

ELSA LANCOM™ DSL/I-IO Office

© 2000 ELSA AG, Aachen (Germany)

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.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from ELSA. We reserve the right to make any alterations that arise as the result of technical development.

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

20502/0500

Preface

Thank you for placing your trust in this ELSA product.

By selecting the *ELSA LANCOM DSL/I-10 Office* you have chosen a router which you can use to connect local area networks or single workstations to the Internet via an xDSL connection. It makes it possible for you to surf the Internet at previously unknown speeds. You can now surf the Internet twelve times faster than over a single B channel in the ISDN network—and parallel calling over two lines is always possible!

Documentation

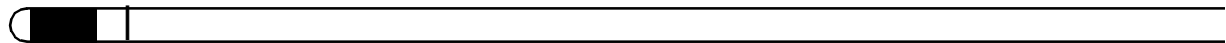
The accompanying documentation comprises:

- Manual
Hardware installation, description of functions and operating modes and examples of configurations
- CD containing electronic documentation
Basic technical information (e.g. on ADSL, 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

Introduction	1
What does a router do?	2
What does the <i>ELSA LANCOM DSL/I-10 Office</i> offer?	4
Installation	9
Package contents	9
System preconditions	9
Setting up the computer	10
Windows 95 and Windows 98	10
Windows NT 4.0	11
Introducing the <i>ELSA LANCOM DSL/I-10 Office</i>	13
The front of the unit	13
The back of the unit	15
How to connect the device	16
Software installation	17
Configuration	17
Basic settings	17
<i>ELSA LANconfig</i>	19
Setup online access	21
Configuration modes	25
Many paths lead to the <i>ELSA LANCOM</i>	25
The direct method: outband	25
Requirements for outband configuration	26
Outband configuration using <i>ELSA LANconfig</i>	26
Outband configuration using a terminal program	26
The user-friendly method: inband	26
Preconditions	27
Alternatively: address administration with the DHCP server	27
Configuration using <i>ELSA LANconfig</i>	27
Configuration using telnet	28
Remote access: configuration using a Dial-Up Network	28
This is what you need for remote configuration	28
This is how you prepare the remote configuration	29
The first remote connection using a Dial-Up Network (<i>ELSA LANconfig</i>)	29
The first remote connection using a PPP client and telnet	29
Limiting remote configuration	30
New firmware with FirmSafe	31
This is how FirmSafe works	31
How to load new software	32

What's happening on the line?	33
<i>ELSA LANmonitor</i>	34
Trace outputs	35
Configuration using SNMP	37

Operating modes and functions 39

Security for your configuration	39
Password protection	40
Login barring	40
Access control via TCP/IP	40
Security for your LAN.....	41
Security check	41
Callback	42
The hiding place—IP masquerading (NAT, PAT)	43
Call charge management.....	43
Limiting the number of online minutes for DSL connections	44
Charge-based ISDN connection limits.....	44
Time-dependent ISDN connection control	44
Settings in the charge module.....	45
xDSL connections.....	46
DSL name list.....	47
ISDN connections	48
ISDN name list.....	49
Interface settings	50
Router interface settings	50
LANCAPi interface settings	51
Layer list.....	52
Round-robin list.....	52
Script	53
Call acceptance.....	53
Number list	54
Point-to-point protocol.....	54
The protocol	54
The PPP list	56
Everything OK? Checking the line with LCP.....	57
Assigning IP addresses via PPP	57
Callback functions.....	58
Channel bundling with MLPPP.....	61
IPX routing.....	63
IPX addressing	63
Information on LAN.....	63
IPX routing table	64
What happens during data transmission in the IPX network?	65

RIP and SAP tables	65
There are so many routers here.....	66
Redundant routes.....	66
Exponential backoff	66
IPX packet filters	67
IP routing	69
The IP routing table.....	69
TCP/IP packet filters	71
Proxy ARP	72
Local routing	73
Dynamic routing with IP RIP	73
IP masquerading (NAT, PAT).....	76
DNS forwarding	78
Time control setting for the default route	79
Policy-based routing	79
Automatic address administration with DHCP	80
The DHCP server	80
DHCP – 'on', 'off' or 'auto'?	81
How are the addresses assigned?.....	81
Configuring the DHCP server	84
DHCP relay agent.....	86
Network configuration transmitted via ISDN	86
Acquiring DHCP information from the remote network	87
Adapting DHCP information.....	87
Obtaining boot images from the remote network	88
DNS.....	88
What does a DNS server do?	88
Setting up the DNS server	89
NetBIOS proxy.....	91
To the point: What is NetBIOS?	92
Handling of NetBIOS packets	92
Which preconditions must be fulfilled?.....	93
Linking two Windows Networks via ISDN	96
Dial-up procedure for a remote access station	97
Search and find: the Network neighborhood	98
The least-cost router.....	99
<i>ELSA CAPI Faxmodem</i>	104
Installation	104
Faxing with the <i>ELSA CAPI Faxmodem</i>	104
Office communications and <i>LANCAPI</i>	104
<i>The ELSA LANCAPI</i>	104
Reserving B channels.....	109
Accounting	109

Configuring accounting	110
Reading the accounting data	111
<hr/>	
Appendix	113
Technical data.....	113
Declaration of conformity	115
Warranty conditions	115
<hr/>	
Index	119

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.

The *ELSA LANCOM DSL/I-10 Office* gives you a router that has been specially developed for xDSL terminals.

ELSA LANCOM DSL/I-10 Office can connect individual workstations or entire local networks to the Internet. It makes it possible for you to surf the Internet at previously unknown speeds. You can now surf the Internet at speeds up to 768 Kbps and that is twelve times faster than over a single B channel in the ISDN network. The special thing about it: since data and other signals such as language are transmitted over the same cable line. Parallel calling and faxing are also possible because they are run on separate lines and do not affect one another.

A *ELSA LANCOM DSL/I-10 Office* also provides all functions of an ISDN router by means of an integrated ISDN interface.

Special highlights:

- ISDN-backup: In case the xDSL connection becomes distorted, the router automatically establishes a backup connection over the ISDN line, thus providing additional security for data transmission.
- ISDN remote configuration: It is also possible to easily monitor the devices at various operating sites from a central location with remote configuration via ISDN.
- Office communications using *LANCAP!* Normal ISDN applications such as remote access or faxing using a *ELSA LANCOM DSL/I-10 Office* can also be carried out with the integrated *LANCAP!*

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.

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.

For example, this is available in the form of a xDSL connection, which can be transmitted via normal copper telephone lines. An ISDN connection with a full-functioning ISDN router, the functions of *LANCAPi*, and as a backup for the xDSL connection is also possible with a *ELSA LANCOM DSL/I-10 Office*.

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.

In addition, the ISDN connection can be used to create network bindings (IP, IPX) and develop remote-access services for fieldworkers.

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.

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* 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.

What does the *ELSA LANCOM DSL/I-10 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* to the power supply.
- Establish a link to the LAN.
- Connect to the xDSL terminal.
- Plug in the ISDN 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/I-10 Office* can be connected to the Ethernet interface of an xDSL connection.

Furthermore, the *ELSA LANCOM DSL/I-10 Office* is connected to the S_0 interface(s) of an ISDN Basic Rate Interface in point-to-multipoint configuration (multi-device terminal) or in point-to-point configuration (system terminal). The router automatically detects your port type and the D-channel protocol being used.

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 through a Web browser, telnet or any other terminal program.

This means that you can access the device from the WAN (via ISDN), 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

Along with password protection and call number recognition (CLIP), the router offers protection against unauthorized access to the company network by means of a callback function which only permits a connection to be established to previously defined ISDN telephone numbers only. Authentication mechanisms in PPP, Firewall filters and IP masquerading complete the security concept. 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 Internet usage 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/I-10 Office*.

Subscribing to "Advice of charge during connection" on the ISDN network (AOCD) allows you to set the charge units available for a specified period for the ISDN connection. This puts you in constant control of your phone bill.

If charge information is not available from your ISDN connection, you can also limit the active ISDN connect time for a specified period. The router will not permit the active establishment of connections once this time has elapsed.

Least-cost routing

Even if there is a large selection of telecommunications service providers you can always use the cheapest ISDN lines using the least cost router.

You define once which providers have the most favorable charges for your purposes, and the router automatically selects the most economical provider for you, regardless of whether you are using the router or the *LANCAPi*.

Automatic time check

In order to generate sound statistics and to select the correct connection paths using the least cost router, the device always must have the exact time. It can read the time from the ISDN network itself. The router's internal time is always compared to ISDN time either each time a connection is established or each time the device is switched on. Of course, the time can also be set manually.

Channel bundling and compression

The device supports static and dynamic channel bundling via MLPPP and BACP on the ISDN line. Stac data compression (hi/fn) can be used to achieve increases in the data transfer rate of up to 400%.

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.:

- Connection status for each B transfer channel
- Name of the remote side
- The connected unit module (router, *LANCAPi*)
- 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 xDSL, ISDN 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/I-10 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 LANCAP and ***ELSA CAPI Faxmodem***

The main advantages of using *LANCAP* are economic. The *LANCAP* 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 *LANCAP* 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 ISDN adapters or modems. 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 *LANCAP*, the PC forwards the fax via the network to the router which establishes the connection to the recipient.

The *ELSA CAPI Faxmodem* furthermore provides a Windows fax driver (fax class 1) as an interface between the *ELSA LANCAP* and applications, permitting the use of standard fax programs with an *ELSA LANCOM DSL/I-10 Office*.

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. If 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.

Accounting

Most data transfers through the router from ELSA take place via dial-up connections, where the charges are calculated based on the online time, or via static connections, where the charges are calculated based on the transferred data volume. Only a small portion of users use true leased-line connections with flat-rate charging.

For many users it is important to determine which of the immediate LAN computers use the connection to the router the what charges they incur.

With its accounting feature, *ELSA LANCOM DSL/I-10 Office* offers the ability to breakdown online times and data transfer volumes based on the individual computers that use the connections. This allows you to determine the incorrect configuration of the computer or router quickly and allocate the resulting expenses to their appropriate causes.

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.

Package contents

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

- *ELSA LANCOM DSL/I-10 Office*
- Power supply unit
- LAN connection cable
- xDSL connection cable
- ISDN 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.

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

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.

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 automatically**. 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.

Windows NT 4.0

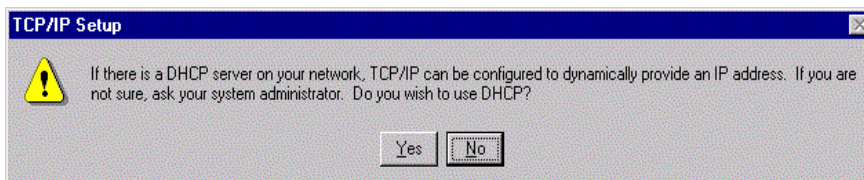
Using Windows NT 4.0 as an example, this section will show what needs to be done, if it is not already done for you, to ensure smooth communication between computers in a TCP/IP network with the router connected to the workstations.

- 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)

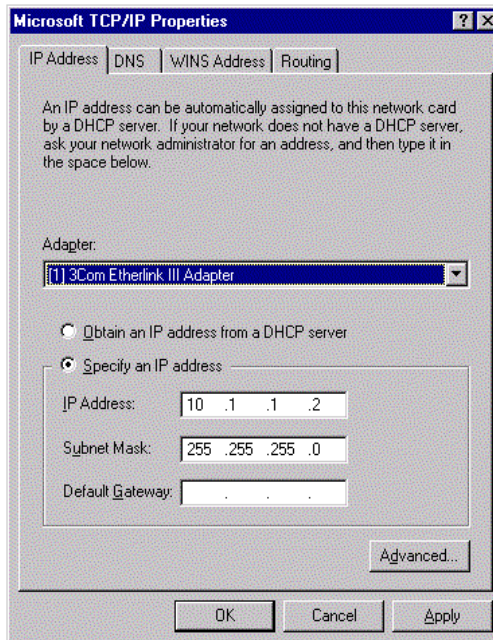
If you are going to use the router as a DHCP server, set the workstations to obtain IP addresses automatically. To do so, select **Yes** when completing the network protocol installation.



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

- Setting fixed IP addresses (not using DHCP)

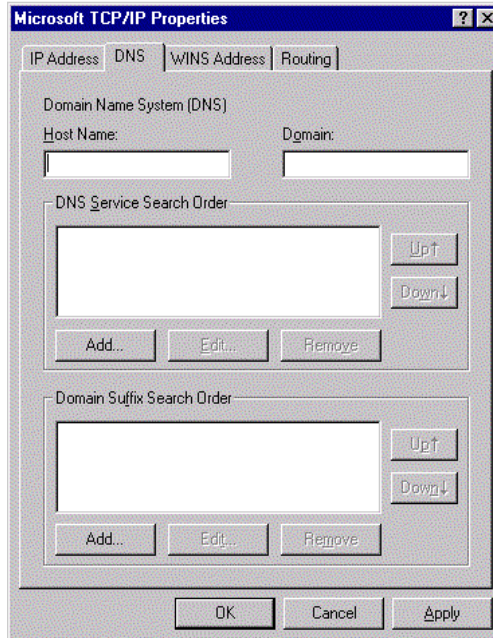
If you are not going to use a DHCP server on your network, assign the workstations fixed IP addresses: **Start ► Settings ► Control Panel ► Network ► Protocols ► Properties...** This page also lets you set the standard gateway.



