/Tx** – Data packet sent from device to the LAN or from the LAN to the device

❸ **Coll** – Transmission collision

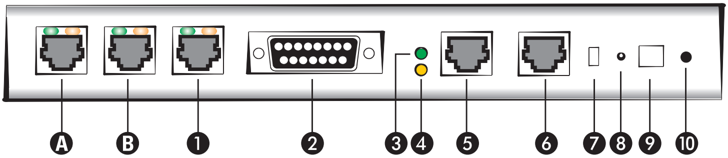
❹ **Link** – The connection to the LAN has been established and is ready

❺ **FDpx** – The router sends and receives data simultaneously

❻ **Fast** – The device is in 100-Mbit mode

2.2 Back

Several interfaces for the connection of a wide variety of devices and networks can be found on the back.



Ⓐ G.703 interface (*ELSA LANCOM Business 6021* only) – this interface is addressed by the router as the second G.703 interface: 'G.703-2' or channel 4-1 in the channel table.

Ⓑ G.703 interface (*ELSA LANCOM Business 6011* and *ELSA LANCOM Business 6021* only) – this interface is addressed by the router as the first G.703 interface: 'G.703-1' or channel 3-1 in the channel table.

❶ ISDN S_0 connection

❷ X.21 interface

❸ Status LED of the X.21 interface

❹ Line LED of the X.21 interface

❺ V.24 configuration interface (COM), Cisco-compatible

❻ 10/100Base-Tx for 10-Mbit or 100-Mbit networks

❼ Node/hub selector switch

❽ Reset button, resets the hardware or restores the unit's factory defaults (after holding for approx. 5 seconds).

❾ Connection for power supply unit

❿ On/off switch

2.3 Status displays for the WAN interfaces

The *ELSA LANCOM Business* features two LEDs for the continuous display of status information for each of its WAN interfaces (X.21, G.703, ISDN). The status of the interface is shown by the green LED marked 'Status'. The orange LED marked 'Line' indicates the status of the logical connection at the router level.

X.21 interface

Status LED (green)	off	Interface not active
	flashing	Interface active, no signal from external device
	on	Interface active, device connected
Line LED (orange)	off	No connection established
	flashing	Connection establishment/protocol negotiation (e.g. via PPP)
	on	Active connection to remote station

G.703 interface (not *ELSA LANCOM Business 6001*)

Status LED (green)	off	Interface not active
	flashing	Structured connection only: G.704 framing error or RAI (**R**emote **A**larm **I**ndicator)
	on	Interface active, G.703 signal OK; Structured connection: G.704 framing OK
Line LED (orange)	off	No connection established
	flashing	Connection establishment/protocol negotiation (e.g. via PPP)
	on	Active connection to remote station

ISDN S_0 interface

Status LED (green)	off	Interface or S_0 bus not active
	flashing	Dial-up connections only: no TEI (**T**erminal **E**ndpoint **I**dentifier) assigned
	on	S_0 bus active

Line LED (orange)	off	No connection established
	flashing	Connection establishment/protocol negotiation (e.g. via PPP)
	on	Active connection to remote station

3 Installation of hardware and software

This section will help you connect as quickly as possible. You will first find out what your product includes. Then we will show you how to connect the device and get it working quickly.

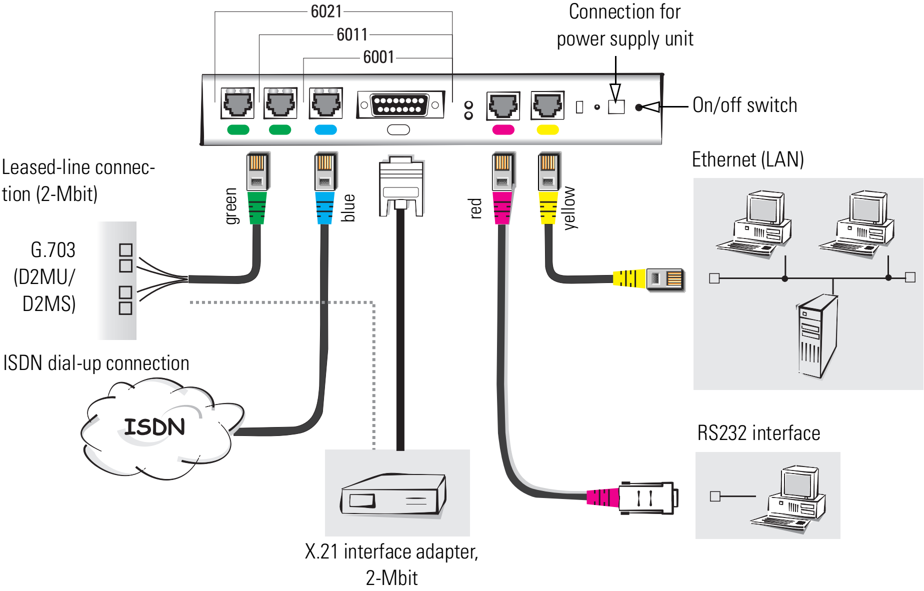
3.1 Package contents

Please check the package contents for completeness before starting the installation. The following components should be in the box:

- *ELSA LANCOM Business*
- Power supply unit
- LAN connector cable, 100Base-TX, yellow plug
- Cable for G.703 interface (*LANCOM Business 6011* and *6021* only), green plug
- Cable for the X.21 interface
- ISDN connector cable, blue plug
- Connector cable for the serial configuration interface (RJ45-RJ45) with RJ45-D-sub-9 adapter (not as per category 5), red plug
- Documentation
- *ELSA LANCOM Business* CD containing *ELSA LANconfig*, other software and electronic documentation

3.2 How to connect the device

All of the cables required to connect the *ELSA LANCOM Business 6000* are included with the device. The plugs and sockets are color-coded to ensure their correct connection.



3.2.1 Connecting to the local network (LAN)

Connect your *ELSA LANCOM Business* to the LAN. Plug the network cable (supplied) into the 10/100Base-TX terminal of the device and into a free network connector on your local network (or into a free socket on a hub in your LAN). The cable for the LAN connector is labeled with a colored bend-proof protector.

The 'LAN-Link' LED on the front side of the device indicates that a usable connection to the LAN has been established.

If this LED does not come on, reverse the node/hub selector switch. If the LED still does not light, there may be a problem with the network card or the wiring.

3.2.2 Connecting to remote networks (WAN)

Depending on the model, up to three 2-Mbit interfaces are available for connections to remote networks or the Internet:

- *ELSA LANCOM Business 6001*
  - ○ One X.21 interface for connection to an interface adapter

- *ELSA LANCOM Business 6011*
  - ○ One X.21 interface for connection to an interface adapter
  - ○ One G.703 interface for direct installation on a fixed line (D2MU or D2MS)
- *ELSA LANCOM Business 6021*
  - ○ One X.21 interface for connection to an interface adapter
  - ○ Two G.703 interfaces for direct installation on fixed lines (D2MU or D2MS)

Connection to the X.21 interface

The X.21 interface permits the connection of a 2-Mbit fixed connection (D2MU or D2MS) via an external terminal adapter. The X.21 terminal adapter is connected to a fixed line via its own G.703 interface.

Fixed connections via G.703

ELSA LANCOM Business 6011 and 6021 only!

You can connect the *ELSA LANCOM Business 6011* or *6021* directly to a fixed line (in Germany under the designations D2MU or D2MS) via the G.703 interface. Insert the appropriate connector cable in the device's G.703 socket. Connect the stranded wires at the other end of the cable to the D2MU or D2MS terminals of the network terminator.

In some countries alternative cables are supplied for G.703 connections, with plugs rather than bare wires, for example.

3.2.3 Connection to the ISDN

The ISDN interface is the direct access for remote computers, for example for remote configuration. In addition, the ISDN interface can be used to provide the workstations in the LAN with a variety of office communications functions such as fax transmission. This can be realized using the included *ELSA LANCAPI* software.

Connect the router's ISDN interface to the ISDN network. Insert the supplied ISDN connector cable in the ISDN/S_0 bus connection (BRI) of the device and an ISDN/S_0 point-to-point or point-to-multipoint connection.

3.2.4 Connection to the serial interface (COM)

The serial interface can be used to configure the device without going over the network, either with *ELSA LANconfig* or a terminal program.

The pin assignment of the serial configuration interface (COM) of the *ELSA LANCOM Business* devices is CISCO-compatible. The corresponding connector cables or adapters therefore can also be used with *ELSA LANCOM Business* routers.

The serial interface automatically sets itself to data rates in the 9,600–230,400 bps range.

3.3 Activating the router

Finally, connect the router to an AC power socket using the included AC adapter and switch the device on with the on/off switch on the back.

The router will run a number of test routines to ensure its functionality after it has been switched on. The progress of the test routines can be monitored on the display on the front of the device. Once the test routines have been completed successfully, the device name 'LANCOM BUSINESS 6000' will appear on the display. The device is now ready for use.

3.4 Installation of the accessory software

The included CD contains a setup program with which you can install the ELSA software. Place the CD in your CD-ROM drive. If the Setup program doesn't start automatically, you can start in manually. The file SETUP.EXE is located in the root folder of the CD.

Follow the onscreen instructions and confirm the queries of the setup program.

The following applications will be installed:

- *ELSA LANconfig* for the administration of the device under Windows
- *ELSA LANmonitor* to monitor the device under Windows
- *ELSA LANCAPI* for office communications functions via the LAN

The CD also contains a beta version of *LANconfig* for Linux, *xLANconfig*, which features all of the functions of *LANconfig*. *xLANconfig* is currently available for Linux running on x86 and Alpha processors. *xLANconfig* is based on the X-Windows standard commonly used in UNIX systems. The complete functionality of *xLANconfig* can be provided for any number of X-Windows clients in the network via an X-Windows server. These clients can use *xLANconfig* without the need for a local *xLANconfig* installation. This feature makes *xLANconfig* particularly interesting for deployment in large networks.

3.5 Wizards make life easier

The following chapter will show you how to configure your *ELSA LANCOM Business*. This configuration procedure used to be a complicated business which could easily baffle specialists. ELSA developed software wizards to simplify the procedure, however, making possible to even realize complex configurations quickly and reliably.

The wizards can be called up in two ways:

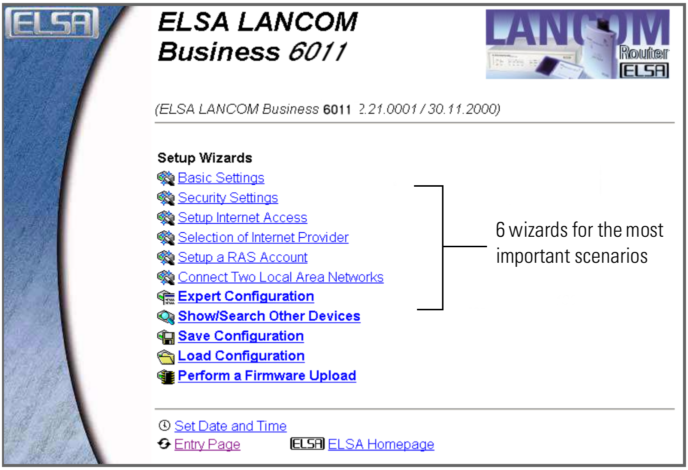
① ***ELSA LANconfig***
Available under all Windows operating systems. It has also recently been introduced as *xLANconfig* for Linux on x86 or Alpha processors.

② ***ELSA WEBconfig***
An application permanently installed in the router. It can be called up with any web browser (including text-only browsers) from any operating system.
The precondition: access to the router via the network.

The same wizards are available for both options. Your choice thus depends on the operating system of the workstation you intend to use for configuration. The following overview will be based on *WEBconfig*. The information provided also applies to *LANconfig* and *xLANconfig*, however.

It's our goal to make the configuration as simple as possible for you. We thus would like to refer you to the wizards at an early stage in the procedure. The following chapter contains a complete list of all of the possible configuration methods. The wizards under *LANconfig* and *WEBconfig* are one option. However, they are the simplest and most reliable option—which is why we are pointing them out at this early stage.

It's thus worth taking the time for a brief look at the wizards that are available for the configuration of the *ELSA LANCOM Business 6000*:


ELSA LANCOM Business 6011

(ELSA LANCOM Business 6011 2.21.0001 / 30.11.2000)

Setup Wizards

- Basic Settings
- Security Settings
- Setup Internet Access
- Selection of Internet Provider
- Setup a RAS Account
- Connect Two Local Area Networks
- Expert Configuration
- Show/Search Other Devices
- Save Configuration
- Load Configuration
- Perform a Firmware Upload

Set Date and Time

Entry Page ELSA Homepage

In addition to handling the basic and security settings, the wizards can be used to configure Internet access, set up dial-up access points for remote access, or establish a direct connection between two local networks. Needless to say, the full range of expert configuration options is also available in addition to the wizards. It's only rarely necessary to use these options, however.

The wizards have been designed so as to permit the router to be set up easily, quickly and reliably for typical applications using the wizards alone. The use of the wizards is self-explanatory. You can find a detailed description of all of the required information directly in the input window. It's thus not necessary to refer to the manual. We therefore will not be covering the individual steps when using the wizards in detail in this manual.

Experience has shown that hardly any problems related to faulty configurations occur when using the wizards. So, take it easy and simplify your life with the wizards!

4 Configuration and management

ELSA routers are always dispatched with up-to-date software in which several of the settings have already been made.

It will nevertheless be necessary for you to add some information and configure the router to your specific needs. These settings are made as part of the configuration process.

This section will show you the programs and routes you can use to access the device and specify further settings.

We will also provide instructions on a simple approach to performing the basic configuration of the unit.

And, if the team at ELSA has produced new firmware with new features for your use, we will show you how to load the new firmware.

4.1 Configuration tools and approaches

ELSA LANCOM Business are flexible devices that support a variety of tools (i.e. software) and approaches (in the form of communication options) for their configuration. First, a look at the “approaches”.

4.1.1 Configuration access to the *ELSA LANCOM Business*

A *ELSA LANCOM Business* can be accessed via three different options:

- Through the configuration interface (config interface) on the rear of the router (also known as outband)
- Through the LAN or WAN network (inband)
- Through a dial-up or fixed-line ISDN connection (remote configuration)

What is the difference between these three possibilities?

On one hand, the availability: Configuration via outband is always available. Inband configuration is not possible, however, in the event of a network fault. Remote configuration is also dependent on an ISDN connection.

On the other hand, whether or not you will need additional hardware and software: The inband configuration requires one of the computers already available in the LAN or WAN, as well as only one suitable software, such as *ELSA LANconfig* (see following section). In addition to the configuration software, the outband configuration also requires one of the computers (with a serial port) and a suitable configuration cable. The preconditions are most extensive for remote configuration: An ISDN board or ISDN modem is required, as well as PPP access software, which in the case of Windows is included in Dial-Up Networking, however.

4.1.2 Configuration software

It's obvious with a glance at the configuration access options: configuration requires suitable software.

Situations in which the device is configured vary—as do the personal requirements and preferences of the person doing the configuration. *ELSA LANCOM Business* routers thus feature a broad selection of configuration software:

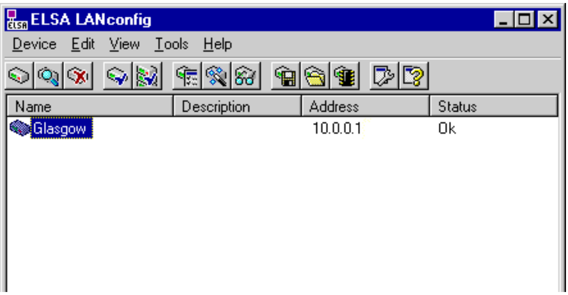
- ***ELSA LANconfig*** – Nearly all parameters of the *ELSA LANCOM Business* can be set quickly and with ease using this menu-based application. In addition, *ELSA LANconfig* provides an insight into the router's internal processes. *ELSA LANconfig* is a complete router manager under Windows. Outband, inband and remote configuration are supported.
- ***ELSA WEBconfig*** – this software is permanently installed in the router. All that is required on the workstation used for the configuration is a web browser. *WEBconfig* is thus independent of operating systems. Inband and remote configuration are supported.
- **SNMP** – Programs for the management of IP networks are generally based on the SNMP protocol. It is possible to access the *ELSA LANCOM Business* inband and and via remote configuration using SNMP.
- **Terminal program, Telnet** – a *ELSA LANCOM Business* can be configured with a terminal program via the config interface (e.g. Hyper Terminal) or within an IP network (e.g. Telnet).
- **TFTP** – the file transfer protocol TFTP can also be used within IP networks (inband and remote configuration).

4.2 Configuration using *ELSA LANconfig*

Start *ELSA LANconfig* e.g. via the Windows taskbar with **Start** ▶ **Programs** ▶ **ELSAlan** ▶ ***ELSA LANconfig***. *ELSA LANconfig* searches the local area network for devices. *ELSA LANconfig* will automatically launch the setup wizard if a device which has not yet been configured is found on the local area network. For the description of the basic configuration using the setup wizard, please refer to the section 'Basic configuration under Windows with ELSA LANconfig' on page 25.

Click on the **Find** button or call up the command with **Device** ▶ **Find** to initiate a search for a new device manually. *ELSA LANconfig* will then prompt for a location to search. You will only need to specify the local area network if using the inband solution, and then you're off.

Once *ELSA LANconfig* has finished its search, it displays a list of all the devices it has found, together with their names and, perhaps a description, the IP address and its status.



Name	Description	Address	Status
Glasgow		10.0.0.1	Ok

Two different display options can be selected for configuring the devices with *ELSA LANconfig*:

- The 'Simple configuration' display shows only the settings required for standard cases.
- The 'Complete configuration' display shows all available settings. Some of them should only be modified by experienced users.

Select the display mode in the **View** ▶ **Options** menu.

Double-clicking the entry for the highlighted device and then clicking the **Configure** button or the **Edit** ▶ **Edit Configuration File** option reads the device's current settings and displays the 'General' configuration selection.

The remainder of the program's operation is self-explanatory or you can use the online help. You can click on the question mark top right in any window or right-click on an unclear term at any time to call up context-sensitive help.

4.3 Configuration with *ELSA WEBconfig*

You can use any web browser, even text-based, for basic setup of the device. The *ELSA WEBconfig* configuration application is integrated in the *ELSA LANCOM Business*. All you need is a web browser in order to access *ELSA WEBconfig*.

ELSA WEBconfig offers setup wizards similar to *ELSA LANconfig* and has all you need for easy configuration of the *ELSA LANCOM Business*—contrary to *ELSA LANconfig* but under all operating systems for which a web browser exists.

A LAN connection via TCP/IP (PPP for remote configuration) must be established to use *ELSA WEBconfig*. *ELSA WEBconfig* is accessed via the IP address of the *ELSA LANCOM Business* device.

The Browser-based basic configuration with *ELSA WEBconfig* covers accessing an unconfigured device for the first time using *WEBconfig* and performing the basic configuration.

4.4 Configuration using Telnet

Start up the configuration (e.g. from a DOS box) using Telnet with the command:

```
C:\>telnet 10.0.0.1
```

Telnet will then establish a connection with the device using the IP address.

After entering the password (if you have set one to protect the configuration), all commands are available from the 'Configuration commands' section.

4.5 Configuration using SNMP

The Simple Network Management Protocol (SNMP V.1 as specified in RFC 1157) allows monitoring and configuration of the devices on a network from a single central instance.

A variety of SNMP-based configuration and management programs are available, such as Hewlett-Packard OpenView or the simple SNMP agent included on the CD.

4.6 The basic configuration

The most important configuration tasks that you can and should perform with your new device include:

- Assignment of a fixed IP address
- Activation of the DHCP server in the router
- Security settings
- Setup of Internet access or the fixed connection
- Configuration of the ISDN interface

All of these configuration tasks can be performed using the so-called *LANconfig* wizards. These are controlled input menus that provide information and assistance for each configuration step. Performing the basic configuration with the assistance of the wizards will simplify the process of entering the basic data. Complete beginners can configure a complex router with the help of the wizards and professionals also have a lot to gain from them.

The wizards are available in two programs:

- in *ELSA LANconfig* under Windows operating systems
- in *ELSA WEBconfig* which can be accessed from any web browser

4.6.1 Basic configuration under Windows with *ELSA LANconfig*

Launch *ELSA LANconfig* with **Start** ▶ **Programs** ▶ **ELSAlan** ▶ **LANconfig**.

LANconfig searches the network for existing devices. The basic configuration wizard starts automatically as soon as the new *ELSA LANCOM Business 6000* is found.

This wizard will assist you with the most important basic settings: The fixed IP address of the device and the netmask to be used. In addition, you can determine whether the DHCP server in the router should be enabled or not.

Once these basic settings have been made, you will be offered the wizards for typical device functions such as Internet access, network interconnection, security options, etc. Start the desired wizard and make the required settings. This will then set up the router for the tasks selected.

The *LANconfig* list window will now display your device and its associated IP address. You can also access the device using a web browser. *WEBconfig* provides access to all of the wizards and the device's internal menu system for the advanced configuration of the router.

A beta version of xLANconfig for Linux can be found on the ELSA LANCOM Business CD. Alternatively, the current version can be downloaded from the drivers section of the ELSA website.

4.6.2 Browser-based basic configuration with *ELSA WEBconfig*

As you know, *ELSA WEBconfig* lets you configure your *ELSA LANCOM Business* using any web browser. You are thus not dependent on the Windows operating system as you are with *ELSA LANconfig*.

There's only precondition for accessing the router: you must know its IP address.

What is the IP address of the router?

An unconfigured *ELSA LANCOM Business 6000* router will appear in your network under the IP address x.x.x.254. In the case of Class A networks with a subnet mask of 255.255.0.0 and network address of 10.1.x.x, the address will be 10.1.0.254. To determine the effective IP address of your router, you therefore need to know your network number and netmask.

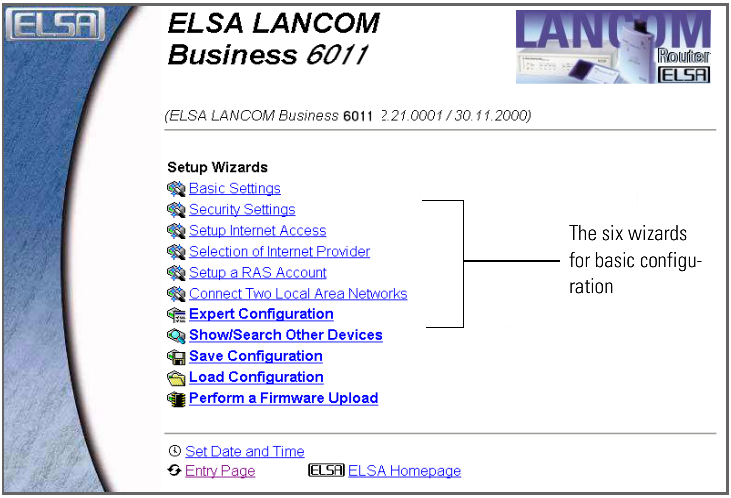
Communication with the device can then be realized within the network using a web browser and Telnet via this IP address.

Starting the wizards in *WEBconfig*

Start your web browser (Internet Explorer, Netscape Navigator) and enter the following Internet address:

```
http://<IP address of LANCOM>
```

The following main menu will be displayed:



ELSA LANCOM Business 6011

(ELSA LANCOM Business 6011 2.21.0001 / 30.11.2000)

Setup Wizards

- Basic Settings
- Security Settings
- Setup Internet Access
- Selection of Internet Provider
- Setup a RAS Account
- Connect Two Local Area Networks
- Expert Configuration
- Show/Search Other Devices
- Save Configuration
- Load Configuration
- Perform a Firmware Upload

Set Date and Time

Entry Page ELSA Homepage

The six wizards for basic configuration

Comprehensive, context-sensitive documentation on the individual *WEBconfig* pages and fields is accessible at all times in *WEBconfig* via the link 'Help (reference manual)'.

The *ELSA WEBconfig* help files (HTTP module)

The Help (Reference Manual) link points to help files in HTML format. In its default setting the Help link points to the ELSA web site.

You may also download the help files from the ELSA web site and save them at the location of your choice. We recommend storing the help files on your local computer, or on a server that you can access at any time. This can be either a file server or a web (HTTP) server.

Storing the files on a local machine has the advantage that the files are accessible in the event of a network malfunction. On the other hand, installing the files on a server will permit access to the help function from anywhere in the network without the need to install the help files on every computer. Access to the server via the network is a precondition for this, of course.

Once you have selected an option and stored the help file at the appropriate place, the path to the file must be entered in *ELSA WEBconfig*. In *ELSA*

WEBconfig, please select **Expert Configuration ▶ Setup ▶ HTTP Module ▶ Document Root**.

Two important points should be noted with regard to the syntax:

① Specify the path only up to the directory containing the complete help file structure.

For example, if you have created the help file structure '\400\1\6001\' in the local directory 'C:\ELSA\HTMLRef', then specify 'file://C:/ELSA/HTMLRef' as the document root.

② Minor differences will apply to the path depending on the type of installation (local, file server, HTTP server) and operating system. Examples are given in the table, with. The names and paths used can be selected freely.

Version	Operating systems	Example
local	Windows	file://C:/ELSA/HTMLRef
	Linux	file://usr/lib/ELSA/HTMLRef
Fileserver	Windows NT, Windows 2000, Novell, UNIX	file://Server1/ELSA/HTMLRef
HTTP server	all	http://<IP sddress>/ELSA/HTMLRef

Replace the placeholder <IP address> with the valid IP address of the HTTP servers in 'x.x.x.x' format, for example '128.7.9.155'.

You can download the current version of the HTML Help from the ELSA web site at any time.

4.7 Advanced settings

When the basic configuration is finished, the required settings for the specific deployment of the *ELSA LANCOM Business 6000* are complete in most cases.

Of course, you can also configure a large number of additional settings. For a detailed description of these options, please refer to the 'Operating modes and functions' chapter.

4.8 *ELSA LANmonitor*—know what's happening

The *ELSA LANmonitor* includes a monitoring tool with which you can view the most important information on the status of your routers on your monitor at any time under Windows operating systems—of all of the *ELSA LANCOM Business* routers in the network.

Many of the internal messages generated by the devices are converted to plain text, thereby helping you to troubleshoot.

You can also use *ELSA LANmonitor* to monitor the traffic on the router's various interfaces to collect important information on the settings you can use to optimize data traffic.

In addition to the device statistics that can also be read out during a Telnet or terminal session or using *ELSA WEBconfig*, a variety of other useful options are also available in the *ELSA LANmonitor*.

4.8.1 *ELSA LANmonitor* installation

Usually, *ELSA LANmonitor* is automatically installed together with *ELSA LANconfig* on the computer from which you wish to configure your router.

If *ELSA LANmonitor* is not yet installed on your computer, place the *ELSA LANCOM Business* in your CD drive. If the setup program does not automatically start when you insert the CD, simply click 'autorun.exe' on the *ELSA LANCOM Business* CD in the Windows Explorer. Otherwise, click on the **My Computer** icon and double-click the icon of your CD-ROM drive. Double-click on 'Autorun.exe' to launch the file. The setup program will then start.

During the installation you should activate the *LANmonitor*.

With ELSA LANmonitor you can only monitor those devices that you can access inband in the local network via IP. With this program you cannot access a router via the serial interface. It is also not possible to access devices in remote networks that can only be reached via intermediate routers with ELSA LANmonitor.

4.8.2 Checking you Internet connection

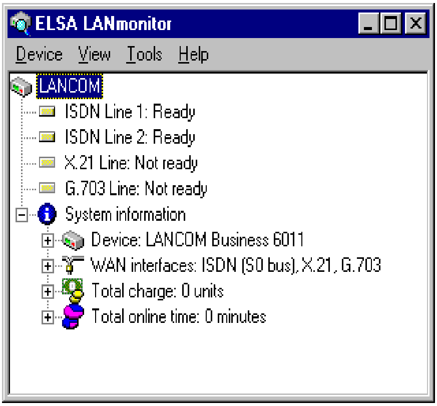
To demonstrate the functions of *ELSA LANmonitor* we will first show you the types of information *ELSA LANmonitor* provides about connections being established to your Internet provider.

① So you should setup the router to connect to your provider, e.g. with the *ELSA LANconfig* setup wizard.

② Start up *ELSA LANmonitor* by clicking **Start** ▶ **Programs** ▶ **ELSAlan** ▶ ***LANmonitor***. Generate a new device by selecting **Device** ▶ **New** and, in the following window, enter the IP address of the router you wish to monitor. If the configuration of the device is protected by password, enter the password too.

Alternatively, you can select the device via the *ELSA LANconfig* and monitor it using **Options** ▶ **Monitor Device**.

③ *ELSA LANmonitor* automatically creates a new entry in the device list and initially displays the status of the transfer channels. Start your Internet browser and enter any web page you like. *ELSA LANmonitor* now shows a connection being established on one channel and the name of the remote site being called. As soon as the connection is established, a plus sign against the B channel entry indicates that further information on this channel is available. Click on the plus sign to open a tree structure in which you can view various information.



LANCOM
ISDN Line 1: Ready
ISDN Line 2: Ready
X.21 Line: Not ready
G.703 Line: Not ready
System information
Device: LANCOM Business 6011
WAN interfaces: ISDN (S0 bus), X.21, G.703
Total charge: 0 units
Total online time: 0 minutes

In this example, you can determine from the PPP protocol information the IP address assigned to your router by the provider for the duration of the connection and the addresses transmitted for the DNS and NBNS server.

Under the general information you can watch the transmission rates at which data is currently being exchanged with the Internet.

