

LANCOM™ 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, April 2000

Preface

Thank you for placing your trust in this ELSA product.

By selecting the *ELSA LANCOM Office* you have chosen a router which you can use to connect local area networks or single workstations to the Internet via an ISDN connection.

Model varieties

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

- *ELSA LANCOM 800 Office*
- *ELSA LANCOM 1000 Office*
- *ELSA LANCOM 1100 Office*
- *ELSA LANCOM 2000 Office*

*Model
restrictions*

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

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 general network technology, TCP/IP), reference section with complete menu description

This documentation was compiled by several members of our staff from a variety of departments in order to ensure you the best possible support when using your ELSA product.



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\ELSA\SIDE\index.htm.*

Contents

1 Introduction	11
1.1 What does a router do?	11
1.2 What does the <i>ELSA LANCOM Office</i> offer?	13
2 Installation	21
2.1 Package contents	21
2.2 System preconditions	21
2.3 Setting up the computer	22
2.3.1 Windows 95 and Windows 98	22
2.3.2 Windows NT 4.0	23
2.4 Introducing the <i>ELSA LANCOM Office</i>	25
2.4.1 The Front of the Unit	25
2.4.2 The Back of the Unit	28
2.5 How to connect the device	28
2.5.1 Software installation	30
2.6 Configuration	30
2.6.1 Basic settings	30
2.6.2 Setting up Internet access	35
3 Configuration modes	39
3.1 Many paths lead to the <i>ELSA LANCOM</i>	39
3.2 The direct method: outband	40
3.2.1 Requirements for outband configuration	40
3.2.2 Outband configuration using <i>ELSA LANconfig</i>	40
3.2.3 Outband configuration using a terminal program	41
3.3 The user-friendly method: inband	41
3.3.1 Preconditions	41
3.3.2 Alternatively: Address administration with the DHCP server	41
3.3.3 Configuration using <i>ELSA LANconfig</i>	42
3.3.4 Configuration using telnet	43
3.4 Remote access: configuration using a Dial-up Networking	43
3.4.1 This is what you need for remote configuration	43
3.4.2 This is how you prepare the remote configuration	43
3.4.3 The first remote connection using a Dial-up Networking (<i>ELSA LANconfig</i>)	44
3.4.4 The first remote connection using a PPP client and telnet	44
3.4.5 Limiting remote configuration	45
3.5 New firmware with FirmSafe	46

3.5.1 This is how FirmSafe works	47
3.5.2 How to load new software	47
3.6 What's happening on the line?	49
3.6.1 <i>ELSA LANmonitor</i>	49
3.7 Trace outputs	51
3.7.1 How to start a trace	52
3.8 Configuration using SNMP	54

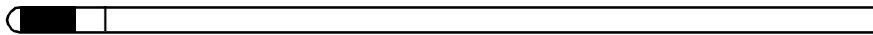
4 Operating modes and functions 55

4.1 Security for your configuration	55
4.1.1 Password protection	56
4.1.2 Login barring	56
4.1.3 Access control via TCP/IP	57
4.2 Security for your LAN	57
4.2.1 Security check	57
4.2.2 Callback	59
4.2.3 The hiding place – IP masquerading (NAT, PAT)	60
4.3 Call charge management	60
4.3.1 Charge-based ISDN connection limits	61
4.3.2 Time-dependent ISDN Connection control	61
4.3.3 Settings in the charge module	62
4.4 ISDN connections	62
4.4.1 ISDN name list	64
4.4.2 Interface settings	65
4.4.3 Router interface settings	65
4.4.4 <i>LANCAP</i> / interface settings	66
4.4.5 Layer list	67
4.4.6 Round-robin list	67
4.4.7 Script	68
4.4.8 Call acceptance	68
4.4.9 Number-list	69
4.5 Automatic address administration with DHCP	69
4.5.1 The DHCP server	70
4.5.2 DHCP – 'on', 'off' or 'auto'?	70
4.5.3 How are the addresses assigned?	71
4.5.4 Configuring the DHCP server	75
4.6 DNS	77
4.6.1 What does a DNS server do?	77
4.6.2 Setting up the DNS server	78
4.7 NetBIOS proxy	81