Assign unique IP addresses, for example taken from a reserved range of addresses. For example, the workstations can be assigned addresses 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 '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

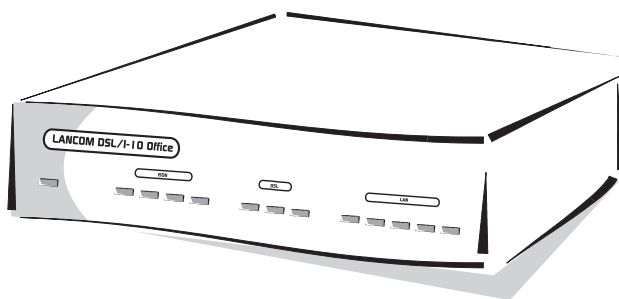
Under Windows NT 4.0 you can query the current IP configuration of your computer with **Start ► Run... ► ipconfig**. This shows you which IP address was assigned to the computer by the DHCP server and which addresses have been specified for the gateway (not for the DNS server).

Introducing the **ELSA LANCOM DSL/I-10 Office**

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

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
red	inter.	Error message or a charge block prevents outgoing calls

S₀ status

This LED shows the status of the S₀ connection:

Off		Not connected or no S ₀ voltage (often, the S ₀ voltage is disabled at ISDN connections after certain length of inactivity)
green	flashing	Initializing (establishing contact with the connection point)
green		Operational (S ₀ bus activated, TEI exists and D channel protocol checked)
green	Power off	LED is on, but power LED is off: unit in boot monitor

*WAN
Chan1
Chan2*

These LEDs indicate the status of the corresponding logical ISDN-WAN channels (in both router and CAPI modes):

Off		Channel idle
red	flashing	Incoming call pending
green	flashing	Outgoing call being executed
red		Channel is physically established/protocol negotiation in process
green		Corresponding protocol negotiation (X.75, PPP, etc.) completed; channel is logically online
green/red	short red flashes (duration approx. 1/10 s)	Indicate a received data packet



The ISDN-WAN channels do not have any fixed assignments to B channels!



The connection is active and incurring charges so long as the 'Chan1' or 'Chan2' LED is green!

*WAN
Chan 1+2*

This LED indicates whether the current ISDN connection is a static or dynamic channel bundling.

Off	no connection or no bundle connection active
green	static or dynamic bundle connection active

- DSL-Rx/Tx* This yellow LED shows that data is moving on the DSL connection.
- DSL-Link* This green LED shows that the Ethernet connection between *ELSA LANCOM DSL/I-10 Office* and the DSL terminal is operating properly.
- DSL-Chan* This LED shows the status of the DSL connection to the switching center:

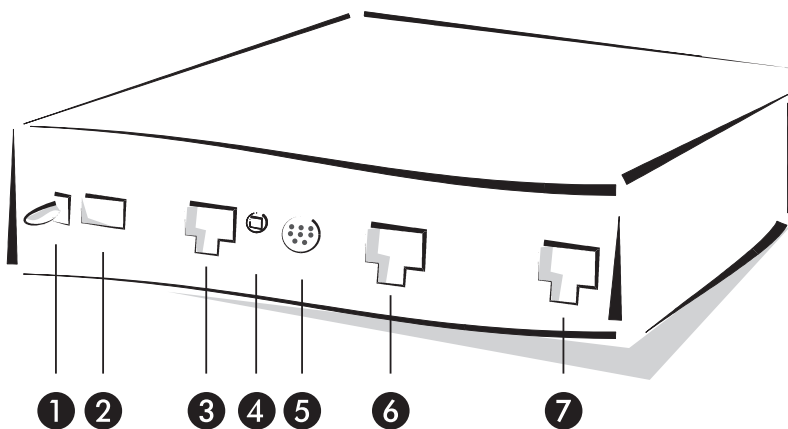
Off	<i>ELSA LANCOM DSL/I-10 Office</i> has not requested a login at the switching center
red	<i>ELSA LANCOM DSL/I-10 Office</i> has requested a login at the switching center; it is logging in
green	It has successfully logged in and is connected to the DSL network.



The connection is active and incurring charges so long as the 'DSL-Chan' LED is green!

The back of the unit

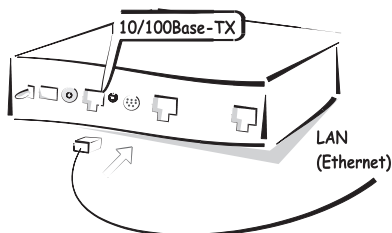
Now turn the whole thing around and take a look at the rear. Beginning again on the left-hand side, you have:



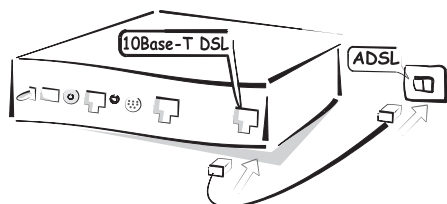
- ❶ On/off switch
- ❷ Connection for power supply unit
- ❸ 10/100Base-Tx for 10 Mbit or 100 Mbit networks (green, yellow)
- ❹ Node/hub selector switch
- ❺ V.24 configuration interface
- ❻ ISDN S_0 port (light blue)
- ❼ 10Base-T DSL connection (dark blue)

How to connect the device

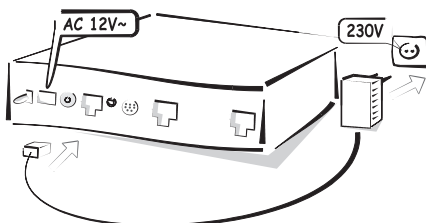
- ① Connect your *ELSA LANCOM DSL/I-10 Office* to the LAN. Plug the network cable (supplied) into the 10/100Base-TX terminal of the device and into a free network connector on your local network (or into a free socket on a hub in your LAN).



- ② Connect your *ELSA LANCOM DSL/I-10 Office* to the ISDN network. To do so, connect the supplied ISDN line connection cable to the ISDN/S₀ terminal on the unit and to an ISDN/S₀ multi-device terminal or system terminal (point-to-multipoint or point-to-point configuration).
- ③ Connect your *ELSA LANCOM DSL/I-10 Office* to the xDSL network. Plug the xDSL connection cable provided in the 10Base-T-DSL connection of the device and in the Ethernet interface of the xDSL modem (also called NTBBA).



- ④ 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.

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. With other operating systems, you can use an HTML browser to carry out the configuration.

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 CD *ELSA LANCOM* and follow the instructions in the install program.

Configuration

This example shows a simple LAN to Internet link.

Configure the unit using the following steps:

- Basic settings
- Setup online access

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.

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.

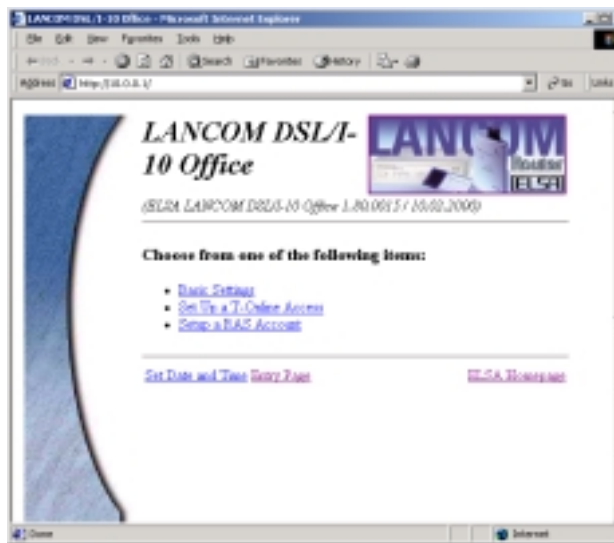
HTML browser

If you do not wish to or cannot use *ELSA LANconfig* (e.g. because you have installed a different operating system), you can also make the basic settings with a regular HTML browser.

- ① Start your browser.
 - If you do not yet have a DHCP or DNS server on your LAN, the router reacts to any address that you specify in the address field. Since most browsers call a specific page by default, in most cases the browser will display the startup screen of the router configuration utility.
If the default page for your browser is a blank page, enter any name in the

address field (such as 'ELSA LANCOM DSL/I-10 Office'). The startup page will appear automatically.

- If you already use a DHCP server or work with fixed IP addresses on your LAN, enter the address as 'x.x.x.254' in the browser's address field, where 'x.x.x' stands for the currently configured range of addresses.



If you do not know whether IP addresses have been used in your network, first click under Windows 95 or Windows 98 on **Start ► Run**, enter the following command in the window `winipcfg` and confirm with **OK**. Select your network adapter in the following window. If the 'IP Address' field contains the value '0.0.0.0', the network adapter does not have an IP address yet.



In Windows NT you can check IP addresses with the command `ipconfig`.

- ② Select 'Basic Settings'.
- ③ Enable the 'Specify IP parameters automatically' option 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 LAN.

or

 - You do not wish to use IP addresses, perhaps because you have a Windows-only network.
- ④ Disable the 'Specify IP parameters automatically' option 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 new device 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 new device a free address from the previously used address range, and select whether the device 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.

- ⑤ Enter a password for access to the unit and choose whether to use it as a DHCP server on your LAN.



Disable 'Automatically configure workstations via DHCP' only if you want to use IP addresses on your network or already use another DHCP server. The functions of the DHCP server are described later in this manual.

- ⑥ For every S₀ bus, specify a phone number to which the router is to react, as well as the prefix for external calls if you connect your router to a PBX.

Also specify here whether charge information will be sent to your ISDN connection.

If you leave the field for the phone number blank, the router will react to all phone numbers that are valid for this connection.

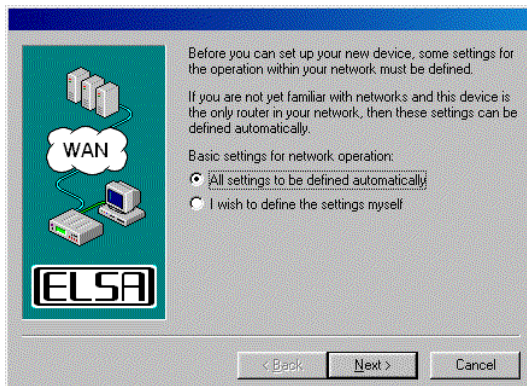
With these settings, you have completed making your new router known on the local network. The router itself is addressable using the IP address of '10.0.0.1'. After you reboot your system, all units on the local network will be assigned IP addresses by the DHCP server in the router. It will use an address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

The unit reacts only to the phone numbers of calls from the ISDN network that you have entered for each S₀ bus.

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 ► ELSAan ► ELSA LANconfig**.



- 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.*



In Windows NT you can check IP addresses with the command `ipconfig`.

- 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

If you do not wish to or cannot use *ELSA LANconfig* or a HTML browser (e.g. because you have installed a different operating system without browser), you can also make the basic settings over a telnet connection.

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 10.0.254` 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.

Setup online access

To configure Internet access via T-Online, use the wizards provided for both the *ELSA LANconfig* and HTML browsers, which really make the configuration very easy.

HTML browser

- ① Launch your browser and enter the IP address of the unit, which you configured in the Basic Settings section in the address field. If you did not specify an IP address while carrying out the basic settings, the address is '10.0.0.1'.
- ② Select 'Online access setup' entry.

- ③ Enter the access data which you have received with your online registration in the following window.

- ④ Select whether a backup connection via an ISDN line should be established in case of technical difficulties with the xDSL connection. In this case, enter the calling number with which online access can be reached.



The default calling number for online access via ISDN is '0191011'. You may change the default setting if you are unable to reach online access with this calling number!

ELSA LANconfig

- ① Start *ELSA LANconfig* with **Start ► Programs ► ELSAan ► ELSA LANconfig**.
- ② Mark your *ELSA LANCOM DSL/I-10 Office* in the list of devices and call the wizards.
- ③ Select the wizard for the Internet access and then the option for the online access.



- ④ Enter the access data which you have received with your online registration in the following window.



- ⑤ Select whether a backup connection via an ISDN line should be established in case of technical difficulties with the xDSL connection. In this case, enter the calling number with which online access can be reached.



The default calling number for online access via ISDN is '0191011'. You may change the default setting if you are unable to reach online access with this calling number!

That's it!

By clicking a few buttons, you have completed the configuration of the unit for Internet access through an xDSL connection. All of the computers on your LAN that obtain their own IP addresses and the IP addresses for the gateway through the DHCP server from their *ELSA LANCOM DSL/I-10 Office* can now surf the Internet at full performance.

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.

Many paths lead to the *ELSA LANCOM*

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)
- Through a PPP connection via a dial-up line or similar (remote configuration)

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. Remote configuration is also dependent on the transfer medium, such as the ISDN connection.