④ To break the connection manually, click on the active channel with the right mouse button. You may be required to enter a configuration password.

⑤ If you would like a log of the *ELSA LANmonitor* output in file form, select 'Options' from the 'View' menu and go to the 'Log' tab. Enable logging and specify whether *ELSA LANmonitor* should create a log file daily, monthly, or on an ongoing basis.

4.9 Remote configuration via Dial-Up Networking

Configuring routers at remote sites is particularly easy using the remote configuration method via a Dial-Up Network from Windows. The device is accessible by the administrator immediately without any settings being made after it is switched on and connected to the WAN interface. This means that you save a lot of time and costs when connecting other networks to your network because you do not have to travel to the other network or instruct the staff on-site on configuring the router.

You can also reserve a special calling number for remote configuration. Then the support technician can always access the router even if it is really no longer accessible due to incorrect settings.

4.9.1 This is what you need for remote configuration

- A computer with a PPP client, e.g. Windows Dial-Up Networking
- A program for inband configuration, e.g. *ELSA LANconfig* or Telnet
- an ISDN card, a terminal adapter or a *ELSA LANCOM Business* with *ELSA LANCAPI*

4.9.2 The first remote connection using a dial-up connection

① In the *ELSA LANconfig* program select **Device** ▶ **New**, enable 'Dial-Up Network' as the connection type and enter the calling number of the WAN interface to which the *ELSA LANCOM Business* is connected. If you wish, you can also enter the time period after which an idle connection is to be disconnected automatically.

② *ELSA LANconfig* now automatically generates a new entry under Dial-Up Networking. Select a device that supports PPP (e.g. the NDIS WAN driver included with the *LANCAPI*) for the connection and press **OK** to confirm.

③ Then the *ELSA LANconfig* program will display a new device with the name 'Unknown' and the dial-up call number as the address in the device list.

Once the entry appears in the device list the Dial-Up Networking connection is broken.

④ You can configure the device remotely just like all other devices. *ELSA LANconfig* establishes a dial-up connection enabling you to select a configuration.

4.9.3 The first remote connection using a PPP client and Telnet

① Establish a connection to the *ELSA LANCOM Business* with your PPP client using the following details:

- User name 'ADMIN'
- Password as set on the *ELSA LANCOM Business*, factory default setting is no password
- An IP address for the connection, only if required

② Open a Telnet session to the *ELSA LANCOM Business*. Use the following IP address for this purpose:

- '172.17.17.18', if you have not defined an IP address for the PPP client. The *ELSA LANCOM Business* automatically uses this address if no other address has been defined. The calling PC then responds to the IP address '172.17.17.17'.
- Raise the IP address of the PC by one, if you have defined an address. For example: If you have defined the IP address '10.0.200.123' for the PPP client, the *ELSA LANCOM Business* will respond to '10.0.200.124'. Exception: If the digits '254' are at the end of the IP address, the router responds to 'x.x.x.1'.

③ You can configure the *ELSA LANCOM Business* remotely just like all other devices.

4.9.4 Limiting remote configuration

The PPP connection of any other remote site to the router, of course, will only succeed if the device answers every call with the corresponding PPP settings.

This is the case using the factory default settings because the default protocol (default layer) is set to PPP.

You may, however, want to change the default layer for LAN-to-LAN connections, for example, to a different protocol after the first configuration run. Then the device will no longer take calls on the dial-up connection using the PPP settings. The solution to this is to agree upon a special calling number for configuration access. If the device receives a call on this number, it will always use PPP, regardless of any other settings made on the router. Only a specific user name which is automatically entered by the *ELSA LANconfig* program during call establishment will be accepted during the PPP negotiations.

① Switch to the 'Security' tab in the 'Management' configuration section.

② In the 'Configuration access' field, choose whether the configuration is fully accessible, read-only or not accessible from remote networks.

Alternatively, enter the following command during a Telnet or terminal connection:

```
set /setup/config-module/WAN-config [on][read][off]
```

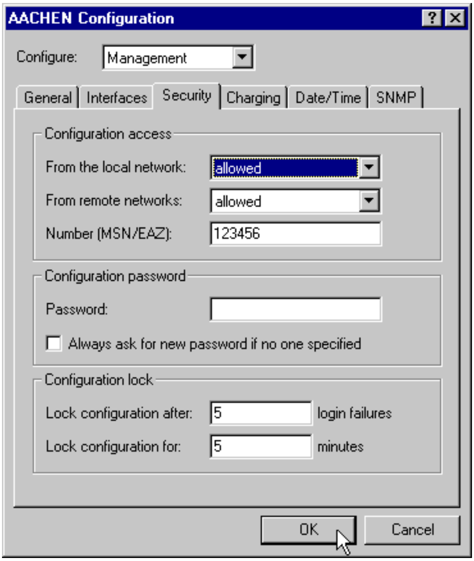
If you wish to block access to the router from the WAN entirely, set configuration access from remote networks to 'denied'.

③ In the 'Configuration access' field, enter a calling number of your connection which is not used for other purposes as the calling number.

Alternatively, enter the following command:

```
set /setup/config-module/Farconfig 123456
```

④ You can protect the configuration of the device by assigning a password.



Configure: Management

Configuration access

From the local network: allowed

From remote networks: allowed

Number (MSN/EAZ): 123456

Configuration password

Password:

□ Always ask for new password if no one specified

Configuration lock

Lock configuration after: 5 login failures

Lock configuration for: 5 minutes

Alternatively, enter the following command during a Telnet or terminal connection:

```
passwd
```

You will then be prompted to enter and confirm a new password.

4.10 Trace outputs—Information for pros

Trace outputs may be used to monitor the internal processes in the router during or after configuration. One such trace can be used to display the individual steps involved in negotiating the PPP. Experienced users may interpret these outputs to trace any errors occurring in the establishment of a connection. A particular advantage of this is: The errors being tracked may stem from the configuration of your own router or that of the remote site.

The trace outputs are slightly delayed behind the actual event, but are always in the correct sequence. This will not usually hamper interpretation of the displays but should be taken into consideration if making precise analyses.

4.10.1 How to start a trace

Trace output can be started in a Telnet session, for example. The command to call up a trace follows this syntax:

```
trace [code] [parameters]
```

The trace command, the code, the parameters and the combination commands are all separated from each other by spaces. And what is lurking behind the code and parameters?

This code...	... in combination with the trace causes the following:
?	Displays a help text
+	Activates a trace output
-	Deactivates a trace output
#	Switches between different trace outputs (toggle)
no code	Displays the current status of the trace

This parameter...	... brings up the following display for the trace:
Status	Status messages for the connection
Error	Error messages for the connection
ELSA	ELSA protocol negotiation
PPP	PPP protocol negotiation
IPX-router	IPX routing
RIP	IPX Routing Information Protocol
SAP	IPX Service Advertising Protocol
IPX-watchdog	IPX watchdog spoofing
SPX-watchdog	SPX watchdog spoofing
NetBIOS	NetBIOS management
IP router	IP routing
IP RIP	IP Routing Information Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
SCRPT	Script negotiation

This parameter...	... brings up the following display for the trace:
IP-masquerading	Processes in the masquerading module
DHCP	Dynamic Host Configuration Protocol
D channel	Trace on the D channel of the connected ISDN bus

This combination command...	... brings up the following display for the trace:
All	All trace outputs
Display	Status and error outputs
Protocol	ELSA and PPP outputs
TCP-IP	IP-Rt., IP-RIP, ICMP and ARP outputs
IPX-SPX	IPX-Rt., RIP, SAP, IPX-Wd., SPX-Wd., and NetBIOS outputs
Time	Displays the system time in front of the actual trace output
Source	Includes a display of the protocol that has initiated the output in front of the trace

Any appended parameters are processed from left to right. This means that it is possible to call a parameter and then restrict it.

Examples

This code...	... in combination with the trace causes the following:
trace	Displays all protocols that can generate outputs during the configuration, and the status of each output (ON or OFF).
trace + all	Switches on all trace outputs
trace + protocol display	Switches on the output for all connection protocols together with the status and error messages
trace + all - icmp	Switches on all trace outputs with the exception of the ICMP protocol
trace ppp	Displays the status of the PPP
trace # ipx-rt display	Toggles between the trace outputs for the IPX router and the display outputs
trace - time	Switches off the system time output before the actual trace output

4.11 New firmware with ELSA FirmSafe

The software for the ELSA devices is constantly being updated. We have fitted the devices with a flash ROM which makes child's play of updating the operating software so that you can enjoy the benefits of new features and functions. No need to change the EPROM, no need to open up the case: simply load the new release and you're away.

4.11.1 This is how ELSA FirmSafe works

ELSA FirmSafe makes the installation of the new software safe: The used firmware is not simply overwritten but saved additionally in the device as a second firmware.

Of the two firmware versions saved in the device only one can ever be active. When loading a new firmware version the active firmware version is not overwritten. You can decide which firmware version you want to activate after the upload:

- 'Immediate': The first option loads the new firmware and activates it immediately. This can result in the following situations:
  - The new firmware is loaded successfully and works as desired. Then all is well.
  - The device no longer responds after loading the new firmware. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots.
- 'Login': To avoid problems with faulty uploads there is the second option with which the firmware is uploaded and also immediately booted.
  - In contrast to the first option, the device will wait for five minutes until it has successfully logged on. Only if this login attempt is successful does the new firmware remain active permanently.
  - If the device no longer responds and it is therefore impossible to log in, the firmware automatically loads the previous firmware version and reboots with it.
- 'Manual': With the third option you can define a time period during which you want to test the new firmware yourself. The device will start with the new firmware and wait for the preset period until the loaded firmware is manually activated and therefore becomes permanently effective.

4.11.2 How to load new software

There are various ways of carrying out a firmware upload (which is the term given to the installation of software), all of which produce the same result:

- *ELSA LANconfig*
- *ELSA WEBconfig*
- Terminal programs
- TFTP

All settings will remain unchanged by a firmware upload. All the same you should save the configuration first for safety's sake (with **Edit** ▶ **Save Configuration to File** if using *ELSA LANconfig*, for example).

If the newly installed release contains parameters which are not present in the device's current firmware, the device will add the missing values using the default settings.

ELSA LANconfig

When using *ELSA LANconfig*, highlight the desired device in the selection list and click on **Edit** ▶ **Firmware Management** ▶ **Upload New Firmware**, or click directly on the **Firmware Upload** button. Then select the directory in which the new version is located and mark the corresponding file.

ELSA LANconfig then tells you the version number and the date of the firmware in the description and offers to upload the file. The firmware you already have installed will be replaced by the selected release by clicking **Open**.

You also have to decide whether the firmware should be permanently activated immediately after loading or set a testing period during which you will activate the firmware yourself. To activate the firmware during the set test period, click on **Edit** ▶ **Firmware Management** ▶ **After upload, start the new firmware in test mode**.

ELSA WEBconfig

Launch your browser and enter the IP address of the unit in the address field. For example, if your *ELSA LANCOM Business* has the IP address 194.162.200.17, enter: 'http://194.162.200.17'.

On the starting page, follow the 'Upload new Firmware' link. In the next window you can browse the folder system to find the firmware file and click **Upload** to start the installation.

Terminal program (e.g. Telix or Hyperterminal in Windows)

If using a terminal program, you should first select the 'set mode-firmsafe' command on the 'Firmware' menu and select the mode in which you want the new firmware to be loaded (immediately, login or manually). If desired, you can also set the time period of the firmware test under 'set Timeout-firmsafe'.

Select the 'Firmware-upload' command to prepare the router to receive the upload. Now begin the upload procedure from your terminal program:

- If you are using Telix, click on the **Upload** button, specify 'XModem' for the transfer and select the desired file for the upload.
- If you are using Hyperterminal, click on **Transfer** ▶ **Send File**, select the file, specify 'XModem' as the protocol and start the transfer with **OK**.

TFTP

TFTP is available by default under the Windows 2000 and Windows NT operating systems. It permits the simple transfer of files with other devices across the network.

TFTP can be used to install new firmware on *ELSA LANCOM Business*. This can be done with the command (or target) **writeflash**. For example, to install new firmware in a *ELSA LANCOM Business* with the IP address 194.162.200.17, enter the following command under Windows 2000 or Windows NT:

```
tftp -i 194.162.200.17 put Lc_60xxu.220 writeflash
```

*This command sends the corresponding file to the input IP address using the **writeflash** command (or destination). Binary file transfer must be set for TFTP. However, many systems have the ASCII format preset. This example for Windows 2000 and Windows NT shows you how to achieve this by using the '-i' parameter.*

The device is booted up following a successful firmware upload and this activates the new firmware switch directly. If an error occurs during the upload (write error in the flash ROM, TFTP transmission error or similar) FirmSafe activates the previous firmware. The configuration connection remains in operation.

With TFTP, other configuration commands can be performed too. The syntax is best demonstrated with the following examples:

- tftp 10.0.0.1 get readconfig file1: Reads the configuration from the device with the address 10.0.0.1 and saves it as file1 in the current directory.

- tftp 10.0.0.1 put file1 writeconfig: Writes the configuration from file1 to the device with the address 10.0.0.1.
- tftp 10.0.0.1 get dir/status/verb file2: Saves the current connection information in file2.

5 Connection via 2-Mbit interface

This chapter contains technical details related to the most important feature of your *ELSA LANCOM Business 6000*: connections via the 2-Mbit interface(s). The description will focus on the configuration of connections, i.e. software settings.

5.1 Areas of application

What is your intended use for the 2-Mbit connection? First, a look at the most important applications:

- **Fast Internet connections for a network**
  Many Internet service providers offer 2-Mbit Internet connections. Thanks to the IP router function integrated in the *ELSA LANCOM Business 6000*, Internet access is available to every workstation in the network.
- **Interconnection of two networks**
  A leased line is generally used for the interconnection of two LANs. With the *ELSA LANCOM Business 6000*, this interconnection is realized by routing packets to the remote network. Unlike with a bridging solution, the two networks continue to appear as two separate networks. You can, however, grant any workstation of either network access to the resources of the remote network. Far-reaching interconnected network systems can set up using multiple routers.
- **Dial-up access points for remote access**
  Many telecommunications providers offer primary rate interfaces (PMxA, or PRI for **P**rimary **R**ate **I**nterface). Up to 30 parallel ISDN D channel connections can be established using a PMxA. The individual channels are independent of one another and can establish connections to a variety of remote ISDN stations. For example, up to 30 remote workstations can establish parallel dial-up connections to a corporate network via ISDN in this configuration.

  ELSA LANCOM Business is designed for use on fixed connections. It cannot be used on a PMxA. The further descriptions will thus be limited to covering fixed connections.

LANconfig and *WEBconfig* feature wizards for the configuration of Internet access or network interconnections. Further information will be provided on this topic in this chapter. First however, a brief overview of the technology behind the 2-Mbit interfaces.

5.2 Technical basics

This section contains the most important information about the technology and standards used in conjunction with 2-Mbit connections in the *ELSA LANCOM Business*.

5.2.1 The 2-Mbit interfaces of your device

Let's have a brief look at the 2-Mbit interfaces of your device and the technology behind them.

Depending on the model, your *ELSA LANCOM Business 6000* features up to three 2-Mbit interfaces:

- *ELSA LANCOM Business 6001*
  - one X.21 interface
- *ELSA LANCOM Business 6011*
  - one X.21 interface
  - one G.703 connection
- *ELSA LANCOM Business 6021*
  - one X.21 connection
  - two G.703 connections

X.21 – terminal adapter required

X.21 is a serial communications standard for speeds of up to 2 Mbps and distances of up to 10 meters.

A so-called terminal adapter can be connected to the X.21 interface of the *ELSA LANCOM Business*. This terminal adapter is the link between your telecommunications provider's terminal device connection and one or more routers.

G.703 – directly to the terminal device

Depending on the type, the *ELSA LANCOM Business* models *6011* and *6021* feature one or two G.703 connections in addition to the X.21 interface. These models can be connected directly to your telecommunications provider's terminal device connection. An additional terminal adapter is thus no longer required.

5.2.2 G.703 – simple basis for 2-Mbit connections

G.703 is an ITU (International Telecommunication Union) recommendation for remote digital connections at speeds of 64 kbps or more. In Europe, 2-Mbit connections in accordance with G.703 are referred to as E1 connections. The T1 standard generally used in the USA works in the same manner as E1, but has a bandwidth of only 1544 kbps.

G.703 is a standard on level 1 of the OSI model, i.e. at the physical level. It defines the electrical and functional characteristics of the connections.

G.703 connections are synchronous and bit-oriented. A continuous stream of data is transferred between the terminal points, regardless of whether it actually contains user data.

Higher-level protocols such as G.704 are required to convert the transferred bits into content.

5.2.3 G.704 structures the data stream

A protocol which provides additional information about the structure of the transferred bits is required in order to use the continuous but unstructured data stream for the transmission of content.

The ITU has thus defined a supplementary protocol to G.703: G.704. While G.704 is not required as a protocol to structure the data stream, its use provides a number of advantages that will become apparent later in this chapter.

The combination of G.703 and G.704 is also known as “structured G.703”, as opposed to the unstructured “G.703”.

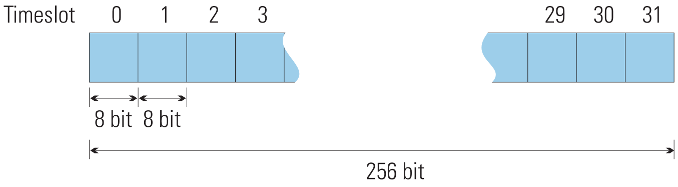
Division of bandwidth into timeslots

But what is this structure exactly? G.704 divides the full G.703 bandwidth into timeslots (timeslots). To determine the bandwidth of an individual timeslot, the standard was oriented according to the minimal bandwidth required at the time for voice communications. At the time that the standard was established, 64 kbps were needed for clean voice communications. As the timeslots are the smallest independent units for an individual connection, they were fixed at a bandwidth of 64 kbps.

Each timeslot was given a defined data width of 8 bits; 8000 data packets (frames) are transferred per second and timeslot. This results in the required bandwidth per timeslot of

8 bits/frame x 8000 frames/second = 64 kbps

The 2-Mbit bandwidth of G.703 is thus broken down into 32 timeslots of 64 kbps each. The timeslots are numbered from 0–31.



Reservation of timeslots for control data

The first of these 32 timeslots (0) is permanently reserved by G.704 for the transmission of framing data. A number of terminal devices, certain terminal adapters for example, also permanently reserve timeslot 0 for the transmission of control data. These reserved timeslots thus perform tasks very comparable to those of the ISDN D channel. All non-reserved timeslots are available for the transmission of user data. In their function and bandwidth, they correspond to the B channels in the ISDN.

As a rule, any combination of timeslots can be used for the user and control data, only timeslot 0 is reserved for G.704 framing information. Intermediate exchanges always treat timeslots 1–31 as user data. The distribution of these 31 timeslots for user data and supplementary control data is determined solely by the configuration of the terminal equipment. Normally, there would be no reason to reserve one of the 31 timeslots for the transmission of supplementary control data in fixed, point-to-point connections.

Free coupling of timeslots

In G.704, timeslots can be optionally coupled for greater bandwidth. The coupling is set in the terminal devices. The coupled timeslots result in connection channels with the appropriate bandwidth. These connection channels can also be used for fixed connections to a variety of remote stations.

The devices of the ELSA LANCOM Business 6000 series are designed for the operation of a single connection channel only and do not support the free assignment of timeslots to connection channels.

G.704 only passes these timeslot blocks for the transmission of user data on to higher-level protocols. The formerly unstructured G.703 data stream remains hidden.

G.704 integrity checking

In addition to structuring the complete G.703 bandwidth in timeslots, G.704 also provides simple integrity checking of the transferred data using a 4-bit CRC algorithm to prevent transfer errors.

5.2.4 Which method for your purpose?

In short: three methods are common under G.703/704. All three result in different user data bandwidths:

Mode	Protocols used	Timeslots reserved for control data	Number of timeslots for user data	Bandwidth for user data
E1 unstructured	G.703	–	32	2,048 kbps
E1 structured	G.703 + G.704	TS0	31	1,984 kbps
E1 structured (TS16 reserved)	G.703 + G.704	TS0, TS16	30	1,920 kbps

Most telecommunications providers offer unstructured G.703 connections as well as structured connections as per G.703/704. In Europe, the designation E1 is commonly used for 2-Mbit connections.

A variety of designations have become common in different countries for the European standards. The following overview for Germany will serve as an example:

	E 1	E1:structured	E1 structured (TS16 reserved)
Germany	D2MU	D2MS	D2MS[1]

[1] D2MS with additional reservation of TS16 for control data.

The choice of E1 mode initially depends on your telecommunications provider. For providers with an infrastructure relying heavily on multiplexers, unstructured G.703 is the preferred, if not only connection type. Providers with an infrastructure based mainly on switching stations also offer G.704 connections.

Even with unstructured G.703–structure thanks to HDLC

A framing protocol is always applied to the data transfer, as unstructured connections are never sufficient for data communications. In the case of unstructured G.703 it is applied to the full bandwidth, for G.704 only to the resulting timeslot blocks.

Data integrity is thus assured, even in the event of varying error rates. A few additional observations on this topic:

Operational security and Error rate

One important advantage of G.704 connections as opposed to a combination of G.703 and a self-monitoring layer 2 protocol is its high guaranteed operational security. Very few providers are willing to guarantee an operational security higher than 95% for unstructured G.703 connections.

As errors in G.704 lines can be monitored and detected by the line providers, the providers can easily localize the sources of errors and take corrective action. In the case of unstructured G.703 connections, errors can only be detected at the terminal devices, making corrections more difficult.

Multiple fixed connections

An important advantage of G.704 is the flexible structuring of multiple fixed connections. Individual timeslots can be bundled on a hardware basis by the exchanges for a variety of fixed connections. Fixed connections to multiple remote stations are not possible without G.704.

Data throughput

G.704 connections have a lower data throughput by nature, as the timeslots occupied with protocol data are not available for the transfer of user data. In the case of a G.704 connection that only occupies TS0, the bandwidth available for user data is reduced by over 3%. If TS16 is also occupied, the loss amounts to over 6% as opposed to unstructured G.703.

Conclusion

The use of the G.704 framing protocol is simpler, more reliable and more flexible. A higher bandwidth can be achieved with an unstructured G.703 connection. In the event of especially favorable line conditions (short distances, few intermediate switching stations, only one remote station), the additional protocol overhead of a G.704 connection may not be worthwhile.

5.2.5 Setting up the basic protocols

As complex as the world of 2-Mbit standards may be, the configuration of your *ELSA LANCOM Business* is still a simple matter.

To set up Internet access or interconnect two networks using a 2-Mbit connection, launch the appropriate wizard using *LANconfig* or *WEBconfig*.

X.21 interface

No further input is necessary when using an X.21 interface and a terminal adapter. In this case the configuration of all connection parameters is performed at the terminal adapter, assuming that these are not already fixed.

G.703 interface

If you choose a G.703 interface for the connection, you will be asked which basic protocols should be used.

Three options are available:

- **E1-U** – unstructured E1
- **E1-S (with TS16)** – structured E1, only TS0 reserved
- **E1-S** – structured E1, TS0 and TS16 reserved

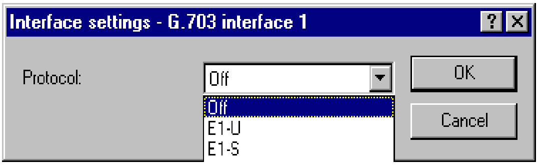
The choice of **E1-U** or **E1-S (with TS16)** depends on how your provider has configured the line—whether it has been set to unstructured G.703, or whether it also uses G.704 framing. **E1-S** should only be selected if the remote device requires the reservation of TS16 for control data. This is the case with some terminal adapters.

Changing the settings manually

You can change the interface settings manually at any time. You can find the menu under:

- ***LANconfig***

  Management ▶ Interfaces ▶ Interface settings



Interface settings - G.703 interface 1

Protocol: Off

Off
E1-U
E1-S

- ***WEBconfig***

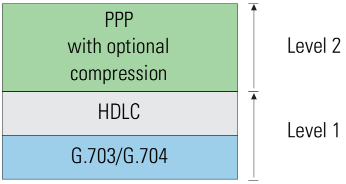
  Expert Configuration ▶ Setup ▶ Interface ▶ G.703 Interface

- **Telnet**

  /Setup/Interfaces/G703 interfaces

Additional settings using the wizards

The wizards automatically take care of a number of additional settings. The following protocol structure is automatically selected for the connection:



These settings are virtually ideal for establishing connections between two ELSA routers. The configuration only needs to be changed manually for terminal devices that require other settings. The appropriate settings tables can be found under *LANconfig* in the 'Communication' section:

- General ▶ Communication Layer
- Remote sites ▶ Name list
- Remote sites ▶ Channel list
- Protocols ▶ PPP list

Under *WEBconfig* the changes can be found in the submenu **Expert Configuration** ▶ **Setup** ▶ **WAN Module** in the tables:

- Name list
- Layer list
- PPP list
- Channel list

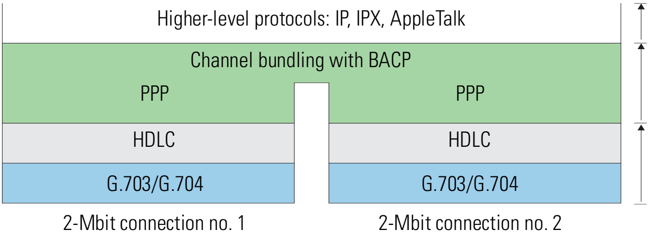
5.3 Bundling of 2-Mbit connections

The *ELSA LANCOM Business 6021* offers the option of establishing a 4-Mbit connection by bundling two 2-Mbit connections. In this case, the remote device must also support the bundling of two 2-Mbit connections.

Only two of the three 2-Mbit interfaces of the *ELSA LANCOM Business 6021* (one X.21 and two G.703 interfaces) can be used simultaneously. You thus have the choice of using the two G.703 interfaces in parallel, or using a G.703 interface in combination with a X.21 connection.

The bundling takes place in the datalink layer of the OSI model, i.e. on level 2. It is realized using the BACP protocol (**B**andwidth **A**llocation **C**ontrol **P**rotocol) in conjunction with PPP (**P**oint-to-**P**oint **P**rotocol). This protocol combination is also often referred to as MLPPP (**M**ulti**L**ink **PPP**).

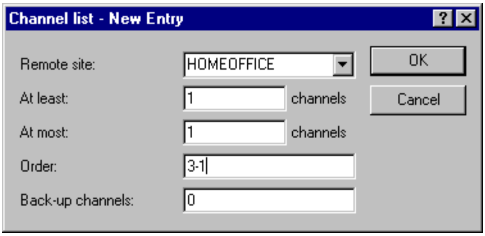
The protocol structure of the bundled connection is as follows for two 2-Mbit connections:



The channel bundling is entered in the channel list:

- ***LANconfig***

  Communication ▶ Channel list



Channel list - New Entry

Remote site:	HOMEOFFICE	
At least:	1	channels
At most:	1	channels
Order:	3-1	
Back-up channels:	0	

- ***WEBconfig***

  Expert Configuration ▶ Setup ▶ WAN Module ▶ Channel list

- **Telnet**

  /Setup/WAN-module/Channel-list

Enter the appropriate number of channels in the 'Minimum' and 'Maximum' fields. The highest suitable value for a 4-Mbit connection is '2'.

'Order' determines which channel is used to establish a connection and which is then added for channel bundling. The connection established first is referred to in the BACP conventions as the 'Master', the additional channel is the 'Slave'.

The channel designation used in the 'Order' field consists of two digits separated by a dash—for example '1-1'. The first digit specifies the device's interface (in this example the ISDN interface), the second refers to the channel used within the interface (in this example the first B channel). The following channels are available in the *ELSA LANCOM Business 6021*:

Designation	Interface and channel number
1-1	ISDN S_0 bus, first B channel
1-2	ISDN S_0 bus, second B channel
2-1	X.21 interface (only has one channel)
3-1	First G.703 interface (next to the ISDN interface)
4-1	Second G.703 interface (far left)

The ISDN channels are only mentioned in this table for the sake of completeness. In practice there is no point in bundling ISDN channels with 2-Mbit connections. Further information will be provided on this topic later in this section.

The channels entered in the 'Order' field are separated with semicolons. A typical entry would be '3-1;4-1'. With this entry, the connection is initially established using the first G.703 interface (this is the master), the connection via the second G.703 interface is then added (as the slave).

The slowest connection is decisive

Take care with connections involving differing user data bandwidths: In channel bundling, the slowest connection is decisive for the speed of the connection as a whole. The additional bandwidth of the faster connection is not used!

For example, if a connection over channel 4-1 with a user data bandwidth of 1,920 kbps is bundled to a connection over channel 3-1 with 2,048 kbps, only 1,920 kbps of the faster channel will be used. The total bandwidth will only be 3,840 kbps instead of the expected 3,968 kbps.

This loss of speed is especially pronounced when bundling a 2-Mbit connection with an ISDN channel. In this case, the slow ISDN connection will restrict the data throughput of the 2-Mbit connection to a mere 64 kbps.

6 Operating modes and functions

This section is an introduction to the functions and operating modes of your device. It includes information on the following points:

- Security settings
  - Security for your configuration
  - Security for your LAN
- IP address management for the LAN
  - Automatic address administration with DHCP
  - DNS server
- NetBIOS proxy for the interconnection of Windows networks
- SYSLOG function
- ISDN
  - Establishment of ISDN dial-up connections
  - Office communications with *ELSA LANCAPI*
  - Reserving B channels
  - Modem dial-up (up to V.90)
  - Charge management
  - Accounting
  - Least-cost router

Alongside the description of the individual points, we will also give you concrete instructions to support you as you configure your device.