4.7.1 To the point: What is NetBIOS?	81
4.7.2 Handling of NetBIOS packets	82
4.7.3 Which preconditions must be fulfilled?	83
4.7.4 Linking two Windows networks	86
4.7.5 Dial-up procedure for a remote access station	87
4.7.6 Search and Find: the Network Neighborhood	88
4.8 The least-cost router	90
4.8.1 Function of the <i>ELSA LANCOM</i> least-cost router	90
4.8.2 Setting up the least-cost router	93
4.9 <i>ELSA CAPI Faxmodem</i>	95
4.9.1 Installation	95
4.9.2 Faxing with the <i>ELSA CAPI Faxmodem</i>	96
4.10 Office communications and <i>LANCAPI</i>	96
4.10.1 <i>ELSA LANCAPI</i>	96
4.11 The Integrated Branch Exchange	101
4.11.1 Connecting analog terminal equipment	101
4.11.2 Configuration using <i>ELSA LANconfig</i> and the setup wizards	102
4.11.3 Manual configuration using <i>ELSA LANconfig</i>	104
4.11.4 Operating the PBX by phone	113
4.12 Accounting	120
4.12.1 Configuring accounting	121
4.12.2 Reading the accounting data	121
5 Appendix	123
5.1 Technical data	123
5.2 Declarations of conformity	125
5.3 Warranty conditions	128
● Index	133
● Technical basics (on CD only)	R-1
Network technology	R-1
The network and its components	R-1
Connection modes	R-2
Kinds of networks	R-3
IP addressing	R-3
IP routing and hierarchical IP addressing	R-6
Expansion through local networks	R-8
Point-to-point protocol	R-12
The protocol	R-13

The PPP list	R-14
Everything ok? Checking the line with LCP	R-15
Assigning IP addresses via PPP	R-16
Callback functions	R-17
Fast ELSA callback	R-20
Callback as specified in RFC 1570 (PPP LCP extensions)	R-20
Channel bundling with MLPPP	R-21
IPX routing	R-22
Naming IPX addresses	R-23
Information about the LAN	R-23
IPX routing table	R-23
What happens when data is transmitted on an IPX network?	R-24
RIP and SAP tables	R-25
So many routers around here.....	R-25
Redundant routes	R-25
Exponential backoff.....	R-26
IPX packet filters	R-26
IP routing	R-28
The IP routing table	R-28
TCP/IP packet filters	R-31
Proxy-ARP	R-32
Local routing	R-32
Dynamic routing with IP RIP	R-33
IP masquerading (NAT, PAT)	R-35
DNS forwarding	R-37
Policy Based Routing	R-38
Bridging	R-38
● Description of the menu options (on CD only)	R-41
Status	R-43
Display and keyboard	R-44
Status/Connection	R-45
Status/Current-time	R-45
Status/Operating-time	R-45
Status/WAN-statistics	R-46
Status/LAN-statistics	R-48
Status/PPP-statistics	R-49
Status/IPX-statistics	R-57
Status/TCP-IP-statistics	R-62
Status/IP-router-statistics	R-68

Status/Config-statistics	R-70
Status/Queue-statistics	R-70
Status/Connection-statistics	R-71
Status/Info-connection	R-72
Status/Layer-connection	R-73
Status/Call-info-table	R-73
Status/Remote-statistics	R-74
Status/SO-bus	R-75
Status/Channel-statistics	R-75
Status/Time-statistics	R-76
Status/LCR-statistics	R-77
Status/Delete-values	R-77
Setup	R-77
Setup/WAN-module	R-78
Setup/LAN-module	R-88
Setup/IPX-module	R-89
Setup/TCP-IP-module	R-97
Setup/IP-router-module	R-101
Setup/SNMP-module	R-109
Setup/DHCP-module	R-110
Setup/NetBIOS-module	R-112
Setup/Config-module	R-114
Setup/LANCAPI-module	R-116
Setup/LCR-module	R-117
Setup/DNS-module	R-118
Setup/Time-module	R-119
Firmware	R-120
Other	R-122