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. Remote configuration requires a computer with a PPP client, ISDN card or terminal adapter. The easiest method to use is remote configuration using a dial-up connection and *ELSA LANconfig*.

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.

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

Outband configuration using *ELSA LANconfig*

Start up *ELSA LANconfig* from the Windows Start Menu, for instance, by clicking **Start ► Programs ► ELSA LAN ► ELSA LANconfig**. *ELSA LANconfig* will now automatically search for *ELSA LANCOM* 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 device types.

If your device is new and has not yet been configured at the configuration interface, you can call up various configuration tools with **Tools ► Setup Wizard**. Select one of the wizards offered and simply answer its questions. This will then set up your *ELSA LANCOM* for the task selected.

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

Outband configuration using a terminal program

After starting the terminal program, press return 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'.

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.

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.

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').

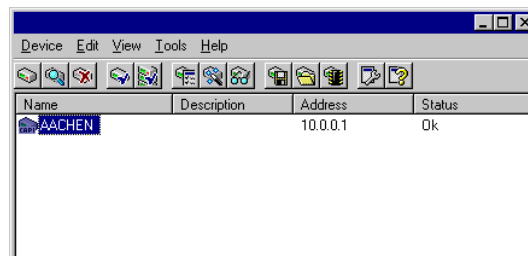
Configuration using *ELSA LANconfig*

Start *ELSA LANconfig* e.g. via the Windows taskbar with **Start ► Programs ► ELSAlan ► ELSA LANconfig**. *ELSA LANconfig* searches the local area network for devices.



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.



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.

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.

Remote access: configuration using a Dial-Up Network

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

This is what you need for remote configuration

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

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.

The first remote connection using a Dial-Up Network (*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* 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 *LANCAP*) 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 Network connection is broken.

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

The first remote connection using a PPP client and telnet

- ① Establish a connection to the *ELSA LANCOM* with your PPP client using the following details:
 - User name 'ADMIN'
 - Password as set on the *ELSA LANCOM*, factory default setting is no password
 - An IP address for the connection, only if required
- ② Open a telnet session to the *ELSA LANCOM*. 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* 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* 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* remotely just like all other devices.

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'.

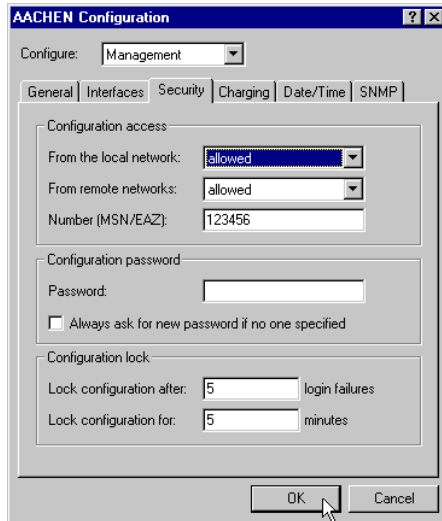
- ③ In the 'Configuration access' field, enter a calling number of your connection which is not used for other purposes as the calling number.

Alternatively, enter the following command:

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

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





Alternatively, enter the following command:

```
passwd
```

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

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.

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.

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. *Telnet* 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 *Telnet*, 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 **writelflash** 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 lc_di10u.180 writelflash
```

*This command sends the corresponding file to the input IP address using the **writelflash** 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.

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.

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* CD 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 *ELSA LANCOM* CD 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.

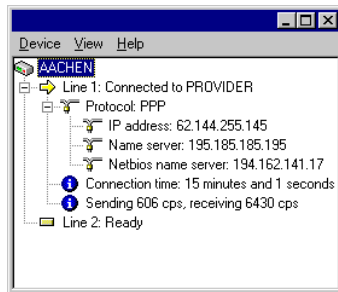
Checking your internet connection with *ELSA LANmonitor*

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

- ① So you should setup the router to connect to your provider, e.g. with the *ELSA LANconfig* Setup Wizard.
- ② Start up *ELSA LANmonitor* by clicking **Start ► Programs ► ELSAlan ► LANmonitor**. Generate a new device by selecting **Device ► New** and, in the following window, enter the IP address of the router you wish to monitor. If the configuration of the device is protected by password, enter the password too.

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

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



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

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

- ④ To break the connection manually, click on the active channel with the right mouse button. You may be required to enter a configuration password.
- ⑤ If, in addition to the information in the *ELSA LANmonitor* device list, you wish to see a minimized status window in the form of an LC display, right-click on the name of the device and select **Line Display**.

Right-click on the line display area to configure this virtual display to remain in the foreground on your monitor.

- ⑥ If you would like a log of the *ELSA LANmonitor* output in file form, select 'Options' from the 'View' menu and go to the 'Log' tab. Enable logging and specify whether *ELSA LANmonitor* should create a log file daily, monthly, or on an ongoing basis.

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
ELSA	ELSA protocol negotiation
PPP	PPP protocol negotiation
IPX-router	IPX routing
RIP	IPX Routing Information Protocol
SAP	IPX Service Advertising Protocol
IPX-watchdog	IPX watchdog spoofing
SPX-watchdog	SPX watchdog spoofing
NetBIOS	NetBIOS management
IP router	IP routing
IP RIP	IP Routing Information Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
SCRPT	Script negotiation
IP-masquerading	Processes in the masquerading module
DHCP	Dynamic Host Configuration Protocol
D-channel	Trace on the D channel of the connected ISDN bus

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

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

Examples

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

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.

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
- Charge management
- xDSL connections
- ISDN connections
- PPP support
- IPX routing
- IP routing
- Automatic address administration with DHCP
- DHCP relay agent
- DNS server
- NetBIOS proxy
- Least-cost router
- *ELSA LANCAPI*
- Time control
- Reserving B channels
- Accounting

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.

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/I-10 Office* thus offers a variety of options to protect the configuration.

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`.

Login barring

The configuration in the *ELSA LANCOM DSL/I-10 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, run 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 log in can be set. If this limit is reached, 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`)

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.

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 computers. The *ELSA LANCOM DSL/I-10 Office* offers you various ways of restricting access from outside:

- Access protection using name, password and call number
- Callback to defined call numbers
- Data packet filtering
- IP masquerading (also known as NAT or PAT)

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

When using the ELSA or PPP layer on the B channel, the name of the calling party can also be transmitted. This requires a connection to be established first, since the name cannot be transferred over the D channel.

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 name list if the ELSA protocol is being used.

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 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?

If you are using the ELSA protocol for the B channel, identification is, in fact, made by name only and without a password. The device name of the router making the call is used as the name.

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.

Checking the number

When calling via an ISDN line, in most cases the caller's number is transmitted via the D channel even before a connection is established (CLI—Calling line identifier).

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

Protection by call number can be used with all B channel protocols (layers).

Callback

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

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

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

And all the while you can use the settings to dictate how the cost of the connection is to be apportioned. The router accepts all unit charges, except for the unit required to send the name, if call back '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.

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 IP address can be fixed or assigned dynamically by the provider. The computers in the LAN then use the router as a gateway so that they themselves cannot be detected. To do this, the router separates Internet and Intranet, as if by a wall. Therefore, IP masquerading is also called a "firewall function".

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.

Call charge management

The capability of the router to automatically establish connections to all required remote stations 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.
- The available ISDN connection charges can be restricted to a specific period.

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

Limiting the number of online minutes for DSL connections

Although DSL has the characteristics of a leased line that does not require the establishment of a connection (so that neither the beginning nor the end of a connection are identifiable), the charges for a xDSL connection may be billed by the provider on the basis of time.

The telephone charges can be controlled by limiting the maximum connection time. A time limit for DSL connections within a given period must be set for this purpose. In the router's default state, for example, connections may only be established for a maximum of 600 minutes per week.



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

It's not necessary to change the time limit if you need a bigger online budget for a single action, such as downloading a large file from the Internet. You can establish an additional limit that can be enabled separately for occasions such as this. Enter the following command during a telnet connection:

```
/setup/charges-module/do spare-minutes
```

This will enable the additional limit for the current period. The normal time limit will once again apply during the next period.

Charge-based ISDN connection limits

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



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



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

Time-dependent ISDN connection control

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

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



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

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



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

Settings in the charge module

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

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

- Day(s)/Period
The duration of the monitoring period in days can be specified here.
- Budget units, ISDN minutes budget
The maximum number of ISDN units or ISDN online minutes in a monitoring period
- Spare units, spare ISDN minutes
Available ISDN units or ISDN online minutes remaining in the current period
- Router units, router ISDN minutes
ISDN units or ISDN online minutes over all periods
- DSL minutes budget
The maximum DSL online minutes in a monitoring period

- Reserve DSL budget
Additional DSL online minutes, which can be activated for the current monitoring period.
- Spare units, spare DSL minutes
Available DSL online minutes remaining in the current period
- Router DSL units
DSL online minutes over all periods
- Router units
All charges incurred through the unit
- Table-budget, time-table
Tables with charges or times for the respective modules

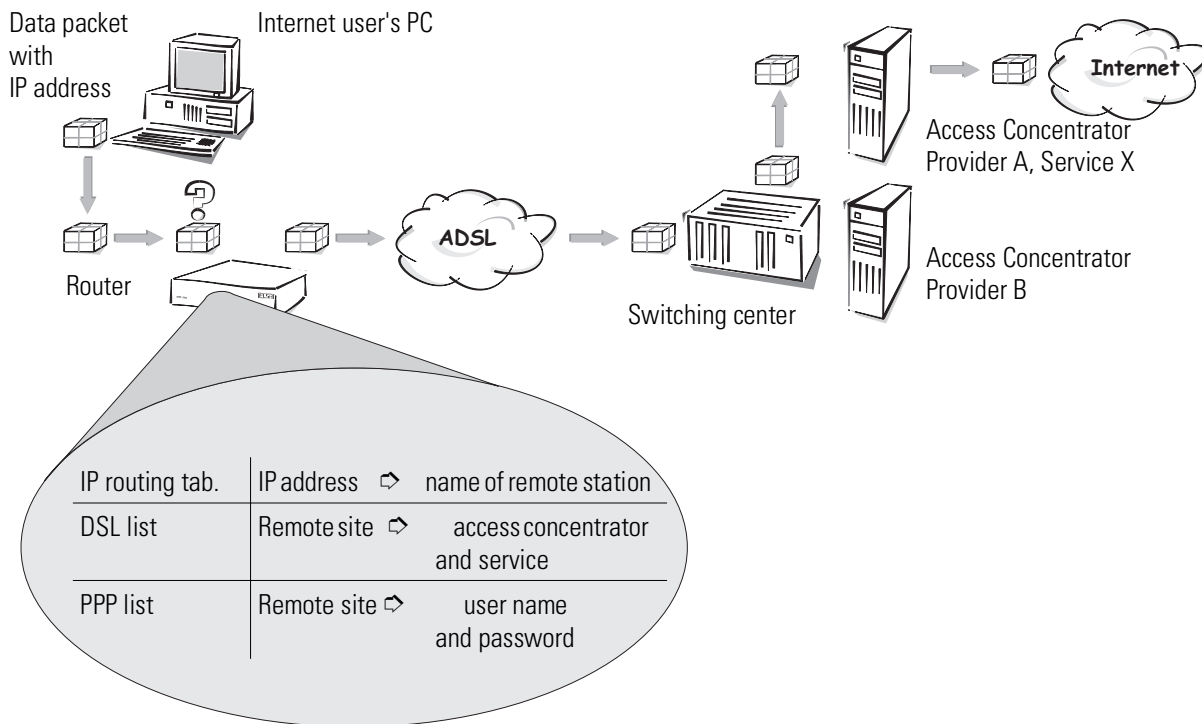


The current charge and connect-time information is retained when rebooting (e.g. when installing new firmware) is not lost until the unit is switched off. All of the time values indicated here are in minutes.

xDSL connections

Data communications between *ELSA LANCOM DSL/I-10 Office* and the Internet run over ADSL connections. Initially the router modules only determine the remote station to which a data packet is to be sent. The various parameters for all required connections must be arranged so that a given connection can be selected and established as required. These parameters are stored in a variety of lists, the interaction of which permits the correct connections.

A simplified example will clarify this process.



A data packet from a computer initially finds the path to the Internet through the IP address of the receiver. The computer sends the packet with this address over the LAN to the router. Using the IP address, the router then searches the IP routing table and locates the remote station that belongs to this address, for example 'Provider_A'. Using this name, the router then checks the DSL name list and locates the names of the accompanying access concentrators and service, which should be claimed at this AC. The router also obtains the user name and password required for login to Provider A from the PPP list.

The router can then establish a connection on the xDSL line and indicate that it wants a connection to the access concentrator of Provider A and to use Service X there. Once the connection has been established, the router can forward the data packet to the Internet over the ADSL line.

You can find more information on IP networks, etc. in the technical documentation provided on the CD.

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

The PPP list is not only used for establishing connection via xDSL, but also via ISDN, and is therefore described in the chapter entitled 'PPP list'.

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

DSL name list

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

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

- **Name**
This name is used to identify the remote station in the router modules. Once the router module has used the IP address to find which remote station can be used to reach the desired destination, the associated connection parameters can be determined from the name list.
- **Time out**
This period indicates how long the connection will remain active after no more data are transferred.
If a zero is given as time out, the connection will not be automatically terminated!
- **Access Concentrator**
The access concentrator (AC) represents the server that can be accessed over this connection. If more than one provider is available over your ADSL terminal, select the one that is responsible for the IP address group of this remote station with the name of the AC.
The value for the AC will be supplied by your provider. If a value for the AC is not entered, every AC that offers the requested service will be accepted.
- **Service**
Enter the service that you wish to use with your provider. This can be simple Internet browsing, video downstream or other.
The value for the service will be supplied by your provider. If a value for the service is not entered, every service that offers the requested AC will be accepted.



If neither access concentrator nor service is given, the router will connect to the first AC that reacts to the query through the switching center.

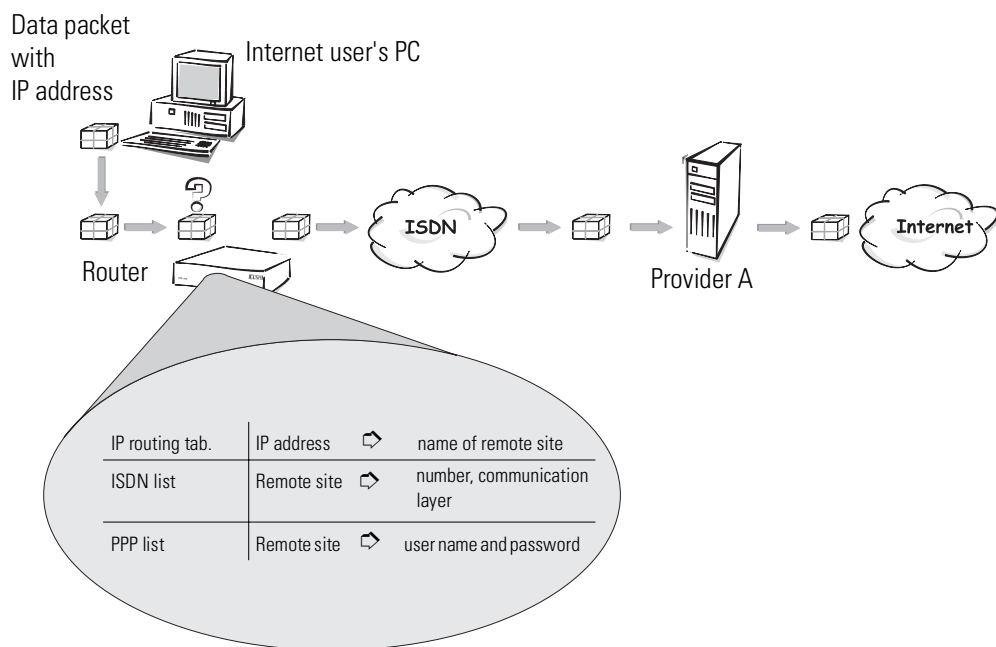
ISDN connections

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

Initially the router modules only determine the remote station to which a data packet is to be sent. The various parameters for all required ISDN connections must be arranged

so that a given connection can be selected and established as required. These parameters are stored in a variety of lists, the interaction of which permits the correct connections.

A simplified example will clarify this process.



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

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

You can find more information on IP networks, etc. in the technical documentation provided on the CD.

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

The PPP list is not only used for establishing connection via xDSL, but also via ISDN, and is therefore described in the chapter entitled 'PPP list'.

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

ISDN name list

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

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

- Name
This name is used to identify the remote station in the router modules.
- Dialup-remote
This number should be dialed when the router actively establishes a connection to the remote station.

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

If the remote station is available via a leased line, the number for a dial-up backup connection can be entered here.
- Timeouts
These times indicate the length of time the B channels should remain active after
 - the last data has been exchanged across static connections for the holding time B1.
 - the data throughput has dropped below a specified level for the holding time B2 in dynamic connections.
- Layer name
The layer stands for a collection of protocols to be used for this connection. The layer must be set up identically on both sides of the connection.
- Callback
If the router receives a call from this specific remote site, it may be set to refuse the connection. Instead, the remote station is called back using the following options:
 - Normal callback
 - Callback using the fast ELSA process
 - Callback after name verification
 - Await the callback from the remote station using the fast ELSA process

Interface settings

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

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

- The D channel protocol used on the S_0 port
Automatic recognition: DSS1 (Euro-ISDN), DSS1 point-to-point, 1TR6, Group 0 leased-line connections
- Leased line option
B channel to be used for the leased line
- Dialing prefix
Number to precede outgoing calls, e.g. the prefix for external calls when using a PBX.

Router interface settings

The router interface settings for the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'General' tab, or under `/Setup/WAN-module/Router-interface-list` during telnet or terminal sessions.

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

- Subscriber numbers (MSN/terminal device selection numbers)
The router responds to incoming calls for these numbers. Multiple numbers are separated by semicolons. If no number is specified, the router will respond to all incoming calls.

The first number specified will be transmitted to the remote station during the active establishment of a connection. If no number is specified, the main MSN of the connection will be transmitted.
- Option for Y connections
Enable this option if it should be possible for both B channels of the connection to establish parallel connections to different remote stations.
- Suppression of own subscriber number
Enable this option in order to suppress the display of your own subscriber number to the remote station during call establishment.

This function must be supported by the network operator.



LANCAPI interface settings

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

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

- Subscriber numbers (MSN/terminal device selection numbers)
The *LANCAPI* responds to incoming calls for these numbers. Multiple numbers are separated by semicolons. If no number is specified, the router will respond to all incoming calls.
- Access to *LANCAPI*
Here you can completely disable the *LANCAPI* functions for the interface, or enable it only for incoming or outgoing calls.
- Transfer of own subscriber number
Normally the number specified in the CAPI application is transferred to the remote station via the *LANCAPI* during active call establishment. No number is transferred by the *LANCAPI* if this number has not been specified or the number is invalid. This option lets you transfer the first number entered in the 'Subscriber number' field if no number has been specified in the CAPI application.

Layer list

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

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

- WAN layer
The protocol settings will be saved under this name. In the name list, select the settings with the layer name for the appropriate connection.
- Encapsulation
Specify here whether an Ethernet header should be added to the data packets. Normally the setting 'Transparent' will be sufficient; this setting may only be required for HDLC connections to third-party devices.

- Layer 3
Layer 3 protocol for the connection. Recognized automatically in the case of some incoming connections.
An additional entry is required in the PPP list when using PPP.
An additional entry is required in the scripts list when using scripts.
- Layer 2
Layer 2 protocol for the connection.
- Options
Enables data compression and channel bundling. These options are only effective when supported by the protocols of layer 2 and layer 3.
- Layer 1
Layer 1 protocol for the connection. Recognized automatically in the case of some incoming connections.

Round-robin list

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

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

- Remote site
Name of the remote station as specified before in the name list.
- Round-robin
Additional numbers for this remote site. Multiple numbers are separated by hyphens.
- Start with:
Indicate whether a new call establishment should start with the last successfully used number, or always with the first number of the list.

Script

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

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

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

- Remote site
Name of the remote station as specified before in the name list.
- Script
Enter the script here as described in the reference section of the documentation.

Call acceptance

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

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

- all
Every call is accepted.
- by name
Every call is accepted at first. During the protocol negotiation the name is determined and checked against the name list. The connection is maintained if the name is present, otherwise it will be rejected.
- by number
The call will only be accepted if the remote station is entered in the number list and the number is transferred to the remote station.
- by name or number
The call will be accepted if one of the two checks was successful.

Number list

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

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

- Dialup-remote
subscriber number transmitted by the remote station (incl. country and long distance codes if available).
- Remote site
Name of the remote site as specified in the name list. The remote station will be called back if so specified in the name list.

Point-to-point protocol

The routers for ELSA also support the point-to-point protocol (PPP). PPP is a collective term for a complete range of WAN protocols, which facilitates the interaction of routers from various manufacturers, since this protocol is supported by almost all manufacturers.

And since PPP cannot be assigned to a specific type of router operation, and also because of the large and increasing importance of this protocol family, we would like to briefly introduce to you the functions of the devices in connection with PPP.

The protocol

What is PPP?

Point-to-point protocol (PPP) was especially developed for network connections over serial channels and has proven to be the standard for connections between routers. It carries out the following functions:

- Password protection according to PAP, CHAP or MS CHAP
- Callback functions
- Negotiating the network protocols to be used via the established connection (e.g. IP). Necessary parameters such as IP addresses are also required for these protocols. This negotiation is executed via the protocol IPCP (IP Control Protocol).
- Monitoring connection with LCP (Link Control Protocol)
- Bundling of several channels (multilink PPP)

For router connections, PPP is the standard for communication between devices or WAN connection softwares from various manufacturers. In order to ensure a successful data transmission if possible, the negotiation of connection parameters and a common agreement regarding standardized control protocols (e.g. LCP, IPCP, CCP) must occur, which are included in PPP.

For what purpose is PPP used?

Point-to-point protocol is used with the following applications:

- For compatibility reasons such as when communicating with foreign routers
- Remote access of remote workstations with ISDN adapters
- Internet access (with the transmission of addresses)

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

The phases of a PPP negotiation

The connection setup via PPP always begins with a negotiation of parameters, which should be used for the connection. This negotiation is executed in four phases, of which knowledge is important for the configuration and troubleshooting.

- Establish phase

After a connection setup via the data communication area, the negotiation of the connection parameters via LCP begins.

It is determined whether the remote station is also prepared to use PPP, the packet sizes and the authentication protocol (PAP, CHAP, MS CHAP or none) are established. The LCP then switches to the opened position.

- Authenticate phase

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

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

- Network phase

In *ELSA LANCOM*, 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 und/oder IPX-be transmitted on the opened (logical) line.

- Terminate phase

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

PPP negotiation in the *ELSA LANCOM*

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.

The PPP list

In the PPP list, a custom definition of the PPP negotiation can be specified for each of the remote stations 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 station uses to identify itself to your router.
Username	The router identifies itself to the remote station with this name. 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 station 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 station (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 multiples of 10 seconds (i.e. 2 for 20 seconds, for instance). The time simultaneously between two checks of the connection according to CHAP. This time is entered in minutes. The time must be set at '0' for remote stations 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 maximally sends before it assumes a line error and drops the connection itself.
Conf, Fail, Term	These parameters may be used to influence the operation of the PPP. 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 changed via SNMP or TFTP (using the <i>ELSA LANconfig</i>)!

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 station 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.

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

The LCP request behavior is configured in the PPP list for each individual connection. The intervals at which LCP requests should be made are set by the entries in the 'Time' and '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'.

Assigning IP addresses via PPP

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

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



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

● Example: Remote access

The assignment of the address is possible by making a special entry in the IP routing table. In addition to entering the IP address, which should be assigned to the remote station from the 'Router name' field, the 255.255.255.255 is indicated as the network mask. In this case, the router name is the name, with which the remote station must identify itself to the *ELSA LANCOM*.

In addition to the IP address, the addresses of the DNS and NBNS servers (Domain Name Server and NetBIOS Name Server) including the backup server from the entries in the TCP/IP module are transmitted to the remote station during this configuration.

So that everything functions properly, the remote station must also be adjusted in such a way that it can obtain the IP address and the name server from the *ELSA LANCOM*. This occurs e.g. in the Dial-up Network of Windows using the entries in the 'TCP settings' under 'IP address' or 'DNS configuration'. Here the 'IP address

assigned by server' and the 'Name server addresses assigned by server' options are activated.

- Example: Internet access

If Internet access for a local network is realized via the *ELSA LANCOM*, the assignment of IP addresses can occur in a reverse manner. Configurations are possible in which the *ELSA LANCOM* does not have a valid IP address in the Internet and is assigned one by the Internet provider for the duration of the connection. In addition to the IP address, the *ELSA LANCOM* also receives information via the DNS server of the provider during the PPP negotiation.

In the local network, the *ELSA LANCOM* is only known by its internal valid Intranet address. All workstations in the local network can then access the same Internet account and also reach e.g. the DNS server.

Windows users are able to view the assigned addresses via *ELSA LANmonitor*. In addition to the name of the associated remote station, you will also find the current IP address as well as the addresses of the DNS and NBNS servers. Options such as channel bundling or connection duration are displayed.

The monitoring tool ELSA LANmonitor is usually automatically installed when installing ELSA LANconfig. A description is found in the chapter called 'Configuration possibilities' in the paragraph 'What is happening online'.

Callback functions

ELSA LANCOM support not only callback via the D channel and callback via the ELSA protocol, but also callback via CBCP specified by Microsoft as well as callback via PPP according to RFC 1570 (PPP LCP extensions). In addition, it is possible for a rather quick callback to occur via a procedure developed by ELSA.

PCs with Windows 95, Windows 98 or Windows NT can be called back only via the CBCP. So that a calling number could be additionally checked in the *ELSA LANCOM*, the following values are available in the name list for the callback entry.

With this entry...	...the callback is thus entered:
Off	No callbacks.
Auto (not Windows 95, Windows 98 or Windows NT, see below)	The remote station will be called back if so specified in the name list. At first, the call is denied and as soon as the channel is clear again, it is called back (duration is approx. 8 seconds). If the remote station is not found in the numerical list, it is first accepted as the DEFAULT remote station, and the callback is negotiated during the protocol negotiation. Thus a one-unit charge is applied.
Name	Before a callback occurs, a protocol negotiation is always carried out even when the remote station was found in the numerical list (e.g. for computers with Windows having direct dialing on the device). Thus a one-unit charge is applied.
ELSA	When the remote station is found in the numerical list, a quick callback is carried out, i.e., the <i>ELSA LANCOM</i> sends a special signal to the remote station and calls back immediately when the channel is clear again. After approx. 2 seconds, the connection is established. If the remote station does not take back the call immediately after the signal, then after two seconds the situation reverts back to normal callback procedures (duration is once again approx. 8 seconds). This procedure is only available with DSS1 connections.



With this entry...	...the callback is thus entered:
Looser	Use the 'Looser' option when a callback is expected from the remote station. This setting carries out two functions simultaneously. On the one hand, it ensures that a custom connection setup is taken back when there is an incoming call from the called remote station, and on the other hand, the function is activated with this setting to be able to react to the rapid callback procedure. In other words, in order to be able to use rapid callback, the caller must be in the 'Looser mode' while the party being called must discontinue callback with 'ELSA'.

The 'Name' setting provides the highest level of security when an entry is not only configured in the numerical list, but also in the PPP list. The 'ELSA' setting provides the quickest callback method between two ELSA routers.

With Windows remote stations, the 'Name' setting **must** be selected.

Callback using Microsoft CBCP

With Microsoft CBCP, the callback number can be determined in various ways.

- The called party does not call back.
- The called party allows the caller to indicate the callback number.
- The called party knows the callback number and **only** calls this number back.

Via CBCP, it is possible to establish connection to *ELSA LANCOM* from a Windows 95, Windows 98 or Windows NT PC and also to be called back by this PC. Three possible settings are selected in the name list via the callback entry as well as the calling number entry.

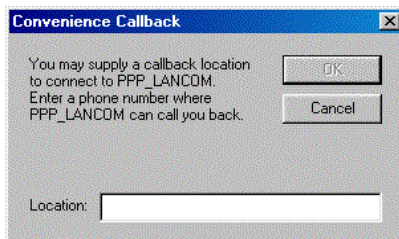
Do not carry out any callbacks

For this setting, the callback entry must be set on 'Off' when configuring via the terminal program or telnet.

Dial callback number

The remote station is called back after name verification. For this setting, the callback entry must be set on 'Name', and in the name list, **no** calling number should be indicated.

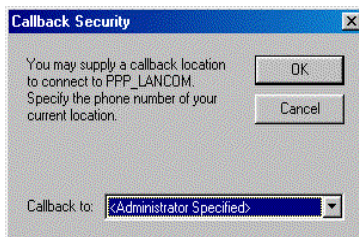
After authentication, the following dialog box appears in Windows 95, in which the user can indicate the calling number.



The calling number is determined by *ELSA LANCOM*

The remote station is called back after name verification. For this setting, the callback entry of the corresponding remote station must be set on 'Name', and in the name list, **a** calling number must be indicated.

After authentication, the following message appears in Windows 95, which the user can only confirm:



The callback to a Windows 95, Windows 98 or Windows NT workstation occurs approx. 15 seconds after the connection has been dropped. This time setting cannot be decreased since it is a Windows default setting.

Rapid callback using *ELSA*

Should two *ELSA LANCOM* communicate with each other whereby one is called back, then rapid callback via *ELSA*-specific procedures is provided.

