ELSA LANCOM™ DSL/25 Office

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

Windows®, Windows NT® and Microsoft® are registered trademarks of Microsoft, Corp.

The ELSA logo is a registered trademark of ELSA AG. All other names mentioned may be trademarks or registered trademarks of their respective owners.

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

ELSA AG
Sonnenweg 11
52070 Aachen
Germany

www.elsa.com

Aachen, May 2000

20661/0500

Preface

Thank you for placing your trust in this ELSA product.

By selecting the *ELSA LANCOM DSL/25 Office* you have chosen a router which you can use to connect local area networks or single workstations with other networks via an ATM line. Connection to the ATM network is realized via a ADSL connection.

Documentation

The accompanying documentation comprises:

- Manual

  Hardware installation, description of functions and operating modes and examples of configurations

- CD containing electronic documentation

  Basic technical information (e.g. on ATM, general network technology, TCP/IP), workshop with comprehensive usage examples, reference section with complete menu description

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 under 'Know-How', 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.

The KnowledgeBase can also be found on the CD. Just open the file \Misc\Support\MISC\ELSASIDE\index.htm.

Contents

1 Introduction

The sheer speed of development of computer technology over the last few years has resulted in a huge increase in the volume of electronic data traffic. More users every day want to send and receive a constantly increasing volume of data. Conventional transmission technologies (modem or ISDN devices) are no longer equal to the demand.

New technologies are eliminating the restrictions and are offering the user true broadband communications at significantly higher transfer speeds. An important criterion for the spread of these new access technologies is their availability in as many offices and companies as possible. One new technology is transmission by xDSL, which covers the “last mile” over conventional copper wires. For example, connection to ATM high-speed networks becomes possible.

The *ELSA LANCOM DSL/25 Office* gives you a router that has been specially developed for the ATM interface of xDSL terminals. *ELSA LANCOM DSL/25 Office* allows connection of individual workstations or entire local networks and provides considerably higher transmission rates than what was possible via ISDN.

Special highlights:

- Rapid Internet connection. *ELSA LANCOM DSL/25 Office* allows transmission rates up to 6 MB/s downstream and 0.6 MB/s upstream in the ATM network.
- LAN connection via ATM or ISDN. *ELSA LANCOM DSL/25 Office* supports not only fixed connections but also dial-up connections to remote stations in the ATM and ISDN network (now in process at several network operating companies) and thus providing connection of individual local networks to a common WAN (Wide Area Network).
- Office communication via broadband CAPI. With the integrated broadband CAPI, normal ISDN-CAPI applications such as remote access or fax can also profit from the available transmission bandwidth.

This section is a brief introduction to the device and its functions. See the following sections for a detailed description of the functions, the software and how to use it and an introduction to the technical basics.

1.1 What does a router do?

A router connects local networks (LANs) and individual PCs to form a Wide Area Network (WAN). This allows any computer in this WAN to access the computers and services on the entire network, depending on its access privileges. The router does this by seeking out a path over which data can be exchanged between the computers.

This is available in the form of an ATM connection, for example, that can be realized via normal copper telephone lines with xDSL technology.

Connection to the Internet is a particularly widespread form of network connection. If the local network in a company is connected with the network of an Internet service provider, all computers in the LAN will be able to access the services and sites on the World Wide Web.

But routers are capable of more. Using a special interface called the *ELSA LANCAPI*, modern office communications functions such as fax or EuroFileTransfer etc. can be provided on the entire local network. The corresponding communications programs forward their data via the *LANCAPI* to the router which then takes care of the data transmission. Equipping the individual workstations with their own data communications equipment—a costly, high-maintenance scenario—thus becomes superfluous.

The router is incorporated into the network in the same way as any normal PC. Any data traveling on the network cable, therefore, is seen by the router too. It automatically determines whether or not the data needs to be transmitted to another network. If necessary, it establishes the connection to the destination network. Of course, a dedicated line does away with the process of establishing a connection.

When precisely should the router be used?

As a matter of fact, wherever computers need to be joined together and a simple modem operation no longer fits the bill. Here are some example applications:

- Internet on the LAN

  Many companies are experiencing an increasing demand for Internet access from all workstations on the LAN. Online research, file transfer and e-mail are just some of the applications intended to lighten the workload of those working at a PC.

  The router links all the workstation computers on your local area network to the global Internet. Security features such as IP masquerading not only save you money but also shield your network against access from outside.

- LAN to LAN coupling

  When business is going well, the time eventually comes for a sister company or subsidiary to be established in the global markets. Of course, the branch office, too, has its own network and must to be kept up-to-date.

  LAN to LAN coupling links the individual LANs to form one large network, even if this means crossing continents. When connecting via a dial-up connection, an intelligent line management function together with sophisticated filter mechanisms keeps connections costs low. Of course, it is also possible to operate a combination of dedicated lines and dial-up connections.

- Teleworking using remote access

  The work of many office workers in modern organizations is less and less dependent on any definite location—the most important factor here is unimpaired access to shared and freely available information.

  Remote access is the key to this. The router on the local network at the head office enables colleagues to telecommute from their home offices and traveling staff to access the office while on the road. The *ELSA LANCOM DSL/25 Office* naturally also does everything necessary to protect the company's data holdings during remote access: the callback function uses the names and call numbers entered to provide access to specified users only. And telephone charges are calculated at head office, simplifying the billing process.

- Office communications using *LANCAPI*

  Faxing directly from within applications, voice mail with different announcements according to the time of day, banking without having to leave the office: These functions are made possible by using the *LANCAPI*.

  LANCAPI is a special form of the CAPI 2.0 interface that applications such as *ELSA-RVS-COM* or *ELSA-ZOC* can use to access the router.

1.2 What does the *ELSA LANCOM DSL/25 Office* offer?

The following is an outline of the principal features of the device giving you a quick overview of its capabilities.

Easy installation

- Connect the *ELSA LANCOM DSL/25 Office* to the power supply.
- Establish a link to the LAN.
- Inserting the ATM cable.
- Switch it on.
- Go!

LAN connection

DSL router from ELSA can be connected to a (Fast) Ethernet network using the 10/100Base-T port. The connection automatically determines the speed at which the local network is running.

WAN connection

The *ELSA LANCOM DSL/25 Office* can be connected to the ATM interface of an xDSL connection. In principle, it then has access to all of the functions of a direct connection into the ATM network.

ELSA LANCOM DSL/25 Office supports not only continuous ready connections (fixed connections, but also PVC, Permanent Virtual Connection) as well as dial-up connections (SVC, Switched Virtual Connection).

IP via ATM, Classical IP

ELSA LANCOM DSL/25 Office transmits data of various network protocols such as IP and IPX via the ATM line. For example, networks of various locations can be connected via ATM or to the Internet with high bandwidths.

PPP using ATM

ELSA LANCOM DSL/25 Office also transmits PPP via the ATM line. Therefore, all advantages of PPP connections for data transmission via ATM are available.

- Data compression via Stac
- Negotiating and assigning IP addresses via the WAN line.

- Callback functions
- Password protection

Subadressing

ELSA LANCOM DSL/25 Office supports subaddressing when transmitting and evaluating calling numbers. Various devices can also be directly addressed with connections having only one calling number.

Configuration

Setting up and configuring the device to your specific needs is made quick and easy in the Windows operating systems by the configuration tool supplied, *ELSA LANconfig*.

Users of other operating systems use the HTML-based configuration tool, Telnet or any other terminal program.

This means that you can access the device from the WAN, from the LAN or directly via your own configuration interface. TFTP is supported along with SNMP if configuring from the LAN or WAN.

The integrated Setup Wizards from *ELSA LANconfig* and HTML configuration help you get the unit operating in a few steps.

Software update

Your devices have a flash ROM memory to ensure that its software remains state of the art. This allows new firmware to be loaded onto the device without the need to open it up.

The current version is always available to you on our online media and can be loaded via the LAN, the WAN or the configuration interface.

FirmSafe

There is no risk involved with loading the new firmware. The FirmSafe function enables two firmware files to be managed on one device. If the new firmware version does not function as desired after the upload you can simply revert to the previous version.

If an error occurs during the upload (e.g. a transmission error) the functioning previous version is automatically reactivated.

Intruder protection

For protection against unauthorized access to the company network, the router provides not only the simple password protection with authentication mechanisms in PPP, but also a closed security concept for firewall filters and IP masquerading. Furthermore, login barring prevents any “brute force attacks” and denies access to the router after a configurable number of login attempts using an incorrect password.

Charge monitoring

The charges for ATM connections are calculated by the provider depending on the time used. To avoid unpleasant surprises at the end of the month, you can establish the amount of online time for your WAN connection within a given period (e.g. 600 minutes in 6 days) that will be permitted via the *ELSA LANCOM DSL/25 Office*. Depending on the network operating company, cost information is also transmitted, which can be used for cost protection.

ELSA LANmonitor

Under Windows operating systems, this tool displays the status of the router on the screen at all times. For each device on the local network, the most important information are displayed, e.g.:

- Name of the remote side
- Connection duration and transmission rates
- Excerpts of the device statistics (e.g. PPP negotiation data)

Additionally, the software allows you to log and save the messages on the PC for further processing.

Status displays

LED indicators on the front of your device allow you to monitor the ATM and Ethernet connection, thus simplifying the process of diagnosing any systems failures.

Statistics

The comprehensive statistics function lets you keep track of your *ELSA LANCOM DSL/25 Office*. These statistics give you all the information you need on the data packets transferred, for example, so that you can optimize the configuration of your device.

DHCP

ELSA routers also incorporate the functions of a DHCP server. Thus you can define a certain range of IP addresses which the DHCP server then independently assigns to the individual devices on the local network.

When in automatic mode, the router can also define all addresses on the network and assign them to the devices connected to the network.

DNS server

The router's DNS server functions allow you to set up links between IP addresses and names of computers or networks. The correct route can be directly assigned on queries for known computer names.