6.1 Security for your configuration

A number of important parameters for the exchange of data are established in the configuration of the device. These include the security of your network, monitoring of costs and the authorizations for the individual network users.

Needless to say, the parameters that you have set should not be modified by unauthorized persons. The *ELSA LANCOM Business* thus offers a variety of options to protect the configuration.

6.1.1 Password protection

The simplest option for the protection of the configuration is the establishment of a password. As long as a password hasn't been set, anyone can change the configuration of the device.

The password input field can be found in the *ELSA LANconfig* in the 'Management' configuration section on the 'Security' tab. The password prompt can be activated in a terminal or Telnet session in the `/Setup/Config-module/passw.required` menu. In this case, the password it-self is set with the command `passwd`.

6.1.2 Login barring

The configuration in the *ELSA LANCOM Business* is protected against “brute force attacks” by barring logins. A brute-force attack is the attempt by an unauthorized person to crack a password to gain access to a network, a computer or another device. To achieve this, a computer can, for example, go through all the possible combinations of letters and numbers until the right password is found.

As a measure of protection against such attacks, the maximum allowed number of unsuccessful attempts to Login can be set. If this limit is reached, access will be barred for a certain length of time.

If barring is activated on one port all other ports are automatically barred too.

The following entries are provided in the *ELSA LANconfig* for configuring login barring in the 'Management' configuration area on the 'Security' tab or under `/Setup/Config-module` in the menu:

- 'Lock configuration after' (`Login-errors`)
- 'Lock configuration for' (`Lock-minutes`)

6.1.3 Access control via TCP/IP

Access to the internal functions of the devices through TCP/IP can be restricted using a special filter list. Internal functions in this case are configuration sessions via *ELSA LANconfig*, *ELSA WEBconfig*, SNMP or Telnet.

This table is empty by default and so access to the router can therefore be obtained by TCP/IP from computers with any IP address. The filter is activated when the first IP address with its associated network mask is entered and from that point on only those IP addresses contained in this initial entry will be permitted to use the internal functions. The circle of authorized users can be expanded by inputting further entries. The filter entries can describe both individual computers and whole networks.

The access list can be found in the *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'General' tab, or in the `/Setup/TCP-IP-module/Access-list` menu.

6.2 Security for your LAN

You certainly would not like any outsider to have easy access to or to be able to modify the data on your computer. The *ELSA LANCOM Business* offers you various ways of restricting access from outside:

- Identification control
  - Access protection using name and password
  - Access protection via caller ID
- Callback to defined call numbers
- Data packet filtering – firewall
- IP masquerading (also known as NAT/PAT)

6.3 Identification control

The “identifier” to be used for determining the caller can be specified in the 'Communication' configuration section under the 'Call accepting' tab, or under the `/Setup/WAN-module/Protect` menu. You have a choice of the following:

- all calls are accepted from any remote station.
- by name: Only calls from those remote stations entered in the name list are accepted.
- by number: Only calls from those remote stations entered in the number list are accepted.
- by name or number: Only calls from those remote stations entered in the name list **or** number list are accepted.

It is an obvious requirement for identification that the corresponding information is also sent by the caller.

Verification of name

The routers' response is obvious: Only those calls with recognized names are accepted if protection by name is set; all others are rejected.

In the case of the PPP protocol, the user name of the remote station (frequently identical to the device name) is checked against the local PPP list.

Only a name, no secret password? The PPP does also offer this option: It is also possible here to request a form of protection available specifically to this protocol based on PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) or MS CHAP (a Microsoft variety of CHAP).

In the case of PPP, a user name (and in conjunction with PAP, CHAP or MS-CHAP, a password) is sent to the remote station during connection establishment. When a computer dials into the *ELSA LANCOM Business*, the communications software, for example Windows Dial-Up Networking, prompts the user for the user name and password to be transferred.

If the router itself establishes a connection, to an Internet service provider for example, it uses the user name and password from the PPP list. If no user name has been entered there, the device name will be used instead.

The PPP list can be found in the *ELSA LANconfig* in the 'Communication' configuration section on the 'Protocols' tab, or in the `/Setup/WAN-module/PPP-list` menu.

In addition, the PPP protocol also permits the caller to require an authentication from the remote station. The caller then requests a user or device name and password from the remote station.

Obviously you will not need to use the PAP, CHAP or MS CHAP security procedures if you are using the ELSA LANCOM Business to dial up an Internet service provider yourself, for example. You will probably not be able to persuade the ISP to respond to a request for a password...

Checking the number

When a call is placed over an ISDN line, the caller's number is normally sent over the D channel before a connection is even made (CLI—Calling Line Identifier).

Access to your own network is granted if the call number appears in the number list, or the caller is called back if the callback option is activated. If the *ELSA LANCOM Business* is set to provide security using the telephone number, any calls from remote stations with unknown numbers are denied access.

You can use call numbers as a security measure with any B-channel protocol (layers).

6.3.1 Callback

The callback function offers a special form of access privilege: This requires the 'Callback' option to be activated in the name list for the desired caller and the call number to be specified, if required.

The callback characteristics of your router can be controlled using the settings in the name and number lists and the selection of the (PPP) protocol:

- The router can refuse to call back.
- It can call back using a preset call number.
- The caller can opt to specify the call number to be used for callback.

And all the while you can use the settings to dictate how the cost of the connection is to be apportioned. The router accepts all unit charges, except for the unit required to send the name, if call back 'After name verification' is set in the name list. The caller also accepts a unit if the caller is not identified via CLIP (**C**alling **L**ine **I**dentifier **P**rotocol). On the other hand, the caller incurs no costs if identification of the caller's number is possible and is accepted (callback via the D channel).

An especially effective callback method is the fast callback procedure (patent pending). This speeds up the callback procedure considerably. The procedure only works if it is supported by both stations. All current ELSA routers are capable of fast callback.

6.3.2 Data packet filtering—Firewall

The firewall filters of the *ELSA LANCOM Business* devices offer filter functions for individual computers and also for entire networks. These filters effectively protect your network against intruders.

Setting up the filter

There are several options for setting up the firewall filters:

- ***LANconfig***

  IP router ▶ Filtering

The filter function can only be accessed in LANconfig if 'Complete View of Configuration' is selected under ***View ▶ Options****.*

- ***WEBconfig***

  Expert configuration ▶ Setup ▶ IP router module ▶ Firewall

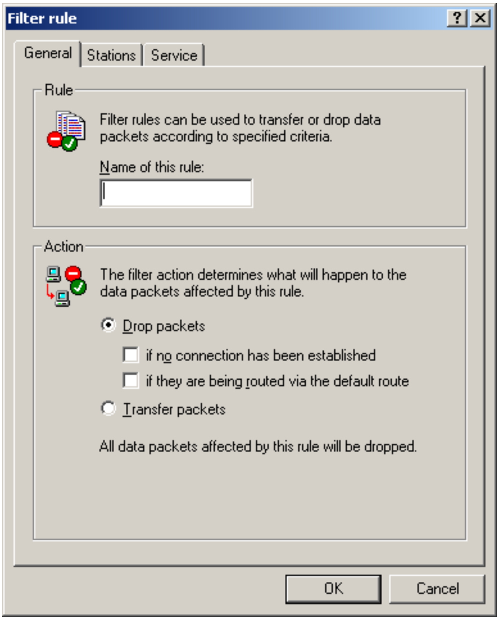
- **Telnet**

  /Setup/IP router module/Firewall

Please note that all procedures access the same configuration data. For example, if you change the filter settings in LANconfig, this will also have a direct effect on the values under WEBconfig and Telnet.

Setting up filters under *ELSA LANconfig*

It is particularly easy to set up the filter with *ELSA LANconfig*. The following tabs under 'Filter' can assist you to define the filter rules.



Rule

Filter rules can be used to transfer or drop data packets according to specified criteria.

Name of this rule:

Action

The filter action determines what will happen to the data packets affected by this rule.

● Drop packets

□ if no connection has been established

□ if they are being routed via the default route

○ Transfer packets

All data packets affected by this rule will be dropped.

- 'General'

  The name of the filter service and what should happen with the data packets (action) are specified here.

- 'Stations'

The stations for which the filter rule should apply as sender or receiver of the packets are specified here.

- 'Service'

  The IP protocols, source and destination ports to which the filter rule should apply are specified here.

Setting up filters under ***ELSA WEBconfig*** or Telnet

The configuration under *WEBconfig* or Telnet is somewhat more difficult than under *LANconfig*.

Here the filter functions are set in the filter list which is based on the entries of two other tables. The first is an object table in which the computer, networks, protocols, etc. are defined as objects. The second is a rules table in which source, target and action are described with the aid of the individual objects. The actual filter list is generated from these two lists.

The filter list can also be created directly, but this is not required. Making the required entries in the object and rules tables is sufficient for the filter list to be generated. This ensures that no inconsistent entries are made in the filter list.

What can be filtered? Source and target filters can be set for individual ports or for ranges of ports. In addition, individual protocols or any combinations of protocols (TCP/UDP/ICMP) can be filtered.

A previously defined action is executed as soon as a filter condition occurs.

Object table

The object table defines the elements or objects to be used in the rule table. Objects can be:

- Protocols
- Single computers
- Whole networks
- Services

These elements can also be combined in any way. Objects can also be defined hierarchically. Therefore, objects for the TCP and UDP protocols can be defined first. Then objects can be added later for items such as FTP (= TCP + Ports 20 and 21), HTTP (= TCP + Port 80) and DNS (= TCP, UDP + Port 53). They can then be combined to one object that contains all object definitions.

The direct descriptions that you can include here will be covered in greater detail in the following section on the Rules table.

The rules table

In the rules table the objects are linked into filter rules. The rules table contains the protocol to be filtered (the one you defined in the object table), the source objects, the target objects and the required filter action.

The protocol and the source or target objects can contain combined objects and also direct descriptions (e.g. %P6 for TCP), which are separated by '+' or spaces. A direct description is indicated by '%'. Possible descriptions are:

Description	Function
%A	IP address
%M	Network mask
%S	Sevice (port)
%L	Local network
%H	Host name
%P	Protocol (TCP/UDP/ICMP etc.)

Similar descriptions can generate lists separated by commas, such as host lists/address lists (%A10.0.0.1, 10.0.0.2) or ranges separated by hyphens, such as port lists (%S20-25). Insertion of a '0' or an empty string indicates the any object:

all computers:	%A0.0.0.0
all services:	%S0
all protocols:	%P0

Host names can only be used if the *ELSA LANCOM Business* can resolve the names in IP addresses. To do this the *ELSA LANCOM Business* must have learnt the names via DHCP or NetBIOS, or the assignment must be entered statically in the DNS or IP routing table. An entry in the IP routing table can associate an entire network to a host name.

The filter list

The filter list is ultimately put together from the object table and the rule table. This forms the merge quantity of all filters defined by the rules and objects.

Please note that filters are not created in the event of an error in input nor are error messages output. If you configure the filters manually, you should always check that the desired filters have been created.

6.3.3 The hiding place—IP masquerading (NAT, PAT)

One of today's most common tasks for routers is connecting the numerous workstation computers in a LAN to the network of all networks, the Internet. Everyone should have the potential to access the WWW from his workstation and be able to fetch bang up-to-date information for his work.

But this provokes objections from the network manager responsible for the security of data on the company's network: Every workstation computer on the Internet? Surely this means that anyone can get in from outside? —Not true!

IP masquerading provides a hiding place for every computer while connected with the Internet. Only the router module of the unit and its IP address are visible on the Internet. The IP address can be fixed or assigned dynamically by the provider. The computers in the LAN then use the router as a gateway so that they themselves cannot be detected. To do this, the router separates Internet and intranet, as if by a wall. Therefore, IP masquerading is also called a “firewall function”. Another very effective firewall technology is the targeted filtering of incoming data packets.

The use of IP masquerading is set individually for each route in the routing table. The routing table can be found in the *ELSA LANconfig* in the 'IP router' configuration section on the 'Routing' tab, or in the `/Setup/IP-router-module/IP-routing-table` menu.

6.4 Automatic IP address administration with DHCP

In order to operate smoothly in a TCP/IP network, all the devices in a local network must have unique IP addresses.

They also need the addresses of DNS server and NBNS server as well as that of a default gateway through which the data packets are to be routed from addresses that are not available locally.

In a smaller network, it is still conceivable that these addresses could be entered manually in all the computers in the network. In a larger network with many workstation computers, however, this would simply be too enormous of a task.

In such situations, the DHCP (Dynamic Host Configuration Protocol) is the ideal solution. Using this protocol, a DHCP server in a TCP/IP-based LAN can dynamically assign the necessary addresses to the individual stations.

6.4.1 The DHCP server

As a DHCP server, the *ELSA LANCOM Business* can administer the IP addresses in its TCP/IP network. In doing so, it passes the following parameters to the workstation computers:

- IP address
- Network mask
- Broadcast address
- DNS server
- NBNS
- Default gateway
- Period of validity for the parameters assigned

The DHCP server takes the IP addresses either from a freely defined address pool or determines the addresses automatically from its own IP address (or intranet address).

In DHCP mode, a completely unconfigured device can even automatically assign IP addresses to itself and the computers in the network.

In the simplest case, all that is required is to connect the new device to a network without other DHCP servers and switch it on. The DHCP server then interacts with *ELSA LANconfig* using a wizard and handles all of the address assignments in the local network itself.

6.4.2 DHCP—'on', 'off' or 'auto'?

The DHCP server can be set to three different states:

- 'on': The DHCP server is permanently active. The configuration of the server (validity of the address pool) is checked when this value is entered.
  - ○ When correctly configured, the device will be available to the network as a DHCP server.
  - ○ In the event of an incorrect configuration (e.g. invalid pool limits), the DHCP server is disabled and switches to the 'off' state.
- 'off': The DHCP server is permanently disabled.

- 'auto': The server is in automode. In this mode, after switching it on, the device looks for other DHCP server within the local network. This search can be recognized by the Tx LED flashing momentarily after activation.
  - The device then disables its own DHCP server if any other DHCP servers are found. This prevents the unconfigured device from assigning addresses not in the local network when switched on.
  - The device then enables its own DHCP server if no other DHCP servers are found.

  Whether the DHCP server is active or not can be seen in the DHCP statistics.

  The default state is 'auto'.

6.4.3 How are the addresses assigned?

IP address assignment

Before the DHCP server can assign IP addresses to the computers in the network, it first needs to know which addresses are available for assignment. Three options exist for determining the available selection of addresses:

- The IP address can be taken from the address pool selected (start address pool to end address pool). Any valid addresses in the local network can be entered here.
- If '0.0.0.0' is entered instead, the DHCP server automatically determines the particular addresses (start or end) from the IP or Intranet address settings in the 'TCP-IP-module' using the following procedure:
  - If only the IP address or only the Intranet address is entered, the start or end of the pool is determined by means of the associated network mask.
  - If both addresses have been specified, the Intranet address has priority for determining the pool.

  From the address used (IP or Intranet address) and the associated network mask, the DHCP server determines the first and last possible IP address in the local network as a start or end address for the address pool.
- If the router has neither an IP address of its own nor an Intranet address, the device has gone into a special operating mode. It then uses the IP address '10.0.0.254' for itself and the address pool '10.x.x.x' for the assignment of IP addresses in the network. In this state, the DHCP server

only assigns IP addresses and their validity to the computers in the network, but not the other information.

If only one computer in the network is booted and requests an IP address via DHCP with its network settings, a device with an activated DHCP module will assign this computer an address. A valid address is taken from the pool as an IP address. If the computer was already assigned an IP address at some point in the past, it requests this same address and the DHCP server attempts to reassign it this address if it has not already been assigned to another computer.

The DHCP server also checks whether the address selected is still available in the local network. As soon as the uniqueness of an address has been established, the requesting computer is assigned the address found.

Netmask assignment

The network mask is assigned in the same way as the address. If a network mask is entered in the DHCP module, this mask is used for the assignment. Otherwise, the network mask from the TCP/IP module is used. The order is the same as during the assignment of the addresses.

Broadcast address assignment

Normally, an address yielded from the valid IP addresses and the network mask is used for broadcast packets in the local network. In special cases, however (e.g. when using subnetworks for some of the workstation computers), it may be necessary to use a different broadcast address. In this case, the broadcast address to be used is entered in the DHCP module.

The default setting for the broadcast address should be changed by experienced network specialists only. Incorrect configuration of this section can result in the undesired establishment of connections subject to connect charges!

DNS and NBNS assignment

This assignment is based on the associated entries in the 'TCP/IP module'.

If no server is specified in the relevant fields, the router passes its own IP address as a DNS address. This address is determined as described under 'IP address assignment'. The router then uses DNS forwarding (also see 'DNS forwarding'), to resolve DNS or NBNS requests from the host.

Default gateway assignment

The device always assigns the requesting computer its own IP address as a gateway address.

If necessary, this assignment can be overwritten with the settings on the workstation computer.

Period of validity for an assignment

The addresses assigned to the computer are valid only for a limited period of time. Once this period of validity has expired, the computer can no longer use these addresses. In order for the computer to keep from constantly losing its addresses (above all its IP address), it applies for an extension ahead of time that it is generally sure to be granted. The computer loses its address only if it is switched off when the period of validity expires.

For each request, a host can ask for a specific period of validity. However, a DHCP server can also assign the host a period of validity that differs from what it requested. The DHCP module provides two settings for influencing the period of validity:

- Maximum lease time in minutes

  Here you can enter the maximum period of validity that the DHCP server assigns a host.

  If a host requests a validity that exceeds the maximum length, this will nevertheless be the maximum available validity!

  The default setting is 6000 minutes (approx. 4 days).

- Default lease time in minutes

  Here you can enter the period of validity that is assigned if the host makes no request. The default setting is 500 minutes (approx. 8 hours).

Priority for the DHCP server—request assignment

In the default configuration, almost all the settings in the Windows network environment are selected in such a way that the necessary parameters are requested via DHCP. Check the settings by clicking **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network**. Select the 'TCP/IP' entry for your network adapter and open **Properties**.

Check the various tabs for special entries, such as for the IP address or the standard gateway. If you would like all of the values to be assigned by the DHCP server, simply delete the corresponding entries.

Under the 'WINS Address' tab, the 'Enable DHCP for Windows Resolution' option must also be activated if you wish to use Windows networks via IP with name resolution via NBNS. In this case, the DHCP server must also have an NBNS entry.

Priority for computer—overwriting an assignment

If a computer uses parameters other than those assigned to it (e.g. a different default gateway), these parameters must be set directly on the workstation computer. The computer then ignores the corresponding parameters assigned to it by the DHCP server.

Under Windows, this can, for example, be performed via the properties of the network environment.

Click **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network**. Select the 'TCP/IP' entry for your network adapter and open **Properties**.

You can now enter the desired values by selecting the various tabs.

The assignment of IP addresses to the various computers can be checked using the 'Setup/DHCP/Table-DHCP' item in the DHCP module. This table contains the assigned IP address, the MAC address, the validity, the name of the computer (if available) and the type of address assignment.

The 'Type' field specifies how the address was assigned. This field can assume the following values:

- new

  The computer has made its initial request. The DHCP server verifies the uniqueness of the address that is to be assigned to the computer.

- unknown

  While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the DHCP server has no means of obtaining additional information on this computer.

- status

  A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.

- dynamic

  The DHCP server assigned an address to the computer.

6.4.4 Configuring the DHCP server

Basically, two starting points are possible when the devices are configured as a DHCP server:

- You have not yet configured a network or your existing local network does not use TCP/IP. The DHCP server in your new ELSA device lets you assign IP addresses to all of the computers in the network and to the router in a single operation.
- You are already using TCP/IP but without a DHCP server, and you would now like to convert to DHCP operation.

Configuration using *ELSA LANconfig* and the wizards

The *ELSA LANconfig* includes a wizard to help you with the required settings:

① Connect the unconfigured device to your local network using a network cable. If you are connecting the device to a hub, the node/hub switch must be set to 'Node'. If you are connecting the router directly to the network adapter of a computer in your network, set the switch to the 'Hub' position.

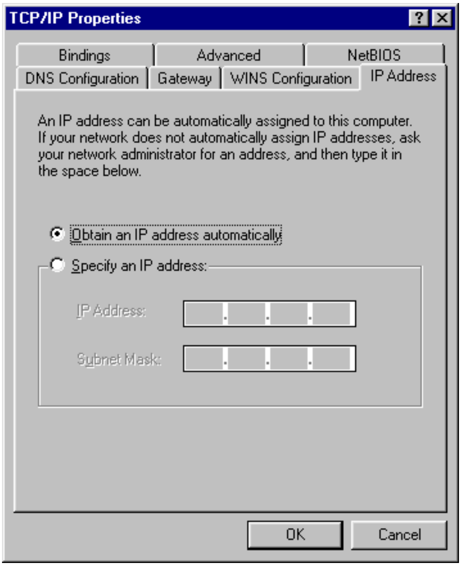
② Switch the device on. It will not find any other DHCP servers in the network and will thus enable its own DHCP functions.

③ If you have not done so already, install the TCP/IP protocol on all computers in the LAN.

  ○ Usually when the protocol is installed, the default configuration is such that the computers are automatically ready to obtain the IP address from a DHCP server. After rebooting at the end of the protocol installation, the computers automatically request an IP address from the DHCP server.

  ○ If the protocol is already installed, enable the DHCP function on all of the computers in the local network. Under Windows 95, for example, this is done by selecting **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network** to open the window for configuring network properties. Double-click the entry for the 'TCP/IP' protocol.
  Enable the 'Obtain an IP address from a DHCP server' option. Switch over to the 'DNS' tab and delete all of the existing DNS addresses. Next, delete any entries under the 'Gateway' tab and click **OK** to close all the windows. This change will require a reboot, after which

the computer will automatically request an IP address from the DHCP server's address pool.



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address:

Subnet Mask:

④ Install the *ELSA LANconfig* on a computer in the network.

⑤ Start the program from the 'ELSAlan' program group. When loading, the *ELSA LANconfig*, will detect an unconfigured router in the network and will launch the wizard for the basic settings.

○ If you have not previously used any IP addresses in your network, select the option 'Make all settings automatically' in this wizard and confirm your selection with **Finish** in the next window.
The wizard assigns the IP address '10.0.0.1' with the netmask '255.255.255.0' to the router and enables the DHCP server. On the basis of this IP address, the device then determines the valid address pool for the DHCP assignment.

○ In the event that IP addresses were already in use in your network before converting to DHCP operation, select the option 'I would like to adjust the settings manually' in the wizard. In the next window, enter an unused IP address from the previously-used address range and activate the DHCP server.

The wizard now assigns the selected IP address and associated netmask to the device. On the basis of this IP address, the device then determines the valid address pool for the DHCP assignment.

○ After a few seconds, all of the computers in the network will be checked and are assigned a new IP address by the DHCP server as required. The computers also receive additional parameters such as the broadcast address, DNS server, default gateway, etc.

Manual configuration

If configuration using the *ELSA LANconfig* wizard is not for you, set the parameters for the DHCP server manually: in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'DHCP' tab or in the `/Setup/DHCP-module` menu).

6.5 DNS

The domain name service (DNS) in TCP/IP networks provides the association between computer names or network names (domains) and IP addresses. This service is required for Internet communications, to return the correct IP address for a request such as 'www.elsa.com' for example. However, it's also useful to be able to clearly associate IP addresses to computer names within a local network or in a LAN interconnection.

6.5.1 What does a DNS server do?

The names used in DNS server requests are made up of several parts: one part consisting of the actual name of the host or service to be addressed; another section specifies the domain. Specifying the domain is optional within a local network. These names could thus be 'www.domain.com' or 'ftp.domain.com', for example.

If there is no DNS server in the local network, all locally unknown names will be searched for using the DEFAULT route. By using a DNS server, it's possible to immediately go to the correct remote station for all of the names with known IP addresses. In principle, the DNS server can be a separate computer in the network. However, the following reasons speak for locating the DNS server directly in the *ELSA LANCOM Business*:

- *ELSA LANCOM Business* can automatically distribute IP addresses for the computers in the local network when in DHCP server mode. In other words, the DHCP server already knows the names and IP addresses of all of the computers in its own network that were assigned IP addresses via DHCP. With the dynamic address assignments of a DHCP server, an external DNS server might have difficulties in keeping the associations between the names and IP addresses current.

- When routing Windows networks via NetBIOS, the *ELSA LANCOM Business* also knows the computer names and IP addresses in the other connected NetBIOS networks. In addition, computers with fixed IP addresses can also enter themselves in the NetBIOS table and thus be known by their names and addresses.
- The DNS server in the *ELSA LANCOM Business* can also be used as an extremely convenient filter mechanism. Requests for domains can be prohibited throughout the LAN, for subnetworks, or even for individual computers—simply by specifying the domain name.

When processing requests for specific names, the DNS server takes advantage of all of the information available to it:

- First, the DNS server checks whether access to the name is not prohibited by the filter list. If that is the case, an error message is returned to the requesting computer stating that access to the address has been denied.
- Next, it searches in its own static DNS table for suitable entries.
- If the address cannot be found in the DNS table, it searches the dynamic DHCP table. The use of DHCP information can be disabled if required.
- If no information on the name can be located in the previous tables, the DNS server then searches the lists of the NetBIOS module. The use of the NetBIOS information can also be disabled if necessary.

If the requested name cannot be found in any of the information sources available to it, the DNS server sends the request to another server—that of the Internet provider, for example—using the normal DNS forwarding mechanism, or returns an error message to the requesting computer.

6.5.2 Setting up the DNS server

The settings for the DNS server can be found in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'DNS Server' tab. To set up the DNS server, proceed as follows:

① Switch the DNS server on.

```
set Setup/DNS-Module/Operating on
```

② Enter the domain in which the DNS server is located. The DNS server uses this domain to determine whether the requested name is located in the LAN. Entering the domain is optional.

```
set Setup/DNS-Module/Domain yourdomain.com
```

③ Specify whether information from the DHCP server and the NetBIOS module should be used.

```
set Setup/DNS-Module/DHCP-usage yes
set Setup/DNS-Module/NetBIOS-usage yes
```

④ The main task of the DNS server is to distinguish requests for names in the Internet from those for other remote stations. Therefore, enter all computers into the DNS table

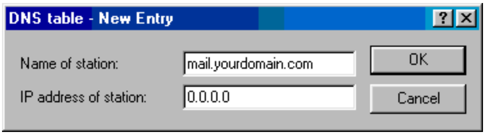
○ for which you know the name and IP address,

○ that are not located in your own LAN,

○ that are not on the Internet and

○ that are accessible via the router.

For example, if would like to access the mail server at your headquarters (name: mail.yourdomain.com, IP: 10.0.0.99) via the router from a branch office, enter:



Name of station: mail.yourdomain.com

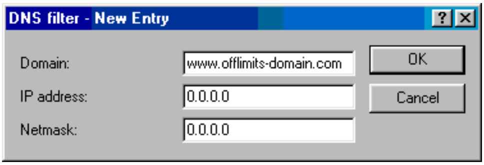
IP address of station: 0.0.0.0

```
cd Setup/DNS-Module/DNS-table
set mail.yourdomain.com 10.0.0.99
```

Stating the domain is optional but recommended.

When you now start your mail program, it will probably automatically look for the server 'mail.yourdomain.com'. The DNS server thereupon returns the IP address '10.0.0.99'. The mail program will then look for that IP address. With the proper entries in the IP routing table and name list, a connection is automatically established to the network in the headquarters, and finally to the mail server.

⑤ Finally, use the filter list to specify the users that cannot access certain names or domains.



Domain: www.offlimits-domain.com

IP address: 0.0.0.0

Netmask: 0.0.0.0

```
cd Setup/DNS-Module/Filter-list
set 001 www.offlimits-domain.com 0.0.0.0 0.0.0.0
```

This entry (with the index '001') prohibits this domain for all of the computers in the local network. The index '001' was selected freely and is only intended to enhance the overview. The wildcards '?' (stands for exactly one character) and '*' (for a random number of characters) are valid when entering the domain. For example, if only a single computer (IP 10.0.0.123) is to be prohibited from accessing DE-domains, enter:

```
set 002 *.de 10.0.0.123 255.255.255.255
```

The hit list in the DNS statistics contains the 64 most frequently requested names and provides a good basis for setting up the filter list.

If your LAN uses subnetting, you can also apply filters to individual departments by carefully selecting the IP addresses and subnet masks. The IP address '0.0.0.0' stands for all computers in the network, and the subnet mask '0.0.0.0' for all networks.

6.6 NetBIOS proxy

With the NetBIOS proxy function, a *ELSA LANCOM Business* can also route NetBIOS packets or respond locally as a proxy. As a result, it is now possible to economically link Windows networks using the router function.

This section describes the general functions of NetBIOS proxy, as well as the configuration of the router and workstations for the interconnection of Windows networks.

6.6.1 To the point: What is NetBIOS?

NetBIOS provides a simple, trouble-free means of networking multiple computers. An important example for NetBIOS networks is the Windows network, with which several Windows workstations can be networked simply by sharing the resources (drives or printers) of the individual computers with the other participants.

In a Windows network, the computers are only addressed via their names. Multiple computers can be organized into groups, and multiple groups can be grouped further as name rooms scopes. The names used must be known throughout the network for all computers to be able to access the resources of the others. NetBIOS computers issue their names into the network at regular intervals to eliminate the necessity of maintaining tables of known names on each computer.