1

Introduction

The use of ISDN router solutions is constantly increasing in the construction of corporate-wide infrastructures. High transfer rates and a full range of security mechanisms make the ISDN network attractive to businesses as the foundation for spanning the distances involved in wide-area networks. Local-area networks (LANs) that have evolved at various locations as well as individual PCs can be connected inexpensively by routers. Corporate branches and offices can be linked to the central network transparently using ISDN, making a single, central database available to all systems.

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

1.1

What does a router do?

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

This path is available in the form of an ISDN connection.

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 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 connection 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 the 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.

- Telephone functions

In addition to its ISDN router features, the *ELSA LANCOM 2000 Office* also contains an integrated private automatic branch exchange with four analog connections (a/b ports). Analog terminal devices such as telephones or fax machines can be connected to these ports, making the expense of acquiring new ISDN terminal devices unnecessary in the transition from an analog telephone connection to a modern ISDN Basic Rate Interface.

The *ELSA LANCOM* provides many useful functions such as internal call switching, internal calls, brokering, consultation hold, call redirection, call pickup, call charge metering, etc.

1.2

What does the *ELSA LANCOM 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.
- Plug in the ISDN cable.
- Switch it on.
- Go!

LAN connection

ELSA's ISDN routers work on Ethernet networks.

- Connect the *ELSA LANCOM 1100 Office* or *ELSA LANCOM 2000 Office* with the 10 Mbit LAN using the 10Base-2 or 10Base-T ports.

- An *ELSA LANCOM 800 Office* will find its way into the local 10-Mbit network through the 10Base-T connection.
- An *ELSA LANCOM 1100 Office* can be connected to a (Fast) Ethernet network using the 10/100Base-T port.

WAN connection

The *ELSA LANCOM Office* is connected to the S₀ 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. Switched connections using DSS1 or 1TR6 can also be used, as can leased-line connections.

Leased-line options that involve additional charges must be enabled separately.

Configuration

You can configure and customize the devices easily and quickly using the integrated configuration tool *ELSA LANconfig* for Windows operating systems. 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, 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 installation wizards of *ELSA LANconfig* and HTML configuration help you to put the devices into operation in only 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

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 device automatically selects the most economical provider for you, regardless of whether you are using the router, the *LANCAPI*, the *a/* b ports etc.).

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 the status information about the routers is always available on the screen with the help of this tool. For each device on the local network, the most important information is displayed, e.g.:

- Connection status for each B transfer channel
- Name of the remote side
- The device module (router, *LANCAP*, a/b port) connected
- Connection time and transfer speed
- 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 ISDN router allow you to monitor the ISDN and Ethernet connections and the current line connections, thus simplifying the process of diagnosing any systems failures.

Statistics

The comprehensive statistics function lets you keep track of your *ELSA LANCOM 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 provide a special range of IP addresses which the DHCP server automatically assigns to the devices in 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 be used as an efficient filter for the users in your own LAN. Access to specified domains can be denied to individual computers or complete networks.

ELSA LANCAPI and ELSA CAPI Faxmodem

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

Alle Workstations, die im LAN (Local Area Network) integriert sind, erhalten über die *LANCAPI* uneingeschränkten Zugriff auf Bürokommunikations-Funktionen wie Fax und 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 ISDN fax device is simulated at the workstation so that faxes can be sent. With the *LANCAPI*, the PC forwards the fax via the network to the router which establishes the connection to the recipient.

The *ELSA CAPI Faxmodem* furthermore 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 Office*.

The integrated branch exchange

An *ELSA LANCOM 2000 Office* can do even more. Four integrated a/b ports allow the connection of analog telephones, fax devices or modems.