The DNS server can also access the name and IP information from the DHCP server and the NetBIOS module.

The DNS server can also serve as an effective filter for the users in your local network. Access to specified domains can be denied to individual computers or complete networks.

ELSA LANCAPI and *ELSA CAPI Faxmodem*

The main advantages of using *LANCAPI* are economic. The *LANCAPI* is a special type of CAPI 2.0 interface through which various communications programs (e.g. *ELSA-RVS-COM* or *ELSA-ZOC*) via the network can access the router.

Any workstation which has been integrated into the LAN (Local Area Network) can use *LANCAPI* to give unlimited access to office communication functions such as fax and EuroFileTransfer. All functions are made available throughout the network without the need to add hardware to the workstations. This does away with the cost of equipping workstations with ATM adapters. The office communications software simply needs to be loaded onto the individual workstations.

An fax device is simulated at the workstation so that faxes can be sent. With the *LANCAPI*, the PC forwards the fax via the network to the router which establishes the connection to the recipient.

Line connection and management

The router checks all data on the network to determine whether they have to be sent to another network or computer. Is data transfer is necessary, the router establishes the connection itself and closes the connection once the transfer is complete. Any partly used call charge units are used up fully if call charge information is transmitted during the connection.

To reduce transfer costs, the router offers various filter options depending on the mode of operation. They can be used to exclude from the transfer data that come from the entire network or from parts of the network. Similarly, data that belong to specific services (such as printing services) can be filtered out of the transfer.

NetBIOS proxy

ELSA routers offer a special feature for the interconnection of Microsoft peer-to-peer networks. With the integrated routing of IP NetBIOS packets, the linking of Windows networks becomes child's play. The remote stations relevant for the exchange of data are entered in a list to ensure that not every NetBIOS packet results in the establishment of a connection.

As a NetBIOS proxy, the router answers the queries for known workstations locally to prevent connections from being established unnecessarily.

Compatibility through PPP

The router uses PPP, a widely used protocol, and other protocols to exchange network data through point-to-point connections with devices made by other manufacturers.

Remote configuration using PPP

One special configuration feature of the routers from ELSA which cannot and should not be setup locally is its ability to be configured remotely via PPP connections and the Windows Dial-up Network. All you have to do is to plug the new device into the power supply and connect it to the WAN Basic Rate Interface. Now you can access the router using a PPP connection and configure it from your location. The first time the device is configured, access to it is secured by a password and thereafter it remains inaccessible to unauthorized callers.

2 Installation

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

The following information is intended for experienced users familiar with hardware and network configuration.

2.1 Package contents

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

- *ELSA LANCOM DSL/25 Office*
- Power supply unit
- LAN connection cable
- ATM connection cable
- Cable for the configuration interface
- Adapter for configuration cable
- Documentation
- CD containing *ELSA LANconfig*, other software and electronic documentation

Please contact your dealer directly if anything is missing.

2.2 System preconditions

The system that you want to connect to the Internet with the unit must meet the following requirements:

- Any operating system that supports the TCP/IP network protocol, such as Windows 95, Windows 98, Windows 2000, Windows NT 4.0, OS/2, Linux or BeOS
- Windows 95, Windows 98, Windows 2000 or Windows NT 4.0 and a CD-ROM drive for those computers on which you want to install the *ELSA LANconfig* configuration software
- Ethernet network card
- Network protocol TCP/IP installed and bound to the network card

2.3 Setting up the computer

Routers from ELSA make it extremely simple to manage addresses on local networks. A few settings might have to be made at the workstations to ensure that the routers and workstation communicate together properly.

2.3.1 Windows 95 and Windows 98

Using Windows 95 and Windows 98 as examples, this section will show what needs to be done, if it is not already done for you, to ensure smooth communication between computers in a TCP/IP network with the router connected to the workstations.

- Installing TCP/IP

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

- Allocate IP addresses (using DHCP)

  If you are going to use the router as a DHCP server, set the workstations to obtain IP addresses automatically: **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network** ▶ **TCP/IP** ▶ **Properties** ▶ **IP Address** ▶ **Obtain an IP address automaticaly**. Also, delete any existing entries for DNS servers and gateways (found under the 'Gateway' and 'DNS Configuration' tabs). When the computer is restarted, it then searches for a DHCP server on the network and lets it assign an IP address to it.

- Setting fixed IP addresses (not using DHCP)

  If you are not going to use a DHCP server on your network, assign the workstations fixed IP addresses: **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network** ▶ **TCP/IP** ▶ **Properties** ▶ **IP Address** ▶ **Specify an IP address**.

  Assign unique IP addresses, for example taken from a reserved range of addresses. For example, the workstations can be assigned addressed from '10.1.1.2' to '10.1.1.253', the router can be given '10.1.1.1' and all can have the subnet mask of '255.255.255.0'. To test whether or not a specific IP address, such as '10.1.1.1', is free, enter `ping 10.1.1.1` in a DOS session. If you do not receive a response, the address is most likely free.

- Entering the Gateway and DNS Server (not necessary when using DHCP)

  On the workstation computers, specify the address of the local network router as the Gateway and as the Domain Name Server (DNS server): **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network** ▶ **TCP/IP** ▶ **Properties** ▶ **Gateway** and **DNS Configuration**. Also enter a host name on the DNS Configuration page. In doing so, use the name of the PC, which ideally matches the user's name, to maintain a certain amount of consistency.

- Checking the IP configuration

  Under Windows 95 and Windows 98, you can view the current IP configuration of your computer with by using **Start** ▶ **Run...** ▶ **winipcfg**. Among other information, this shows you which IP address was assigned to the computer by the DHCP server and which addresses have been specified for DNS servers and the gateway.

2.3.2 Windows NT 4.0

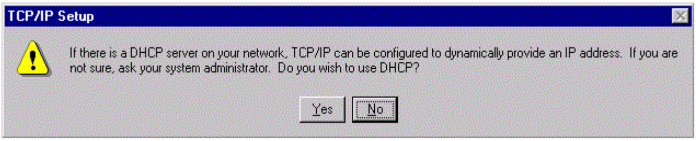
Using Windows NT 4.0 as an example, this section will show what needs to be done, if it is not already done for you, to ensure smooth communication between computers in a TCP/IP network with the router connected to the workstations.

- Installing TCP/IP

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

- Allocate IP addresses (using DHCP)

  If you are going to use the router as a DHCP server, set the workstations to obtain IP addresses automatically. To do so, select **Yes** when completing the network protocol installation.



TCP/IP Setup

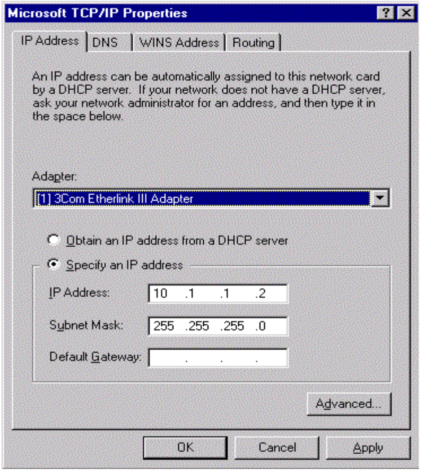
If there is a DHCP server on your network, TCP/IP can be configured to dynamically provide an IP address. If you are not sure, ask your system administrator. Do you wish to use DHCP?

  Windows then copies the required files and, when finished, requests you to reboot.

- Setting fixed IP addresses (not using DHCP)

  If you are not going to use a DHCP server on your network, assign the workstations fixed IP addresses: **Start** ▶ **Settings** ▶ **Control Panel** ▶

Network ▶ Protocols ▶ Properties.... This page also lets you set the standard gateway.



An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter:
[1] 3Com Etherlink III Adapter

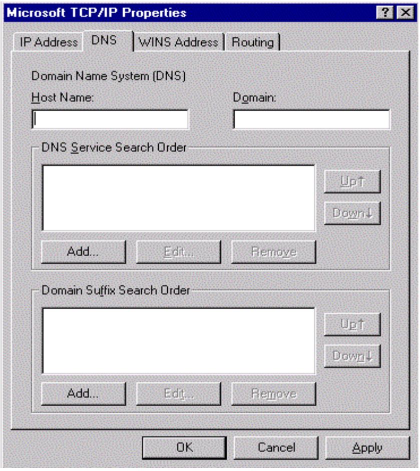
○ Obtain an IP address from a DHCP server
● Specify an IP address

IP Address: 10 .1 .1 .2
Subnet Mask: 255 .255 .255 .0
Default Gateway: . . .

Assign unique IP addresses, for example taken from a reserved range of addresses. For example, the workstations can be assigned addressed from '10.1.1.2' to '10.1.1.253', the router can be given '10.1.1.1' and all can have the subnet mask of '255.255.255.0'. To test whether or not a specific IP address, such as '10.1.1.1', is free, enter `ping 10.1.1.1` in a DOS session. If you do not receive a response, the address is most likely free.

- Entering the DNS server (not necessary when using DHCP)

  On the workstation computers, specify the address of the local network router as the Domain Name Server (DNS server) on the on the 'DNS' page. Also enter a host name on the DNS configuration page. In doing so, use the name of the PC, which ideally matches the user's name, to maintain a certain amount of consistency.



- Checking the IP configuration

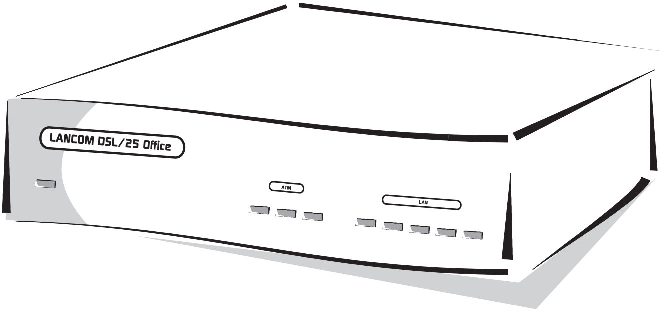
  Under Windows NT 4.0 you can querry the current IP configuration of your computer with **Start** ▶ **Run...** ▶ **ipconfig**. This shows you which IP address was assigned to the computer by the DHCP server and which addresses have been specified for the gateway (not for the DNS server).