The names publicized in this manner should, of course, be collected and made available at a central location in the Windows network. If two Windows networks are to be connected using a router, then such a name collection point, a so-called NetBIOS name server (NBNS), must be present on both sides.

- A WINS server (Windows Internet Name Service Server) can be installed in the network for this purpose.
- However, a second option is also available, since many Windows networks can or must make do without a server of their own: Information about the names in use can be placed on a “billboard” of sorts, on which all participating computers only post their names and IP addresses. In this case, the individual computers are responsible for the consistency of their names within the network.

The *ELSA LANCOM Business* offers such a billboard. The interconnection of Windows networks is thus possible without a server as a result of this simple realization of the NBNS. The computers in the networks to be interconnected thus publicize their names and add them to the billboards in the respective remote networks.

6.6.2 Handling of NetBIOS packets

The highly verbose nature of Windows computers can result in high charges for dial-up connections, as each NetBIOS packet containing name information automatically launches a call establishment (e.g. to a previously set up ISP). The connection remains permanently established due to these packets, resulting in high connect charges without the transfer of actual user data.

An *ELSA LANCOM Business* can either route or spoof the NetBIOS packets to prevent the establishment of unnecessary connections:

- In the NetBIOS module, it is possible to specify the remote stations to which the name information should be transferred via NetBIOS to ensure the routing of those packets that are actually required. After the NetBIOS module has been switched on and an unspecified waiting time has elapsed, a connection is established to the NetBIOS remote stations (insofar as these are not individual remote access workstations). The duration of the waiting period will be increased if the connection cannot be established. The following exchange of NetBIOS information then fills the billboard for the first time.

- In its proxy function, the unit answers queries to computers already known in the NetBIOS module (on the billboard) by proxy for those computers. After the initial exchange of information, no new connections are established as a result of queries to workstations in the local network, or to known workstations in the remote network.

The preset IP filter for NetBIOS ports intercepts packets with queries for stations not present in either the LAN, or as established NetBIOS remote stations, thus preventing the establishment of a connection via the DEFAULT route to the Internet.

6.6.3 Which preconditions must be fulfilled?

A number of components must be installed on the participating workstations and a variety of settings made in the operating system to ensure correct communications via routers for the interconnection of Windows networks.

Installed components

The installation of the required components will be illustrated here on the basis of Windows 95 or Windows 98; the procedure for Windows 2000 and Windows NT 4.0 is similar. Install the following components on all workstations in the Windows networks to be interconnected:

- Network protocol

  NetBIOS is completely independent of the transport protocol used. NetBIOS network data can thus be transferred using the NetBEUI (NetBIOS Extended User Interface), IPX (Internet Packet eXchange, Novell) or IP (Internet Protocol) protocols.

Unlike IPX and IP, NetBEUI is not routable and is thus only available in Windows networks. If multiple Windows networks are to be interconnected *using routes, NetBIOS must be based on a ratable protocol in the ELSA LANCOM Business, such as IP.*

The routing of NetBIOS packets in the *ELSA LANCOM Business* is based on TCP/IP due to its superior filter mechanisms. This protocol must therefore be installed on all participating workstations.

To install the network protocol, click **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network** ▶ **Add** ▶ **Protocol**. Select the manufacturer 'Microsoft' and the 'TCP/IP' network protocol.

- Client

  The Windows network client is required to permit all of the workstations in the Windows network to log on with names and passwords.

  To install the client, click **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network** ▶ **Add** ▶ **Client**. Select the manufacturer 'Microsoft' and the 'Client for Windows networks'.

- Service

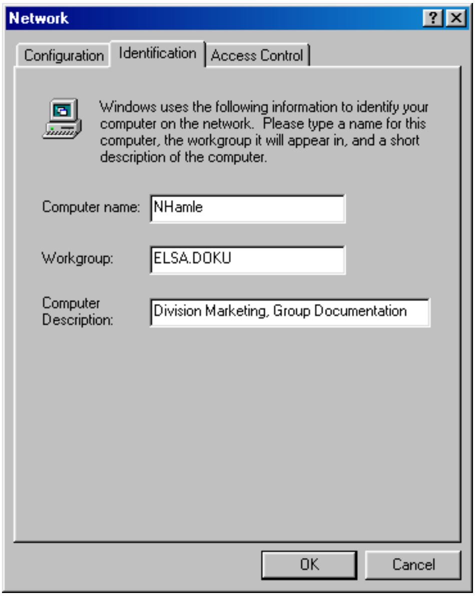
  File and printer sharing permits drives and printers to be shared with other users in the Windows Network.

  To install file and printer sharing, click **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network** ▶ **Add** ▶ **Service**. Select the manufacturer 'Microsoft' and 'File and printer sharing for Windows networks'.

Windows Network settings

- Name and group designation

  Click **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network** and switch to the **Identification** tab.



Windows uses the following information to identify your computer on the network. Please type a name for this computer, the workgroup it will appear in, and a short description of the computer.

Computer name: NHamle

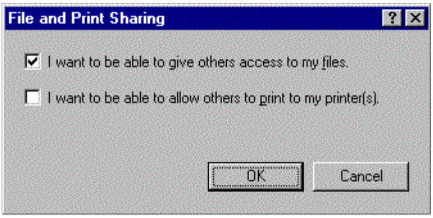
Workgroup: ELSA.DOKU

Computer Description: Division Marketing, Group Documentation

The name of the workstation must be unique. That applies to all Windows networks, and all groups that you intend to connect using NetBIOS within these networks. Names also may not recur in different groups.

- File and printer sharing

  Ensure that file and printer sharing is enabled after the installation is complete. To do so, select **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network** ▶ **File and Print Sharing...**. Specify whether other users in the Windows Network should be allowed access to the printer and/or files of this workstation.



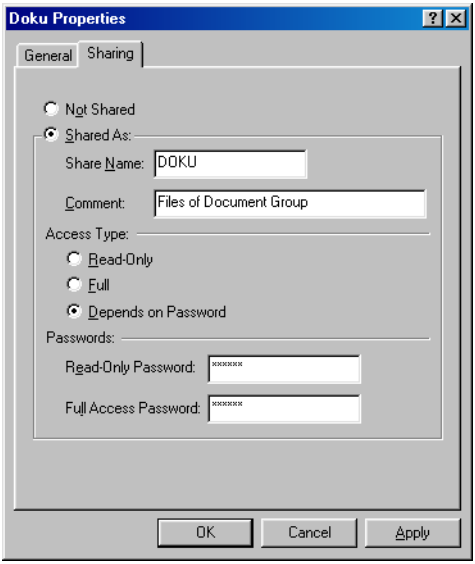
File and Print Sharing

☑ I want to be able to give others access to my files.

□ I want to be able to allow others to print to my printer(s).

All users intending to access shared resources must log on with their names and passwords when booting Windows.

In the Windows Explorer, right-click the drives, folders or printers that you would like to share with others on the network and select the item **Sharing** from the context menu.



Doku Properties

○ Not Shared

● Shared As:

Share Name: DOKU

Comment: Files of Document Group

Access Type:

○ Read-Only

○ Full

● Depends on Password

Passwords:

Read-Only Password: ******

Full Access Password: ******

Enter a name for the shared resource and a description if required. The manner in which the resource can be accessed can be selected under 'Access Type', and by entering passwords as required.

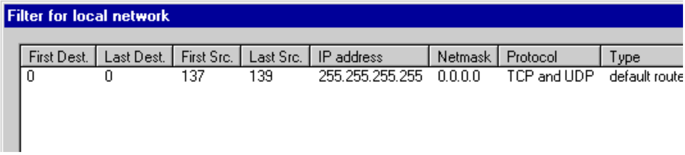
It's easy to check whether the Windows network settings have been made correctly: the local computer must appear with its name in the Network Neighborhood.

6.6.4 Linking two Windows networks

Two Windows networks can be interconnected once these preparations have been completed. The settings for Workgroup networks and Domain Networks (Windows NT and Windows 2000) are similar. The following steps must be performed for both sides of the connection.

① Set up both networks for a LAN-LAN interconnection via TCP/IP as described in the Workshop. We recommend using the convenient *ELSA LANconfig* wizard.

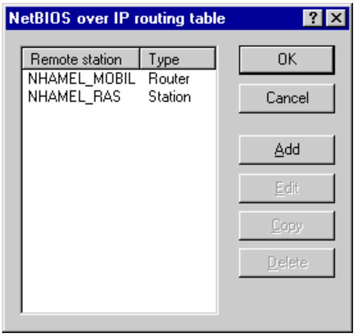
② Check the settings of the IP filter. This filter must capture all NetBIOS packets to be sent over the DEFAULT route to ensure that they do not lead the establishment of a connection on the DEFAULT route. This has been preset in the unit's factory defaults.



Filter for local network

First Dest.	Last Dest.	First Src.	Last Src.	IP address	Netmask	Protocol	Type
0	0	137	139	255.255.255.255	0.0.0.0	TCP and UDP	default route

③ Next, enter the remote station for routing via NetBIOS. Change over to the *ELSA LANconfig* 'NetBIOS' configuration section and create a new entry in the 'NetBIOS via IP Routing' table.



NetBIOS over IP routing table

Remote station	Type
NHAMEL_MOBIL	Router
NHAMEL_RAS	Station

Alternatively, enter the following when configuring via Telnet:

```
cd /Setup/NetBIOS-module/Remote-table
set nhamel.mobil router
```

The entry in the 'Type' field specifies whether a connection to the remote station should be dialed up to exchange name information after switching on the NetBIOS module.

The 'NT-domain' parameter can generally be left blank in the case of Windows 95 or 98 networks. The corresponding domain and/or workgroup must be entered manually when accessing Windows NT and Windows 2000 computers.

④ If the NetBIOS link uses a PPP connection, check the PPP list for the activation of NetBIOS for the corresponding entry.

⑤ Once all remote stations have been entered, activate the NetBIOS function.

```
cd /Setup/NetBIOS-module
set operating on
```

After switching the module on, a connection is established after an unspecified waiting time to all remote stations not identified as dial-up nodes. The required information regarding the other computers in the networks is then exchanged during this initial connection. Computers on the remote site cannot be accessed until this operation is complete.

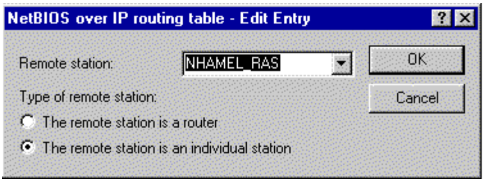
6.6.5 Dial-up procedure for a remote access station

Accessing a Windows Network with a single computer via remote access can also be taken care of quickly.

① The *ELSA LANCOM Business* and the remote access computer must be prepared for network access as described in the Workshop. In this case as well, check the IP filters in the *ELSA LANCOM Business* (See 'Connecting two Windows networks').

② A route must also be entered in the IP routing table if the assignment of the IP address for the remote station is realized from the IP pool.

③ Also create an entry for the remote stations in the NetBIOS IP routing table.



NetBIOS over IP routing table - Edit Entry

Remote station: NHAMEL_RAS

Type of remote station:

○ The remote station is a router

● The remote station is an individual station

```
cd /Setup/NetBIOS-module/Remote-table
set nhamel.ras workstation
```

Be sure to identify this entry as an 'individual station' to ensure that this remote station is not automatically contacted when the NetBIOS module is switched on.

④ If the NetBIOS link uses a PPP connection, check the PPP list for the activation of NetBIOS for the corresponding entry.

6.6.6 Search and find: the Network Neighborhood

Once the participants have all been prepared for NetBIOS routing, it's time to launch Windows Networking.

NetBIOS routing via LAN-LAN coupling

Once the NetBIOS modules have been activated and the networks have exchanged their information regarding the available workstations, a list of these computer names is now available in the *ELSA LANCOM Business*. Using Telnet, enter

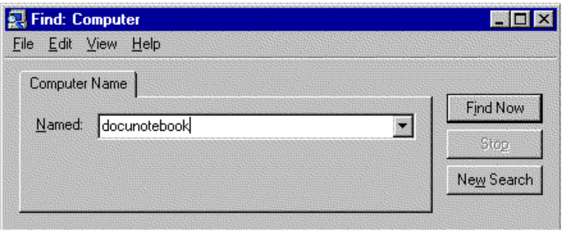
```
dir /Setup/NetBIOS-module/Host-list
```

to call up the list of currently available workstations, which could look like the following:

Name	Type	IP address	Remote station	Timeout	Flags
DOKUNOTEBOOK	00	10.10.0.53	NHAMEL.MOBIL	4939	0020
DOKUNOTEBOOK	20	10.10.0.53	NHAMEL.MOBIL	4939	0020
ELSA	1d	10.10.0.53	NHAMEL.MOBIL	4939	0020
ELSA.DOKU	1d	10.1.253.246	4935	0000	
ELSA.DOKU	1d	192.168.100.162	4997	0000	
NHAMEL.MOBIL	00	10.10.0.1	NHAMEL.MOBIL	0	0020

This table shows, for example, that the computer named 'DOKUNOTEBOOK' with the IP address '10.10.0.53' is available via the remote station 'NHAMEL.MOBIL'. The further parameters are covered in the description of the menus.

To access the shared resources of this computer, simply use the Windows Explorer to search for it with **Start** ▶ **Find** ▶ **Computer**:



Named: docunotebook

The workgroups and computers of the remote network cannot be found in the 'Explore Entire Network' function of the Windows Network Neighborhood for technical reasons. Instead, search for remote computers and create associations as described above.

NetBIOS routing via RAS

The procedure for access to the Windows Network via RAS is somewhat different. These are the two fundamental differences to LAN-LAN interconnection:

- A host list with the computers in the Windows Network is not available on the dial-up node side. RAS users must know the names of the computers that they intend to access and for which they have access rights.
- The connection is not established automatically. RAS users must first establish a connection to the *ELSA LANCOM Business* via Dial-Up Networking.

Once the connection has been established, RAS users can access computers in the remote network (using **Find** ▶ **Computer**, not the Network Neighborhood!) in the same way as with the LAN-LAN interconnection.

6.7 The SYSLOG module

The SYSLOG module gives the option of recording accesses to the *ELSA LANCOM Business*. This function is of particular interest to system administrators, because it allows a full history of all activities to be kept.

To be able to receive the SYSLOG messages, you will need an appropriate daemon or client. In UNIX/Linux the SYSLOG daemon, which is installed by default, generally does the recording. It reports either directly through the console or writes the protocol to a SYSLOG file.

In Linux the file `/etc/syslog.conf` directs which facilities (this expression will be explained later) should be written to which log file. Check in the configuration of the daemon whether network connections are explicitly monitored.

Windows does not have any corresponding system functions. You will need special software that fulfills the function of a SYSLOG daemon.

6.7.1 Setting up the SYSLOG module

There are several options for setting up the SYSLOG module:

- ***LANconfig***
  Management ▶ Log & Trace
- ***WEBconfig***
  Full configuration ▶ Setup ▶ SYSLOG module, or
  Log and Trace ▶ Configure SYSLOG module
- **Telnet**
  /Setup/SYSLOG-module

6.7.2 Example configuration with *ELSA LANconfig*

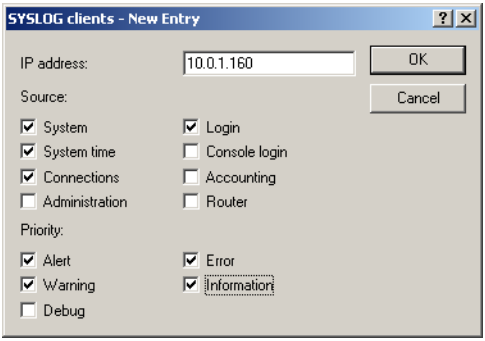
Create SYSLOG client

① Start *ELSA LANconfig*. Under 'Management', choose the 'Log & Trace' tab.

② Turn the module on and click **SYSLOG clients**.

③ In the next window click **Add...**.

④ First enter the IP address of the SYSLOG client, and then set the sources and priorities.



SYSLOG clients - New Entry

IP address: 10.0.1.160

Source:

☑ System
☑ System time
☑ Connections
☐ Administration
☑ Login
☐ Console login
☐ Accounting
☐ Router

Priority:

☑ Alert
☑ Warning
☐ Debug
☑ Error
☑ Information

SYSLOG comes from the UNIX world, in which specified sources are predefined. *ELSA LANCOM Business* assigns its own internal sources to these predefined SYSLOG sources, the so-called “facilities”.

The following table provides an overview of the significance of all news sources that can be set in the *ELSA LANCOM Business*. The last column of the table also shows the alignment between the internal sources of the *ELSA LANCOM Business* and the SYSLOG facilities.

Source	**Meaning**	**Facility**
System	System messages (boot processes, timer system etc.)	KERNEL
Login	Messages regarding login and logout of a user during the PPP negotiation and errors occurring during this process.	AUTH
System time	Messages regarding changes to the system time	CRON
Console login	Messages regarding console logins (Telnet, outband, etc), logouts and errors occurring during this process.	AUTHPRIV
Connections	Messages regarding establishing and releasing connections and errors occurring during this process (display trace).	LOCAL0
Accounting	Accounting information after release of a connection (user, online time, transfer volume).	LOCAL1
Administration	Messages regarding configuration changes, remotely executed commands etc.	LOCAL2
Router	Regular statistics on the most frequently used services (sorted by port numbers) and messages regarding filtered packets, routing errors etc.	LOCAL3

The eight priority stages defined initially in the SYSLOG are reduced to five stages in the *ELSA LANCOM Business*. The following table shows the relationship of alarm level, significance and SYSLOG priorities.

Priority	**Meaning**	**SYSLOG priority**
Alert	All messages requiring the attention of the administrator are collected under this heading.	PANIC, ALERT, CRIT
Error	All error messages that can occur during normal operation without requiring administrative intervention are sent to this level (e.g. connection errors).	ERROR
Warning	Error messages that do not affect normal operation of the device are sent to this level.	WARNING
Information	All messages that are purely informative in character are sent to this level (e.g. accounting information).	NOTICE, INFORM
Debug	Transfer of all debug messages. Debug messages generate a high data volume and interfere with the normal operation of the device. They should therefore be disabled during normal operation and should only be activated for troubleshooting.	DEBUG

⑤ When you have defined all parameters, confirm your input with **OK**. The SYSLOG client will be written to the SYSLOG table.

Facilities

All messages from *ELSA LANCOM Business* can be assigned to a facility with the **Facility mapping** button and then are written to a special log file by the SYSLOG daemon with no additional input.

Example All facilities are set to 'local7'. Under Linux in the file '/etc/syslog.conf' the entry

```
local7.*        /var/log/lancom.log
```

writes all outputs of the *ELSA LANCOM Business* to the file:

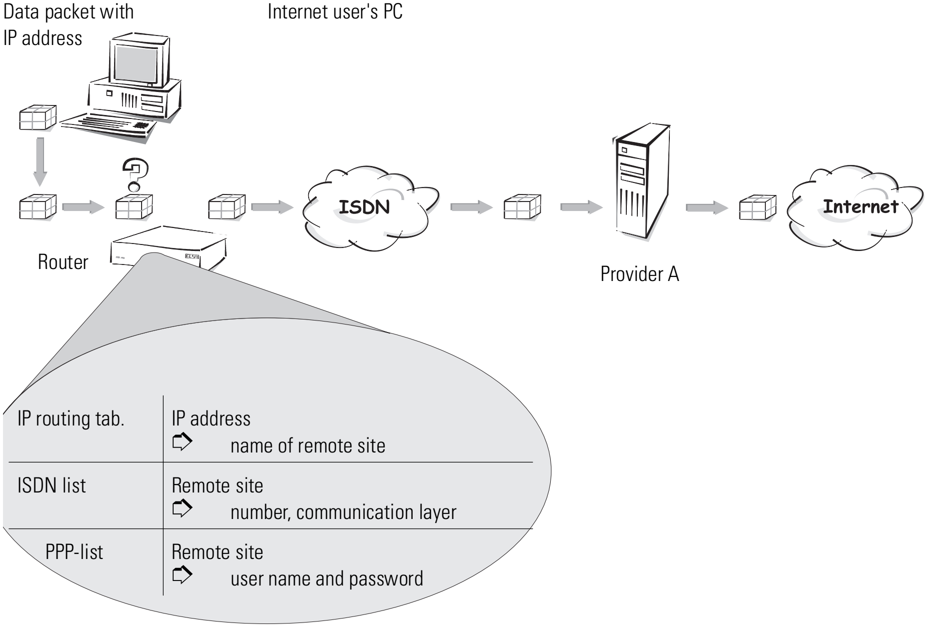
'/var/log/lancom.log'.

6.8 ISDN connections

Data communications between two ISDN terminal devices takes place via ISDN connections. These connections can be realized either as dial-up or leased-line connections.

Initially the router modules only determine the remote station to which a data packet is to be sent. The various parameters for all required ISDN connections must be arranged so that a given connection can be selected and established as required. These parameters are stored in a variety of lists, the interaction of which permits the correct connections.

A simplified example will clarify this process.



IP routing tab.	IP address ➪ name of remote site
ISDN list	Remote site ➪ number, communication layer
PPP-list	Remote site ➪ user name and password

A data packet from a computer initially finds the path to the Internet through the IP address of the receiver. The computer sends the packet with this address over the LAN to the router. Using the IP address, the router then searches the IP routing table and finds the remote station that belongs to the address, for example 'Provider_A'. Using this name, the router then checks the ISDN name list and finds the call number for the corresponding remote station that can be reached by ISDN, including the communication layer that is to be used. The router also obtains the user name and password required for login to provider A from the PPP list.

When this is done, the router can establish a connection to the router of the provider over the ISDN line. Once the connection has been established, the router can forward the data packet to the Internet over the ISDN line.

The following sections introduce the ISDN name list and briefly describe the parameters they contain, describe their connections to other lists and their parameters, and how they are configured in the software.

The PPP list is described in a separate chapter (see 'PPP List').

For further information on the IP routing table, see the 'IP routing' section.

6.8.1 ISDN name list

The name list in the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'Remote sites' tab, or under `/Setup/WAN-module/ Name-list` during Telnet or terminal sessions.

To define the available remote stations, enter them in the name list with a suitable name and additional parameters:

- Name

  This name is used to identify the remote station in the router modules.

- Phone number

  This number should be dialed when the router actively establishes a connection to the remote station.

  If the remote station can be reached under a variety of numbers, enter the other numbers in the round-robin list.

  If the remote station is available via a leased line, the number for a dial-up backup connection can be entered here.

- Short hold

  These times indicate the length of time the B channels should remain active after

  - the last data has been exchanged across static connections for the holding time B1.
  - the data throughput has dropped below a specified level for the holding time B2 in dynamic connections.

- Layer name

  The layer stands for a collection of protocols to be used for this connection. The layer must be set up identically on both sides of the connection.

- Callback

  If the router receives a call from this specific remote site, it may be set to refuse the connection. Instead, the remote station is called back using the following options:

  - Normal callback
  - Callback using the fast ELSA process
  - Callback after name verification

○ Await the callback from the remote station using the fast ELSA process

6.8.2 Interface settings

You can find the interface settings in *ELSA LANconfig* in the 'Management' configuration section on the 'Interfaces' tab, in *WEBconfig* under **Expert Configuration ▶ Setup ▶ Interface**, and in Telnet or terminal sessions under `/Setup/Interfaces.`

The overall parameters are set for each interface (i.e. each S_0 port) in the interface settings. These parameters apply to all operating modes of the device. Specifically, they are:

- The D channel protocol used on the S_0 port

  Automatic recognition: DSS1 (Euro-ISDN), DSS1 point-to-point, 1TR6, Group 0 leased-line connections
- Leased line option

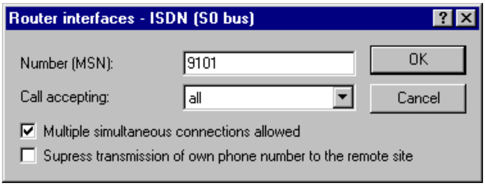
  B channel to be used for the leased line
- Dialing prefix

  Number to precede outgoing calls, e.g. the prefix for external calls when using a PBX.

6.8.3 Settings for dial-up connection interfaces

A number of advanced router settings apply to interfaces for dial-up connections. You can find the 'router interface settings' in *ELSA LANconfig* under 'Communication' on the 'General' tab, in *WEBconfig* under **Expert Configuration ▶ Setup ▶ WAN Module ▶ Router Interface List** and in Telnet or terminal sessions under `/Setup/WAN-module/Router-interface-list`.

The router interface settings determine the parameters to be used for each dial-up interface while in router mode. These parameters do not apply to the other operating modes of the units.



Router interfaces - ISDN (S0 bus)

Number (MSN): 9101

Call accepting: all

☑ Multiple simultaneous connections allowed

☐ Supress transmission of own phone number to the remote site

Specifically, they are:

- Subscriber numbers (MSN/EAZ: terminal device selection numbers)

  The router responds to incoming calls for these numbers. Multiple numbers are separated by semicolons. If no number is specified, the router will respond to all incoming calls.

  The first number specified will be transmitted to the remote station during the active establishment of a connection. If no number is specified, the main MSN of the connection will be transmitted.

- Call acceptance

  Here you can restrict call acceptance to digital or analog calls.

- Permit multiple simultaneous connections

  Here you can specify whether multiple simultaneous connections to differing remote stations are permissible. Disabling this option will ensure that you always have channels free for connections to specific remote stations.

- Suppression of own subscriber number

  Enable this option in order to suppress the display of your own subscriber number to the remote station during call establishment.

  This function must be supported by the network operator.

6.8.4 *LANCAPI* interface settings

The *LANCAPI* interface settings for the *ELSA LANconfig* can be found in the 'LANCAPI' configuration section on the 'General' tab, or under `/Setup/LANCAPI-module/Interface-list` during Telnet or terminal sessions.

Use the router interface settings to determine the parameters to be used for each interface (i.e. each S_0 port) for the *LANCAPI*. These parameters do not apply to the other operating modes of the units. Specifically, they are:

- Subscriber numbers (MSN/terminal device selection numbers)

  The *LANCAPI* responds to incoming calls for these numbers. Multiple numbers are separated by semicolons. If no number is specified, the router will respond to all incoming calls.

- Access to *LANCAPI*

  Here you can completely disable the *LANCAPI* functions for the interface, or enable it only for incoming or outgoing calls.

- Transfer of own subscriber number

  Normally the number specified in the CAPI application is transferred to the remote station via the *LANCAPI* during active call establishment. No number is transferred by the *LANCAPI* if this number has not been specified or the number is invalid. This option lets you transfer the first number entered in the 'Subscriber number' field if no number has been specified in the CAPI application.

6.8.5 Layer list

The list of communications layers in the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'General' tab, or under `/Setup/WAN-module/Layer-list` during Telnet or terminal sessions.

A layer defines a specific combination of protocol settings to be used for data transfer to other devices. Specifically, they are:

- Layer name

  The protocol settings will be saved under this name. In the name list, select the settings with the layer name for the appropriate connection.

- Encapsulation

  Specify here whether an Ethernet header should be added to the data packets. Normally the setting 'Transparent' will be sufficient; this setting may only be required for HDLC connections to third-party devices.

- Layer-3

  Layer-3 protocol for the connection. Recognized automatically in the case of some incoming connections.

  An additional entry is required in the PPP list when using PPP.

  An additional entry is required in the scripts list when using scripts.
- Layer-2

  Layer-2 protocol for the connection.
- Options

  Enables data compression and channel bundling. These options are only effective when supported by the protocols of layer 2 and layer 3.
- Layer-1

  Layer-1 protocol for the connection. Recognized automatically in the case of some incoming connections.

6.8.6 Round-robin list

The round-robin list in the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'Remote sites' tab, or under `/Setup/WAN-module/RoundRobin-list` during Telnet or terminal sessions.

If a remote site can be reached using several numbers, enter the first number in the name list and the rest in the round-robin list.

- Remote site

  Name of the remote station as specified before in the name list.
- RoundRobin

  Additional numbers for this remote site. Multiple numbers are separated by hyphens.
- Begin with:

  Indicate whether a new call establishment should start with the last successfully used number, or always with the first number of the list.

6.8.7 Channel list

The channel list in the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'Remote Sites' tab, or under `/Setup/WAN-module/Channel-list` during Telnet or terminal sessions.

Use the channel list to determine the minimum and maximum number of B channels to be used for the connection, which channels are to be connected in which sequence, and the number of channels to be used as a dial-up backup for a fixed connection if required.

- Remote site

  Name of the remote station as specified before in the name list.

- Min

  Minimum number of channels to be used to establish a connection.

  If more than one channel is specified, static channel bundling will be used for this connection. The layer to be used must be set up for bundling in the layer-2 options.

- Max

  Maximum number of channels to be used to establish a connection.

  If a larger maximum number of channels is stated than the minimum, dynamic channel bundling will be used for this connection. The layer to be used must be set up for bundling in the layer-2 options.

- Order

  The sequence in which connections for the individual channels are established; stated with the syntax [Interface]-[Channel];[Interface]-[Channel] etc.

- Back-up Channels

  Number of channels to be opened over dial-up lines when a leased line is down.

6.8.8 Script

The script list in the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'Protocols' tab, or under `/Setup/WAN-module/Script-list` during Telnet or terminal sessions.

If the processing of a script is required to connect to a remote station, enter the script here and assign it to a remote station.

The layer-3 protocol selected in the layer list for this connection must support scripting.

- Remote site

  Name of the remote station as specified before in the name list.

- Script

  Enter the script here as described in the reference section of the documentation.