- The caller who may wish to be called back can activate the function 'Expecting callback from remote station' in the name list (or 'Looser' when configuring via the terminal program or telnet).
- The callback party selects 'Callback remote station (rapid procedure)' in the name list and enters the calling number ('*ELSA*').

Callback with RFC 1570 (PPP LCP extensions)

With RFC 1570, there are five possibilities to request a callback. All versions are recognized by *ELSA LANCOM*. The same applies to all options:

ELSA LANCOM drops the connection after authenticating the remote station and then calls back the station three seconds later.

Channel bundling with MLPPP

When establishing a ISDN connection to a remote station with PPP capability, you can transmit data more quickly. Data can be compressed and/or several B channels can be used for data transmission. (channel bundling).

Connecting with cable bundling is distinguished from “normal” connections in that not only one, but rather several B channels are used parallel-wise for data transmission.

MLPPP (Multilink PPP) is used for channel bundling. This procedure is only available when PPP is used as B channel protocol. MLPPP is used e.g. for Internet access via Internet provider, which also operate remote stations with MLPPP capability from your direct dialing nodes.

- Static channel bundling

When a connection is established with static channel bundling, the *ELSA LANCOM* attempts to also establish the second B channel immediately after the first B channel. If this is not successful because this channel e.g. is occupied by another device or by another connection in *ELSA LANCOM*, this connection attempt is repeated automatically and regularly until the second channel is available for this connection.

- Dynamic channel bundling

When connecting with dynamic channel bundling, the *ELSA LANCOM* establishes only a B channel at first, and then begins with the data transmission. When it recognizes that the throughput remains over a specific threshold value awhile during connection, it attempts to use the second channel.

When the second channel is established and the data throughput returns below the limit value again, the *ELSA LANCOM* waits the set B2 hold time and then closes the channel again automatically. Any partly used call charge units are used up completely if call charge information is transmitted during the connection. The *ELSA LANCOM* uses the second B channel only when and as long as it is really needed!

Channel bundling is thus established

The configuration of channel bundling for a connection is made up of three settings.

- ① In the name list, create an entry for the connection which should use channel bundling. Select a layer which established the bundling in the 'Layer 2' options.
 - **Data compr.** according to LZS data compression procedures (Stac) reduces the data volume when the data has not yet been compressed. This procedure is also supported by routers of other manufacturers and by ISDN adapters under Windows operating systems.

- **Bundling** uses two B channels for a connection. The type of channel bundling is established via configuration of the 'Layer 2' options in the layer list, the hold times in the name list, and the entry for the Y connection in the interface table.
 - **bnd+compr** uses both (compression and channel bundling) and provides the maximum possible data transmission performance.
- ② Set the hold times for this connection in the name list. Please note the following points:
- Depending on the type of application, the B1 hold time should be increased to such a level so that the connection is not dropped prematurely because of packets not being transmitted for a short time. Customarily, values between 60 and 180 seconds are a good base to begin with which one can continue to adjust during operation.
 - The B2 hold time determines whether it concerns a static or dynamic channel bundling (see above). With a B2 hold time of '0' or '9999', the bundling becomes static, whereas with values in between and below the B1 hold time, a dynamic channel bundling is possible.
- ③ With the entry for the Y connection in the interface list, determine what should happen when a second connection to another remote station is desired during a running connection with channel bundling.
- Y connection **On**: The router interrupts the bundling connection in order to establish the second connection to the other remote station. When the second channel is clear again, the bundling connection automatically returns to this channel (this is always the case with static bundling, and only as needed with dynamic bundling).
 - Y connection **Off**: The router holds the existing bundling connection, and the second connection must wait.



Please note that when using channel bundling, the costs for two connections are accrued. Therefore, no parallel connections are possible via LANCAP! Only use channel bundling when the double data transmission capacity can also be used up.



CAP1 connections can interrupt router connections (see 'Priority switching' in the description of the corresponding chapter)!

IPX routing

The IPX router transmits data from networks, which use IPX/SPX as network protocol (e.g. Novell networks). With the entry in the IPX routing table, a remote network becomes available for the computers in the local network. Up to 16 various networks can be entered in the routing table.

IPX addressing

A complete address in a IPX network contains three parts: a network number, the MAC address of the network card and the socket number:

- The network number can be selected as an option. This number must be distinct beyond all accessible IPX networks in order to guarantee a proper assignment.
- 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, a IPX network uses the socket numbers. The various services are thus distinctly identified.

Information on LAN

When several isolated LANs are required at a location, they must not necessarily have to have their own cabling. Various logical networks can share a cable. So that the data of various networks does not interfere with one another and a network remains undisclosed for the others, use various formats for the Ethernet packets. These formats are determined by the binding, which belong to a distinct network number on this cable.

So that the router recognizes to which network it belongs, the network number and the associated binding must be indicated. If the network address remains at the default setting '00000000', the router then indicates the address and the binding. Then on the connected cable it searches the network, on which it receives the most SAP replies.

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 then indicate several parameters for the connection. The table with a maximum of 16 entries has the following setup:

Remote site	Network	Binding	Propagated	Backoff
FILIALE01	00000245	802.3	Route	On
FILIALE02	00000320	SNAP	Filter	On
HEAD OFFICE	00000420	802.2	Filter	Off

- Remote site
The name of the remote station as it is entered in the corresponding opposing router as device name.

- Network

Address of WAN. This is not the address of the target network, but rather a third address which represents the network between the two networks to be connected. The following applies:

LAN address 1 \neq WAN address 1 = WAN address 2 \neq LAN address 2 \neq LAN address 1

- Binding

It is determined here which Ethernet binding should be used on the WAN. This entry is only effective when the layer for this connection supports Ethernet encapsulation. If there is no entry, then 802.3 is used.

- Propagated

Filters 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'.

What happens during data transmission 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.

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.

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.

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'.

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`).

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 transmitted without filters, i.e. always transmitted. 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 therefore sensible.
 - IPX and SPX watchdogs can also be routed naturally, 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.

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.

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	Netmask	Router	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 a network mask of "0.0.0.0" is the default route. Any data packets which cannot be routed by other routing entries are transmitted via this route.

- Router name

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 destination IP addresses 192.168.130.x are transmitted to the local router with the IP address 192.168.140.123.
192.168.0.0	255.255.0.0	0.0.0.0	0	Prevents transfer of all data packets in 10er nets.
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.

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 manual). The source ports, on the other hand, may be selected freely within certain ranges.

The router can check the source and destination ports of data packets using the TCP or UDP protocols. It can then deduce the purpose of the data from these ports. For example, FTP accesses or telnet sessions can be identified.

The appropriate filter table can be used to determine that certain data is not to be transferred from the LAN to the WAN. Data for particular ports can also be blocked from entering the LAN from the WAN in the same way.

The filter tables can use the filter type along with the definition of the port ranges and associated protocols to determine whether the data in question should never be transmitted or whether it should simply not lead to a call being established (i.e. only be transmitted if a connection already exists).

The router has two separate filter tables, for packets coming from the LAN and from the WAN.

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

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' option (in the 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	IP netmask	Router name	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, which sends that data on to the computer at the other end of the ISDN connection.

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). This is how you tell the router in your device to send the data packet to the other, responsible router itself. The router will then no longer send any ICMP redirects.

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.

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. This protocol is used by all devices with RIP to exchange information regarding the reachable routes.

What information is propagated by IP RIP?

A router uses the IP RIP information to inform the other routers in the network of the routes it finds in its own static table. The following entries are ignored in this process:

- Rejected routes with the '0.0.0.0' router setting.
- Routes referring to on other routers in the local network.
- Routes linking individual computers to the LAN by proxy ARP.

Although the entries in the static routing table are set manually, this information changes according to the connection status of the router and so do the RIP packets transmitted.

- If the router has established a connection to a remote station, it propagates all the networks which can be reached via this route in the RIPs with the distance '1'. Other routers in the LAN are thus informed by these means that a connection to the remote station has been established on this router which they can use. The establishment

of additional connections by routers with dial-up connections can be prevented, thus reducing connection costs.

- If this router cannot establish a further connection to another remote station, all other routes are propagated with the distance '16' in the RIPs. The number '16' stands for "This route is not reachable at the moment." A router may be prevented from establishing a connection in addition to the present one may be due to one of the following causes:
 - Another connection has already been established on all the other channels (also via the *LANCAP* or a/b ports).
 - Y connections for the S_0 port have been explicitly excluded in the interface table.
 - The existing connection is using all B channels (channel bundling).
 - The existing connection is a leased-line connection. It is not possible to establish a parallel dial-up connection in this case.



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	IP netmask	Time	Distance	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

What do the entries mean?

IP address and network mask identify the destination network, the distance shows the number of routers between the transmitter and receiver, the last column shows which router has revealed this route. This leaves the 'Time'. The dynamic table thus shows how old the relevant route is. The value in this column acts as a multiplier for the intervals at which the RIP packets arrive. A '1', therefore, stands for 30 seconds, a '5' for about 2.5 minutes and so on. New information arriving about a route is, of course, designated as directly reachable and is given the time setting '1'. The value in this column is automatically incremented when the corresponding amount of time has

elapsed. The distance is set to '16' after 3.5 minutes (route not reachable) and the route is deleted after 5.5 minutes.

Now if the router receives an IP RIP packet, it must decide whether or not to incorporate the route contained into its dynamic table. This is done as follows:

- The route is incorporated if it is not yet listed in the table (as long as there is enough space in the table).
- The route exists in the table with a time of '5' or '6'. The new route is then used if it indicates the same or a better distance.
- The route exists in the table with a time of '7' to '10' and thus has the distance '16'. The new route will always be used.
- The route exists in the table. The new route comes from the same router which notified this route, but has a worse distance than the previous entry. If a device notifies the degradation of its own static routing table in this way (e.g. releasing a connection increases the distance from 1 to 2, see below), the router will believe this and include the poorer entry in its dynamic table.



RIP packets from the WAN will be ignored and will be rejected immediately. RIP packets from the LAN will be evaluated and will not be propagated in the LAN.

Interaction: static and dynamic tables

The router uses the static and dynamic tables to calculate the actual IP routing table it uses to determine the path for data packets. In doing so, it includes the routes from the dynamic table which it does not know itself or which indicate a shorter distance than its own (static) route with the routes from its own static table.

Routers without IP RIP support

Routers which do not support the Routing Information Protocol are also occasionally present on the local network. These routers cannot recognize the RIP packets and look on them as normal broadcast or multicast packets. Connections are continually established by the RIPs if this router holds the default route to a remote router. This can be prevented by entering the RIP port in the filter tables.

Scaling with IP RIP

If you use several routers in a local network with IP RIP, you can represent the routers outwardly as one large router. This procedure is known as "scaling". A router like this, with its supposedly inexhaustible supply of routes is created by the continual exchange of information between the routers.

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 so that it can be reached from the LAN, 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 **Internet** address and an **Intranet** 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 *ELSA LANconfig* in the 'IP router' configuration section on the 'Masq.' tab or in the *Setup/IP-router-module/Masquerading/Service-table* menu). The packet is forwarded to this computer. All packets that come from the FTP server in the local network (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

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: "What 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 finds one it retrieves the required 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. The 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.

Time control setting for the default route

Similar to the least-cost routing (LCR), the time control setting for the default route is a function in which connections are automatically made at the most economical rate according to the time of the provider.

As soon as an IP packet establishes connection via the default route, the remote station entered in the default route is not dialed at first, but rather in the time control table, it is determined beforehand which remote station should be used.

In this time control table, indicate on which weekdays and at which times a specific provider can be used. As soon as an IP packet requires the establishment of the default route, it is first checked whether the use of the time control table is activated. Then an entry is searched in the table, which covers the current weekday and the current time. When such an entry is found, the router establishes a connection to the remote station that has been entered there. If no suitable entry can be found in the time control table, the router returns to the IP routing table and uses the remote station entered there.

The time control settings of the default route can be found in the *ELSA LANconfig* 'IP router' configuration area on the 'Routing' tabs, and when configuring via telnet, these settings are found in `Setup/IP-router-module`. The individual days are entered in the same syntax as for the LCR. Holidays are also defined by the LCR module.

Policy-based routing

Policy-based routing describes a process in which particular data packets are given preferential treatment. This requires evaluation of a special field within the IP data packet, known as the type of service (TOS) field. This preferential treatment of a number of data packets can, for example, simplify the configuration of the router via the WAN when large data volumes are to be transferred simultaneously.



You can find more information on policy-based circuit routing in the 'Description of the menu options' in the reference manual.

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.

The DHCP server

As a DHCP server, the *ELSA LANCOM DSL/I-10 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 server
- 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.

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'.

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 started up that is requesting an IP address via DHCP with its network settings, a device with an activated DHCP module will offer this computer an address assignment. 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 router 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.

Configuring the DHCP server

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

- You have not yet configured a network or your existing local network does not use TCP/IP. The DHCP server in your new ELSA device lets you assign IP addresses to all of the computers in the network and to the device 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

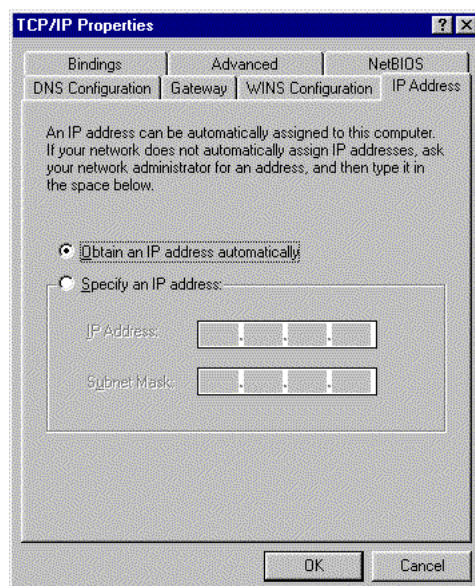
The *ELSA LANconfig* includes a wizard to help you with the required settings:

- 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.



- ④ Install the *ELSA LANconfig* on a computer in the network.
- ⑤ Start the program from the 'ELSAan' 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 'All settings to be defined 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).

DHCP relay agent

Network configuration transmitted via ISDN

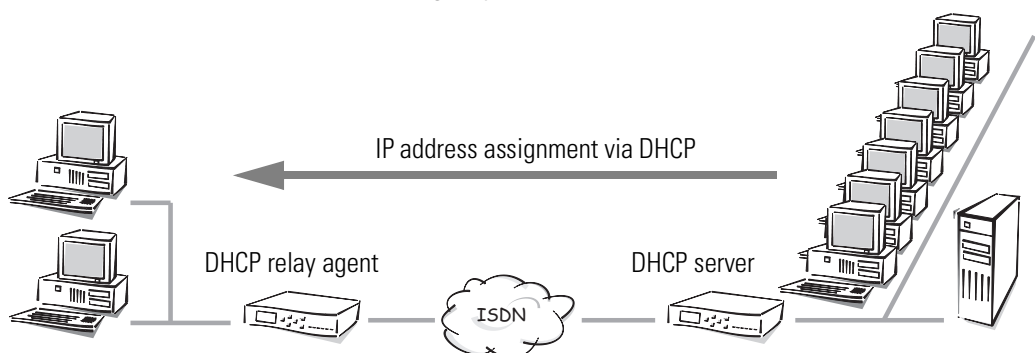
When connecting individual workstations via IP to the LAN of a head office, the Proxy-ARP function is customarily used. A prior established IP address from the address area of the head office is assigned to the computer being accessed via switched lines.

Should an entire IP network of a branch center with several computers be connected with the LAN of the head office, a LAN-LAN connection is realized. Both networks are thus found in various IP address groups.

While all addresses and other network information within the LANs of the head office can be easily assigned via DHCP, this is not the case with LAN-LAN couplings.

Acquiring DHCP information from the remote network

The function "DHCP relay agent" also allows the transmission of DHCP information via ISDN lines. Therefore it is also possible to connect several computers beyond an ISDN route in a network in the IP address group of the head office.



The DHCP server in the network of the branch center is switched in the relay agent mode. DHCP requests are forwarded to another server whose address is securely entered. Connection to the network of the head office is established via a corresponding entry in the IP routing table.

If a computer is launched in the network of the branch center, which requires an IP address from a DHCP server, the DHCP relay agent forwards this request via the ISDN route to the DHCP server in the network of the head office. This server forwards a prior established IP address to the requesting computer from the transmitted MAC address.

Therefore, all necessary settings are designated:

- ① The DHCP server in the router of the branch center network is adjusted to forward DHCP requests. To that end, the IP address of the DHCP server is entered in the LAN of the head office.
- ② This router must also contain all information on establishing connection with the network of the head office (normal LAN-LAN coupling).
- ③ In the DHCP server in the head office, all remote stations with their assigned MAC address and IP address are entered along with the usual routing information. In addition, the name of the corresponding computer is entered, which should be used for the DNS server.

Adapting DHCP information

All DHCP information are gathered from the DHCP server in the head office. As a result, the router in the head office is also known as the gateway for the branch center. If a computer from the branch center wishes to access the Internet, the request is forwarded to the gateway in the head office. The Internet connection runs over the network of the head office. In order to avoid this detour, the DHCP relay agent can use a function in which the replies of the remote DHCP server can be adapted to the requests of its own LAN. Network masks, broadcast address, and gateway are no longer obtained from the network of the head office.

Obtaining boot images from the remote network

For the connection of branch center networks in which there are no complete workstations, but rather only terminals without bootable hard disks, the DHCP server makes it possible to obtain a complete boot image via the ISDN line. Therefore, the entire configuration of the terminals can be carried out and maintained at a central location.

The DHCP relay agent is also configured in the network of the branch center. In the network of the head office, not only the entries of the IP address are determined for the respective MAC address, but also which boot image should be used. The boot image is

indicated by a symbolic name. In an image table, a server is assigned the symbolic name and a directory and file information, with which the boot image can be found.

If a terminal is launched in the network of the branch center, it automatically establishes connection via the router to the network of the head office and then obtains the current boot image from there.

The settings for the DHCP relay agent, the accompanying server, and the boot images are found in the *ELSA LANconfig* in the 'TCP-IP' configuration area on the 'DHCP' and 'DHCP/BOOTP' tabs or when configuring via telnet, these settings are found in the *Setup/DHCP-module*.

DNS

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

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/I-10 Office*:

- An *ELSA LANCOM DSL/I-10 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/I-10 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/I-10 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.

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
```