2.4 Introducing the *ELSA LANCOM DSL/25 Office*

This section introduces the unit's hardware. It covers the unit's display elements and connection options.

2.4.1 The front of the unit

You will find a number of LEDs as display elements on the front panel.



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

ATM status

This LED shows the status of the ATM connection to the switching center:

Off	No signal from the ATM switching center
flashing	Signal of the switching center is active, but no valid connection to the switching center is established.
on	At least one valid connection is established

ATM-rx
ATM-tx

This LEDs show that data is moving on the ATM connection:

ATM-rx	green	Data packet received from the ATM switching center
ATM-tx	yellow	Data packet sent from the device to the ATM switching center

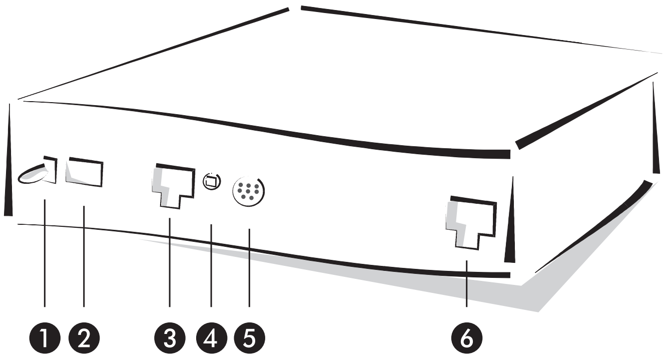
LAN-tx, -rx,
LAN-coll, -link
LAN-FDpx, -Fast

These LEDs show the corresponding network controller status:

LAN-rx/tx	yellow	Data packet sent from the device to the LAN or vice versa
LAN-coll	red	Sending collision
LAN-link	green	Connection to LAN is established and ready
LAN-FDpx	green	Router is transmitting and receiving data simultaneously
LAN-fast	green	*ELSA LANCOM DSL/25 Office* is operating at 100 Mbit

2.4.2 The back of the unit

Now turn the whole thing around and take a look at the rear. Beginning again on the left-hand side, you have:



❶ On/Off switch

❷ Connection for power supply unit

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

❹ Node/hub selector switch

❺ V.24 configuration interface

❻ ATM-25.6 connection

2.5 How to connect the device

① Connect your *ELSA LANCOM DSL/25 Office* 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).

② Connect your *ELSA LANCOM DSL/25 Office* to the ATM network. Plug the ATM connection cable provided in the ATM-25.6 connection of the device and in the Ethernet interface of the NTBBA.

③ Connect the AC adapter to the device and switch it on. After a short device self-test the 'Power/Msg' LED will be permanently lit. The 'LAN Link' LED indicates that your router is correctly connected to the LAN.

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.

2.6 Software installation

The *ELSA LANconfig* configuration software for Windows operating systems enable you to set up your router easily and conveniently for the desired application.

You will need a Windows PC on the LAN to run *ELSA LANconfig*.

① Install the TCP/IP network protocol on the computer that will be used to set up your device.

② Then install *ELSA LANconfig*. If the setup program does not start up automatically after insertion of the *ELSA LANCOM* CD, start Windows Explorer, click on 'autorun.exe' on the *ELSA LANCOM* CD and follow the instructions in the install program.

2.7 Configuration

Configure the unit using the following steps:

- Basic settings
- ATM connection setting
- Router configuration

There is an information table for each of the stages of configuration, which describes the information you will have to have available. Fill out the tables before starting the process of configuration.

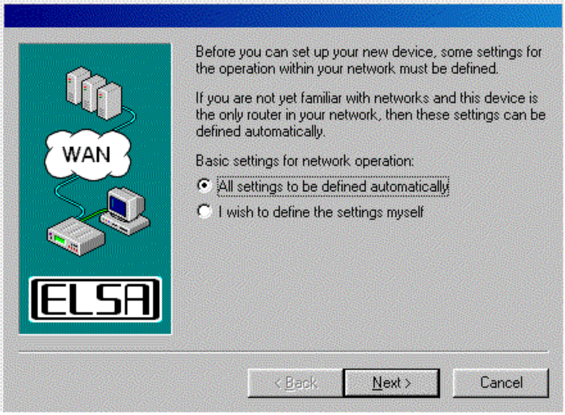
2.7.1 Basic settings

With the basic settings, you assign a name to the unit and define the IP addresses for operation in the local network. In this example, the DHCP server in the router automatically takes over the task of assigning IP addresses.

ELSA LANconfig

The first time *ELSA LANconfig* is run, the new device is detected on the TCP/IP network and can immediately be configured. A wizard is automatically started to help you with the basic settings of the device or it can even the complete setup itself.

① Start the new software with **Start** ▶ **Programs** ▶ **ELSAlan** ▶ ***ELSA LANconfig***.



Before you can set up your new device, some settings for the operation within your network must be defined.

If you are not yet familiar with networks and this device is the only router in your network, then these settings can be defined automatically.

Basic settings for network operation:

● All settings to be defined automatically

○ I wish to define the settings myself

② Select the option 'All settings to be defined automatically' if you are **not** familiar with networks and IP addresses and one of the following conditions applies:

- You have not used any IP addresses previously in your network but would now like to do so. You do not care which IP address should be used. The router as a DHCP-server will automatically set and assign the IP addresses for all devices in the network (LAN and WLAN).

or

- You do not wish to use IP addresses, perhaps because you have a Windows-only network.

If you do not know whether IP addresses have been used in your network, first click on ***Start*** ▶ ***Run...****, enter the following command in the window* `winipcfg` *and click* ***OK****. If the next window shows the value '0.0.0.0' in the field 'IP address', the computer has never had an IP address.*

③ Select the option 'I wish to define the settings myself' if you are familiar with networks and IP addresses and one of the following conditions applies:

- You have not used any IP addresses previously in your network but would now like to do so. However, you wish to set the IP address for the router and assign it an address from an address range reserved for private use, e.g. '10.0.0.1' with the network mask '255.255.255.0'. At the same time you will set the address range that the DHCP server uses for the other devices in the network (so long as the DHCP server is not switched off).

○ You have previously used IP addresses on the computers in the LAN. Assign the router a free address from the previously used address range, and select whether the router should run as a DHCP server or not.

You can find more information on the general structure of networks and setting IP addresses in the electronic documentation on the ELSA LANCOM CD. The functions of the DHCP server are described later in this manual.

Telnet

Start the telnet connection to the address '10.0.0.254' if you have not previously used IP addresses in your network, or to address 'x.x.x.254', where 'x.x.x' stands for the address group previously used in the network.

Enter the following command:

① You can start the telnet connection with the command **Start ▶ Run...** and entering the command `telnet 10.0.0.254` in the window.

② Change the language for the configuration with the command:

```
set /Setup/config-module/language english
```

③ Intranet address and network mask:

```
set /setup/TCP-IP-module/Intranet addr. 10.0.0.1
set /setup/TCP-IP-module/Intranet-mask
255.255.255.0
```

When the internet address is changed, the telnet connection is interrupted.

④ To switch off the DHCP function:

```
set setup/DHCP-module/operating off
```

Even if the entries at this point are not very clear without further explanation, you can reach the same destination as with the setup with ELSA LANconfig.

With these settings, you have completed making your new router known on the local network. The router itself is addressable using the IP address of '10.0.0.1'. After you reboot your system, all units on the local network will be assigned IP addresses by the DHCP server in the router. It will use an address pool from '10.0.0.2' to '10.0.0.253' automatically.

2.7.2 ATM connection setting

Enter the values for your ATM connection and the connections to other devices. Some of these values are provided by your telephone company.

Which type of information do you need?

❶	Protocol for the signalization channel	
❷	Dialing prefix (required only for ATM-TK installations and private networks)	
❸	Virtual Path Identifier (VPI)	
❹	Link Cell Rate (LCR) for the ATM connection (upstream)	
❺	Traffic contract for signalization channel	
❻	Calling number(s) for ATM interface	

Setting with *ELSA LANconfig* or telnet

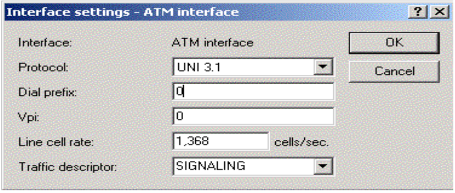
① Start up *ELSA LANconfig* from the program group 'ELSAlan'. *ELSA LANconfig* automatically searches for new devices in the local network and on the configuration interface.

Alternatively, establish a connection to your new device with telnet. For example, enter the following command when prompted:

```
telnet 10.0.0.1
```

② Open the configuration dialog box by clicking on the corresponding entry in the device list.

③ Go to the 'Interfaces' register card and open the list of **interface settings**. For the ATM interface, indicate the protocol for the signalization channel ❶, a dialing prefix ❷ if necessary, the number of the virtual connection path (VPI ❸), the physical speed of the connection (LCR ❹), and the traffic contract for the signalization channel ❺.

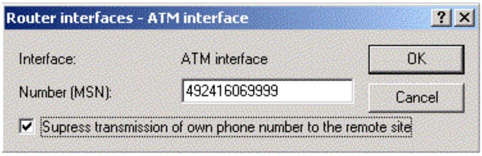


Interface: ATM interface
Protocol: UNI 3.1
Dial prefix: 0
Vpi: 0
Line cell rate: 1,368 cells/sec.
Traffic descriptor: SIGNALING

```
set Setup/WAN-module/ ATM-1 UNI3.1 1368 0 0
SIGNALING-interface-list
```

The traffic contract established here refers exclusively to the signalization channel during dial-up connections. This setting does not effect the data transmission channels! Traffic contracts can be established in the 'Communication' configuration area on the 'General' register card or via telnet under `/Setup/WAN-module/Traffic-contracts`*.*

④ Go to the 'General' register card in the 'Communcation' configuration area and open the settings for the ATM interface under 'Router interfaces'. Enter the calling number(s) ❻ to which the router should respond. The first calling number entered is used for outgoing calls. In addition, select whether the custom calling number should be displayed at the remote station.