The a/b ports are especially of interest when switching from analog lines to digital connections (ISDN). Analog terminal devices such as telephones and fax machines can also be used at the workstation with an *ELSA LANCOM 2000 Office*. This saves additional finances that would otherwise be invested in new digital end-user equipment. Furthermore, the PBX of the *ELSA*

*ELSA LANCOM
2000 Office only*

LANCOM 2000 Office modern additional ISDN supports functions such as call forwarding, callback, brokering, holding and three-way conference calls, internal calls, hotline, call charge metering and several more.

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 ISDN 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 ISDN 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 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.

2 Installation

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

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

2.1 Package contents

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

- *ELSA LANCOM Office*
- Power supply unit
- LAN connection cable
- ISDN connection cable
- Cable for the configuration interface (only *ELSA LANCOM 1000 Office*, *ELSA LANCOM 2000 Office* and *ELSA LANCOM 1100 Office*)
- Adapter for configuration cable (only *ELSA LANCOM 1000 Office*, *ELSA LANCOM 2000 Office* and *ELSA LANCOM 1100 Office*)
- Documentation
- CD containing *ELSA LANconfig*, other software and electronic documentation

Please contact your dealer directly if anything is missing.

2.2 System preconditions

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

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

- Network protocol TCP/IP installed and bound to the network card

2.3

Setting up the computer

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

2.3.1

Windows 95 and Windows 98

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

- Installing TCP/IP

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

- Allocate IP addresses (using DHCP)

If you are going to use the router as a DHCP server, set the workstations to obtain IP addresses automatically: **Start ► Settings ► Control panel ► Network ► TCP/IP ► Properties ► IP address ► Automatically receive IP address**. 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 ► Determine IP address**.

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 Gateway and DNS Server (not necessary when using DHCP)

On the workstation computers, specify the address of the local network router as the Gateway and as the Domain Name Server (DNS server):

Start ► Settings ► Control panel ► Network ► TCP/IP ► Properties ► Gateway and DNS configuration. Also enter a host name on the DNS Configuration page. In doing so, use the name of the PC, which ideally matches the user's name, to maintain a certain amount of consistency.

- Checking the IP Configuration

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

2.3.2

Windows NT 4.0

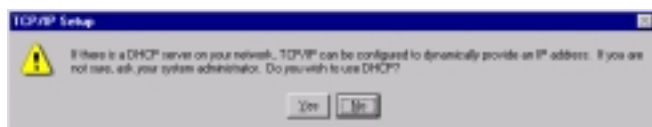
Using Windows NT 4.0 as an example, this section will show what needs to be done, if it is not already done for you, to ensure smooth communication between computers in a TCP/IP network with the router connected to the workstations.

- Installing TCP/IP

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

- Allocate IP addresses (using DHCP)

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



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

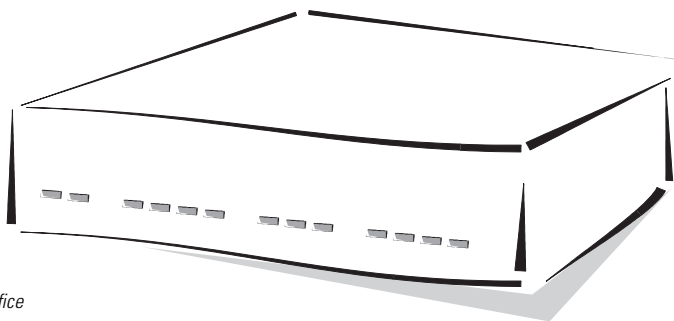
Under Windows NT 4.0 you can query the current IP configuration of your computer with **Start ► Run ► ipconfig**. This shows you which IP address was assigned to the computer by the DHCP server and which addresses have been specified for the gateway (not for the DNS server).

2.4 Introducing the **ELSA LANCOM Office**

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

2.4.1 The Front of the Unit

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



Model example:
ELSA LANCOM 2000 Office

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

a/b 1 to a/b 4

These LEDs show the status of the analog connections at the *ELSA LANCOM 2000 Office*:

Off		a/b port idle
green		Connection established
green	flashing	Outgoing call being executed (port offhook) (flashing normally)
green	flashing	- B channel not available (at bus or internal) - DTMF receiver not (or no longer) present - ISDN line not available
red	flashing	Incoming call pending (LED flashing in sync with ring)
red	once (flashing)	Incoming call, MSN OK, port for incoming calls blocked

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

NE



WAN
Chan 1+2

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!