6.8.9 Call acceptance

The call acceptance settings for the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'Call accepting' tab, or under `/Setup/WAN-module/Protect` during Telnet or terminal sessions.

Use the call acceptance settings to determine the circumstances under which the unit will accept incoming calls. These settings only apply to the unit's router functions.

- all

  Every call is accepted.

- by name

  Every call is accepted at first. During the protocol negotiation the name is determined and checked against the name list. The connection is maintained if the name is present, otherwise it will be rejected.

- by number

  The call will only be accepted if the remote station is entered in the number list and the number is transferred to the remote station.

- by name or number

  The call will be accepted if one of the two checks was successful.

6.8.10 Number list

The number list in the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'Call accepting' tab, or under `/Setup/WAN-module/Number-list` during Telnet or terminal sessions.

The number list is used as a call acceptance control measure during passive call establishment and to initiate callbacks.

- Phone number

  Number transferred by the calling remote station (including country and area codes as applicable).

- Remote site

  Name of the remote site as specified in the name list. The remote station will be called back if so specified in the name list.

6.9 Office communications and *LANCAPI*

LANCAPI from ELSA is a special version of the popular CAPI interface. CAPI (Common ISDN Application Programming Interface) establishes the connection between ISDN adapters and communications programs. For their part, these programs provide the computers with office communications functions such as a fax machine or answering machine.

This chapter briefly introduces you to *LANCAPI* and the accompanying application programs for office communications as well as providing you with instructions that are important for installing the individual components.

6.9.1 *ELSA LANCAPI*

What are the advantages of *LANCAPI*?

Above all, the use of *LANCAPI* offers you economic advantages. *LANCAPI* provides all workstations integrated in the LAN (local-area network) with unlimited access to office communications functions such as fax machines, answering machines, online banking and eurofile transfer. All functions are supplied via the network without the necessity of additional hardware at each individual workstation, thus eliminating the costs of equipping the workstations with ISDN adapters or modems. All you need do is install the office communications software on the individual workstations.

For example, faxes are sent by simulating a fax machine at the workstation. With *LANCAPI*, the PC forwards the fax via the network to the router which establishes the connection to the recipient.

Fax operation via hardware

The processing power required for fax operation via *LANCAPI* is provided by the processor of the *ELSA LANCOM Business*. The device thus provides a genuine hardware-based fax function via *LANCAPI* which significantly reduces the processor loads of the faxing workstations.

During the installation of most fax programs that support CAPI operation, the *LANCAPI* is identified as a Class II hardware fax and used automatically.

Installing the *LANCAPI* client

The *LANCAPI* is made up of two components, a server (in the *ELSA LANCOM Business*) and a client (on the PCs). The *LANCAPI* client must be installed on those computers in the LAN that will be using the *LANCAPI* functions.

① Place the *ELSA LANCOM Business* CD in your CD-ROM drive. If the setup program does not automatically start when you insert the CD, simply click 'autorun.exe' on the *ELSA LANCOM Business* CD in the Windows Explorer.

② Select the 'Install LANCOM software' entry.

③ Highlight the 'ELSA LANCAPI' option. Click **Next** and follow the instructions for the installation routine.

If necessary, the system is restarted and *LANCAPI* is then ready to accept all jobs from the office communications software. After successful installation, an icon for *LANCAPI* will be available in the Start menu. A double-click on this icon opens a status window that permits current information on the *LANCAPI* to be displayed at any time.

Configuring the *LANCAPI* client

The configuration of the *LANCAPI* client is used to determine which *LANCAPI* servers will be used and how these will be checked. All parameters can remain at their default settings if you are using only one *ELSA LANCOM Business* in your LAN as a *LANCAPI* server.

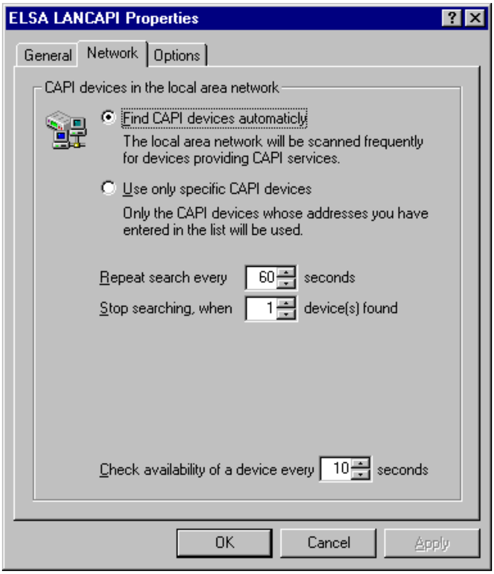
① Start the *LANCAPI* client in the 'ELSAlan' program group. Information regarding the drivers for the available service can be found on the 'General' tab.

② Switch to the 'LANCAPI Server' tab. First, select whether the PC should find its own *LANCAPI* server, or specify the use of a particular server.

   ○ For the former, determine the interval at which the client should search for a server. It will continue searching until it has found the number of servers specified in the next field. Once the required number of servers has been found, it will stop searching.

   ○ In the event that the client should not automatically search for servers, list the IP addresses of the servers to be used by the client. This can be useful if you are operating several *ELSA LANCOM Business* in your LAN as *LANCAPI* servers and you would like to specify a server for a group of PCs, for example.

   ○ It is also possible to set the interval at which the client checks whether the found or listed servers are still active.



CAPI devices in the local area network

● Find CAPI devices automaticly

The local area network will be scanned frequently for devices providing CAPI services.

○ Use only specific CAPI devices

Only the CAPI devices whose addresses you have entered in the list will be used.

Repeat search every 60 seconds

Stop searching, when 1 device(s) found

Check availability of a device every 10 seconds

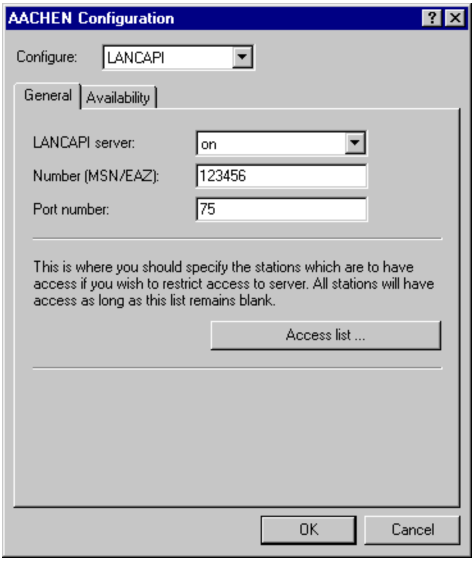
Configuring the *LANCAPI* servers

Two basic issues are important when configuring the *LANCAPI* server:

- What call numbers from the telephone network should *LANCAPI* respond to?
- Which of the computers in the local network should be able to access the telephone network via *LANCAPI*?

Set the relevant parameters as follows:

① Start *ELSA LANconfig* which can be found in the 'ELSAlan' program group. Open the configuration of the router by double-clicking on the device name in the list and select the 'LANCAPI' section.



Configure: LANCAPI

LANCAPI server: on

Number (MSN/EAZ): 123456

Port number: 75

This is where you should specify the stations which are to have access if you wish to restrict access to server. All stations will have access as long as this list remains blank.

② Activate the *LANCAPI* server, or set it to permit outgoing calls only. In the latter case, the *LANCAPI* will not respond to incoming calls—to receive faxes, for example. Permitting outgoing calls only is useful if you do not have a specific call number available for the *LANCAPI*.

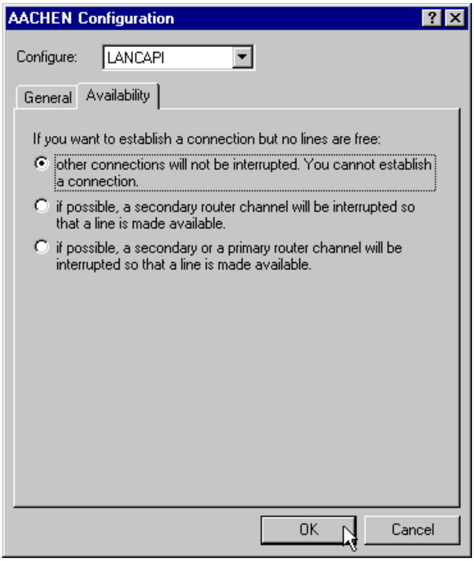
③ When the *LANCAPI* server is activated, enter the call numbers to which the *LANCAPI* should respond in the 'Number' field. You can enter several call numbers separated by semicolons. If you do not enter a call number here, all incoming calls are reported to *LANCAPI*.

④ *LANCAPI* is preset to use port '75' (any private telephony service). Do not change this setting unless this port is already in use by a different service in your LAN.

⑤ If you do not wish all the computers in the local network to be able to access the *LANCAPI* functions, you can define all the authorized users (by means of their IP addresses) by entering them in the access list.

If you enter more than one call number for the LANCAPI, you can, for example, provide each individual workstation with a personal fax machine or personal answering machine. Proceed as follows: When installing communications programs such as ELSA-RVS-COM on the different workstations, specify the various call numbers to which the program should respond.

Switch to the 'Availability' tab. Here you can determine how the *ELSA LANCOM Business* should respond if a connection is to be established via the *LANCAPI* (incoming or outgoing) when both B channels are already busy (priority control). The available options are:



Configure: LANCAPI

If you want to establish a connection but no lines are free:

● other connections will not be interrupted. You cannot establish a connection.

○ if possible, a secondary router channel will be interrupted so that a line is made available.

○ if possible, a secondary or a primary router channel will be interrupted so that a line is made available.

- The connection cannot be established via the *LANCAPI*. A fax program using the *LANCAPI* will then probably attempt to send again at a later time.
- The connection via the *LANCAPI* can then be established when a main channel is free. A main channel is the first B channel used when a router connection is established. Secondary channels are used for channel bundling.
- A connection via *LANCAPI* can always be established; an existing router connection will be terminated for the duration of the call if required. This can be used to ensure the permanent availability of the fax function, for example.

Using the *LANCAPI*

Two options are available for the use of the *LANCAPI*:

- You may use software which interacts directly with a CAPI (in this case, the *LANCAPI*) port, such as *ELSA-RVS-COM*. This type of software searches for the CAPI during its installation and uses it automatically.
- Other programs such as LapLink can establish a variety of connection types, for example, using Windows Dial-up Networking. You may select the installed communications device that you would like to use when creating a new dial-up connection. For the *LANCAPI*, select the entry 'ISDN WAN Line 1'.

6.10 *ELSA CAPI Faxmodem*

The *ELSA CAPI Faxmodem* provides a Windows fax driver (Fax Class 1) as an interface between the *ELSA LANCAPI* and applications, permitting the use of standardfax programs with an *ELSA LANCOM Business*.

Installation

The *ELSA CAPI Faxmodem* can be installed from the CD setup. Always install the *ELSA CAPI Faxmodem* together with the current version of *ELSA LANCAPI*. After restarting, the *ELSA CAPI Faxmodem* will be available to your system. Under Windows 95 or Windows 98, it can be found under **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Modems**.

Faxing with the *ELSA CAPI Faxmodem*

Most major fax programs recognize the *ELSA CAPI Faxmodem* automatically during installation and identify it as a 'Class 1' fax modem. Fax transmissions can thus be realized at speeds of up to 14,400 bps. If your fax program offers you a choice (such as WinFax and Talkworks Pro), select the option 'CLASS 1 (Software Flow Control)' when setting up the modem.

The ELSA CAPI Faxmodem requires ELSA LANCAPI for the transmission of fax messages. A small CAPI icon in the lower right corner of your screen confirms that LANCAPI is enabled. Please also take care with the settings of the LANCAPI itself.

6.11 Call charge management

The capability of the router to automatically establish connections to all required remote sites and close them again when no longer required provides users with extremely convenient access, e.g. to the Internet. However, quite substantial costs may be incurred by data transfer over paid lines if the router is not configured properly (e.g. in the filter configuration) or by excessive use of the communications opportunities (e.g. extended surfing in the Internet).

To reduce these costs, the software provides various options:

- The available ISDN connection charges can be restricted to a specific period.
- The available ISDN connection minutes can be restricted to a specific period.

6.11.1 Charge-based ISDN connection limits

If charge information is sent to an ISDN connection, the resulting connection charges can be limited quite easily. For example, in its default state, a maximum of 830 charge units may be used in six days. The router will not permit the establishment of any further connections once this limit has been reached.

The best way to use the router's call charge monitoring function is if you have "call charge information enabled ***during*** *the connection" to the ISDN network (i.e. AOCD). If necessary, subscribe to this facility from your telecommunications carrier. Charge monitoring with the "Charge information* ***after*** *connection" feature is also possible in principle, but in this case continuous connections may not be detected!*

If you have enabled least-cost routing on the router modules, connections may be established to providers who do not transmit any charge information!

6.11.2 Time-dependent ISDN connection control

However, this mechanism of ISDN connection monitoring will not work if the ISDN connection does not provide charge information. That may be the case, for example, if the provision of charge information was not requested for the connection, or if the telecommunications provider generally does not supply this information.

To reduce the costs of ISDN connections even if no call charge information is available, maximum connection lengths based on time can be regulated. This requires setting up a time budget for a specified period. In the router's default state, for example, connections may only be established for a maximum of 210 minutes within six days.

When the limit of a budget is reached, all open connections that were initiated by the router itself will be shut down automatically. The budgets will not be reset to permit the establishment of connections until the current period has elapsed. Needless to say, the administrator can reset the budgets at any time if required!

The charge and time monitoring of the router functions can be disabled by entering a budget of 0 units or 0 minutes.

Only the router functions are protected by the charge and time monitoring functions! Connections via LANCAPI are not affected.

6.11.3 Settings in the charge module

The interface settings for the *ELSA LANconfig* can be found in the 'Management' configuration section on the 'Costs' tab, or under `/Setup/Charges-module` during Telnet or terminal sessions.

In the charge module, the online time and registered charges can be set, monitored and used to control call establishment.

- Day(s)/period

  The duration of the monitoring period in days can be specified here.

- Budget units, ISDN minutes budget

  The maximum number of ISDN units or ISDN online minutes in a monitoring period

- Spare units, spare ISDN minutes

  Available ISDN units or ISDN online minutes remaining in the current period

- Router-units, router ISDN minutes

  ISDN units or ISDN online minutes over all periods

- Total units

  All charges incurred through the unit

- Table-budget, time-table

  Tables with charges or times for the respective modules

The current charge and connect-time information is retained when rebooting (e.g. when installing new firmware) is not lost until the unit is switched off. All of the time values indicated here are in minutes.

6.12 Accounting

The accounting tool determines online times and data transfer volumes and breaks them down according to the computers that used the connections. The accounting data are stored in a list for current connections and in an accumulated list.

The data collected include the following:

- User (name, IP address, MAC address)

  The online times and data transfer volumes are assigned the MAC addresses of the system network interfaces in the LAN. The router can supply additional information regarding the assignments of MAC addresses and computer names from the DHCP or DNS server modules, if available. In this case, online times can be assigned directly to computer names. If the assignment of MAC addresses to computer names is not possible, other existing information is recorded to identify the user, such as the IP address.

  Usually the MAC address cannot be determined for network users who access the LAN via dial-in connections. In this case, the router generates a pseudo address that allows the remote dial-in stations to be identified during accounting.

- Remote station to which the connection was established
- Type of connection
- Sent and received data volumes
- Online time

  The entire connection time of a dial-up connection that is used by several users at a time can be longer than the amount of time a user actually uses it. So in such cases, the length of the connection is determined based on the first and last user actions plus the valid hold time for the connection.

- Number of connections

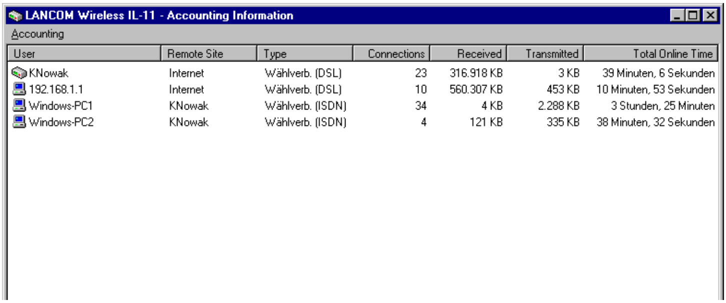
  This field specifies how often a user's action led to the establishment of a connection.

6.12.1 Configuring accounting

Settings for accounting are found under `/Setup/Accounting-module`. From there, you can enable or disable accounting and enable storage to flash ROM. Furthermore, you can influence the sorting of the accumulated table based online time or transfer volume.

6.12.2 Reading the accounting data

ELSA LANmonitor provides the means of viewing the listed data. It also allows you to save the data to a file on a drive.



User	Remote Site	Type	Connections	Received	Transmitted	Total Online Time
KNowak	Internet	Wählverb. (DSL)	23	316.918 KB	3 KB	39 Minuten, 6 Sekunden
192.168.1.1	Internet	Wählverb. (DSL)	10	560.307 KB	453 KB	10 Minuten, 53 Sekunden
Windows-PC1	KNowak	Wählverb. (ISDN)	34	4 KB	2.288 KB	3 Stunden, 25 Minuten
Windows-PC2	KNowak	Wählverb. (ISDN)	4	121 KB	335 KB	38 Minuten, 32 Sekunden

The listed data can also be called up using Telnet access under `/Setup/Accounting-module`.

Organized by user name and remote station, the following information is listed:

- User

  The name of the user or his or her layer 3 address (IP address, IPX address or, in bridge mode, the MAC address again)

- Remote site

  The remote station with which the user exchanged data

- Type

  Type of connection

- Received, Transmitted
  Data volumes on the interface
- Total online time
  Total online time for this user to this remote station
- Connections
  The number of counted connections for this user to this remote station

If a user establishes a connection to another remote station, a new entry is created in the table. All of the transfer volumes and online times incurred by one user to one remote station are recorded in a single entry.

Depending on how the list is sorted, the 512 entries with the largest transfer volumes or longest online times are included in the table.

6.13 The least-cost router

The liberalization of the European telecommunications market has led to the availability of a variety of providers (network operators) that often offer a range of different charges. These providers also provide the option of the preselection of a given network or the placement of long-distance calls on a call-by-call basis without a contract with a specific provider. The prefix of the provider must be dialed to access the desired network on a call-by-call basis. The normal telephone number is dialed after the network identification prefix.

Unfortunately, the most inexpensive rates vary from provider to provider depending on the time of day and region. In the morning Provider 1, Provider 2 in the afternoon and possibly Provider 3 for international calls. To always have the most economical connection for telephone calls, surfing the Internet or transferring data to other networks, it would be necessary to decide which provider is the least expensive before each connection. A *ELSA LANCOM Business* does this for you. Least-cost routing (LCR) is the function for this task. You define once which providers have the most favorable charges for your purposes, and the device automatically selects the most economical provider for you, regardless of whether you are using the router, the *LANCAPI* etc).

6.13.1 Function of the least-cost router in *ELSA LANCOM Business*

The LCR analyzes the digits dialed by the router or *LANCAPI*.

The unit checks the LCR table after each digit for a correspondence to a previously dialed number (prefix). If a suitable entry is found for which the current time and date is valid, the network identification prefix for the connection will be prepended to the prefix. The number is not sent out to the exchange until it has been completed in this manner.

The LCR also requires the following information:

- A dialing prefix (area code) to determine which calls are relevant for the router.
- One or more network identification prefixes to determine the provider to be used for this prefix.
- The days of the week and holidays for which the entry is valid.
- The time of day for which the entry is valid.

Initial tests

It's possible to achieve a considerable savings with only a few entries. We would like to describe the programming of the LCR using this simple example.

You know, for example, that considerable savings can be had by selecting a provider on a call-by-call basis for long distance and international calls. You have also checked the rates of a number of call-by-call (CbC) providers and selected the most economical ones. The first entries in the LCR table will then appear as follows:

Prefix	CbC network prefix	Days of week	Time of day
089	01097	Sat + Sun	0:00h to 23:59h
089	01098	Mon + Tue + Wed + Thu + Fri	8:00h to 18:00h
00	01097	Sun	0:00h to 23:59h

These four entries mean that all connections to Bristol (or other numbers with the prefix '0117') on weekends will be made using the provider with the network prefix '4'. Between 8:00 AM and 6:00 PM on weekdays, these calls will be made using the provider with the network prefix '01098'. International calls on Sundays will be made using the provider with the network prefix '01097'.

For advanced users: systematic use of the LCR

- The first example has shown how connect charges can be reduced with only a few entries. If you would like to put the least-cost router to optimal use, detailed information is required with regard to the connect-charge structure of the call-by-call providers. Next, decide how these rates and rate zones can be best organized in the *ELSA LANCOM Business* LCR table. A variety of approaches are possible:
- Obvious options for saving telephone charges can be entered directly:
  - '00' for international connections
- Entering a single '0' will initially reroute all numbers starting with a zero. However, as neighboring local exchanges may also start with a '0' and yet be billed as local calls, their prefixes should be listed separately to prevent these calls from being rerouted. This strategy should also be applied to special prefixes such as '1800', '0190', etc.
- Another strategy aims to achieve the highest possible level of control over the routing activities. Start with the prefixes of the local area and then define the next larger zones. The closer, and thus less expensive, tariff zones are set with longer prefixes, the remaining more distant prefixes with a smaller number of digits.

This setting can be expanded and refined as required. Here are a number of further ideas for your consideration:

- An area code is required to dial a number of local exchanges, but these calls may be billed as local. If these areas have been routed using a general entry, you could route the area codes that are billed as local calls via the network prefix of your telephone company If the entry for the network prefix is left empty, the entry will not be rerouted.
- Perhaps a large number of your ISDN connections go to the same area codes. If most of your remote stations are in Munich, for example, you can reach these numbers using a specific provider.
- Study the various tariff zones. Check the Internet for the assignments of area codes to zones.

Once you have found the area codes that you would like to reroute, you can start assigning them to call-by-call providers. For this, you need the current rates of as many telephone providers as possible. These can also be found in the Internet. With this information on hand, you can now begin feeding your least-cost router...

6.13.2 Setting up the least-cost router

Two essential questions must be clarified with regard to configuring the least-cost router:

- Which operating modes of the *ELSA LANCOM Business* should the services of the least-cost router use?
- Which calls should be routed over which provider?

To answer these questions, proceed as follows:

① In *ELSA LANconfig*, go to the 'Least-Cost-Router' configuration section on the 'General' tab.

② Enable the least-cost router function. The least-cost router can only be enabled if you have already set the unit time manually or the time has already been received from the ISDN network itself (see also 'Time for the Selection' further below). Activate the following operating modes for the least-cost router as required:

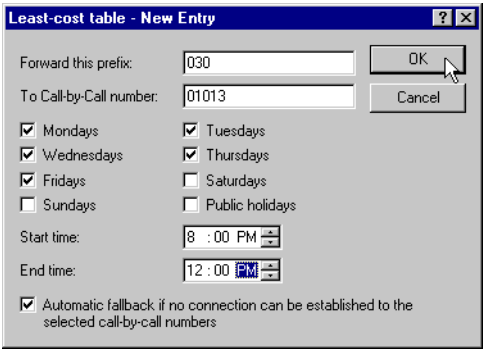
- ○ The Router
- ○ The *LANCAPI*

If you have also activated least-cost routing for the router module, connections may be established via providers that do not transmit connect-charge information. The connect-charge monitoring may thus be inadvertently lost. In this case, use the time budget as an alternative.

③ Change over to the 'Time periods and public holidays' tab. Open the **Least-cost table**, create a new entry and enter the following data:

- ○ Which prefix should be rerouted?
- ○ Which provider should be used for this prefix? If you have entered several network prefixes separated by semicolons, the LCR will automatically try the next prefix if the current one is busy.
- ○ On which days and what times should the routing be active? Please note that time blocks cannot extend from one date to another (i.e. 6:00 p.m. to 6:00 a.m.).
- ○ Should the call be handled by the default telephone provider if all call-by-call providers are busy? If 'Automatic fallback' is disabled, the

LCR will start at the beginning after unsuccessfully trying the last network prefix.



Least-cost table - New Entry

Forward this prefix: 030

To Call-by-Call number: 01013

☑ Mondays ☑ Tuesdays

☑ Wednesdays ☑ Thursdays

☑ Fridays □ Saturdays

□ Sundays □ Public holidays

Start time: 8 : 00 PM

End time: 12 : 00 PM

☑ Automatic fallback if no connection can be established to the selected call-by-call numbers

④ If you have also made entries in the LCR table for holidays, open the **Public holidays** list. Enter each holiday with its full date (DD.MM.YYYY).

⑤ Check the internal clock of the unit (incl. the date), to ensure that the LCR activates the routing at the correct time (see also 'Time for the Selection' further below).

Build the LCR table one step at a time and check your results. Open the ELSA LANmonitor, for example, and establish connections to the remote stations to be rerouted according to the table using the ELSA LANCAPI. Use the dialed number to verify whether the LCR settings suit your requirements. For router connections, check the log file for the number dialed (LANmonitor: ***View* ▶ *Options...* ▶ *Protocol* ▶ *Display****).*

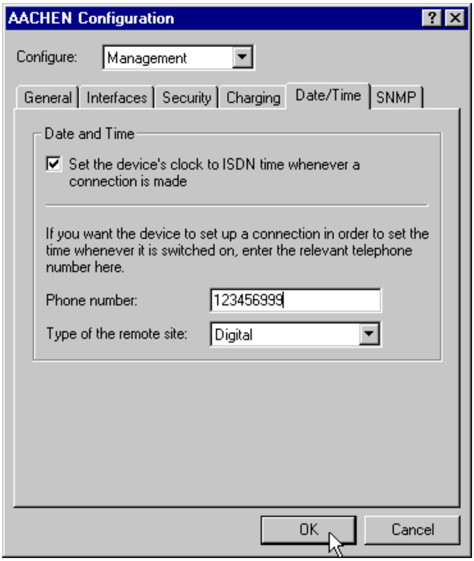
Time for the selection

It goes without saying that the internal clock of the *ELSA LANCOM Business* must be set properly to ensure that the least-cost router correctly applies the information in the table. The router can also help itself in this respect as well, however: It can synchronize its internal clock with the time in the ISDN, either when switched on, or during each call establishment.

① In *ELSA LANconfig*, switch to the 'Date&Time' tab in the 'Management' configuration section.

② Activate the option for automatic device clock setting at each call establishment. If you would rather enter the time manually, disable this option.

③ The current time is lost when the unit is switched off. Enter the number of a random remote station and the maximum number of connection attempts if you would like the device to establish a connection immediately upon being switched on, in order to synchronize the time with that of the ISDN network. Your *ELSA LANCOM Business* can automatically detect whether the remote station is digital (e.g. BBSs or Internet providers) or analog (telephone message or voice services).



Configure: Management

Date and Time

☑ Set the device's clock to ISDN time whenever a connection is made

If you want the device to set up a connection in order to set the time whenever it is switched on, enter the relevant telephone number here.

Phone number: 123456999

Type of the remote site: Digital

Please check the time after the first connection. Some PBXs may transfer incorrect times to the router, which would impair the function of the least-cost router!

7 Technical basics

This chapter is a short introduction into the technology used by your device. Network professionals will find themselves just skimming these pages, but novices will find this section to be very helpful for understanding the technical terms and processes.

7.1 Network technology

This paragraph will give you a brief introduction to the basics of network technology. These descriptions do ***not*** *cover* ***all*** *possible techniques, processes and terms associated with network technology. They only covered to the degree necessary to provide an understanding of the product information.*

7.1.1 The network and its components

Network, transmission medium, interfaces

Whenever several computers communicate with one another, this connection is called a network. For computers to be able to communicate, they need a physical medium through which the information can be transmitted. This can be a cable or radio link, for example, that is connected to the computers using special interfaces (e.g. network adapters).

The term network cable (or simply cable) in the following text also refers to any other physical medium that can take on the function of the cable, such as wireless links.

Packets Cells

The individual bits of electronic information that are sent from one computer to another through a medium are called packets or cells, depending on the process.

For most of the following explanations, the difference between packets and cells is irrelevant. Therefore, we will use the term packet or data packet in a general sense and only detail the special characteristics of cells as necessary.

Host

The computer and other terminal devices (e.g. the printer) in a network that generate or process information are called hosts. Ideally, the host is not responsible for the task of forwarding information. A host normally has exactly one interface to the network.

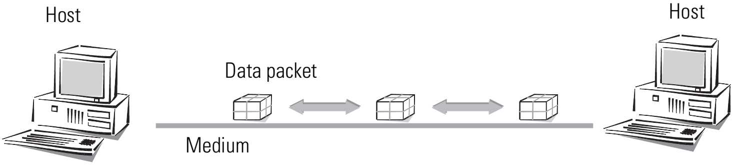
Router

The transport of packets between two hosts occurs indirectly through exchanges that pass packets on to the target computer. These exchanges are called routers. A router has at least two interfaces so that it can receive the data from a sender and pass them on to a recipient. Apart from the exchange function, the router also has the properties of a host so that it can also be the recipient of data packets, for configuration purposes for example.

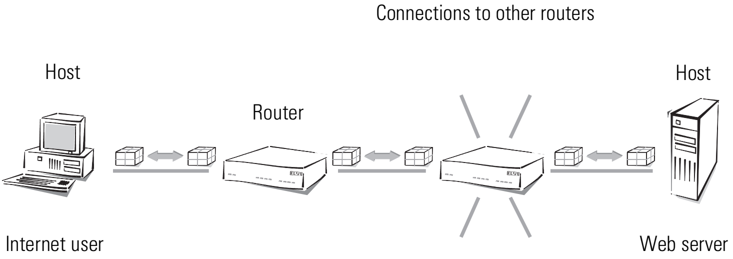
7.1.2 Connection modes

Point-to-point connection

When exactly two hosts are connected via a medium, this is referred to as a point-to-point connection. One host transmits packets that can only be received by exactly **one** recipient (unambiguous connection).