Interface: ATM interface
Number (MSN): 492416069999
☑ Supress transmission of own phone number to the remote site

The calling numbers in the ATM network are always entered in the complete international format without the beginning zeros!

```
set /Setup/WAN-module/Router-interface-list ATM-
1 492416069999 On
```

After the general settings have been carried out, connections can be established to the desired remote stations.

2.7.3 Establishing ATM fixed connection

A fixed connection via the ATM network is configured by simply assigning a remote station name to a VCI

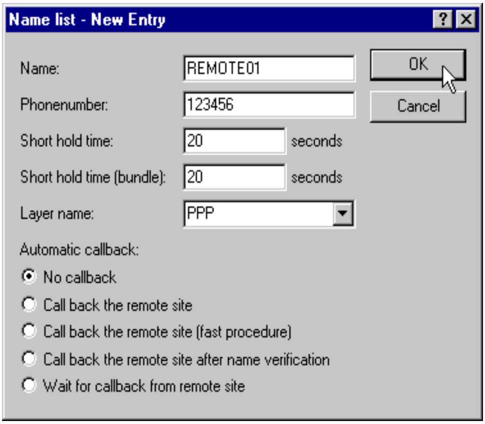
Which type of information do you need?

❶	Name of the remote station	
❷	WAN-layer	
❸	Traffic-contract	
❹	Virtual Channel Identifier (VCI)	

Setting with *ELSA LANconfig* or telnet

① Open the configuration, then go to the 'Remote sites' register card and open the **name list**. Enter the name of the remote station ❶ and select the layer name ❷ and the traffic contract ❸ for this connection.

```
set /Setup/WAN-module1/BERLIN * * * LLCPPP
DEFAULT name-list
```



Name list - New Entry

Name: REMOTE01

Phonenumber: 123456

Short hold time: 20 seconds

Short hold time (bundle): 20 seconds

Layer name: PPP

Automatic callback:

● No callback

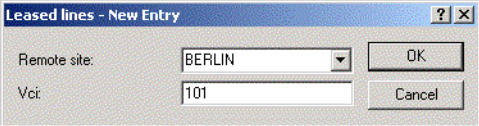
○ Call back the remote site

○ Call back the remote site (fast procedure)

○ Call back the remote site after name verification

○ Wait for callback from remote site

② Go to the 'Remote sites' register card and open the list of **fixed connections**. Select the remote station to which you would like to define the fixed connection ❶, and indicate the number of the virtual connection channel (VCI) ❹.



Leased lines - New Entry

Remote site: BERLIN

Vci: 101

```
set /Setup/WAN-module/ BERLIN 101 fixed
connection
```

That's it! All data packets, which are assigned to the 'Berlin' remote station using the settings in the routing table, use the fixed connection over the virtual '101' connection channel.

2.7.4 Establishing ATM dial-up connection

A dial-up connection via the ATM network is configured by a traffic contract agreement and by assigning a calling number to a remote station name.

Which type of information do you need?

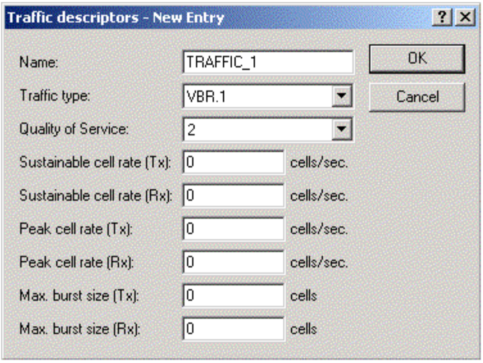
❶	Name for the traffic contract	
❷	Traffic type	
❸	QoS	
❹	Sustainable Cell Rate (Tx/Rx)	
❺	Peak Cell Rate (Tx/Rx)	
❻	Maximum Burst Size (Tx/Rx)	
❼	Name of the remote station	
❽	Remote station call number	
❾	WAN-layer	

Setting with *ELSA LANconfig* or telnet

① Open the configuration, then go to the 'Communication' register card and open the list of **traffic contracts**. Enter a name for the traffic contract and select the type of traffic contract ❷ (variable, non-fixed or constant bit rate or ISDN for remote stations in the ISDN network). Set the value for the quality of service ❸ and then enter the values for the mid-range

❹ and maximum cell rate ❺ as well as the maximum burst length ❻ for sending and receiving data.

```
set /Setup/WAN-module/Traffic-contracts
Traffic_1 VBR.1 2 300 300 800 800 20 20
```



Traffic descriptors - New Entry

Name: TRAFFIC_1

Traffic type: VBR.1

Quality of Service: 2

Sustainable cell rate (Tx): 0 cells/sec.

Sustainable cell rate (Rx): 0 cells/sec.

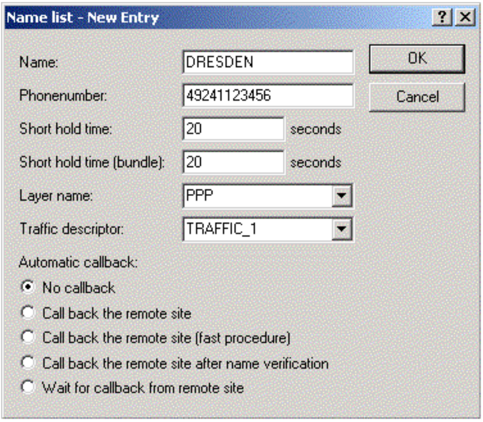
Peak cell rate (Tx): 0 cells/sec.

Peak cell rate (Rx): 0 cells/sec.

Max. burst size (Tx): 0 cells

Max. burst size (Rx): 0 cells

② Open the register card 'Remote sites' and open the **Name list**. Enter the name of the remote station ❼ and the calling number ❽ select the layer name ❾ and the traffic contract ❶ for this connection.



Name list - New Entry

Name: DRESDEN

Phonenumber: 49241123456

Short hold time: 20 seconds

Short hold time (bundle): 20 seconds

Layer name: PPP

Traffic descriptor: TRAFFIC_1

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

```
set /Setup/WAN-module/Name list DRESDEN
49241123456 * * PPP TRAFFIC_1
```

That's it! All data packets, which are assigned to the 'Dresden' remote station using the settings in the routing table, use the dial-up connection with the 'Traffic_1' traffic contract.

3 Configuration modes

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 set it up.

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 software.

3.1 Many paths lead to the *ELSA LANCOM DSL/25 Office*

In principle, there are different methods of accessing the router of ELSA:

- Through the configuration interface (config interface) on the rear of the router (also known as outband)
- Through the LAN or WAN network (inband)

What is the difference between these?

On one hand, the availability of the units: Configuration via outband is always available. Inband configuration is not possible, however, in the event of a network fault.

On the other hand, whether or not you will need additional software or hardware. The inband configuration requires one of the computers already available in the LAN or WAN, as well as suitable software. In addition to the software, the outband configuration also requires one of the computers (with a serial port) and a suitable configuration cable.

3.2 The direct method: outband

Outband configuration gives you direct access to the router via the configuration interface.

You really only need to use the outband configuration method if you cannot access your device via TCP/IP.

3.2.1 Requirements for outband configuration

What’s needed?

- A computer running Windows 95, Windows 98 or Windows NT 4.0 and *ELSA LANconfig*.

  or

  a computer using any operating system and a terminal program (e.g. Telix or Hyperterminal).

- The configuration cable supplied and, if necessary, the 9/25-pin adapter used to connect the computer and the router (the PCs COM port to the router's configuration interface).

3.2.2 Outband configuration using *ELSA LANconfig*

Start up *ELSA LANconfig* from the Windows Start menu, for instance, by clicking **Start** ▶ **Programs** ▶ **ELSAlan** ▶ ***ELSA LANconfig***. *ELSA LANconfig* will now automatically search for *ELSA LANCOM DSL/25 Office* devices in the local area network (but not on the serial ports). New devices can be found with **Device** ▶ **Find** ▶ **Search all ports**. *ELSA LANconfig* displays new routers in the list by their devices types.

Double-clicking on a device designation in the list of found devices opens the current configuration for editing.

3.2.3 Outband configuration using a terminal program

After starting the terminal program, press return just a few times to automatically detect the bit rate (up to 230 kbps, 38.4 kbps as standard).

Once you have entered the password, configuration can be carried out using any of the commands contained in section 'Configuration commands'.

3.3 The user-friendly method: inband

Using inband configuration allows any computer on the WAN or LAN to access the router. However, access can be restricted or blocked altogether using the IP access list. This configuration requires the use of either telnet (supplied with most operating systems) or *ELSA LANconfig* for Windows. *ELSA LANconfig* is supplied with your device. You can always obtain up-to-date releases from our online media.

3.3.1 Preconditions

TCP/IP or TFTP are used to make configurations using telnet or *ELSA LANconfig*. This means that the TCP/IP protocol must be installed on the computer being used and the router must be given an IP address which you will then use when addressing it.

A device that has not been configured yet will respond to the IP address XXX.XXX.XXX.254, in which the Xs are placeholders for the network address in your LAN. If the computers on your network have addresses such as 192.168.130.1, then you will be able to address the device using 192.168.130.254.

If there is already a computer with the address XXX.XXX.XXX.254 on your network you should assign a new address to the device using the outband configuration method before you install it on the LAN.