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

LAN-tx, -rx,
LAN-Coll, -Link
LAN-FDpx, -Fast

These LEDs show the corresponding network controller status:

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

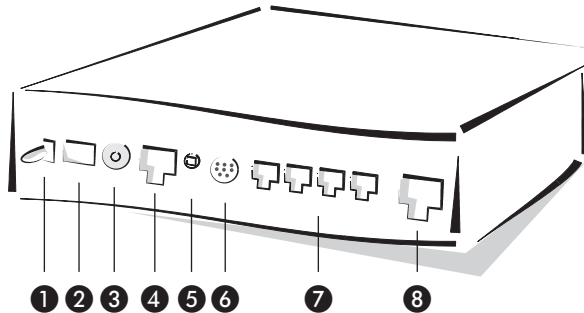


Both the LAN FDpx and LAN Fast LEDs apply only for 100 Mbit networks, so are only present with the ELSA LANCOM 1100 Office.

2.4.2

The Back of the Unit

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



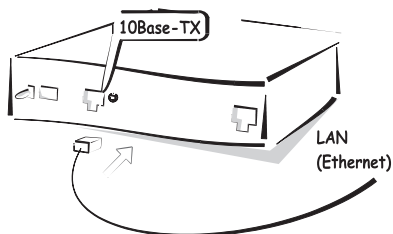
Model example:
ELSA LANCOM 2000
Office

- ❶ On/Off switch
- ❷ Connection for power supply unit
- ❸ 10Base-2 (BNC), only *ELSA LANCOM 1000 Office* or *ELSA LANCOM 2000 Office*
- ❹ 10Base-T (*ELSA LANCOM 800 Office*, *ELSA LANCOM 1000 Office* or *ELSA LANCOM 2000 Office*) for 10 Mbit networks or 10/100Base-Tx (*ELSA LANCOM 1100 Office*) for 10 Mbit or 100 Mbit networks
- ❺ Node/hub selector switch
- ❻ V.24 configuration interface (*ELSA LANCOM 1000 Office*, *ELSA LANCOM 2000 Office* or *ELSA LANCOM 1100 Office*)
- ❼ Four analog terminals (POTS, a/b ports, only *ELSA LANCOM 2000 Office*)
- ❽ ISDN S₀ port

2.5

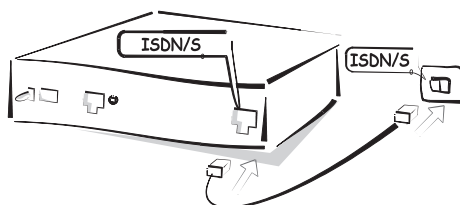
How to connect the device

- ❶ Connect your *ELSA LANCOM 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).



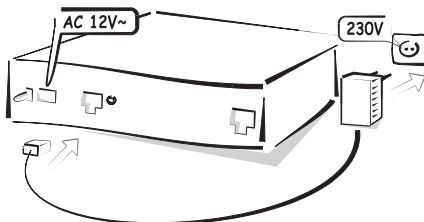
Model example:
ELSA LANCOM 800 Office

- ② Connect your *ELSA LANCOM 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).



Model example:
ELSA LANCOM 800 Office

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



Model example:
ELSA LANCOM 800 Office



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

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

2.6 Configuration

This example shows a simple LAN to Internet link.

Configure the unit using the following steps:

- Basic settings
- Setting up Internet 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.

2.6.1 Basic settings

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

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 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 S_0 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 S_0 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 ► ELSAlan ► ELSA LANconfig**.