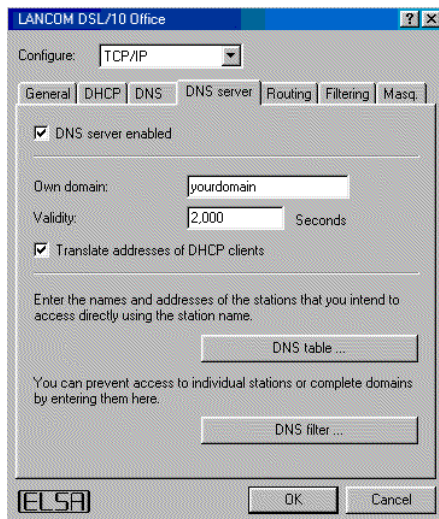
- ② Enter the domain in which the DNS server is located. The DNS server uses this domain to determine whether the requested name is located in the LAN. Entering the domain is optional.

```
set setup/DNS-module/domain yourdomain.com
```

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

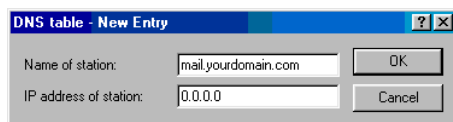
```
set setup/DNS-module/DHCP-usage yes
```

```
set setup/DNS-module/NetBIOS-usage yes
```



- 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 you 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:

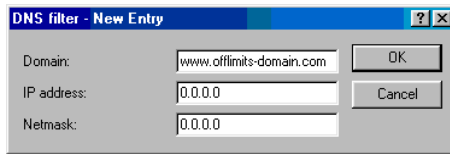


```
cd setup/DNS-module/DNS-table
set mail.yourdomain.com 10.0.0.99
```

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.



```
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.

NetBIOS proxy

With the NetBIOS proxy function, a *ELSA LANCOM DSL/I-10 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.

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/I-10 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.

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/I-10 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.

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, Novel) or PI (Internet Protocol) protocols.



Unlike IX and PI, 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 routable protocol in the ELSA LANCOM DSL/I-10 Office, such as IPA.

The routing of NetBIOS packets in the *ELSA LANCOM DSL/I-10 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... ► Protocols**. 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

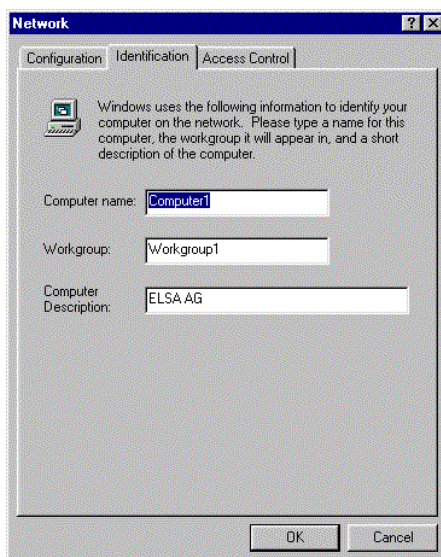
File and printer sharing permits drives and printers to be shared with other users in the Windows Network.

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

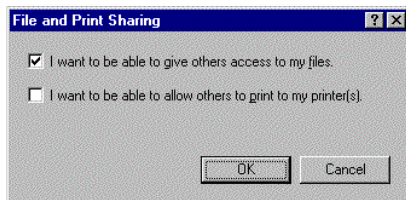
Click **Start ► Settings ► Control Panel ► Network** and switch to the **Identification** tab.



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.

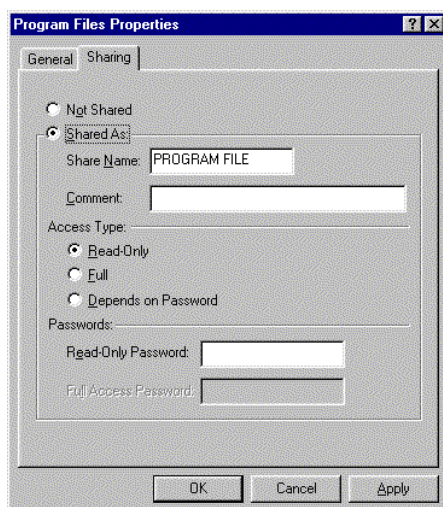
- File and printer sharing

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.



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.



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.

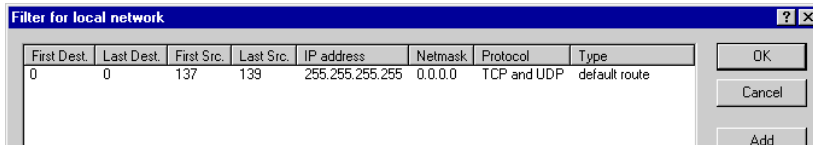


It's easy to check whether the Windows Network settings have been made correctly: the local computer must appear with its name in the Network Neighborhood.

Linking two Windows Networks via ISDN

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.



- 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'.



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.

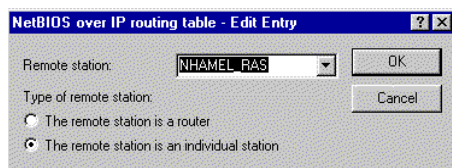
```
cd /Setup/NetBIOS-module
set operating on
```

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 side cannot be accessed until this operation is complete.

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/I-10 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/I-10 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.