3.3.2 Alternatively: address administration with the DHCP server

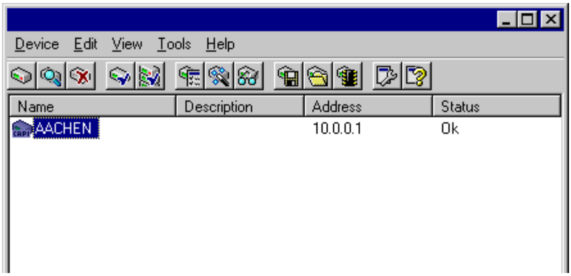
If it is not absolutely essential that you configure the correct IP addresses “manually”, the DHCP server will gladly do this task for you automatically. When using the DHCP server you can have the IP addresses for all computers on the network assigned automatically (see also chapter 'Automatic Address Administration with DHCP'). The router can also establish its own IP address on the LAN.

3.3.3 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.

Just 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
AACHEN		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 pretty much 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.

3.3.4 Configuration using telnet

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

```
telnet 10.1.80.125
```

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.

3.4 Remote access: configuration using a dial-up connection

Configuring routers at remote sites is particularly easy using the remote configuration method via a Dial-up connection. 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.

3.4.1 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 ATM card or a *ELSA LANCOM DSL/25 Office* with *ELSA LANCAPI*

3.4.2 This is how you prepare the remote configuration

① Attach the router to the power supply.

② Connect the device to a WAN basic rate interface.

3.4.3 The first remote connection using a dial-up connection (*ELSA LANconfig*)

① In the *ELSA LANconfig* program select **Device** ▶ **New**, enable 'Dial-up connection' as the connection type and enter the calling number of the WAN interface to which the *ELSA LANCOM DSL/25 Office* 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.

3.4.4 The first remote connection using a PPP client and telnet

① Establish a connection to the *ELSA LANCOM DSL/25 Office* with your PPP client using the following details:

- User name 'ADMIN'
- Password as set on the *ELSA LANCOM DSL/25 Office*, factory default setting is no password
- An IP address for the connection, only if required

② Open a telnet session to the *ELSA LANCOM DSL/25 Office*. 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 DSL/25 Office* 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 DSL/25 Office* 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 DSL/25 Office* remotely just like all other devices.

3.4.5 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]
```

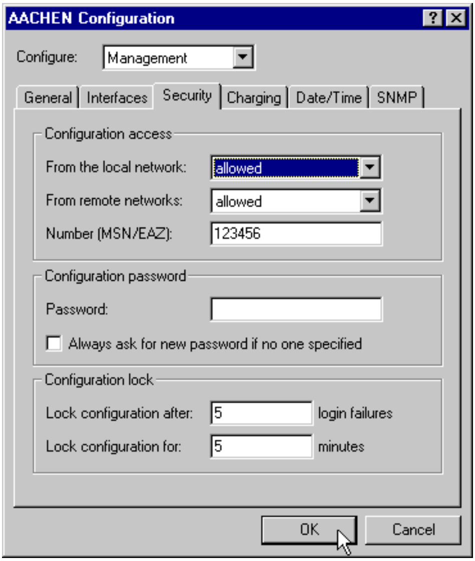
If you wish to block access to the router from the WAN entirely, set configuration access from remote networks to 'denied'.

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:

```
passwd
```

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

3.5 New firmware with 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.

3.5.1 This is how FirmSafe works

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.

3.5.2 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* (recommended)
- 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** ▶ **Upload New Firmware** ▶ **After upload, start the new firmware in test mode**.

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

With TFTP you can use the **writeflash** command to install new firmware. To transmit a new firmware version to a device with the IP address 194.162.200.17, you would enter the following command under Windows NT for example:

```
tftp -i 194.162.200.17 put lcdsl25u.160 writeflash
```

*This command sends the corresponding file to the input IP address using the **writeflash** command. Binary file transfer must be set for TFTP. However, many systems have the ASCII format preset. This example for 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.

3.6 What's happening on the line?

After the basic setup of the devices, further important information can be gained with regard to the parameters still to be modified, especially by observing the data flow on the various ports of the router.

In addition to the device statistics that can be read out during a telnet or terminal session, a variety of other options are also available.

3.6.1 *ELSA LANmonitor*

The *ELSA LANmonitor* includes a monitoring tool with which you can view the most important information on the status of your router on your monitor at any time under Windows operating systems. Many of the internal messages generated by the device are converted to plain text, thereby helping you to troubleshoot.

Installing *ELSA LANmonitor*

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* in your CD drive. If the setup program does not start up automatically after insertion of the CD, start Windows Explorer, click on 'autorun.exe' on the CD *ELSA LANCOM* and follow the instructions in the install program.

During the installation you should activate the 'LANmonitor'.

With ELSA LANmonitor you can only monitor those devices that you can access inband via the local network. Your computer must also have the TCP/IP network protocol installed on it. With this program you cannot access any router connected to the serial interface.

Checking your connection with *ELSA LANmonitor*

① 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**.

② *ELSA LANmonitor* automatically creates a new entry in the device list and initially displays the status of the transfer channels. As soon as the connection is established, a plus sign 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.

3.6.2 Trace outputs

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.

How to start a trace

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
+	Switches on a trace output
-	Switches off 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
PPP	PPP protocol negotiation
IP router	IP routing
IP RIP	IP Routing Information Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
IP-masquerading	Processes in the masquerading module
DHCP	Dynamic Host Configuration Protocol
ATM	Displays defective cells as well as cells which cannot be assigned to a logical connection.
OAM-cells	Displays OAM-cells.
AAL5-frames	Displays the beginning and end of a AAL5-frame.
SSCOP	ATM security protocol
SAAL	Displays AAL5-frames of the signalization layer.

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
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 - time	Switches off the system time output before the actual trace output.

3.6.3 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.

Detailed information on the configuration of ELSA devices with SNMP can be found in the electronic documentation on the CD.

4 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 for your configuration
- Security for your LAN
- ATM connections
- PPP support
- IPX routing
- IP routing
- Automatic address administration with DHCP
- DNS server
- NetBIOS proxy

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

Please refer to the electronic documentation for a detailed description of all parameters and menus.

4.1 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 DSL/25 Office* thus offers a variety of options to protect the configuration.

4.1.1 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.prompt` menu. In this case, the password itself is set with the command `passwd`.

4.1.2 Login barring

The configuration in the *ELSA LANCOM DSL/25 Office* is protected against “brute force attacks” by barring logins. A brute-force attack is the attempt of an unauthorized person to crack a password to gain access to a network, a computer or another device. In order to do so, 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, the access will be barred for a certain length of time.

These parameters apply globally to all configuration options (outband, telnet, TFTP/*ELSA LANconfig* and SNMP). 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`)

4.1.3 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 means telnet or TFTP sessions to configure the *ELSA LANconfig*.

This table is empty by default and so access to the router can therefore be obtained by TCP/IP using telnet or TFTP 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.

4.2 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 DSL/25 Office* offers you various ways of restricting access from outside:

- Access protection using name and password
- Data packet filtering
- IP masquerading (also known as NAT or PAT)

4.2.1 Security check

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 name of the remote station can also be transferred in PPP connections.

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

The name sent by the remote station will be checked for its appearance on the PPP list of user names if the PPP protocol is being used. If the user name is not available, the device name is accepted and verified as the name of the remote station. 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.

No password? The PPP does indeed offer this special 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). This is a form of protection which your device demands 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 DSL/25 Office 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...

And where do a caller's name and password come from?

In PPP connections, the name and password is sent to the remote station during the call establishment, in the Dial-up Networking connection window for example. The device name, password and user name in the PPP list are used if the router establishes the connection itself.

4.2.2 Checking the number

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 DSL/25 Office* is set to provide security using the telephone number, any calls from remote stations with unknown numbers are denied access.

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.

You can use the settings in the name and number list and the selection of the protocol to control the callback action of your router:

- 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 'With name' is set in the name list. Likewise, a unit is charged to the router, if the caller is not identified by means of CLI. On the other hand, the caller incurs no costs if identification of the caller's number is possible and is accepted.

If the router is requested to call back, the Fast Call Back procedure (patent pending) can be used with many other parties. This speeds up the callback procedure considerably.

4.2.3 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 WWW? 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 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”.

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 'TCP/IP' configuration section on the 'Router' tab, or in the `/Setup/IP-router/IP-routing` menu.

For further information, see the 'IP Routing: IP masquerading' section.

4.3 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 online minutes can be restricted to a specific period.

4.3.1 Limiting the number of online minutes

Depending on the provider, the costs for ATM connection are calculated based on time.

The telephone charges can be controlled by limiting the maximum connection time. A time limit within a given period must be set for this purpose. In the router's default state, for example, ATM connections may only be established for a maximum of 210 minutes per week.

When the limit of a budget is reached, all open connections 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!

4.3.2 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

  Duration of the monitoring period in days
- Minutes budget

  The maximum online minutes in a monitoring period
- Spare-units

  Available online minutes remaining in the current period
- Router-units

  Used online minutes by router units over all periods
- Router-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.

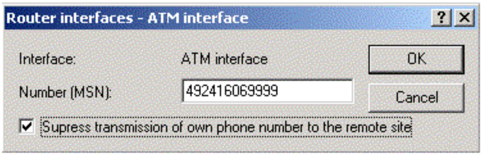
4.4 ATM connections

A *ELSA LANCOM DSL/25 Office* connects networks via ATM fixed connections (PVCs) or ATM dial-up connections (SVCs). In order to provide data transmission via the ATM line, the corresponding parameters must be entered in the router.

4.4.1 Connection settings

Some of the parameters for data transmission in the ATM network are the same for all connections and are only configured once for the connection.

- In the 'Communication' configuration area on the 'General' register card, the calling number (or several calling numbers if necessary) is entered, to which the router should respond. The first calling number entered is used for outgoing calls. In addition, select whether the custom calling number should be displayed at the remote station.



Router interfaces - ATM interface

Interface: ATM interface

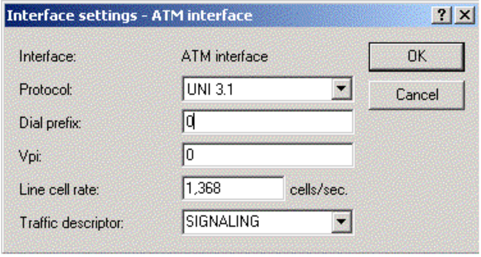
Number (MSN): 492416069999

☑ Supress transmission of own phone number to the remote site

The calling numbers in the ATM network are always entered in the complete international format without the beginning zeros!
Subaddresses can be attached separately to actual calling numbers by a period.

When configuring via telnet, enter these values in the `/Setup/WAN-module/Router-interface-list` menu.

- In the 'Management' configuration area on the 'Interfaces' register card, you will find the **interface settings**. The following values can be entered for the ATM interface.
  - ○ Protocol for the signalization channel
  - ○ A dialing prefix if necessary
  - ○ The number of the virtual connection path (VPI)
  - ○ The physical connection speed (Line Cell Rate LCR)
  - ○ Traffic contract for signalization channel



Interface: ATM interface

Protocol: UNI 3.1

Dial prefix: 0

Vpi: 0

Line cell rate: 1,368 cells/sec.

Traffic descriptor: SIGNALING

When configuring via telnet, enter these values in the `/Setup/WAN-module/Router-interface-list` menu.

The traffic contract established here refers exclusively to the signalization channel during dial-up connections. This setting does not effect the data transmission channels! Traffic contracts can be established in the 'Communication' configuration area on the 'General' register card or via telnet under `/setup/WAN-modul/verkehrskontrakte`*.*