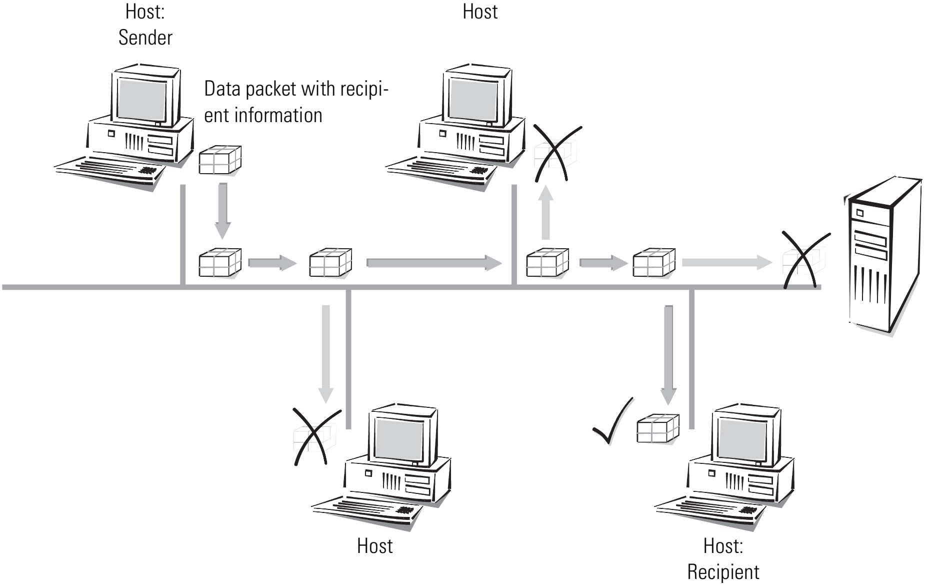
Access to the Internet is also established through point-to-point connections. Even though the data packets are sent from the host at the Internet user to the host at the Internet provider (server) via several routers, every data packet still has its own specific destination. Furthermore, the routers will only forward the data packets to one recipient. That's why we also call this connection unambiguous.



Strictly speaking, the term "point-to-point connection" is not quite correct. For our purposes though, it is sufficient to distinguish this kind of connection from the following "point-to-multipoint connections".

Point-to-multipoint connection

Generally speaking, it would be uneconomical to directly connect all computers in a network via point-to-point connection cables, as the computers would then require multiple interfaces. Computers in a network are therefore plugged into a joint medium shared by all hosts. The sender simply sends its packet with instructions concerning the recipient to the medium to which other hosts are connected. The data packet arrives at **every** host in the network. Each host then decides whether it is the recipient of the packet or not. If the packet is addressed to the corresponding host, it will then accept it. If not, the host will ignore (reject) it. This is a point-to-multipoint connection, since we are not dealing with an unambiguous connection.



7.1.3 Kinds of networks

Protocol

An important prerequisite for communications between computers is a common language among the hosts. In the world of network technology this language is called “network protocol“ or simply “protocol”.

TCP/IP

The most broadly distributed network protocol is the TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol). It is used mainly in the Internet, but nowadays more and more company networks use it. Examples of other network protocols are IPX or Apple Talk. Because of its wide use, this chapter deals mainly with the TCP/IP.

IP network

All hosts wanting to communicate using the TCP/IP protocol have to be plugged into the same network and have to have the TCP/IP protocol (also known as TCP/IP stack) installed. Such a network is referred to as an IP network.

Internetwork
Internet

The connection of multiple networks based on the IP protocol is referred to as an internetwork. The largest union of many small, public IP networks is the Internet.

Local Area Network (LAN)

A network covering a limited area with hosts on the same hierarchical level and using the same medium (shared medium) is called a local network (**L**ocal **A**rea **N**etwork, LAN).

7.2 IP addressing

Packet-oriented transfer

In IP networks the communication between computers takes place in a packet oriented fashion. This means that data or messages are packed together in parcels of variable length and are as such sent from the source computer to the target computer. Apart from the actual information to be transmitted (useful data), the data packet also contains address and control information.

IP address

IP addresses are used in IP networks for communications between various devices. In this case, every host has its own unique address by which it can be identified unambiguously. What does an IP address look like? It consists of four bytes separated by points, making a total of 32 bits. Each of the four bytes can take on values from 0 to 255, e.g. 192.168.130.124.

To be precise, the IP address refers to the interface, and not the host itself. A terminal device with more than one interface (such as a router) has to have an IP address at its disposal for every single interface. This is why ISDN routers from ELSA for example, have an IP address for communication with the hosts in their own network, as well as a second IP address for communication with the "outside world" using the ISDN network. In the same way, ELSA cable modems have an IP address for their own network and another IP address for the exchange of data with the cable network.

Network address

An IP address contains the address of the network as well as that of the host. The network address is the same for all hosts on one network, whereas the address of the host is exclusive and unique to the network. A router, for example, can have more than one IP address, each one unique to the network.

Network mask

How then can you differentiate between the part that determines the network and the part that identifies the host? With the netmask. You know what masks are: they cover up one part of something and only allow a different part to be visible. This is exactly how a netmask operates. It is a number which is identical in structure to the IP address, i.e. 32 zeros or ones. The netmask usually starts with ones at the beginning and ends with zeros. The zeros at the end thus cover the part of the IP address which does not belong to the network address.

Examples:

This address...	...in bytes...	...looks like this in bits:
IP address	192.168.120.253	11000000.10101000.01111000.11111101
Network mask	255.255.255.0	11111111.11111111.11111111.00000000
Network address	192.168.120.0	11000000.10101000.01111000.00000000

The same IP address, this time with another netmask:

This address...	...in bytes...	...looks like this in bits:
IP address	192.168.120.253	11000000.10101000.01111000.11111101
Network mask	255.255.0.0	11111111.11111111.00000000.00000000
Network address	192.168.0.0	11000000.10101000.00000000.00000000

You can see from this that an IP address alone is not enough. A host can only be identified unambiguously in combination with a netmask.

And you can also see that there are more bits available to identify the individual hosts in a connected network if there are fewer bits in a netmask that contain a one. While only 254 different addresses could be allocated in the first example with the network mask 255.255.255.0 (the final numbers '254' and '64.516' are reserved), the second example has as many as 254 x 254 = different addresses available! The first and the last digit of an address space are reserved for the network address and the broadcast address (addresses for packets to all hosts in an IP network). In the netmask 255.255.255.0 this is the '0' for the network address and the '255' for the broadcast address.

A new notation of the netmask simply attaches the number of bits available for the network address to the IP address: 137.226.4.101/24. The number after the slash tells us that the first 24 bits indicate the network address. This notation reduces the length of the entries in the routing tables.

IP address administration

The IP addresses must be unique within a specific network in order to avoid confusion. Since the Internet is based on TCP/IP and thus uses IP addresses for its millions of connected computers, all Internet addresses must also be unique. Bodies exist that manage and distribute these publicly-accessible addresses. Since the number of IP addresses theoretically available is limited, these distributing bodies charge high rates for the addresses.

Private Address Spaces

A range of IP addresses are reserved for use free of charge (private address spaces) so that companies do not have to purchase individual IP addresses for every workstation. In a closed network, these addresses can be used as desired, in a private network or company, for example. The same address can be used in other closed networks (e.g. in different companies), but the addresses within one network must be unique.

However, these reserved IP addresses must **not** be made public (on the Internet). Only **those** devices in a network that are connected to a public network (e.g. the router at the interface to the Internet) must have a registered IP address.

The allocation of IP addresses by the IANA (**I**nternet **A**ssigned **N**umbers **A**uthority) permits the following address ranges to be used for private use:

IP addresses	Network mask	Comment
10.0.0.0	255.0.0.0	“10” networks: All IP addresses beginning with 10. and whose mask begins with 255. belong to the address range reserved for private use.
172.16.0.0	255.240.0.0	All IP addresses beginning with 172.16.–172.31. which are associated with a net mask greater than or equal to 255.240.0.0 are within the address range reserved for private networks.
192.168.0.0	255.255.0.0	All IP addresses beginning with 192.168. and whose mask begins with 255.255. belong to the address range reserved for private use.
224.0.0.0	224.0.0.0	All IP addresses beginning with a 224 which are associated with a net mask also beginning with 224 are within the reserved address range. This range is reserved for broadcasting purposes and should not be used for private networks.

There are two considerations when using these IP addresses:

- The IP addresses used in a private network should not leave this network, i.e. an Internet connection is only possible when using IP masquerading, for example.
- The packets for these IP addresses will not be routed in the Internet, i.e. backbone routers will simply reject such IP packets. Depending on the provider, serious consequences may result if such IP packets are released on the Internet.

7.2.1 IP routing and hierarchical IP addressing

Routing-method

Every IP packet contains the IP addresses of the source and of the recipient. A router receives IP packets at its interface, interprets the destination address and passes the packets on to those interfaces that are nearest to the recipient. Finding the appropriate path is called routing.

Routing-table

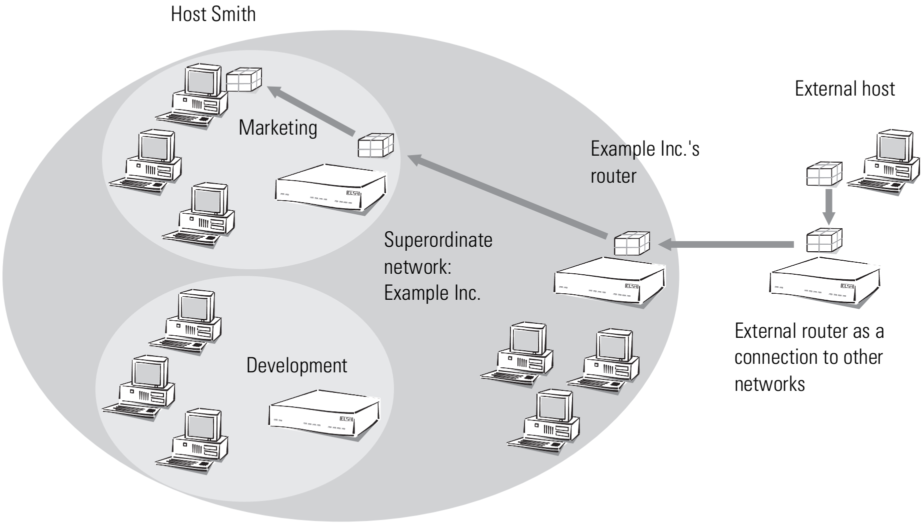
Every router manages a table (routing table). This table indicates the quickest interface connection to the host for every host in the network. You can imagine that, as they grow, these tables may exceed the capacity of the router—the Internet, as a worldwide linking up of publicly accessible IP computers contains several millions of hosts.

Hierarchical IP addresses

For this reason, hierarchical IP addresses were introduced. This means dividing the IP network into subnets in which IP addresses are appointed from a coherent numerical range. It is possible to establish several hierarchy levels, so that different subnets can be merged. The principle is similar to the hierarchical address used by paper mail, consisting of a country, a city, a street and a number.

The consequences of this hierarchical IP addressing:

- Since all hosts within one network have the same network address, the host address is sufficient for the hosts within this network to communicate with one another.
- A router has to know both the addresses of the hosts that are directly connected to it, and the addresses of all networks and subnets that are reachable via adjacent routers.
- It is **not** necessary for a router to know **all** other possible IP addresses.


Host Smith
Marketing
External host
Example Inc.'s router
Superordinate network: Example Inc.
External router as a connection to other networks
Development

As an example, think of a company with one large network, in which the different divisions are incorporated as small subnets. The address of the network for the marketing division is made up hierarchically from the address of the company and that of the department.

Whenever a host external to the company network sends a packet to a host in the Example Inc., this is what happens:

① The sender gives the packet the destination address “host Smith – Marketing – Example Inc.”.

② An external router that establishes the connections to other networks has to know how to reach Example Inc. As soon as it receives a packet with the address for Example Inc., it passes the packet on to the router responsible for Example Inc.

③ The router in Example Inc. receives the packet and extracts from the address the information that it is directed at Example Inc. Since it is itself part of Example Inc., it takes a closer look at the address to find the name of the division. It then passes the packet on to the router in the marketing division.

④ The router in the marketing division receives the packet and extracts from the address the information that it is directed at the marketing division of

Example Inc. Since it is itself part of this division, it takes a closer look at the address to find the name of the host. It then passes the packet on to the host of the employee Sam 'Smith'.

Now we shall take a look at the example using proper IP addresses instead of symbolic names. The network of Example Inc. has the numerical space '192.168.100.0' to '192.168.100.255' at its disposal, with the '0' for the network address and the '255' for the sender address.

The router has to remember that every address beginning with '192.168.100' is located within the network of Example Inc.

Now imagine a router that is connected to the network of Example Inc. through an interface. If it receives a packet with destination address '192.168.100.4' and netmask '255.255.255.0', it will compare this with every network address it knows. In doing so it carries out a logical AND with the netmask, and compares the results with the network address: '192.168.100.4' AND '255.255.255.0' is '192.168.100.0'. This is the network address of the Example Inc. network. The router recognizes that the recipient is located within Example Inc. and passes the packet on to the appropriate interface for Example Inc. Within Example Inc. the packet is then passed on to the appropriate subnet.

The same procedure is used for the transfer of IP packets within a network:

① If a host in the subnet of the development department wants to send a data packet to Mr. Smith, the sender attaches the destination address “Host Smith – Marketing – Example Inc.”.

② The router in the development division receives the packet and extracts from the address the information that it is directed at the marketing division of Example Inc. Since it is itself part of Example Inc., but not of the marketing division, it passes the packet on to the router in the superordinate network.

③ The router in Example Inc. receives the packet and extracts from the address the information that it is directed at Example Inc. Since it is itself part of Example Inc., it takes a closer look at the address to find the name of the division. It then passes the packet on to the router in the marketing division, where the packet is passed on to the recipient.

7.2.2 Expansion through local networks

Medium Access Control

Up to now we have only considered the point-to-point connections. However, many computer networks are based on multipoint cabling such as Ethernet. All computers connected to the same network can then receive the signals of all other computers (so-called broadcast transfer to a shared medium). If several computers are sending simultaneously, the superimposed signals are destroyed. A variety of access methods such as CSMA/CD or Token Ring are implemented in the MAC layer (**M**edia **A**ccess **C**ontrol, MAC) for the avoidance and resolution of such collisions.

LAN and IP network

The connection of all computers communicating through a shared medium using a MAC protocol is called a LAN. A LAN forms an independent network and is subordinate to the IP network, i.e. IP networks can use the physical connections of the LAN to establish connections between the hosts and the routers. A LAN—Local Area Network—is, as the name implies, restricted in its area.

MAC-address

Specific LAN addresses hardwired into the interfaces by their manufacturers are used to manage the transfer in the LAN. Since the LAN addresses are used for communication via the MAC protocol, they are called MAC addresses. They can be thought of as the fingerprint of the interface hardware. MAC addresses can look like this, for example: 00-80-C7-6D-A4-6E.

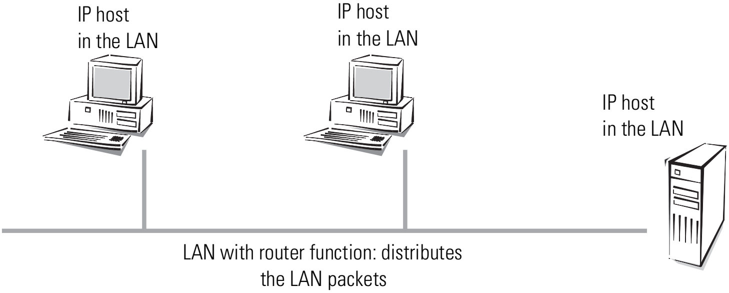
MAC addresses are independent of IP addresses. An IP host whose interface works through a LAN has an IP and a MAC address. Whereas the structure of IP addresses with its similarity to postal addresses is supposed to simplify routing in enormous IP networks, the fingerprint-like MAC addresses are designed to make the connection to a LAN as easy as possible.

Transfer in LAN is also packet-oriented. Every MAC packet contains the MAC addresses of the source and of the recipient. Although every packet is received by all computers, it is processed only by the target computer. There is an additional MAC broadcast address that is processed by all computers in the LAN.

IP in the LAN

Every LAN packet contains an entry with the type of the network protocol. An IP packet can be transferred through a LAN by packing it in a LAN packet and adding the 'IP' protocol type to it. Because of the IP entry, the LAN interface at the receiving host recognizes that the LAN packet contains an IP packet, extracts it and processes it as an ordinary IP packet. In this way, IP packets and packets of other network protocols like IPX can be transferred simultaneously through the same LAN without conflicts (this is why a LAN is called multiprotocol-capable).

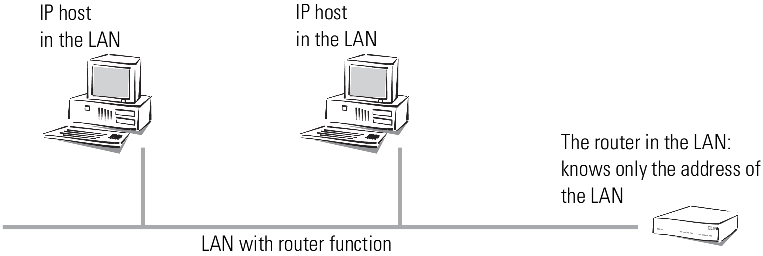
To an IP host, a LAN behaves as if it were an independent network with a router. The hosts gives the packets to the LAN which handles the further distribution of the data packet. This is why only IP addresses from the numerical space of the specific network should be used for the internal communication of the hosts through the IP protocol.



To a router in the LAN, a host in its own LAN seems to be located behind another router. So the task for the router is very simple: all it has to know for operating in the IP network are the IP addresses

- of the directly connected hosts and
- of the available networks and subnets,

i.e. all it has to remember is the network address and the netmask of the subnet in the LAN.



In contrast, the host is confronted with a more difficult task than the router. In case of an interface with a point-to-point cable, the host knows that all packets that it sends through the interface automatically arrive at its router, for example. In case of the point-to-multipoint connection to the LAN, it has to distinguish two cases, however.

- A packet with an address outside the LAN is passed on to a router in the LAN that takes care of the further processing of the packet.
- A packet with an address within the LAN has to be sent immediately to the target host, since the router in the network does not know the addresses of all the different hosts.

Data transfer within the LAN

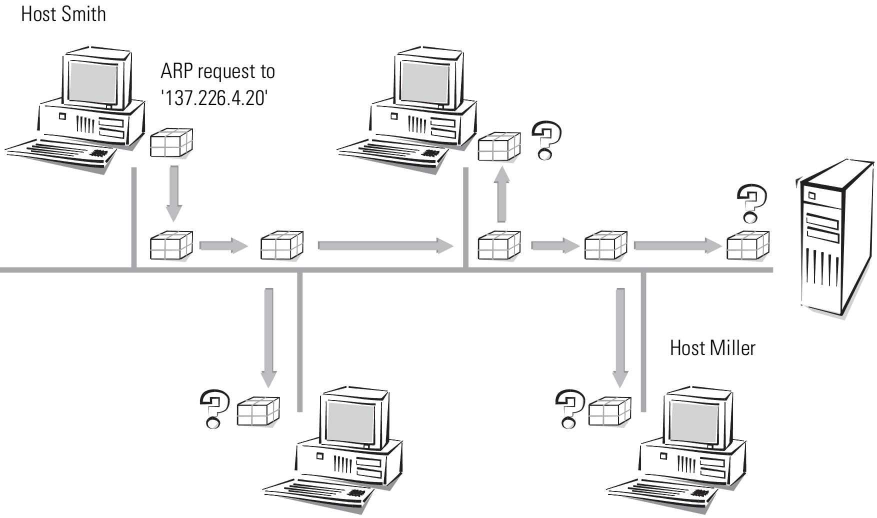
Let's use an example to explain this. Imagine the hosts of the subnet in the marketing division are linked via a LAN. The hosts have IP addresses from the numerical space '137.226.4.1' to '137.226.4.254' (the addresses '137.226.4.0' and '137.226.4.255' are reserved), the network address is '137.226.4.0' and the netmask is '255.255.255.0'. A router connected to the LAN provides access to the wide world of the Internet. Its LAN interface has the IP address '137.226.4.1' and the MAC address '00-80-C7-6D-A4-6E'.

Imagine wanting to send an IP packet from host 'Smith' (with IP address '137.226.4.10' and MAC address '00-10-5A-31-20-DF') to host 'Miller' (with IP address '137.226.4.20' and MAC address '00-10-5A-31-20-EB'). Using the network address and the netmask, host 'Smith' recognizes that host 'Miller' is located in the own network. It therefore has to send the packet through the LAN, directly to host 'Miller'. Unfortunately the LAN interface cannot say: “Send the IP packet to IP address 137.226.4.20”, because the LAN interface only understands MAC addresses.

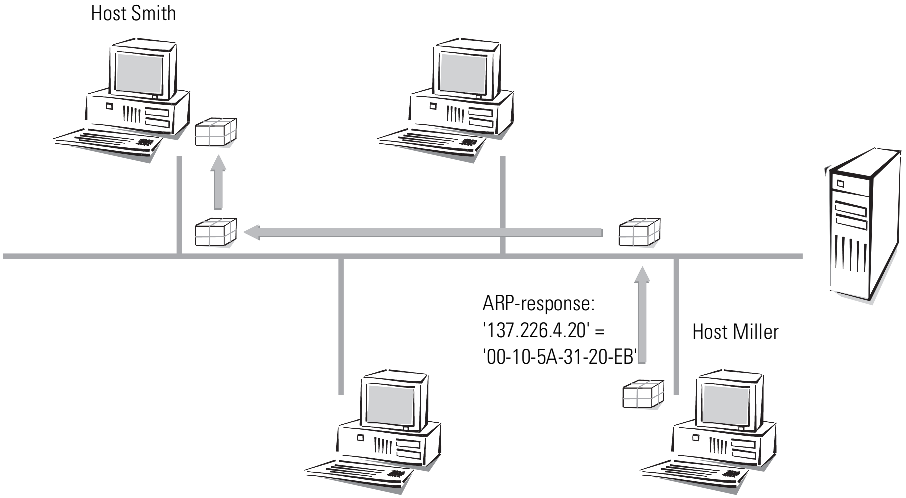
This is why every host has to manage a table that translates IP addresses to MAC addresses. But how do the entries end up in the table? They could be entered manually, but that would not satisfy the objective of making the connecting of a new computer to the LAN as easy as possible.

ARP

Therefore the LAN has a special mechanism that automates this process: the **A**dress-**R**esolution-**P**rotokoll, ARP. The table itself is called the ARP table. Whenever a host does not find an entry in the table for a particular IP address (in our example '137.226.4.20'), it sends an ARP request packet to all hosts in the LAN (with the LAN broadcast address as a target address).



This ARP request packet is simply a question to all hosts listening to the IP address '137.226.4.20'. Host 'Miller' receives the packet, feels addressed and answers with an ARP response packet that it sends directly to host 'Smith'. The MAC address '00-10-5A-31-20-DF' of host 'Smith' is extracted from the sender field in the ARP request packet. Host 'Smith' recognizes this as an answer to its request, extracts the MAC address '00-10-5A-31-20-EB' from the ARP response packet and enters it into his ARP table.



Then it can finally turn to its original task: sending the IP packet to host 'Miller'. It now finds the entry “IP address 137.226.4.20 corresponding to MAC address '00-10-5A-31-20-EB'” in the ARP table and tells his LAN interface: “Send this IP packet to the computer with the MAC address '00-10-5A-31-20-EB'”.

Data transfer from the LAN onto the Internet

Imagine the second task, sending an IP packet from host 'Smith' to the remote host 'External' with IP address 151.189.12.43. Host 'Smith' compares the IP address with his network address and realizes that host 'External' is located outside the LAN. So host 'External' can only be reached through the router. The MAC address of router '00-80-C7-6D-A4-6E' finds out about its IP address by going through the ARP table (if necessary another ARP request is made). So host 'Smith' tells its LAN interface: “Send this IP packet to the computer with the LAN address '00-80-C7-6D-A4-6E'”. The router extracts the IP packet from the LAN packet and finds out about the IP address of host 'External'. In the routing table the router then looks for the network address of this host and thus finds the interface through which to pass on the IP packet.

LAN coupling on MAC basis

You know how LANs simplify the connection of computers to a local network. Nearly all house networks are thus LAN based. In some cases a LAN is covers such a large area that the physical characteristics of the cable prohibit the connection of any more computers. This results in the necessity to couple up several LANs in such a way that electrically and in terms of the MAC protocol they act as independent LANs, but for the IP protocol look like one big LAN.

This coupling of LANs is carried out using bridges. A bridge works somewhat like a router, but uses only MAC addresses for routing, not IP addresses. Since MAC addresses do not give any information on the structure of the network the way IP addresses do, every bridge has to know all MAC addresses in the whole LAN.

And so we encounter the same problem that we had with the routers before the introduction of subnets: As the LAN expands, it will at some point exceed the capacity of the address tables of the bridges. So one cannot use bridges to connect as many LANs as desired. On the other hand, the unstructured MAC addresses allow the bridges to learn automatically about the location of computers in the network, using the received packets. This is called an “intelligent bridge”.

7.3 Point-to-point protocol

ELSA routers also support the point-to-point protocol (PPP). PPP is a generic term for a whole series of WAN protocols which enable the interaction of routers made by different manufacturers since this protocol is supported by practically all manufacturers.

Due to the increasing importance of this protocol family and the fact that PPP is not associated with any specific operating mode of the routers, we will be introducing the functions of the devices associated with the PPP here in a separate section.

7.3.1 The protocol

What is PPP?

The point-to-point protocol was developed specifically for network connections via serial channels and has asserted itself as the standard for connections between routers. It implements the following functions:

- Password protection according to PAP, CHAP or MS CHAP
- Callback functions
- Negotiation of the network protocol to be used over the connection established (IP, for example). Included in this are any parameters

necessary for these protocols, for example IP/IPX addresses. This process is carried out using IPCP (IP Control Protocol).

- Verification of the connection through the LCP (Link Control Protocol)
- Bundling of several channels (multilink PPP)

PPP is the standard used by router connections for communication between devices or the WAN connection software of different manufacturers. Connection parameters are negotiated and a common denominator is agreed using standardized control protocols (e.g. LCP, IPCP, CCP) which are contained in PPP, in order to ensure successful data transfer where possible.

What is PPP used for?

It is best to use the point-to-point protocol in the following applications:

- for reasons of compatibility when communicating with external routers, for example
- Remote access of remote workstations with ISDN adapters
- Internet access (when sending addresses)

The PPP which is implemented in *ELSA LANCOM Business* can be used synchronously or asynchronously not only via a transparent HDLC connection, but also via a X.75 connection.

The phases of a PPP negotiation

Establishment of a connection using PPP always begins with a negotiation of the parameters to be used for the connection. This negotiation is carried out in four phases which should be understood for the sake of configuration and troubleshooting.

- Establish phase

  Once a connection has been made at the data communication level, negotiation of the connection parameters begins through the LCP.

  This ascertains whether the remote site is also ready to use PPP, and the packet sizes and authentication protocol (PAP, CHAP, MS CHAP or none) are determined. The LCP then switches to the opened state.

- Authenticate phase

  Passwords will then be exchanged, if necessary. The password will only be sent once if PAP is being used for the authentication process. An encrypted password will be sent periodically at adjustable intervals if CHAP or MS CHAP is being used.

Perhaps a callback is also negotiated in this phase via CBCP (Callback Control Protocol).

- Network phase

  In *ELSA LANCOM Business*, the protocols IPCP and IPXCP are implemented.

  After the password has been successfully transmitted, the IPCP and/or IPXCP network layer can be established.

  If the negotiation of parameters is successful for at least one of the network layers, IP and/or IPX packets can and/or IPX-be transmitted on the opened (logical) line.

- Terminate phase

  In the final phase the line is cleared, when the logical connections for all protocols are cleared.

PPP negotiation in the *ELSA LANCOM Business*

The progress of a PPP negotiation is logged in the devices' PPP statistics and the protocol packets listed in detail there can be used for checking purposes in the event of an error.

The PPP trace outputs offer a further method of analysis. You can use the command

```
trace + ppp
```

to begin output of the PPP protocol frames exchanged during a terminal session. You can perform a detailed analysis once the connection has been broken if this terminal session has been logged in a log file.

7.3.2 The PPP list

You can specify a custom definition of the PPP negotiation for each of the remote sites that contact your net. The PPP list can be found in the *ELSA LANconfig* in the 'Communication' configuration section on the 'Protocols' tab, or in the `/Setup/WAN-module/PPP-list` menu.