```
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.

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/I-10 Office*. Using telnet, enter

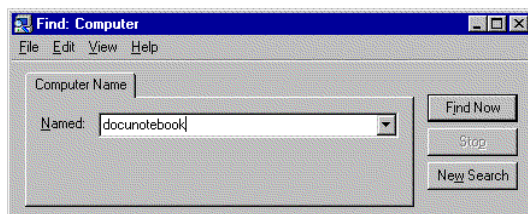
```
dir /Setup/NetBIOS-module/Host-list
```

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...**



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/I-10 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.

The least-cost router

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

Unfortunately, the most inexpensive rates vary from provider to provider depending on the time of day and region. In the morning Provider 1, Provider 2 in the afternoon and possibly Provider 3 for international calls. To always have the most economical connection for telephone calls, surfing the Internet or transferring data to other networks,

it would be necessary to decide which provider is the least expensive before each connection. A *ELSA LANCOM DSL/I-10 Office* does this for you. Least-cost routing (LCR) is the function for this task. You define once which providers have the most favorable charges for your purposes, and the device automatically selects the most economical provider for you, regardless of whether you are using the router, the *LANCAPI* etc).

Function of the *ELSA LANCOM* least-cost router

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

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

The LCR also requires the following information:

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

Initial tests

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

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

Prefix	CbC network prefix	Days of week	Time of day
089	01097	Sat + Sun	0:00h to 23:59h
089	01098	Mon + Tue + Wed + Thu + Fri	8:00h to 18:00h
0172	01099	Every day	0:00h to 23:59h
00	01097	Sun	0:00h to 23:59h

These four entries mean that all connections to Bristol (or other numbers with the prefix '0117') on weekends will be made using the provider with the network prefix '4'. Between 8:00 AM and 6:00 PM on weekdays, these calls will be made using the provider with the network prefix '01098'. Calls to the D2 mobile network ('0172') will be made via the provider with the network prefix '01099'. International calls on Sundays will be made using the provider with the network prefix '01097'.

For advanced users: systematic use of the LCR

- The first example has shown how connect charges can be reduced with only a few entries. If you would like to put the least-cost router to optimal use, detailed information is required with regard to the connect-charge structure of the call-by-call providers. Next, decide how these rates and rate zones can be best organized in the *ELSA LANCOM DSL/I-10 Office* LCR table. A variety of approaches are possible:
- Obvious options for saving telephone charges can be entered directly:
 - Dial prefixes '0177', '0171', '0172' for mobile telephone networks
 - '00' for international connections
- Entering a single '0' will initially reroute all numbers starting with a zero. However, as neighboring local exchanges may also start with a '0' and yet be billed as local calls, their prefixes should be listed separately to prevent these calls from being rerouted. This strategy should also be applied to special prefixes such as '0800', '0190', etc..
- Another strategy aims to achieve the highest possible level of control over the routing activities. Start with the prefixes of the local area and then define the next larger zones. The closer, and thus less expensive, tariff zones are set with longer prefixes, the remaining more distant prefixes with a smaller number of digits.

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

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

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

Setting up the least-cost router

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

- Which operating modes of the *ELSA LANCOM DSL/I-10 Office* should the services of the least-cost router use?
- Which calls should be routed over which provider?

To answer these questions, proceed as follows:

- ① In *ELSA LANconfig*, go to the 'Least-Cost-Router' configuration section on the 'General' tab.
- ② Enable the least-cost router function. The least-cost router can only be enabled if you have already set the unit time manually or the time has already been received from the ISDN network itself (see also 'Time for the Selection' further below). Activate the following operating modes for the least-cost router as required:

- ☐ The router
- ☐ *The LANCAPI*



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

- ③ Change over to the 'Time periods and public holidays' tab. Open the **Least-cost table**, create a new entry and enter the following data:
 - ☐ Which prefix should be rerouted?
 - ☐ Which provider should be used for this prefix? If you have entered several network prefixes separated by semicolons, the LCR will automatically try the next prefix if the current one is busy.
 - ☐ On which days and what times should the routing be active? Please note that time blocks cannot extend from one date to another (i.e. 6:00 p.m. to 6:00 a.m.).
 - ☐ Should the call be handled by the default telephone provider if all call-by-call providers are busy? If 'Automatic fallback' is disabled, the LCR will start at the beginning after unsuccessfully trying the last network prefix.

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

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

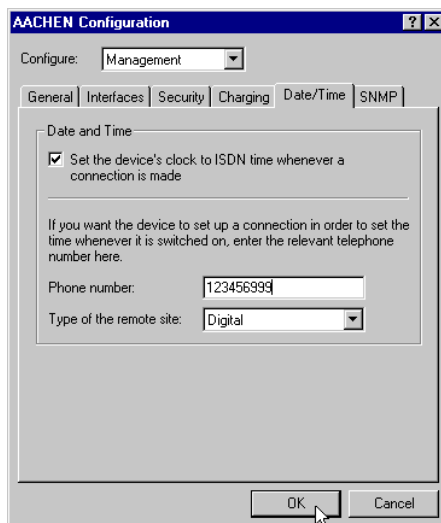


*Build the LCR table one step at a time and check your results. Open the ELSA LANmonitor, for example, and establish connections to the remote stations to be rerouted according to the table using the ELSA LANCAPI. Use the dialed number to verify whether the LCR settings suit your requirements. For router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

Time for the selection

It goes without saying that the internal clock of the *ELSA LANCOM DSL/I-10 Office* must be set properly to ensure that the least-cost router correctly applies the information in the table. The router can also help itself in this respect as well, however: It can synchronize its internal clock with the time in the ISDN, either when switched on, or during each call establishment.

- ① In *ELSA LANconfig*, switch to the 'Date/Time' tab in the 'Management' configuration section.
- ② Activate the option for automatic synchronization at each call establishment. If you would rather enter the time manually, disable this option.
- ③ The current time is lost when the unit is switched off. Enter the number of a random remote station if you would like the device to establish a connection immediately upon being switched on, in order to synchronize the time with that of the ISDN network. Specify whether the remote station is digital (e.g. BBSs or Internet providers) or analog (telephone message or voice services).



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

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 standard fax programs with an *ELSA LANCOM DSL/I-10 Office*.

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**.

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.

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.

The *ELSA LANCAPi*

What are the advantages of *LANCAPi*?

Above all, the use of *LANCAPi* offers you economic advantages. *LANCAPi* provides all workstations integrated in the LAN (local area network) with unlimited access to office communications functions such as fax machines, answering machines, online-banking and 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 ISDN adapters or modems. All you need to do is install the office communications software on the individual workstations.

For example, faxes are sent by simulating an ISDN 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 via ISDN.

The dynamic concept of *LANCAPi* allows for easy scalability of the communication lines. If more B channels are needed, you simply install more routers in the network. All devices in the local network will share the tasks.

Please note: All applications that you run via LANCAPi use direct ISDN connections and do not run via the router of the device. This means that the firewall and call charge management functions do not work here!

Installing the *LANCAPi* client

The *LANCAPi* is made up of two components, a server (in the *ELSA LANCOM DSL/I-10 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.

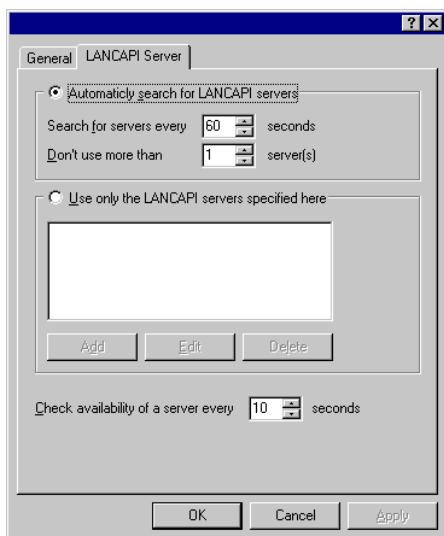


Configuring the *LANCAPi* client

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/I-10 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/I-10 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.



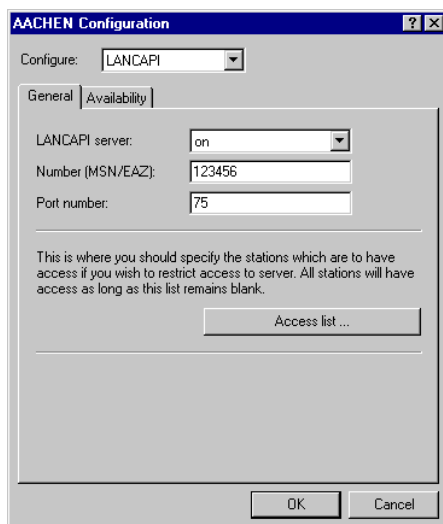
Configuring the *LANCAPI* server

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 'ELSAIlan' program group. Open the configuration of the router by double-clicking on the device name in the list and select the 'LANCAPI' section.

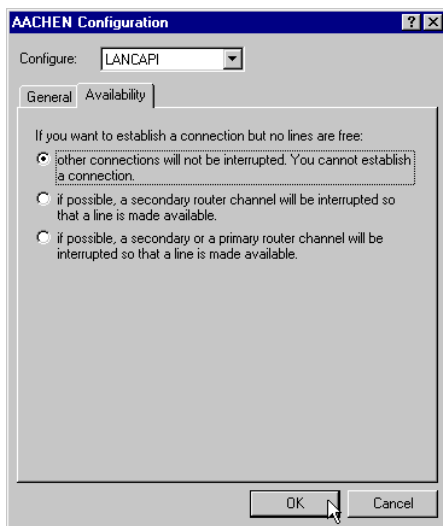


- ② Activate the *LANCAPI* server, or set it to permit outgoing calls only. In the latter case, the *LANCAPI* will not respond to incoming calls—to receive faxes, for example. Permitting outgoing calls only is useful if you do not have a specific call number available for the *LANCAPI*.
- ③ When the *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 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/I-10 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:



- 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'.

Reserving B channels

When reserving B channels, the objective is to always allow incoming or outgoing calls and to always be available for external remote stations or to be able to establish calls at all times.

For each S_0 interface, it is determined how many connections are allowed to occur simultaneously on an interface, which is considered separately for incoming and outgoing calls.



The restriction of the number of connections concerns all types of operation of the device, i.e., the router, LANCAP, and possibly a/b ports, etc.

The values for B channel reservation are entered in the interface table as a maximum value for incoming and outgoing connections:

- As a standard, both values are set at 2. Therefore, two parallel outgoing connections can not only be established, but also two incoming calls can be received.
- If the value is set at 1 for the maximum number of incoming calls, the device can only receive one call on this interface. If another call comes in, it is denied, although a B channel may be unoccupied. This channel is reserved for its outgoing calls. For the maximum number of outgoing calls, this principle applies.
- If the value is set at 0 for the maximum number of incoming calls, no calls can be received on this interface. Only the maximum number of authorized outgoing connections can be established.



If both values are set at 0, then connections can no longer be established over this interface!

The settings for reserving the B channel can be found in the *ELSA LANconfig* in the 'Management' configuration area on the 'Interfaces' tab or when configuring via telnet, these settings are found in the `Setup/WAN-module/Interface-list`.