Your provider has provided the values for your ATM connection.

4.4.2 Layer list

With a layer, a collection of protocol settings are defined, which should be used when connecting to specific remote stations. The list of the communication layer is found in the 'Communication' configuration area on the 'General' register card.

In addition to the name which designates the layer, the following values can be entered:

- Encapsulation, either LLC/SNAP or Transparent
- Layer 3 protocol, either PPP or Transparent
- Layer 2 protocol, either SSCOP or Transparent
- Compression of data as an option

Layer 1 protocol is preset securely at value 'AAL-5'.

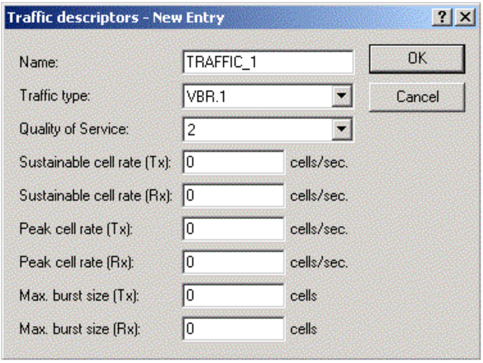
When configuring via telnet, enter these values in the `/Setup/WAN-module/Layer-list` menu.

4.4.3 Traffic contracts

In a traffic contract, the features of an ATM connection are provided on the 'Communication' register card under an available name that can be dialed.These features are as follows:

- Type of traffic contract
  - ○ variable bit rate
  - ○ non-set bit rate
  - ○ constant bit rate
  - ○ ISDN for remote stations in the ISDN network
- The quality of service (0 to 5) is the desired QoS class. The 'Default' entry corresponds to the type which is normally used for the set type of traffic contract.
- The basic part of the transmitted bandwidth (Sustainable Cell Rate, SCR) when sending and receiving data must only be entered for VBR traffic contract types.
- The maximum bandwidth transmitted at peak levels (Peak Cell Rate, PCR) when sending and receiving data must be entered for all traffic contract types except 'ISDN-HDLC-64 KB/s'.
- The length of a SCR transgression in ATM cells (Maximum Burst Size, MBS) when sending and receiving data must only be entered for VBR traffic contract types.

If a '0' value is entered in the Rx fields of SCR, PCR or MBS, the corresponding Tx value is used.



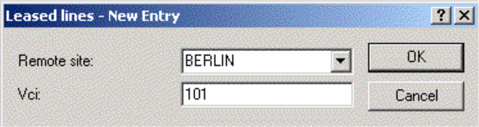
Name: TRAFFIC_1
Traffic type: VBR.1
Quality of Service: 2
Sustainable cell rate (Tx): 0 cells/sec.
Sustainable cell rate (Rx): 0 cells/sec.
Peak cell rate (Tx): 0 cells/sec.
Peak cell rate (Rx): 0 cells/sec.
Max. burst size (Tx): 0 cells
Max. burst size (Rx): 0 cells

Your provider has provided the values for the traffic contracts.

When configuring via telnet, enter these values in the `/Setup/WAN-module/Traffic-contracts` menu.

4.4.4 List of fixed connections

With the entry in the list of fixed connections on the 'Remote site' register card, a connection between a specific remote station and the virtual transmission channel in the ATM network is established.



Remote site: BERLIN

Vci: 101

All other parameters for fixed connections are included by using the remote station name from the corresponding tables.

When configuring via telnet, enter these values in the `/Setup/WAN-module/Fixed-connection` menu.

4.4.5 Name list

With the entry in the name list, a connection between the virtual transmission channel in the ATM network and the protocol layer and traffic contract used during this transmission is established. Designate this assignment which can be indicated in the routing table as a directory for specific data packets from your local network. The name list is located in the 'Communication' configuration area on the 'Remote site' register card.

The name list contains entries with the following parameters:

- Name

  Indicate a meaningful name for the connection. This name can then be selected as 'Router' in the routing table.

- Subscriber number

  The calling numbers in the ATM network are always entered in the complete international format without the beginning zeros!

  With fixed connections, the calling number does not need to be indicated.

- WAN-layer

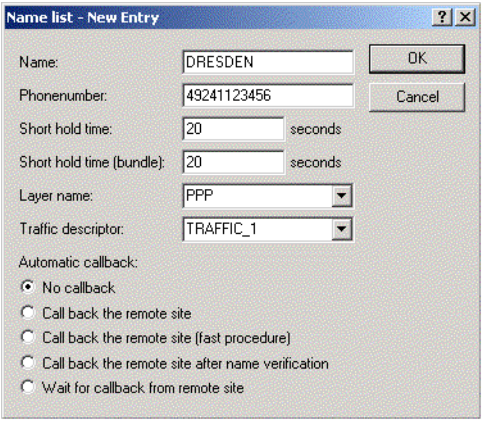
  Select the communication layer which should be used for this connection.

- Traffic contract

  Select the traffic contract which should be used for this connection.

- Automatic callback

  For dial-up connections, you can establish whether and according to which procedure the calling remote station should be called back.



Name list - New Entry

Name: DRESDEN

Phonenumber: 49241123456

Short hold time: 20 seconds

Short hold time (bundle): 20 seconds

Layer name: PPP

Traffic descriptor: TRAFFIC_1

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

When configuring via telnet, enter these values in the `/Setup/WAN-module/Name-list` menu.

4.5 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.

4.5.1 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
- Negotiation of the network protocol to be used over the connection established (IP or IPX, for example). Included in this are any parameters necessary for these protocols, for example IP/IPX addresses. This negotiation runs via the IPCP protocol (IP Control Protocol).
- Verification of the connection through the LCP (Link Control Protocol)

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
- Internet access (when sending addresses)

The phases of 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.
- Network phase

  In *ELSA LANCOM DSL/25 Office*, 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 DSL/25 Office*

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.

4.5.2 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.
Key	Password transferred by your router to the remote site (if demanded). A string of asterisks (*) 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 Windows 95, Windows 98 or Windows NT.
Retr.	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*)!

4.5.3 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.

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 'Retr.' 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'.

4.6 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.

4.6.1 IPX addressing

A complete address in an IPX network consists of three parts: a networknumber, 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.

4.6.2 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.

4.6.3 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'.

4.6.4 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.

4.6.5 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.

4.6.6 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 (third...) 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 (`Setup/IPX-module/LAN-config/RIP-SAP-scal.` connect).

These routes are thus highlighted as reserves when all channels are occupied on the device that is addressed.

4.6.7 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'.

4.6.8 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-router-statistics/Networks`*.*

4.6.9 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.

4.7 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.

4.7.1 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/IP-routing-table`. This, then, is how an IP routing table might look:

IP address	IP netmask	Router name	Distance	Masquerade
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 address and Netmask

  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.

- Masquerade

  Use the 'Masquerade' 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	Distance	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.
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.

4.7.2 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' 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).

These filter tables can be found in the *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Filter' tab, or in the `/Setup/IP-router menu`.

4.7.3 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	Masquerade
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.

4.7.4 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 'IP router' 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.

4.7.5 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:

To take advantage of this function, enable the 'IP RIP' option (in the ELSA LANconfig in the 'TCP/IP' configuration section on the 'Router' 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.

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.

4.7.6 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 2048 **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 can be 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

4.7.7 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 Domain Name Service 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.

4.7.8 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'.

4.8 Automatic 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.

4.8.1 The DHCP server

As a DHCP server, the *ELSA LANCOM DSL/25 Office* can administer the IP addresses in its TCP/IP network. In doing so, it passes the following parameters to the workstation computers:

- IP address
- Netmask
- Broadcast
- 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.

4.8.2 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'.

4.8.3 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 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 Protocol' 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 'Use DHCP for WINS 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 Protocol' 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.

4.8.4 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 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.

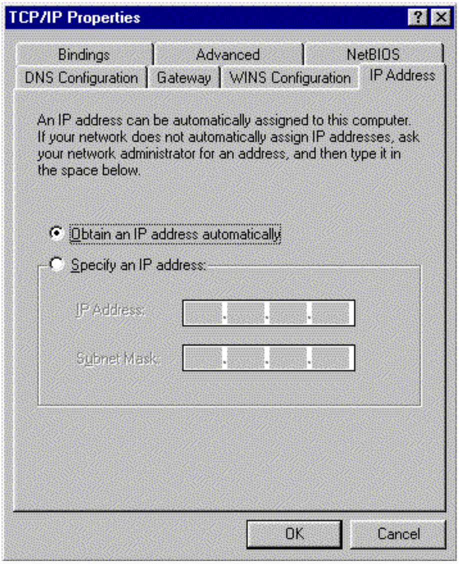
② Switch the device on. It will not find any other DHCP servers in the network and will thus enable its own DHCP functions.

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 automatically' option. Switch over to the 'DNS Configuration' 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).

4.9 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.de' 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.

4.9.1 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 DSL/25 Office*:

- a *ELSA LANCOM DSL/25 Office* 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 Microsoft Networks via NetBIOS, the *ELSA LANCOM DSL/25 Office* 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 DSL/25 Office* 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.

4.9.2 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' tab. To set up the DNS server, proceed as follows:

① Switch the DNS server on.

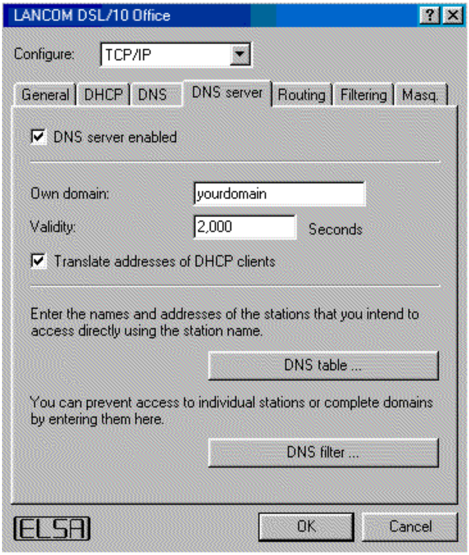
```
set setup/DNS-module/operating on
```

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
```