The PPP list may have up to 64 entries, containing the following values:

In this column of the PPP list...	...enter the following values:
Remote site	Name the remote site uses to identify itself to your router.
Username	The name with which your router logs onto the remote site. The device name of your router is used if nothing is specified here.
Authentication	Security method used on the PPP connection ('PAP', 'CHAP', 'MS CHAP' or 'none'). Your own router demands that the remote site observes this procedure. Not the other way round. This means that 'PAP', 'CHAP' or 'MS CHAP' security is not useful when connecting to Internet service providers, who may not wish to provide a password. Select 'none' as the security attribute for connections such as these.
Password	Password transferred by your router to the remote site (if demanded). An asterisk (*) in the list indicates that an entry is present.
Time	Time between two checks of the connection with LCP. This is specified in multiple of 10 seconds (i.e. 2 for 20 seconds, for instance). Simultaneously the time between two checks of the connection according to CHAP. This time is entered in minutes. The time must be set to '0' for remote sites using a Windows operating system.

In this column of the PPP list...	...enter the following values:
Retry	Number of retries for the check attempt. You can eliminate the effect of short-term line interference by selecting multiple retries. The connection will only be dropped if all attempts are unsuccessful. The time interval between two retries is 1/10 of the time interval between two checks. Simultaneously the number of the “Configure requests“ that the router maximum sends before it assumes a line error and clears the connection itself.
Conf, Fail, Term	These parameters are used to affect the way in which PPP is implemented. The parameters are defined in RFC 1661 and are not described in greater detail here. You will find troubleshooting instructions in this RFC in connection with the router's PPP statistics if you are unable to establish any PPP connections. The default settings should generally suffice. These parameters can only be modified via SNMP or TFTP (using *ELSA LANconfig*)!
Rights	Network protocols to be routed over this connection: IP, IPX, NTB (NetBIOS). NetBIOS always requires one of the other two protocols. Network protocols to be routed over this connection: IP

7.3.3 Everything OK? Checking the line with LCP

The devices involved in the establishment of a connection through PPP negotiate a common behavior during data transfer. For example, they first decide whether a connection can be made at all using the security procedure, names and passwords specified.

The reliability of the line can be constantly monitored using the LCP once the connection has been established. This is achieved within the protocol by the LCP echo request and the associated LCP echo reply. The LCP echo request is a query in the form of a data packet which is transferred to the remote site along with the data. The connection is reliable and stable if a valid response to this request for information is returned (LCP echo reply). This request is repeated at defined intervals so that the connection can be continually monitored.

What happens when there is no reply? First a few retries will be initiated to exclude the possibility of any short-term line interference. The line will be dropped and an alternative route sought if all the retries remain unanswered. This may be found in the form of a backup line, for example.

During remote access of individual workstations with Windows 95, Windows 98 or Windows NT, we recommend switching off the regular LCP requests since these operating systems do not reply to LCP echo requests.

The LCP request behavior is configured in the PPP list for each individual connection. The intervals at which LCP requests should be made are set by the entries in the 'Time' and 'Try' fields, along with the number of retries that should be initiated without a response before the line can be considered faulty. LCP requests can be switched off entirely by setting the time at '0' and the retries at '0'.

7.3.4 Assigning IP addresses via PPP

In order to connect computers which use TCP/IP as network protocol, all participants must have a valid and distinct IP address. If a remote station does not have its custom IP address (e.g. the individual workstation of a teleworker), then the *ELSA LANCOM Business* can assign an IP address for the duration of the connection, thus making communication possible.

This type of address assignment is carried out during PPP negotiation and implemented only for connections via WAN. The assignment of addresses via DHCP is used within a local network.

The assignment of an IP address is only possible when the ELSA LANCOM Business can identify the remote station by an incoming call via the calling number or the name, i.e., the authentication was successful.

- For example: Remote access

  The assignment of the address is possible by making a special entry in the IP routing table. In addition to entering the IP address, which should be assigned to the remote station from the 'Router name' field, the 255.255.255.255 is indicated as the network mask. In this case, the router name is the name, with which the remote station must identify itself to the *ELSA LANCOM Business*.

  In addition to the IP address, the addresses of the DNS and NBNS servers (Domain Name Server and NetBIOS Name Server) including the backup server from the entries in the TCP/IP module are transmitted to the remote station during this configuration.

So that everything functions properly, the remote station must also be adjusted in such a way that it can obtain the IP address and the name server from the *ELSA LANCOM Business*. This occurs e.g. in the Dial-Up Network of Windows using the entries in the 'TCP settings' under 'IP address' or 'DNS configuration'. Here the 'IP address assigned by server' and the 'Name server addresses assigned by server' options are activated.

- For example: Internet access

  If Internet access for a local network is realized via the *ELSA LANCOM Business*, the assignment of IP addresses can occur in a reverse manner. Configurations are possible in which the *ELSA LANCOM Business* does not have a valid IP address in the Internet and is assigned one by the Internet provider for the duration of the connection. In addition to the IP address, the *ELSA LANCOM Business* also receives information via the DNS server of the provider during the PPP negotiation.

  In the local network, the *ELSA LANCOM Business* is only known by its internal valid Intranet address. All workstations in the local network can then access the same Internet account and also reach e.g. the DNS server.

Windows users are able to view the assigned addresses via *ELSA LANmonitor*. In addition to the name of the associated remote station, you will also find the current IP address as well as the addresses of the DNS and NBNS servers. Options such as channel bundling or connection duration are displayed.

The monitoring tool ELSA LANmonitor is usually automatically installed when installing ELSA LANconfig. A description is found in the chapter called 'Configuration possibilities' in the paragraph 'What is happening online'.

7.3.5 Callback functions

ELSA LANCOM Business support not only callback via the D channel and callback via the ELSA protocol, but also callback via CBCP specified by Microsoft as well as callback via PPP according to RFC 1570 (PPP LCP extensions). In addition, it is possible for a rather quick callback to occur via a procedure developed by ELSA.

PCs with Windows operating system can be called back only via the CBCP. So that a calling number could be additionally checked in the *ELSA LANCOM Business*, the following values are available in the name list for the callback entry.

With this entry...	**...the callback is thus entered:**
Off	No callbacks.
Auto (not Windows 95, Windows 98 or Windows NT, see below)	The remote station will be called back if so specified in the name list. At first, the call is denied and as soon as the channel is clear again, it is called back (duration is approx. 8 seconds). If the remote station is not found in the numerical list, it is first accepted as the DEFAULT remote station, and the callback is negotiated during the protocol negotiation. Thus a one-unit charge is applied.
Name	Before a callback occurs, a protocol negotiation is always carried out even when the remote station was found in the numerical list (e.g. for computers with Windows having direct dialing on the device). Thus a one-unit charge is applied.
ELSA	When the remote station is found in the numerical list, a quick callback is carried out, i.e., the *ELSA LANCOM Business* sends a special signal to the remote station and calls back immediately when the channel is clear again. After approx. 2 seconds, the connection is established. If the remote station does not take back the call immediately after the signal, then after two seconds the situation reverts back to normal callback procedures (duration is once again approx. 8 seconds). This procedure is only available with DSS1 connections.
Looser	Use the 'Looser' option when a callback is expected from the remote station. This setting carries out two functions simultaneously. On the one hand, it ensures that a custom connection setup is taken back when there is an incoming call from the called remote station, and on the other hand, the function is activated with this setting to be able to react to the rapid callback procedure. In other words, in order to be able to use rapid callback, the caller must be in the 'Looser mode' while the party being called must discontinue callback with 'ELSA'.

The 'Name' setting provides the highest level of security when an entry is not only configured in the numerical list, but also in the PPP list. The 'ELSA' setting provides the quickest callback method between two ELSA routers.

*With Windows remote stations, the 'Name' setting **must** be selected.*

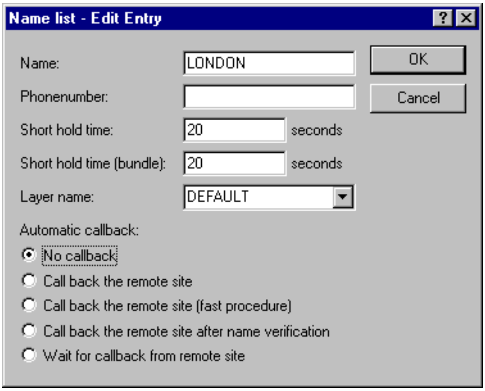
Callback using Microsoft CBCP

With Microsoft CBCP, the callback number can be determined in various ways.

- The called party does not call back.

- The called party allows the caller to indicate the callback number.
- The party called knows the callback numbers and **only** calls these back.

Via CBCP, it is possible to establish connection to *ELSA LANCOM Business* from a PC with Windows operating system and also to be called back by this PC. Three possible settings are selected in the name list via the callback entry as well as the calling number entry.



Name list - Edit Entry

Name: LONDON

Phonenumber:

Short hold time: 20 seconds

Short hold time (bundle): 20 seconds

Layer name: DEFAULT

Automatic callback:

● No callback
○ Call back the remote site
○ Call back the remote site (fast procedure)
○ Call back the remote site after name verification
○ Wait for callback from remote site

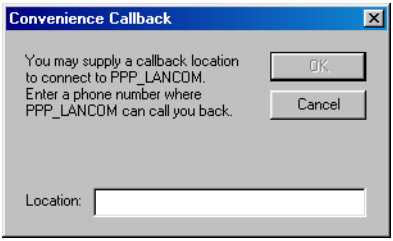
Do not carry out any callbacks

For this setting, the callback entry must be set on 'Off' when configuring via the terminal program or Telnet.

Dial callback number

The remote station is called back after name verification. For this setting, the callback entry must be set on 'Name', and in the name list, **no** calling number should be indicated.

After authentication, the following dialog box appears in Windows 95, in which the user can indicate the calling number.



Convenience Callback

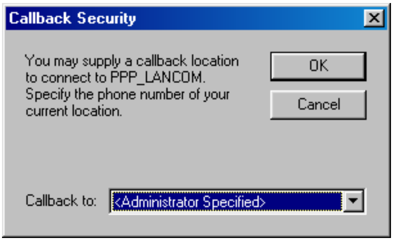
You may supply a callback location to connect to PPP_LANCOM. Enter a phone number where PPP_LANCOM can call you back.

Location:

The calling number is determined by *ELSA LANCOM Business*

The remote station is called back after name verification. For this setting, the callback entry of the corresponding remote station must be set on 'Name', and in the name list, **a** calling number must be indicated.

After authentication, the following message appears in Windows 95, which the user can only confirm:



Callback Security

You may supply a callback location to connect to PPP_LANCOM. Specify the phone number of your current location.

Callback to: <Administrator Specified>

The callback to a Windows workstation occurs approx. 15 seconds after the connection has been dropped. This time setting cannot be decreased since it is a Windows default setting.

Rapid callback using ELSA

Should two *ELSA LANCOM Business* communicate with each other whereby one is called back, then rapid callback via ELSA-specific procedures is provided.

- The caller who may wish to be called back can activate the function 'Expecting callback from remote station' in the name list (or 'Looser' when configuring via the terminal program or Telnet).
- The callback party selects 'Callback remote station (rapid procedure)' in the name list and enters the calling number ('ELSA').

Callback with RFC 1570 (PPP LCP extensions)

With RFC 1570, there are five possibilities to request a callback. All versions are recognized by *ELSA LANCOM Business*. The same applies to all options:

ELSA LANCOM Business drops the connection after authenticating the remote station and then calls back the station three seconds later.

7.3.6 Channel bundling with MLPPP

When establishing a ISDN connection to a remote station with PPP capability, you can transmit data more quickly. Data can be compressed and/ or several B channels can be used for data transmission. (channel bundling).

Connecting with cable bundling is distinguished from “normal” connections in that not only one, but rather several B channels are used parallel-wise for data transmission.

MLPPP (**M**ultilink **PPP**) is used for channel bundling. This procedure is only available when PPP is used as B channel protocol. MLPPP is used e.g. for Internet access via Internet provider, which also operate remote stations with MLPPP capability from your direct dialing nodes.

- Static channel bundling

  If a connection is established with static channel bundling, the router tries to establish the number of B channels specified as 'Minimum' in the channel list. Either the channels specified in the channel list or random free channels are used.

- Dynamic channel bundling

  In the case of dynamic channel bundling, the router initially establishes the number of B channels specified as 'Minimum' in the channel list and starts the data transfer. If the router determines that the throughput stays above a certain threshold for a given period of time, it will attempt to add further channels until the number specified as 'Maximum' in the channel list has been reached. Either the channels specified in the channel list or random free channels are also used in this case.

  If the dynamic channels are established and the data throughput rate drops below the threshold value, the router waits for the set B2 timeout period and then automatically closes the channels again. Any partly used call charge units are used up completely if call charge information is transmitted during the connection. Therefore, the router only uses the dynamic channels if and as long as it really needs them.

Channel bundling is thus established

The configuration of channel bundling for a connection is made up of three settings.

① In the name list, create an entry for the connection which should use channel bundling. Select a layer which established the bundling in the 'Layer 2' options.

- ○ **data compr** according to LZS data compression procedures (Stac) reduces the data volume when the data has not yet been compressed. This procedure is also supported by routers of other manufacturers and by ISDN adapters under Windows operating systems.
- ○ **bundle** uses several B channels per connection. The channel bundling method is determined by the configuration of the layer-2 options in the layer list, the timeouts in the names list, the setting for the Y connection in the interface table and the setting for the channel table.
- ○ **bnd+compr** uses both (compression and channel bundling) and provides the maximum possible data transmission performance.

② Set the hold times for this connection in the name list. Please note the following points:

- ○ Depending on the type of application, the B1 hold time should be increased to such a level so that the connection is not dropped prematurely because of packets not being transmitted for a short time. Customarily, values between 60 and 180 seconds are a good base to begin with which one can continue to adjust during operation.
- ○ The B2 hold time determines the delay time after which the dynamic channels are terminated once the data throughput drops below the threshold value.

③ Use the channel list to determine the number of channels to be used for the connection. You may also specify the channels to be used, thus keeping certain channels free for dial-up connections via RAS, for example.

The channel list entry determines whether static or dynamic channel bundling will be used (see above). More than one minimum channel results in static bundling, whereas a difference between the minimum and maximum number of channels permits dynamic channel bundling.

④ Use the entry for the Y connection in the interface list to determine what should happen if an additional connection to a different remote station is requested during an existing connection using channel bundling, but no further B channels are available.

- ○ Y connection **On**: The router interrupts the bundled connection on this interface to establish a connection to the other remote station. When the channel is free again, the originally bundled connection automatically takes the channel back (always in the case of static bundling, only as required when using dynamic bundling).

○ Y connection **Off**: The router holds the existing bundled connection on this interface, the other connection must try a different interface or wait if none of the interfaces with active channel bundling permit a channel to be terminated.

7.4 IPX routing

The IPX router transmits data from networks which use IPX/SPX as network protocol (e.g. Novell networks). When it is entered in the IPX routing table, a remote network for the computers in the local network is made known. Up to 16 various networks can be entered in the routing table.

7.4.1 IPX addressing

A complete address in an IPX network consists of three parts: a network-number, the MAC address of the network card and the socket number:

- The network number can be dialed without restrictions. However, the number must be clear beyond all accessible IPX networks in order to guarantee a correct allocation.
- The MAC address is securely embedded in each network component. Only in special cases is another address used in the internal network.
- In order to not only address a computer, but also a special service on this computer, an IPX network uses the socket numbers. Therefore, the various services are clearly identified.

7.4.2 Information on the LAN

If several separated LANs are required at a location, they do not necessarily need to have their own cabling. Various logical networks can share a cable. Various formats for the Ethernet packets are used so that the data of various networks do not interfere with one another, and a network remains hidden for the others. These formats are determined by the binding which belongs to a distinct network number on this cable.

The network number and the accompanying binding must be given so that the router can recognize to which network it belongs. If the network address remains at the standard setting of '00000000', the router identifies the address and binding. The router also selects the network on the connected cable from which it receives the most SAP replies.

7.4.3 IPX routing table

In the IPX routing table, determine which remote stations (rather which other routers or computers) are accessible for the local network, and identify several parameters for the connection. The table with a maximum of 16 entries has the following structure:

Remote site	Network	Binding	Propagated	Backoff
BRANCH01	00000245	802.3	Route	On
BRANCH02	00000320	SNAP	Filt.	On
HEAD OFFICE	00000420	802.2	Filt.	Off

- Remote site

  The name of the remote station as it is entered in the corresponding router on the remote site as device name.

- Network

  Address of the WAN. This is not the address of the target network, but rather a third address which represents the network between the both networks to be connected. This applies to:

  LAN address 1 ≠ WAN address 1 = WAN address 2 ≠ LAN address 2 ≠ LAN address 1

- Binding

  Here it is determined which Ethernet binding should be used on the WAN. This entry is only effective when the layer for this connection supports Ethernet encapsulation. If the entry is missing, 802.3 is used.

- Propagated

  Filter for IPX packets of type 20 (NetBIOS propagated frames). The network basic input/output system was originally developed for IBM and is also now used by Microsoft in a modified form. This protocol provides services such as name resolution, data security, and correct packet series in layer 3 and 4 of the OSI model (secured protocol). NetBIOS packets contain a special packet type and socket (propagated packets). NetBIOS is primarily used for data exchange between stations in a local network (LAN).

These IPX packets can be excluded from data transmission or routed with the 'Filter' setting. With the 'Route' setting, packets are transmitted when there is a connection to the corresponding remote station or an unoccupied channel is still available for the establishment of another connection. If all lines are busy with other remote stations, the propagated frames are discarded.

- Backoff

  The IPX router uses a special algorithm (exponential backoff) in order to keep connection costs down during faulty configurations.

  If a server is not available in the network of the remote station (e.g. remote access of a workstation), then the backoff function should be disabled (see 'Exponential Backoff').

  The default state is 'on'.

7.4.4 What happens during data transfer in the IPX network?

When a device logs on in an IPX network, it sends a request to the service advertising protocol (SAP) and then locates the next accessible server (Get Nearest Server Request) in the network with the number '00000000'. If there is a router or server in this network, it will respond to this request and indicate the correct network number.

The servers regularly send information about which services they provide and which other networks they are able to access. They also use special data packets according to the service advertising protocol or routing information protocol (RIP).

When the IPX router is configured and connected, it establishes connection to all remote stations accessible via the routing tables and exchanges SAP and RIP information with these networks. The router stores this data in its internal SAP and RIP tables.

7.4.5 RIP and SAP tables

The RIP and SAP information is sorted alphabetically in the corresponding tables. RIPs are arranged only according to the network, whereas SAPs are arranged at first according to service type then according to server name.

RIP and SAP tables are matched with each new RIP or SAP packet. So that only such services are provided (SAP) which are also accessible (RIP), the router includes only this SAP information in its table, for which there is also a corresponding RIP entry. Besides the information on accessible routes and services, the entries of the tables also indicate, for example, how many routers must be crossed before reaching the destination (hops) or how much time a data packet requires in order to reach the destination network (tics = ca. 1/18 seconds). If, for example, several routes are offered to a destination network via the RIP information, the router selects the route with the least tics and the smallest hopcount according to the tables and stores only this route.

RIP tables can contain 64 entries, SAP tables can contain 128 entries. When each new packet updates the tables, the older entries will naturally disappear after some time. In addition, the entries become artificially aged. For all entries in the RIP/SAP tables which were acquired via local data exchange, the age is increased every 60 seconds by one. A new RIP or SAP packet for an entry sets the age back to zero. After an adjustable age from 1 to 60, the route or service is designated as inaccessible (Down). If double this amount of time has transpired, the entry is removed. In addition, all RIP and SAP information concerning this remote station is deleted from the tables when a connection is established and is replaced with new information.

7.4.6 There are so many routers here...

If connection setup to more remote stations is simultaneously desired in a network than a router can realize, then it is time for a second (or more...) router. In order for the interaction of the routers to function smoothly and to ensure that the network always locates a contact partner, the same entries are carried out in the routing table in all routers. The same routing information is transmitted to each router with higher tic and hopcount via RIP packets (connect `Setup/IPX module/LAN-config/RIP-SAP-scal.)`.

These routes are thus highlighted as reserves when all channels are occupied on the device that is addressed.

7.4.7 Redundant routes

If a router receives information with a RIP packet about routes having the same tic and hopcount as its own routes (redundant routes), these routes naturally do not have to be disclosed to the sender again. It sends these routes only to the router which has not propagated the route. This procedure is called split horizon.

Should it become necessary to disclose redundant routes in the local network, the function 'loop-propagating' can be used (`Setup/IPX-module/LAN-config/Loop-prop.`). The routes thus acquired are designated in the RIP table as 'LOOP'. Even though the distribution of redundant routes is not prohibited according to Novell specifications, it should not be used if possible and so the default setting is 'OFF'.

7.4.8 Exponential backoff

In order to receive routing information (RIP and SAP information) of the IPX remote stations that is necessary for the operation, the IPX router of the device attempts to establish corresponding connections after the device is turned on. In case this is not possible because of a faulty configuration of the IPX router, the exponential backoff algorithm prevents connections from being established thus saving costs.

If the first connection attempt to a remote station is not successful, the router attempts to reach the remote station after a continuously increasing waiting period. The waiting period is determined as follows:

- The first dial occurs after 10 + x seconds. x is a digit between 0 and 10.
- The second attempt begins approximately 10 + x seconds after the first unsuccessful attempt. x now stands for a digit between 0 and 20.
- The top value for x is doubled with each new attempt. After 16 unsuccessful attempts, the router finally stops dialing. After 16 attempts, a maximum of a day has gone by as the result of the continuous increase of the waiting period.

If all attempts to dial the remote station continuously fail, the route is blocked. Further connection attempts can be made only when changing the entry in the routing table.

The time remaining until the next dial and the number of attempts to establish connection can be found in the network statistics (`status/IPX statistics/IPX-router statistic/Networks`*.*

7.4.9 IPX packet filters

With the entries in the routing table, it can be determined which other networks are accessible. These networks are also accessible for such data packets which are not actually required in the network of the remote station. These packets can result in establishing undesired connections thus entailing costs.

Therefore, appropriate filters must be used. For example, data packets which are only used for internal communication of the networks can be excluded from data transmission via WAN or at least restricted:

- Propagated frames

  These special data packets use protocols which cannot actually be routed. In order to become a part of the common routing, this data is encapsulated in normal IPX packets and transmitted as a broadcast.

  Sometimes these packets are not desired when routing. Therefore, you can explicitly adjust whether this packet type should be routed or filtered.

- Socket filter

  Each data packet in an IPX network not only contains target and source addresses but also target and source sockets. Sockets designate the processes for which the data in the packet are determined.

  For the sockets from local as well as remote networks, there is a corresponding filter table which contains the filters, with which individual target sockets or complete socket groups can be excluded from data transmission. Several sockets, which are known to be frequently used for undesired connections, are entered by default in the socket filter table.

- RIP and SAP information

  Via RIPs, a router informs other routers of all known routes (routes in other networks) according to the split horizon principle. This includes not only the entries from its own routing table, but also all routes which the router acquired from other routers. It acquires routes not only from routers from local networks, but also from remote networks. The router enters all available routing information in its internal RIP table.

  In SAP information, the servers provide their services. The various services are represented within the SAP information by numbers. Each service (e.g. file server or print server) has a distinct number. The router includes the information on available services in the internal SAP table, and also enters which service in which network on which MAC address is available. It also learns whether the service provided is local or in a remote network, and can thus propagate the service without establishing a connection.

In the IPX module (`setup/IPX module/RIP-config` *or* `SAP-config`*) of the routers, the RIP and SAP tables are displayed with current values.*

RIP and SAP information is naturally very important for the communication of devices in a network, therefore there are various options in adjusting the transmission of these packets.

- ○ With a LAN and WAN filter table, the router can be ordered not to include information on routes to specific networks or specific available services in the internal RIP or SAP table. Therefore, the concerned routes are not used and are no longer disclosed. The services are not provided in their own network.
- ○ RIP and SAP packets are always transmitted without filters. However, these packets occupy a part of the connection line in all cases.
- ○ The RIP and SAP packets are only sent when there are changes in the information.
- ○ RIPs and SAPs can be transmitted in regular, adjustable time periods. Normally, the information is sent in one-minute intervals. With the time setting, intervals can be extended up to 60 minutes.
- ○ The most economical handling of RIP and SAP packets transmits information only when a connection is established.

- ● IPX and SPX watchdogs:

  With these data packets, the servers are informed e.g. at workstations whether they are still active or whether they can be shut down, if necessary. So that this “Hello, are you still awake?” packet for computers in a remote network does not continuously establish a connection, the reply for these requests can be adjusted as follows:

  - ○ IPX watchdogs remain completely unanswered. After the time has been set on the server, the computers are shut down.
  - ○ IPX and SPX watchdogs can be answered locally. This procedure is called spoofing. The router then answers instead of the computers being addressed, which are naturally never shut down. Setting a time

on the server, according to which the corresponding devices are shut down in all cases, is also sensible.

○ IPX and SPX watchdogs can naturally be routed, thus frequently establishing connection.

Additional information on IPX, IPX router, and accompanying parameters is found in the chapter 'Setup/IPX module' in the reference manual.

7.5 IP routing

An IP router works between networks which use TCP/IP as the network protocol. This only allows data transmissions to destination addresses entered in the routing table. This chapter explains the structure of the IP routing table of an ELSA router, as well as the additional functions available to support IP routing.

7.5.1 The IP routing table

Use the IP routing table to tell the router which remote station (which other router or computer) it should send the data for particular IP addresses or IP address ranges to. This type of entry is also known as a “route“ since it is used to describe the path of the data packet. This procedure is also called “static routing” since you make these entries yourself and they remain unchanged until you either change or delete them yourself. Naturally, there is also “dynamic routing” too. The routers use the routes in this way to exchange data between themselves and continually update it automatically. The static routing table can hold up to 64 entries, the dynamic table can hold 128. The IP router looks at both tables when the IP RIP is activated.

You also use the IP routing table to tell the router the length of this route's path so that it can select the most suitable route in conjunction with IP RIP where there are several routes to the same destination. The default setting for the distance to another router is 2, i.e. the router can be reached directly. All devices which can be reached locally, such as other routers in the same LAN or workstation computers connected via proxy ARP are entered with the distance 0. The “quality level” of this route will be reduced if the entry addressed has a higher distance (up to 14). “Unfavorable” routes like this will only be used if no other route to the remote station in question can be found.

The routing table can be found in the *ELSA LANconfig* in the 'IP-router' on the 'Routing' tab, or in the `/Setup/IP-router-module/IP-routing-table` menu. This, then, is how an IP routing table might look:

IP address	Netmask	Router	Distance	Mask.
192.168.120.0	255.255.255.0	AACHEN	2	On
192.168.125.0	255.255.255.0	BERLIN	3	Off
192.168.130.0	255.255.255.0	191.168.140.123	0	Static

What do the various entries on the list mean?

- IP addresses and netmasks

  This is the address of the destination network to which data packets may be sent and its associated network mask. The router uses the network mask and the destination IP address of the incoming data packets to check whether the packet belongs to the destination network in question.

  The route with the IP address “255.255.255.255” with network mask “0.0.0.0” is the default route. All data packets that cannot be routed by other routing entries are sent over this route.

- Router

  The router transmits the appropriate data packets to the IP address and network mask to this remote station. A name is entered at this point if the remote station is a router in another network or an individual workstation computer. This is where the IP address of another router which knows the path to the destination network is entered if the router on the network cannot address the remote station itself.

  The router name indicates what should happen with the data packets that match the IP address and network mask.

  Routes with the router name “0.0.0.0” identify exclusion routes. Data packets for this “zero route” are rejected and are not routed any further. This is how routes which are forbidden on the Internet (private address spaces, e.g. 10.0.0.0), for example, are excluded from transmission.

  If an IP address is input as router name, this is a locally available router, which is responsible for transfer of the relevant data packets.

- Distance

  Number of routers between your own and the destination router. This value is often equated with the cost of the transmission and used to distinguish between inexpensive and expensive call paths for wide-area connections. The distance values entered are propagated as follows:

  - All networks which can be reached while a connection exists to a destination network are propagated with a distance of 1.
  - All non-connected networks are propagated with the distance entered in the routing table (but with a minimum distance of 2) as long as a free transmitting channel is still available.
  - The remaining networks are propagated with a distance of 16 (= unreachable) if there are no longer any channels available.
  - Remote stations connected using proxy ARP are an exception to this. These “proxy hosts” are not propagated at all.

- Mask.

  Use the masquerading option in the routing table to inform the router which IP addresses to use when transferring the packets.

  - 'Off': No masquerading.
  - 'On': This entry requests a random IP address valid in the Internet from your provider which is then used for the connection and masquerading.
  - 'Stat.': Use this entry to request the assignment of a specific IP address from your provider as entered in the 'TCP/IP' configuration section on the 'General' tab or in the `/Setup/TCP-IP-module` menu. This address will be used for the connection and masquerading.

  For further information see the 'IP masquerading' section.

Examples with explanatory notes:

IP address	Netmask	Router	Dist.	This is what happens:
192.168.1.9	255.255.255.255	FIELD SERVICE	2	The FIELD SERVICE remote station can be reached at IP address 192.168.1.9.
192.168.120.0	255.255.255.0	ROUTER01	2	All data packets with destination IP addresses 192.168.120.x are transmitted to ROUTER01.
192.168.125.0	255.255.255.0	ROUTER02	3	All data packets with destination IP addresses 192.168.125.x are transmitted to ROUTER02.

IP address	Netmask	Router	Dist.	This is what happens:
192.168.130.0	255.255.255.0	192.168.140.123	0	All data packets with the destination IP addresses 192.168.130.x are sent to the locally available router with the IP address 192.168.140.123.
192.168.0.0	255.255.0.0	0.0.0.0	0	Excludes transmission of all data packets to networks using private address spaces.
172.16.0.0	255.255.0.0	0.0.0.0	0	
10.0.0.0	255.0.0.0	0.0.0.0	0	
224.0.0.0	224.0.0.0	0.0.0.0	0	
255.255.255.255	0.0.0.0	HEAD OFFICE	2	All data packets which cannot be allocated to the entries listed above are transmitted to the HEAD OFFICE remote station.