Accounting

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

The data collected include the following:

- User (name, IP address, MAC address)

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

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

- Remote station to which the connection was established

- Type of connection
Dial-up, leased-line or DSL connection
- Sent and received data volumes
- Online time

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

- Number of connections

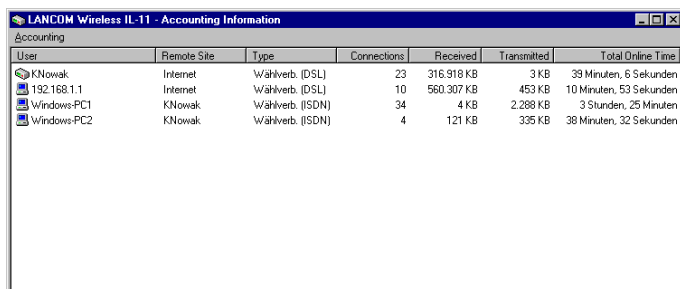
This field specifies how often a user's action led to the establishment of a connection.

Configuring accounting

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

Reading the accounting data

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



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

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

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

- Username
The name of the user or his or her layer 3 address (IP address, IPX address or, in bridge mode, the MAC address again)
- Remote site
The remote station with which the user exchanged data

- Connection type
Type of connection
- Rx-Bytes, Tx-Bytes
Data volumes on the interface
- Total amount of time
Total online time for this user to this remote station
- Connections
The number of counted connections for this user to this remote station



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

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

Appendix

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 via IP, DNS 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) ISDN S ₀
Charge monitoring	The maximum charge amount or connection time can be adjusted in a given time period, which is done separately for DSL and ISDN connections.
Security and firewall functions	PAP and CHAP, PPP authentication mechanisms; filter options in IP mode; protection of configuration using access lists and passwords, IP masquerading; ISDN 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 <i>ELSA LANmonitor</i> , remote configuration via ISDN, configuration via HTML
Operating security	Hardware watchdogs, regular self-testing, FirmSafe concept for remote software upgrades
Statistics	LAN and WAN packet counters; error, connection and charge counters, timer
Display/operation	LEDs for LAN, WAN and device status
Power supply	12 VA with AC adapter for 230 V, 12 VA
Environmental conditions	Temperature: 5-40°C, humidity: 0-80%, non-condensing
Dimensions and design	Rugged metal case, connections on rear panel; dimensions 158 x 40 x 125 mm (W x H x D)

Package contents	Power adapter, cable for outband interface, two LAN twisted-pair cables, ISDN line connection cable, complete documentation and <i>ELSA LANCOM</i> CD <i>ELSA LANconfig</i> , <i>ELSA LANmonitor</i> for status display, terminal program <i>ELSA-ZOC</i>
Approvals	in preparation: Germany, Switzerland and all other EU countries
Service	Warranty: 6 years Support: via hotline and Internet; test inputs

Declaration of conformity



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

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

Geräteart: DSL(10) / ISDN Router
Type of Device:
Typenbezeichnung: ELSA LANCOM DSL/I-10 Office
Product Name:
EG-Baumusterprüfbescheinigungs Nr.: D810547L
Registration No.:
Benannte Stelle: CETECOM ICT Services GmbH
Notified Body: **CE 0682 X**

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)
ISDN Vorschrift (98/515/EG)
Council Decision (98/515/EC)

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

EN 50082-1: 1992 Teile / parts : EN 61000-4-2, 3, 4, 5, 6
EN 50081-1: 1992 Teil / part : EN 55022B: 1994
EN 60950: 1992 +A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997
TBR 3

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, 21. Dezember 1999
Aachen, 21st December 1999

i.V. Stefan Kriebel
Bereichsleiter Entwicklung
VP Engineering

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.

Index

● Numerics

- 10/100Base-TX 15
- 100 Mbit network 15

● A

- Access control 40
- Access protection 5, 41
 - name 41
 - name or number 41
 - number 41
- Access type 96
- Accounting 8
- Adapter 26
- Adapter for configuration cable 9
- Additional limit 44
- Address administration 27, 80
- Address pool 81, 86
- Advice of charge 5
- AOCD 5, 44
- Authentication 5, 56
 - authentication 60
- Automatic synchronization 103
- Availability 107
- Available workstations 98

● B

- B channel 34
 - connection status 6
- B channel protocol 41
- B channel reservation 108
- BACP 6
- Barring 40
- Boot images 88
- Brute force 5, 40

● C

- Call charge information 8, 62
- Call charge limit 43
- Call charge management 43
- Call charge units 62
- Call establishment 92
- Call number recognition 5
- Callback 3, 41, 42
 - fast call back 43
- Callback function 5
- Call-by-call 99, 100

- Calls to the D2 mobile network 100
- CAPI Faxmodem 104
- CAPI interface 104
- CBCP 59
- CD 9
- Challenge Handshake Authentication Protocol 42
- Channel bundling 6, 61
 - dynamic 61
 - static 61
- CHAP 42
- Charge monitoring 5
- Charge units 44
- Charges 99
- CLIP 5
- Common ISDN Application Programming Interface 104
- Compression 6
- Computer names 88, 92
- Configuration 4
 - methods 25
 - SNMP 37
- Configuration interface 9, 25
- Connect charges 92
- Connect-charge structure 100
- Connection 15, 100
- Connection control 44
- Connection duration 6
- Connection limits 44
- Cost reduction 43

● D

- Data compression procedures
 - LZS 62
- Data transmission 61
- Data transmission in the IPX network 65
- Data volume 8
- Days of the week 100
- Dedicated lines 3
- Default route 79
- DHCP 80, 87
 - DHCP for WINS resolution 83
 - DHCP mode 80
 - DHCP relay agent 87
 - DHCP server 7, 27, 80, 87, 89
 - configuration 84

- Dialing prefix 100
 - Dial-up connection 3, 25, 28
 - Dial-Up Networking 42
 - Distance of a route 70
 - DNS 78, 88
 - DNS forwarding mechanism 89
 - DNS server 7, 80, 82, 88
 - available information 89
 - filter list 91
 - filter mechanism 89
 - Documentation 9
 - Domain Name Service 78
 - Domain name service 88
 - Domains 88
 - DSL connection 15
 - Dynamic channel bundling 6, 61
 - Dynamic Host Configuration Protocol ... 80
 - Dynamic routing 69
- **E**
- Electronic documentation 9
 - ELSA CAPI Faxmodem 7
 - ELSA protocol 42
 - ELSA-RVS-COM 3
 - ELSA-ZOC 3
 - E-mail 2
 - End address 81
 - Ethernet 4
 - 10/100Base-T 4
 - Fast Ethernet 4
 - EuroFileTransfer 2, 7
 - Exclusion routes 70
- **F**
- Fast call back 43
 - Fast Ethernet 4
 - Fast-Ethernet
 - 10/100Base-T 4
 - Fax 2, 3, 7, 104
 - Fax Class 1 7, 104
 - Fax driver 7, 104
 - Fax transmission 104
 - Faxmodem 7
 - LANCAPI 104
 - File and printer sharing 94
 - File transfer 2
 - Filter 41
 - Filter mechanisms 3
 - Firewall 5
 - Firewall function 43
 - FirmSafe 5, 31
 - Firmware 5
 - Firmware upload 32
 - using TFTP 33
 - with LANconfig 32
 - with terminal program 32
 - Flash ROM 5, 31
- **G**
- Gateway 43, 80, 83, 87
 - Groups 92
- **H**
- High telephone costs 43
 - Hold time 62
 - Holidays 100
 - Home office 3
 - Host 88
 - Hyperterminal 26
- **I**
- Identification 94
 - Identifying the caller 41
 - Inband 25, 26
 - using telnet 28
 - Inband configuration 25
 - Install software 31
 - Installation 4
 - Interfaces 15
 - Internal clock 102
 - International calls 99
 - Internet 2, 43
 - Internet access 58
 - Internet address 76
 - Internet service provider 2
 - Intranet address 76
 - IP access list 26
 - IP address 7, 27, 35, 43, 57
 - IP filter 93
 - IP masquerading 2, 5, 41, 43, 76
 - simple masquerading 77
 - supported protocols 78
 - IP routing
 - filter 71
 - FTP 72
 - telnet 72
 - IP routing table 69
 - IPX addressing 63

IPX routing	
backoff	65
binding	63, 64
exponential backoff	66
hops	65
loop-propagating	66
network	64
remote site	64
RIP and SAP tables	65
tics	65
IPX routing table	64
IPX watchdogs	68
IPX-Routing	
Propagate	64
ISDN cable	4
ISDN connection cable	9
ISDN connection charges	43
ISDN time	6
ISDN-S0 port	15

● K

Key	56
-----	----

● L

LAN connection	4
LAN connection cable	9
LAN to LAN coupling	3
LANCAP1	2, 3, 7, 28, 104
LANCAP1 client	105
LANCAP1 server	106
LANconfig	17, 25, 26, 27, 28, 32, 34
LANmonitor	6, 34, 102
LCP echo reply	57
LCP echo request	57
LCR	5, 44, 79, 99
LCR table	100
Least-cost router	79, 99, 101
automatic fallback	102
connect-charge monitoring	102
operating modes	102
Least-cost routing	5, 44
LED	13
LED indicators	6
Line connection	7
Line Display	35
Line management	3, 7
Local calls	101
Login	31, 40
Login barring	40

Long distance calls	100
LZS data compression	62

● M

MAC address	87
Mail server	91
Microsoft Network	92
Microsoft Network client	94
MLPPP	6, 61
Mobile telephones	100
Mode	80
Monitoring	34
MS CHAP	54, 55
Multi-device terminal	4
Multilink PPP	54, 61

● N

Name and group designation	94
Name information	92
Names	92
NAT	41, 43, 76
NBNS	92
NBNS server	80, 82, 83
Neighboring local exchanges	101
NetBIOS	8, 89
IP filter	96
LAN-LAN interconnection	96
network protocol	93
remote access	97
remote station	96
TCP/IP	94
NetBIOS nameserver	92
NetBIOS networks	89
NetBIOS ports	93
NetBIOS proxy	91
NetBIOS remote stations	93
Network connection	2
Network identification prefix	99
Network Information Center	76
Network names	88
Network neighborhood	98
Network operators	99
NIC	76
No charge information	44
Node/hub selector switch	15
NTBBA	16

● O

Office communications	104
-----------------------	-----

Online media	26
Online minutes	43
Online research	2
Online time	8
Operating modes	39
Options for saving telephone charges ..	101
Outband	25
Outband configuration	25, 26

● P

Package contents	9
PAP	42
Password	30, 34, 41, 42, 96
Password Authentication Protocol	42
Password protection	5, 40
PAT	41, 43, 76
Peer-to-peer networks	8
Period	43
Period of validity	80, 83
Point-to-multipoint configuration	4
Point-to-point configuration	4
Port	107
Port number	78
Power	14
Power supply unit	9, 15
PPP	8, 35, 42, 61
PPP client	25, 28
PPP connection	25, 30
PPP LCP extensions	61
PPP list	41
PPP negotiation	30
Prefix	99
Preselection	99
Priority control	107
Priority switching	63
Prohibiting domains	91
Propagated frames	67
Provider	79
Providers	99
Proxy	8
Proxy ARP	86

● R

Rate zones	101
Remote access	3, 28, 58, 93
Remote configuration	8, 25
Remote connection	29
Reserving	108
RIP	65

RIP tables	65
Router	70
Routing	93
Routing information protocol	65
Routing Microsoft Networks	91

● S

S ₀ interface	4, 109
S ₀ status	14
SAP	65
SAP tables	65
Scopes	92
Security	39, 41, 43
Security features	2
Security procedures	42
Serial port	25
Service	88
Service advertising protocol	65
Setup Wizard	26
Shared resources	95
Sharing	95
Single user access	43
SNMP	37
Socket filter	67
Software update	5
Special prefixes	101
Split horizon	66
SPX watchdogs	68
Stac	62
Stac data compression	6
Standard fax programs	104
Start address	81
Static channel bundling	6, 61
Static routing	69
Statistics	6
Status Displays	6
System terminal	4

● T

TCP/IP	17, 27, 69
TCP/IP networks	88
Technical data	111, 113
Telephone provider	101
Teleworking	3
Telnet	26
Telnet	21, 28
Terminal	88
Terminal program	4, 26
TFTP	27

- Throughput 62
 - Time 100, 102
 - Time budget 45
 - Time check 6
 - Time control table 79
 - Time in the ISDN 103
 - Time limit 44
 - Time of day 100
 - Time-dependent connection control 44
 - Timeout 62
 - Trace
 - code and parameters 36
 - Examples 37
 - starting 35
 - Trace outputs 35
 - Transfer costs 8
 - Transmission rates 6, 35
 - Troubleshooting 34
 - Type of service 79
- **U**
 - Upload 5, 31
 - User name 30, 42, 56
 - **V**
 - V.24 configuration interface 15
 - Voice mail 3
- **W**
 - WAN connection 4
 - WAN-Chan1 14
 - WAN-Chan2 14
 - Watchdogs 68
 - Wildcards 91
 - Windows Internet Name
 - Service Server 92
 - Windows network 83
 - Windows Networking 98
 - Windows networks 8
 - winipcfg 18, 20
 - WINS address 83
 - WINS server 92
 - WWW 43
 - **X**
 - xDSL connection cable 9
 - **Y**
 - Y connection 62