☑ DNS server enabled

Own domain: yourdomain

Validity: 2,000 Seconds

☑ Translate addresses of DHCP clients

Enter the names and addresses of the stations that you intend to access directly using the station name.

DNS table ...

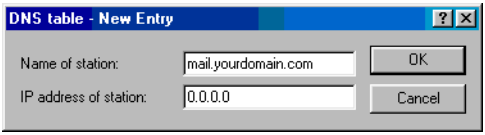
You can prevent access to individual stations or complete domains by entering them here.

DNS filter ...

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:



DNS table - New Entry

Name of station: mail.yourdomain.com

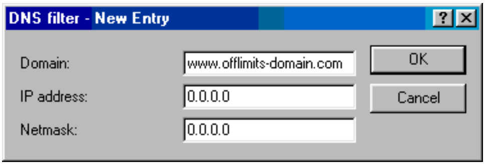
IP address of station: 0.0.0.0

```
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.



DNS filter - New Entry

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.

4.10 NetBIOS proxy

With the NetBIOS proxy function, a *ELSA LANCOM DSL/25 Office* can also route NetBIOS packets or respond locally as a proxy. As a result, it is now possible to economically link Microsoft 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 Microsoft Networks.

4.10.1 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 Microsoft Network, with which several Windows 3.11, 9x and NT workstations can be networked simply by sharing the resources (drives or printers) of the individual computers with the other participants.

In a Microsoft Network, the computers are only addressed via their names. Multiple computers can be organized into groups, and multiple groups can be grouped further as 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 Microsoft Network. If two Microsoft Networks are to be connected using a router, then such a name collection point, a so-called NetBIOS nameserver (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 Microsoft 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 DSL/25 Office* offers such a billboard. The interconnection of Microsoft 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.

4.10.2 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 DSL/25 Office* 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.

4.10.3 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 Microsoft 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 NT 4.0 is similar. Install the following components on all workstations in the Microsoft 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 Microsoft Networks. If multiple Microsoft Networks are to be interconnected using routes, NetBIOS must be based on a ratable protocol in the ELSA LANCOM DSL/25 Office, such as IPA.

  The routing of NetBIOS packets in the *ELSA LANCOM DSL/25 Office* 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 Microsoft Network client is required to permit all of the workstations in the Microsoft 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 Microsoft Networks'.

- Service

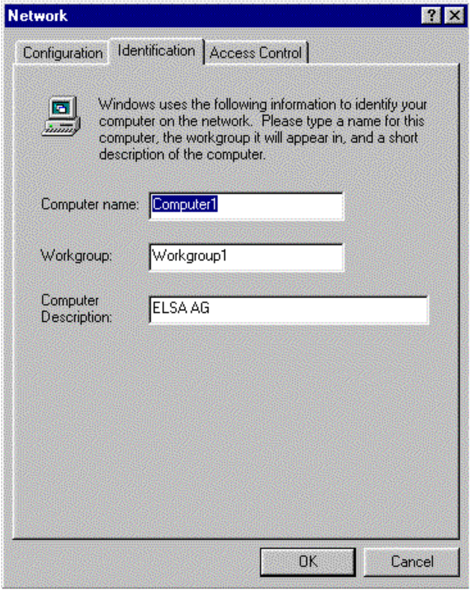
  File and printer sharing permits drives and printers to be shared with other users in the Windows Network.

  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: Computer1

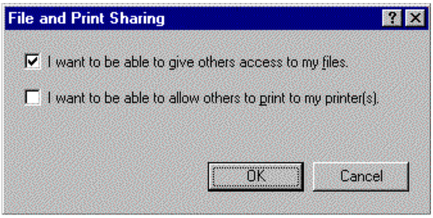
  Workgroup: Workgroup1

  Computer Description: ELSA AG

  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.



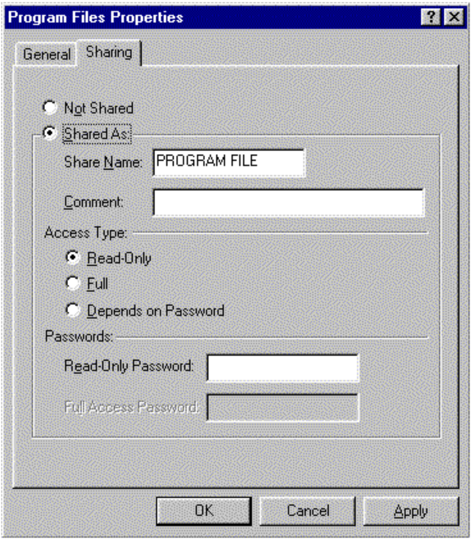
File and Print Sharing

☑ 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.



Program Files Properties

○ Not Shared

● Shared As:

Share Name: PROGRAM FILE

Comment:

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.

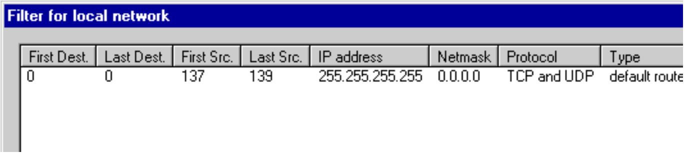
It's easy to check whether the Windows Network settings have been made correctly: the local computer must appear with its name in the Network Neighborhood.

4.10.4 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) 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.

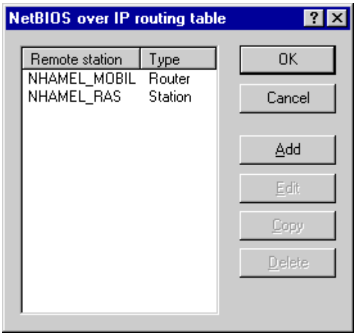
② Check the settings of the IP filter. This filter must capture all NetBIOS packets to be sent over the DEFAULT route to ensure that they do not lead the establishment of a connection on the DEFAULT route. This has been preset in the unit's factory defaults.



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 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 machines.

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.

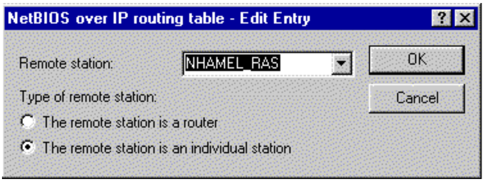
4.10.5 Dial-up procedure for a remote access station

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

① The *ELSA LANCOM DSL/25 Office* 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 DSL/25 Office* (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.

4.10.6 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 DSL/25 Office*. Using telnet, enter

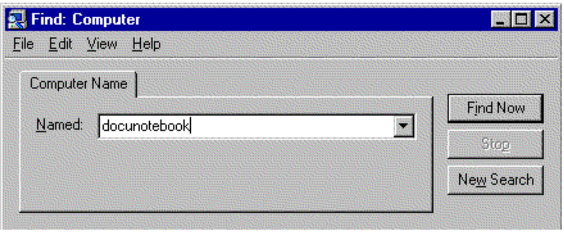
```
dir /Setup/NetBIOS-module/Host-list
```

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

Name	Type	IP address	Remote site	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 DSL/25 Office* 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.

4.11 *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 DSL/25 Office*.

4.11.1 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** ▶ **Control Panel** ▶ **Modems**.

4.11.2 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.

4.12 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.

4.12.1 *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 and EuroFileTransfer. 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 ATM adapters. All you need do is install the office communications software on the individual workstations.

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

Installing the *LANCAPI* client

The *LANCAPI* is made up of two components, a server (in the *ELSA LANCOM DSL/25 Office*) 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* 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* 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.

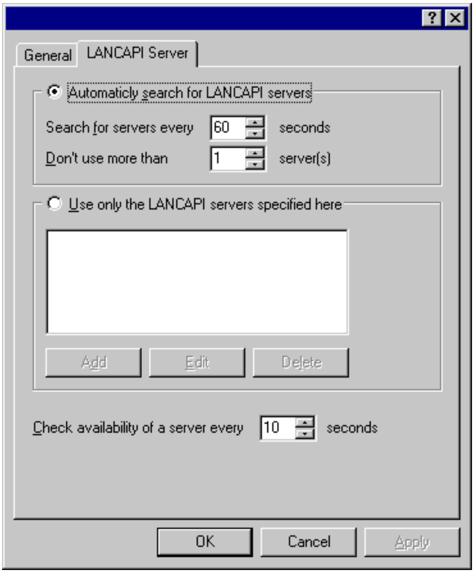
Configuring the *LANCAPI* client

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 DSL/25 Office* 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 DSL/25 Office* 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.



● Automaticly search for LANCAPI servers

Search for servers every 60 seconds

Don't use more than 1 server(s)

○ Use only the LANCAPI servers specified here

Check availability of a server every 10 seconds

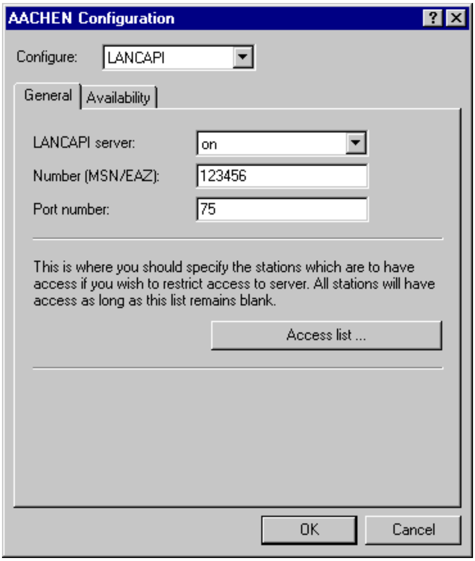
Configuring the *LANCAPI* server

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.

Access list ...

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*.

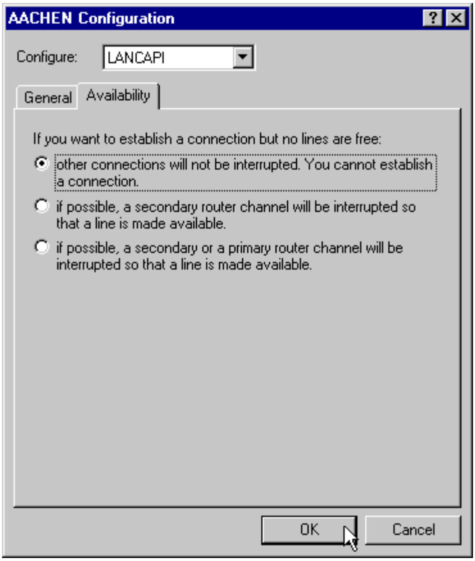
③ When the *LANCAPI* server is activated, enter the call numbers to which the *LANCAPI* should respond in the 'Number' field. You can enter several call numbers separated by semicolons. If you do not enter a call number here, all incoming calls are reported to *LANCAPI*.

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 DSL/25 Office* 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:



AACHEN Configuration

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 can always be established via the *LANCAPI*; 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'.

5 Appendix

5.1 Technical data

Functions	IP router, DHCP server, DHCP client, DNS server, NetBIOS Proxy, IPX router
LAN connection	Ethernet IEEE 802.3, 10/100Base-T (RJ45, node/hub switch), auto-sensing, full duplex operation
Network protocols	**IP:** ARP, PROXY ARP, IP, ICMP, UDP, TCP, TFTP, RIP-1, RIP-2, DHCP, NetBIOS over IP, DNS, PPP over ATM, Classical-IP **IPX:** IPX, SPX, RIP, SAP, Propagate packets
Filter possibilities	Source and target filters for networks, protocols and ports; separate WAN and LAN
WAN interface	Ethernet IEEE 802.3, 10Base-T (RJ45), ATM 25.6F
Charge monitoring	The maximum charge amount (depending on the provider) or connection time can be adjusted in a given time period.
Security and firewall functions	PAP, CHAP and MS-CHAP, PPP authentication mechanisms; filter options in IP mode; protection of configuration using access lists and passwords, IP masquerading; ATM protection mechanisms (CLIP, Callback etc.)
IP masquerading (NAT/PAT)	IP address and port implementation using a single IP address, static/dynamic IP address assignment via PPP or DHCP, masking of TCP, UDP, ICMP, FTP; DNS forwarding; inverse masquerading Intranet IP services such as web server; NetBIOS masquerading
Management	V.24/V.28 outband interface (8-pin mini-DIN), TFTP configuration and firmware upload, SNMP management via SNMP v.1 or v.2, WAN or LAN accesses can be activated separately, diagnosis outputs for protocols and interfaces, diagnosis tools, status display *ELSA LANmonitor*, remote configuration via PPP
Operating security	Hardware watchdogs, regular self-testing, FirmSafe concept for remote software upgrades
Statistics	LAN and WAN packet counters; error, connection and charge counters
Display/operation	LEDs for LAN, WAN and device status
Power supply	12 VA with AC adapter for 230 V, 12 VA
Ambient conditions	Temperature: 5-40°C, humidity: 0-80%, non-condensing
Dimensions and design	Rugged metal case, connections on rear panel; dimensions 158 x 40 x 125 mm (W x H x D)
Package contents	Power adapter, cable for outband interface, ATM line connection cable, LAN twisted-pair cables, complete documentation
Approvals	CE: EN 55022, EN 55024 and EN 60950; T-Nova: 1269510198 and E.000009.07.01
Service Support	Warranty: 6 years Via infoline and Internet

5.2 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 ELSA products is six years. Excepted from this warranty period are ELSA monitors and ELSA videoconferencing systems with a warranty period of 3 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.

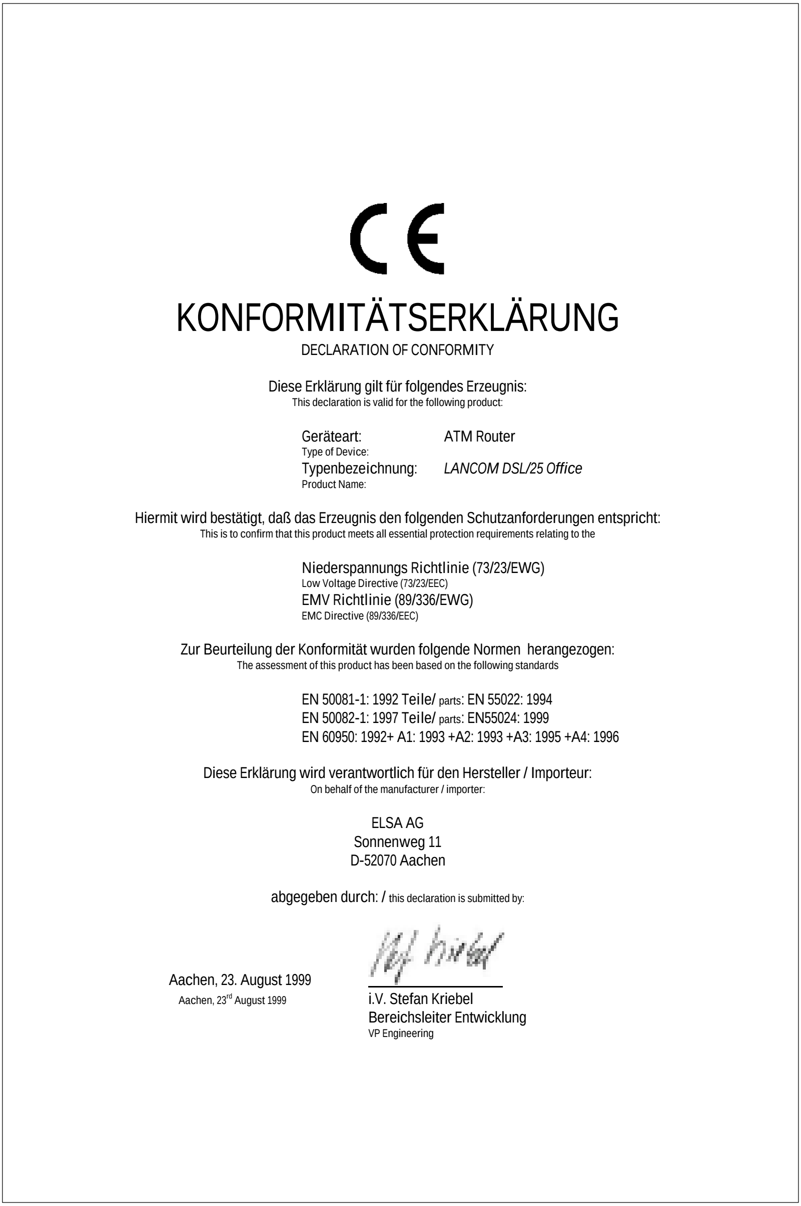
e) In the case that the intentional or culpable negligence of ELSA employees has caused a loss of data, ELSA will be liable for those costs typical to the recovery of data where periodic security data back-ups have been made.

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.

5.3 Declaration of conformity



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:
This declaration is valid for the following product:

Geräteart: ATM Router
Type of Device:
Typenbezeichnung: *LANCOM DSL/25 Office*
Product Name:

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:
This is to confirm that this product meets all essential protection requirements relating to the

Niederspannungs Richtlinie (73/23/EWG)
Low Voltage Directive (73/23/EEC)
EMV Richtlinie (89/336/EWG)
EMC Directive (89/336/EEC)

Zur Beurteilung der Konformität wurden folgende Normen herangezogen:
The assessment of this product has been based on the following standards

EN 50081-1: 1992 Teile/ parts: EN 55022: 1994
EN 50082-1: 1997 Teile/ parts: EN55024: 1999
EN 60950: 1992+ A1: 1993 +A2: 1993 +A3: 1995 +A4: 1996

Diese Erklärung wird verantwortlich für den Hersteller / Importeur:
On behalf of the manufacturer / importer:

ELSA AG
Sonnenweg 11
D-52070 Aachen

abgegeben durch: / this declaration is submitted by:

Aachen, 23. August 1999
Aachen, 23rd August 1999

i.V. Stefan Kriebel
Bereichsleiter Entwicklung
VP Engineering

6 Index