The sequence of the entries is important here: They are processed from top to bottom. The router sorts entries automatically: Firstly by network masks, in descending order. Then by the IP addresses, in ascending order. This places the 'HEAD OFFICE' entry at the very end of the list. If this entry were at the top of the list, the router would send all (!) data packets not belonging to the local network to the network of the head office.

7.5.2 TCP/IP packet filters

You can use your entries in the routing table to determine quite precisely which data should be transferred. Additionally, you can use the '0.0.0.0' entry in the 'Router-name' field to reject whole groups of IP addresses.

Occasionally, you may wish to restrict a transmission even further. You can do this using a characteristic of TCP/IP, which is to send port numbers for destination and source as well as the source and destination IP addresses with a data packet. The destination port in a data packet stands for the service to be addressed in the TCP/IP network. The destination ports are fixed for the various services on the TCP/IP network (see also 'TCP/IP-ports' in the reference section). The source ports, on the other hand, may be selected freely within certain ranges.

The router can check the source and destination ports of data packets using the TCP or UDP protocols. It can then deduce the purpose of the data from these ports. For example, FTP accesses or Telnet sessions can be identified.

The appropriate filter table can be used to determine that certain data is not to be transferred from the LAN to the WAN. Data for particular ports can also be blocked from entering the LAN from the WAN in the same way.

The filter tables can use the filter type along with the definition of the port ranges and associated protocols to determine whether the data in question should never be transmitted or whether it should simply not lead to a call being established (i.e. only be transmitted if a connection already exists).

The router has two separate filter tables, for packets coming from the LAN and from the WAN.

These filter tables can be found in the *ELSA LANconfig* in the 'IP-router' configuration section on the 'Filtering' tab, or in the `/Setup/IP-router-module menu.`

7.5.3 Proxy ARP

The proxy ARP is a special feature of the IP router. This proxy is used if the transmission of data to IP addresses takes place in the same logical network as the sender, but the destination address is still reached via a router. This is the case when individual workstation computers (teleworkers) are networked via TCP/IP to the company network. The teleworker then has an IP address which is located in the same local network as all the other computers in the LAN. A data packet from LAN to the teleworker would usually only search for a receiver locally, but would not be able to find one.

To take advantage of this function, enable the 'Proxy ARP active' option (in LANconfig in the 'IP router' configuration section on the 'General' tab or in the `/Setup/IP-router-module` *menu for other configuration modes).*

The router becomes a proxy for the teleworker with the following entry in the routing table:

IP address	Netmask	Router	Distance	Mask.
192.168.110.123	255.255.255.255	Teleworker01	0	Off

Proxy hosts are not propagated in an RIP packet because the router responds to an ARP request for the proxy computer with its own MAC address. The distance is set to '0' on the routing table to indicate this clearly.

The router now responds to the request for the MAC address to the IP address 192.168.110.123 with its own MAC address. This ensures that all packets in the LAN for the teleworker are now automatically sent to the router, and that data is sent on to the computer at the other end of the ISDN connection.

7.5.4 Local routing

You know the following behavior of a workstation within a local network: The computer searches for a router to assist with transmitting a data packet to an IP address which is not on its own LAN. This router is usually notified to the operating system by its property of being the default router or gateway. It is often only possible to enter one default router which is supposed to be able to reach all the IP addresses which are unknown to the workstation computer if there are several routers in a network. Occasionally, however, this default router cannot reach the destination network itself but does know another router which can find this destination.

How can you assist the workstation computer now?

By default, the router sends the computer a response with the address of the router which knows the route to the destination network (this response is known as an ICMP redirect). The workstation computer then accepts this address and sends the data packet straight to the other router.

Certain computers, however, do not know how to handle ICMP redirects. To ensure that the data packets reach their destination anyway, use local routing (in *ELSA LANconfig* in the 'IPX/SPX' configuration section on the 'Routing' tab or in the `/Setup/IP-router-module/Loc. routing On` menu). In this way you instruct the router itself in your device to send the data packet to other routers. In addition, in this case no more ICMP redirects will be sent.

This may seem to be a good idea in principle, but local routing should still only be used as a last resort, since this function leads to doubling of the number of data packets being sent to the destination network required. The data is first sent to the default router and is then sent on from here to the router which is actually responsible in the local network.

7.5.5 Dynamic routing with IP RIP

In addition to the static routing table ELSA routers also have a dynamic routing table containing up to 128 entries. Unlike the static table, you do not fill this out yourself, but leave it to be dealt with by the router itself. It uses the Routing Information Protocol (RIP) for this purpose. All devices that support RIP use this protocol to exchange information on the available routes.

What information is propagated by IP RIP?

A router uses the IP RIP information to inform the other routers in the network of the routes it finds in its own static table. The following entries are ignored in this process:

- Rejected routes with the '0.0.0.0' router setting.
- Routes referring to on other routers in the local network.
- Routes linking individual computers to the LAN by proxy ARP.

Although the entries in the static routing table are set manually, this information changes according to the connection status of the router and so do the RIP packets transmitted.

- If the router has established a connection to a remote station, it propagates all the networks which can be reached via this route in the RIPs with the distance '1'. Other routers in the LAN are thus informed by these means that a connection to the remote station has been established on this router which they can use. The establishment of additional connections by routers with dial-up connections can be prevented, thus reducing connection costs.
- If this router cannot establish a further connection to another remote station, all other routes are propagated with the distance '16' in the RIPs. The number '16' stands for "This route is not reachable at the moment." A router may be prevented from establishing a connection in addition to the present one may be due to one of the following causes:
  - Another connection has already been established on all the other channels (also via the *LANCAPI* or a/b ports).
  - The existing connection is using all B channels (channel bundling).

To take advantage of this function, enable the 'IP RIP' option (in the ELSA LANconfig in the 'IPX/SPX' configuration section on the 'Routing' tab or in the `Setup/IP-router-module` *menu for other configuration modes).*

Routers with RIP capabilities dispatch the RIP packets approximately every 30 seconds. The router is only set up to send and receive RIPs if it has a unique IP address. The IP RIP module is deselected in the default setting using the IP address XXX.XXX.XXX.254.

Which information does the router take from received IP RIP packets?

When the router receives such IP RIP packets, it incorporates them in its dynamic routing table, which looks something like this:

IP address	Netmask	Time	Distance	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

What do the entries mean?

IP address and network mask identify the destination network, the distance shows the number of routers between the transmitter and receiver, the last column shows which router has revealed this route. This leaves the 'Time'. The dynamic table thus shows how old the relevant route is. The value in this column acts as a multiplier for the intervals at which the RIP packets arrive. A '1', therefore, stands for 30 seconds, a '5' for about 2.5 minutes and so on. New information arriving about a route is, of course, designated as directly reachable and is given the time setting '1'. The value in this column is automatically incremented when the corresponding amount of time has elapsed. The distance is set to '16' after 3.5 minutes (route not reachable) and the route is deleted after 5.5 minutes.

Now if the router receives an IP RIP packet, it must decide whether or not to incorporate the route contained into its dynamic table. This is done as follows:

- The route is incorporated if it is not yet listed in the table (as long as there is enough space in the table).
- The route exists in the table with a time of '5' or '6'. The new route is then used if it indicates the same or a better distance.
- The route exists in the table with a time of '7' to '10' and thus has the distance '16'. The new route will always be used.
- The route exists in the table. The new route comes from the same router which notified this route, but has a worse distance than the previous entry. If a device notifies the degradation of its own static routing table in this way (e.g. releasing a connection increases the distance from 1 to

2, see below), the router will believe this and include the poorer entry in its dynamic table.

RIP packets from the WAN will be ignored and will be rejected immediately. RIP packets from the LAN will be evaluated and will not be propagated in the LAN.

Interaction: static and dynamic tables

The router uses the static and dynamic tables to calculate the actual IP routing table it uses to determine the path for data packets. In doing so, it includes the routes from the dynamic table which it does not know itself or which indicate a shorter distance than its own (static) route with the routes from its own static table.

Routers without IP RIP support

Routers which do not support the Routing Information Protocol are also occasionally present on the local network. These routers cannot recognize the RIP packets and look on them as normal broadcast or multicast packets. Connections are continually established by the RIPs if this router holds the default route to a remote router. This can be prevented by entering the RIP port in the filter tables.

Scaling with IP RIP

If you use several routers in a local network with IP RIP, you can represent the routers outwardly as one large router. This procedure is known as “scaling”. A router like this, with its supposedly inexhaustible supply of routes is created by the continual exchange of information between the routers.

7.6 IP masquerading (NAT, PAT)

One continually growing problem for the Internet is the limited number of generally valid IP addresses available. In addition to this, the allocation of fixed IP addresses for the Internet by the Network Information Center (NIC) is an expensive process. What is more obvious than having several computers share one IP address?

This particular solution is called IP masquerading. This is a procedure whereby only one LAN router appears on the Internet with an IP address. This IP address is allocated to the router either permanently by the NIC or temporarily by an Internet provider. All the other computers on the network then “conceal” themselves behind this one IP address. Aside from the welcome savings, IP masquerading has the added benefit of guarding very effectively against attacks on the local network from the Internet.

Two addresses for the router

Masquerading pits two opposing requirements of the router against one another: While it must have an IP address which is valid on the local network, it must also have an address valid on the Internet. Since these two addresses may not in principle be located on the same logical network, there is only one solution: two IP addresses are required.

The router is therefore assigned an **Inter**net address and an **intra**net address, each with its own fitting network mask. Use the 'Masquerade' option in the routing table to inform the router which of the two addresses to use when transferring the packets.

- 'Off': No masquerading.
- 'Dynamic': This entry requests a random IP address valid in the Internet from your provider which is then used for the connection and masquerading.
- 'Static': This entry requests a specific IP address entered under /setup/TCP from your provider which is then used for the connection and masquerading.

If a specific address is requested from the provider, two options are available for the actual address assignment:

- The provider assigns the desired address to the router. The network mask now decides how many computers are masked behind the router.
  - IP address with full '255.255.255.255' network mask: This is your own unique IP address, registered by the NIC. None of the other computers on the network have valid Internet addresses and are masked behind the router's fixed address.
  - IP address with an incomplete network mask, e.g. '255.255.255.248': You have several registered IP addresses, one of which you assign to the router. The remaining IP addresses are assigned permanently to devices on the Intranet, which can then use unmasked connections to access the Internet. The other devices can still access the Internet using masked connections.
- The provider assigns another address to the router. Then **all** computers in the local network are masked behind the assigned address.

How does IP masquerading work?

Masquerading makes use of a characteristic of TCP/IP data transmission, which is to use port numbers for destination and source as well as the source and destination addresses. When the router receives a data packet for transfer it now notes the IP address and the sender's port in an internal table. It then gives the packet its unique IP address and a new port number, which could be any number. It also enters this new port on the table and forwards the packet with the new information.

The response to this new packet is now sent to the IP address of the router with the new sender port number. The entry in the internal table allows the router to assign this response to the original sender again.

You can view these tables in detail in the router statistics (see also 'Status' in the reference manual).

Simple and inverse masquerading

This masking operates in both directions: The local network behind the IP address of the router is masked if a computer from the LAN sends a packet to the Internet (simple masquerading).

If, on the other hand, a computer sends a packet from the Internet to, for example, an FTP server on the LAN, from the point of view of this computer the router appears to be the FTP server. The router reads the IP address of the FTP server in the LAN from the entry in the service table (in the *ELSA LANconfig* in the 'IP router' configuration area on the 'Masq.' tab or in the menu `Setup/IP-router-module/Masquerading/Service-table`). The packet is forwarded to this computer. All packets that come from the FTP server in the LAN (answers from the server) are hidden behind the IP address of the router.

The only small difference is that:

- Access to a service (port) in the Intranet from outside must be defined in advance by specifying a port number. The destination port is specified with the Intranet address of, for example, the FTP server, on a service table to achieve this.

- When accessing the Internet from the LAN, on the other hand, the router itself makes the entry in the port and IP address information table.

  The table concerned can hold up to 2048 entries, that is it allows 2,048 **simultaneous** transmissions between the masked and the unmasked network.

  After a specified period of time, the router, however, assumes that the entry is no longer required and deletes it automatically from the table.

Which protocols are transmitted using IP masquerading?

Naturally, only those which also communicate using ports. Protocols working without port numbers or using ports above IP in the OSI model cannot be masked without special treatment.

The current version of router implements masquerading for the following protocols:

- TCP (and all protocols based on it such as FTP, HTTP, etc.)
- UDP
- ICMP

7.7 DNS forwarding

Names rather than IP addresses are generally used to access a server over the Internet. Who knows which address is behind 'www.domain.com'? The DNS server, of course.

DNS stands for **D**omain **N**ame **S**ervice and refers to the assignment of domain names (such as domain.com) to the corresponding IP addresses. This information must be constantly updated and be accessible all over the world at any time. DNS servers holding long tables containing IP addresses and domain names exist for this purpose.

If a computer calls up a home page from the intranet, it first sends out a DNS request: "Which IP address belongs to www.domain.com?”

This request is dealt with as follows if the router is registered as the DNS server for the workstation computers:

- Initially the router checks whether a DNS server has been entered in its own settings (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Addresses' tab or in the `/Setup/TCP-IP-module` menu). If it is successful there, it obtains the desired information from this server.

- If no DNS server is entered in the router, it will attempt to reach a DNS server over a PPP connection (e.g. from the Internet provider) to get the IP address assigned to the name from there. This can only succeed if the address of a DNS server is sent to the router during PPP negotiation.
- The default route is established and the DNS server searched for there if no connection exists.

This procedure does not require you to have any knowledge of the DNS server address. Entering the Intranet address of your router as the DNS server for the workstation computers is sufficient to enable you obtain the name assignment. This procedure also automatically updates the address of the DNS server. Your local network always receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

7.8 Policy-based routing

Policy-based routing describes a process in which particular data packets are given preferential treatment. This requires evaluation of a special field within the IP data packet, known as the Type of Service (TOS) field. This preferential treatment of a number of data packets can, for example, simplify the configuration of the router via the WAN when large data volumes are to be transferred simultaneously.

You can find more information on policy based circuit routing in the 'Description of the menu options' in the Reference manual.

8 Technical data

8.1 Performance data and specifications

Functions	IP router, IPX router, CAPI server, DHCP server; least cost router for router and CAPI connections, simultaneous operation of all functions possible
2-Mbit WAN connections	All devices: X.21 (electrical conformity X.24/V.11), max. 2 Mbps, full duplex, external clock
	ELSA LANCOM Business 6011: 1xG.703/G.704, max. 2 Mbps, full duplex
	ELSA LANCOM Business 6021: 2xG.703/G.704, max. 2 Mbps, full duplex
ISDN interface	Connect: ISDN S_0 bus, point-to-point and point-to-multipoint configuration, I.430 D channel: 1TR6, Euro-ISDN (DSS1), auto-sensing, Group 0 fixed connections (D64S, D64S2, D64SY) B channel: PPP (asynch./synch.), MLPPP, X.75, HDLC, V.110, CAPI 2.0 over *ELSA LANCAPI*, Stac data compression
LAN connection	Ethernet IEEE 802.3, 10/100Base-Tx (RJ45, node/hub switch), auto-sensing, full duplex
Network protocols	IP router ARP, Proxy ARP, DHCP server, IP, ICMP, UDP, TCP, RIP-1, RIP-2, Proxy DNS, Proxy NetBIOS/IP IPX router: IPX, SPX, RIP, SAP, Novell NetBIOS, Novell burst mode
Security functions	Calling line identification (CLIP); PAP, CHAP and MS-CHAP for authentication under PPP; automatic callback via ISDN; filtering options in IP, IPX and bridge mode; configuration protected by access lists and passwords; accounting for recent connection information; IP masquerading
Filter possibilities (firewall)	IP router Source and target filters for networks, protocols and ports IPX router: RIP, SAP, IPX and SPX watchdog, sockets, routes, propagated packets
IP masquerading	Translation of internal IP addresses and ports to an external IP address; static/dynamic IP address assignment via PPP; masking of TCP, UDP, ICMP and FTP; DNS forwarding; inverse masquerading of intranet services such as web server (DMZ)
Spoofing	IPX router: RIP and SAP packets; IPX and SPX watchdogs, Novell NetBIOS, keep-alive-packets

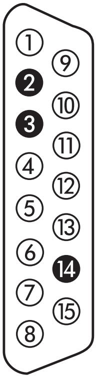
CAPI server	Virtual CAPI 2.0 for Windows operating systems, NDIS-WAN drivers, fax class 1
Line control	Automatic callback with or without call establishment; line-on-demand (dynamic channel bundling), short-hold mode, round-robin dialing, fast callback, dial backup for leased lines
Charge monitoring	Maximum online time or charges per period (AOC-D, AOC-E)
Management	Via LAN, ISDN (remote maintenance) or V.24, *ELSA LANconfig* and *ELSA LANmonitor* for Windows management software, *ELSA xLANconfig* for Linux, configuration via SNMP v.1, TFTP, Telnet or terminal
Operating security	Hardware watchdogs, regular self-testing, ELSA FirmSafe concept for remote software upgrades
Statistics	Separate counter for LAN/WAN; packets, errors, connections and online time; logging of connection control and online time with *ELSA LANmonitor* and SYSLOG; accounting of connections, online time, volume per IP with *ELSA LANmonitor*, trace of protocols for diagnostic purposes
Display/operation	LCD display and keypad, LEDs for LAN and WAN status
Power supply	12 V AC with AC adapter for 230 V, 12 VA
Environmental conditions	Temperature: 5–40°C, humidity: 0–80%, non-condensing
Dimensions and design	Rugged metal case, connections on rear panel; dimensions 230 x 38 x 228 mm (W x H x D)
Package contents	Device including network, ISDN and X.21 connector cables, one (*ELSA LANCOM Business 6011* only) or two (*ELSA LANCOM Business 6021* only) G.703 connector cables, connector cable for serial configuration interface (twisted-pair cable CAT-5), detailed documentation and *ELSA LANCOM Business* CD Software: *ELSA WEBconfig* (in the device firmware), *ELSA LANconfig* and *ELSA xLANconfig* (beta) configuration programs, *ELSA LANmonitor*, *ELSA-ZOC* terminal program
Approvals	For Germany, Switzerland and all other EU countries
Service and warranty	6 years warranty
Support	via hotline and Internet

8.2 Contact assignment

8.2.1 X.21 interface

Electrical connections comply with the X.24/V.11 specifications.

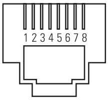
15-pin D-sub plug as per ISO 4903

Plug	Pin No.	X.21	Direction	Function
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	1	–	–	–
	2	Txd(+)	▶	transmit data
	3	Ctrl(+)	▶	control
	4	Rxd(+)	◀	receive data
	5	Ind(+)	◀	indicate
	6	Set(+)	◀	signal element timing
	7	–	–	–
	8	GND		signal ground
	9	Txd(-)	▶	transmit data
	10	Ctrl(-)	▶	control
	11	Rxd(-)	◀	receive data
	12	Ind(-)	◀	indicate
	13	Set(-)	◀	signal element timing
	14	–	–	–
	15	–	–	–

8.2.2 G.703 interface

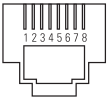
The *ELSA LANCOM Business 6011* and *ELSA LANCOM Business 6021* are the only models that feature this interface.

8-pin RJ45 socket as per ISO 8877

Connector	RJ45 pin	Designation	Function
	1	–	–
	2	–	–
	3	Ta	transmitline
	4	Ra	receiveline
	5	Rb	receiveline
	6	Tb	transmitline
	7	–	–
	8	–	–

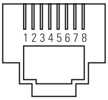
8.2.3 ISDN S_0 interface

8-pin RJ45 socket as per ISO 8877

Connector	RJ45 pin	Line	IAE
	1	–	–
	2	–	–
	3	T+	2a
	4	R+	1a
	5	R-	1b
	6	T-	2b
	7	–	–
	8	–	–

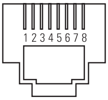
8.2.4 Ethernet interface 10/100Base-T

8-pin RJ45 socket as per ISO 8877

Connector	RJ45 pin	Line
	1	–
	2	–
	3	T+
	4	R+
	5	R-
	6	T-
	7	–
	8	–

8.2.5 Configuration interface(outband)

8-pin RJ45 socket as per ISO 8877, assignment compatible to Cisco

Connector	RJ45 pin	Function
	1	CTS
	2	DSR
	3	RXD
	4	Ground
	5	Ground
	6	TXD
	7	DTR
	8	RTS

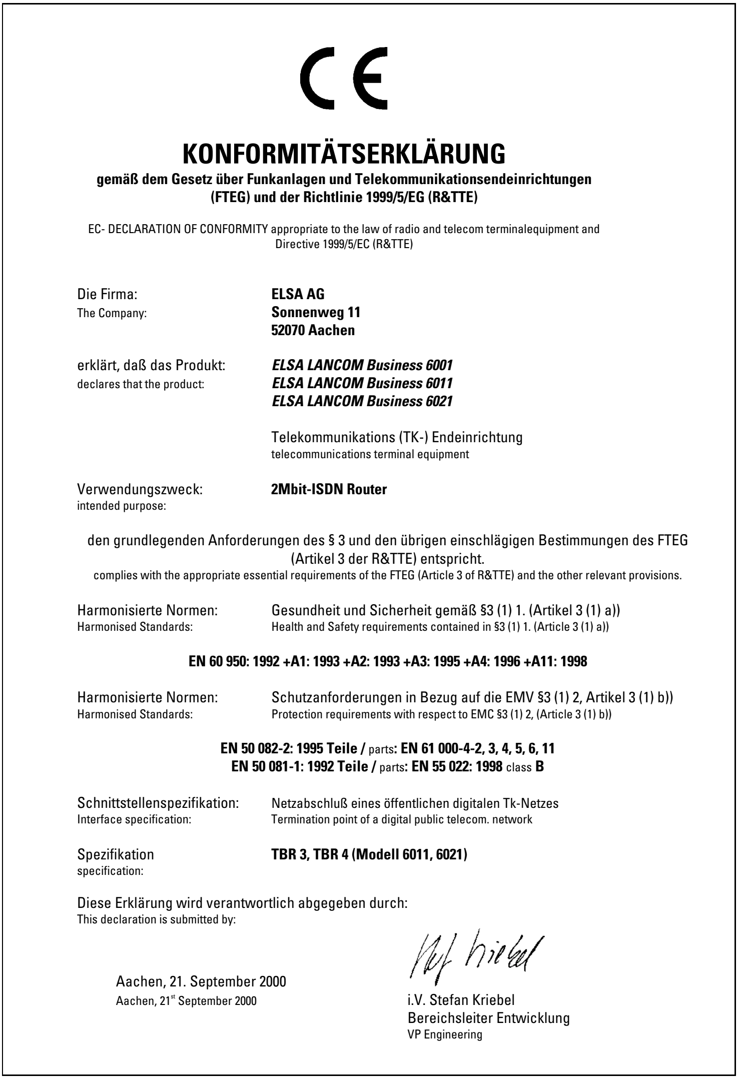
8.2.6 Important recycling information

Please note: This device contains a permanently installed lithium battery. Batteries containing hazardous substances must be disposed of properly!

Please be sure to return ELSA devices with permanently installed batteries to us in the event of a defect or for final disposal.

9 Appendix

9.1 Declaration of conformity



KONFORMITÄTSERKLÄRUNG

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

EC- DECLARATION OF CONFORMITY appropriate to the law of radio and telecom terminalequipment and Directive 1999/5/EC (R&TTE)

Die Firma:
The Company:

ELSA AG
Sonnenweg 11
52070 Aachen

erklärt, daß das Produkt:
declares that the product:

ELSA LANCOM Business 6001
ELSA LANCOM Business 6011
ELSA LANCOM Business 6021

Telekommunikations (TK-) Endeinrichtung
telecommunications terminal equipment

Verwendungszweck:
intended purpose:

2Mbit-ISDN Router

den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the appropriate essential requirements of the FTEG (Article 3 of R&TTE) and the other relevant provisions.

Harmonisierte Normen: Gesundheit und Sicherheit gemäß §3 (1) 1. (Artikel 3 (1) a))
Harmonised Standards: Health and Safety requirements contained in §3 (1) 1. (Article 3 (1) a))

EN 60 950: 1992 +A1: 1993 +A2: 1993 +A3: 1995 +A4: 1996 +A11: 1998

Harmonisierte Normen: Schutzanforderungen in Bezug auf die EMV §3 (1) 2, Artikel 3 (1) b))
Harmonised Standards: Protection requirements with respect to EMC §3 (1) 2, (Article 3 (1) b))

EN 50 082-2: 1995 Teile / parts**: EN 61 000-4-2, 3, 4, 5, 6, 11**
EN 50 081-1: 1992 Teile / parts**: EN 55 022: 1998** class **B**

Schnittstellenspezifikation: Netzabschluß eines öffentlichen digitalen Tk-Netzes
Interface specification: Termination point of a digital public telecom. network

Spezifikation
specification:

TBR 3, TBR 4 (Modell 6011, 6021)

Diese Erklärung wird verantwortlich abgegeben durch:
This declaration is submitted by:

Aachen, 21. September 2000
Aachen, 21st September 2000

i.V. Stefan Kriebel
Bereichsleiter Entwicklung
VP Engineering

9.2 Warranty conditions

The ELSA AG warranty, valid as of June 01, 1998, is given to purchasers of ELSA products in addition to the warranty conditions provided by law and in accordance with the following conditions:

1 Warranty coverage

a) The warranty covers the equipment delivered and all its parts. Parts will, at our sole discretion, be replaced or repaired free of charge if, despite proven proper handling and adherence to the operating instructions, these parts became defective due to fabrication and/or material defects. Also we reserve the right to replace the defective product by a successor product or repay the original purchase price to the buyer in exchange to the defective product. Operating manuals and possibly supplied software are excluded from the warranty.

b) Material and service charges shall be covered by us, but not shipping and handling costs involved in transport from the buyer to the service station and/or to us.

c) Replaced parts become property of ELSA.

d) ELSA are authorized to carry out technical changes (e.g. firmware updates) beyond repair and replacement of defective parts in order to bring the equipment up to the current technical state. This does not result in any additional charge for the customer. A legal claim to this service does not exist.

2 Warranty period

The warranty period for this ELSA product is six years. This period begins at the day of delivery from the ELSA dealer. Warranty services do not result in an extension of the warranty period nor do they initiate a new warranty period. The warranty period for installed replacement parts ends with the warranty period of the device as a whole.

3 Warranty procedure

a) If defects appear during the warranty period, the warranty claims must be made immediately, at the latest within a period of 7 days.

b) In the case of any externally visible damage arising from transport (e.g. damage to the housing), the transport company representative and ELSA should be informed immediately. On discovery of damage which is not externally visible, the transport company and ELSA are to be immediately informed in writing, at the latest within 7 days of delivery.

c) Transport to and from the location where the warranty claim is accepted and/or the repaired device is exchanged, is at the purchaser's own risk and cost.

d) Warranty claims are only valid if the original purchase receipt is returned with the device.

4 Suspension of the warranty

All warranty claims will be deemed invalid

a) if the device is damaged or destroyed as a result of acts of nature or by environmental influences (moisture, electric shock, dust, etc.),

b) if the device was stored or operated under conditions not in compliance with the technical specifications,

c) if the damage occurred due to incorrect handling, especially to non-observance of the system description and the operating instructions,

d) if the device was opened, repaired or modified by persons not authorized by ELSA,

e) if the device shows any kind of mechanical damage,

f) if in the case of an ELSA Monitor, damage to the cathode ray tube (CRT) has been caused especially by mechanical load (e.g. from shock to the pitch mask assembly or damage to the glass tube), by strong magnetic fields near the CRT (colored dots on the screen), or through the permanent display of an unchanging image (phosphor burnt),

g) if, and in as far as, the luminance of the TFT panel backlighting gradually decreases with time, or

h) if the warranty claim has not been reported in accordance with 3a) or 3b).

5 Operating mistakes

If it becomes apparent that the reported malfunction of the device has been caused by unsuitable software, hardware, installation or operation, ELSA reserves the right to charge the purchaser for the resulting testing costs.

6 Additional regulations

a) The above conditions define the complete scope of ELSA’s legal liability.

b) The warranty gives no entitlement to additional claims, such as any refund in full or in part. Compensation claims, regardless of the legal basis, are excluded. This does not apply if e.g. injury to persons or damage to private property are specifically covered by the product liability law, or in cases of intentional act or culpable negligence.

c) Claims for compensation of lost profits, indirect or consequential detriments, are excluded.

d) ELSA is not liable for lost data or retrieval of lost data in cases of slight and ordinary negligence.

e) In the case that the intentional or culpable negligence of ELSA employees has caused a loss of data, ELSA will be liable for those costs typical to the recovery of data where periodic security data back-ups have been made.

f) The warranty is valid only for the first purchaser and is not transferable.

g) The court of jurisdiction is located in Aachen, Germany in the case that the purchaser is a merchant. If the purchaser does not have a court of jurisdiction in the Federal Republic of Germany or if he moves his domicile out of Germany after conclusion of the contract, ELSA’s court of jurisdiction applies. This is also applicable if the purchaser's domicile is not known at the time of institution of proceedings.

h) The law of the Federal Republic of Germany is applicable. The UN commercial law does not apply to dealings between ELSA and the purchaser.

10 Index