- ② Select the option 'make all settings automatically' if you are **not** familiar with networks and IP addresses and one of the following conditions applies:

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

or

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



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

- ③ Select the option 'I want to make 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 adr. 10.0.0.1
set /setup/TCP-IP module/Intranet mask
255.255.255.0
```

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

- ④ To switch off the DHCP function:

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

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

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

2.6.2 Setting up Internet access

To configure Internet access, 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 your country and then choose either one of the preset Internet providers or general access using PPP.
- ③ In the dialogs that follow, enter the required access data, such as phone number, user name and password.



ELSA LANconfig

- ① Start *ELSA LANconfig* with **Start ► Programs ► ELSAan ► ELSA LANconfig**.
- ② Mark your *ELSA LANCOM Office* in the list of devices and call the wizards.
- ③ Select the wizard for Internet access and your country and then choose either one of the preset Internet providers or general access using PPP.
- ④ In the dialogs that follow, enter the required access data, such as phone number, user name and password and leave the wizard by selecting **Finish**.

That's it!

By clicking a few buttons, you have completed the configuration of the unit for Internet access through an ISDN 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 Office* can now surf the Internet at full performance.

3 Configuration modes

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

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

This section will show you the programs and routes you can use to access the device and set it up.

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

3.1 Many paths lead to the *ELSA LANCOM*

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)

The configuration interface is available with the *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1000 Office* and *ELSA LANCOM 1100 Office* models.

- 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*.

3.2 The direct method: outband

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

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



3.2.1 Requirements for outband configuration

What's needed?

- A router with a configuration interface, *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1000 Office* or *ELSA LANCOM 1100 Office*
- 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).

3.2.2 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.

3.2.3 Outband configuration using a terminal program

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

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

3.3 The user-friendly method: inband

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

3.3.1 Preconditions

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

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



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

3.3.2 Alternatively: Address administration with the DHCP server

If it is not absolutely essential that you configure the correct IP addresses "manually", the DHCP server will gladly do this task for you automatically. When using the DHCP server you can have the IP addresses for all computers on the network assigned automatically (see also chapter 'Automatic Address

Administration with DHCP'). The router will automatically define its own IP address for the LAN.

3.3.3

Configuration using *ELSA LANconfig*

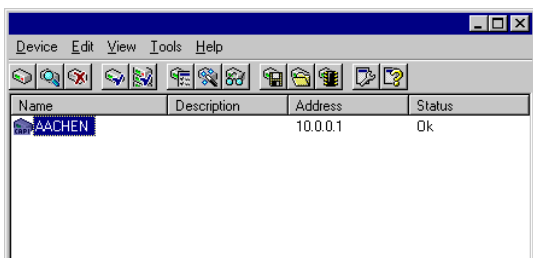
Start *ELSA LANconfig* e.g. via the Windows taskbar with **Start ► Programs ► ELSA LAN ► ELSA LANconfig**. *ELSA LANconfig* searches the local area network for devices. *ELSA LANconfig* will automatically launch the Setup Wizard if a device which has not yet been configured is found on the local area network.

Select one of the wizards offered and simply answer its questions. This will then set up the router for the task selected.



Just click on the **Browse** 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.

3.3.4 Configuration using telnet

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

```
Telnet 10.1.80.125
```

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

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

3.4 Remote access: configuration using a Dial-up Networking

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

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

3.4.1 This is what you need for remote configuration

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

3.4.2 This is how you prepare the remote configuration

- ① Attach the router to the power supply.

- ② Connect the device to an ISDN basic rate interface.

3.4.3

The first remote connection using a Dial-up Networking (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 ISDN 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 Networking connection is broken.

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

3.4.4

The first remote connection using a PPP client and telnet

- ① Establish a connection to the *ELSA LANCOM* 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.

3.4.5

Limiting remote configuration

The PPP connection of any other remote site to the router, of course, will only succeed if the device answers every call with the corresponding PPP settings. This is the case using the factory default settings because the default protocol (default layer) is set to PPP.

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

- ① Switch to the 'Security' tab in the 'Management' configuration section.
- ② In the 'Configuration access' field, choose whether the configuration is fully accessible, read-only or not accessible from remote networks.

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

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

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

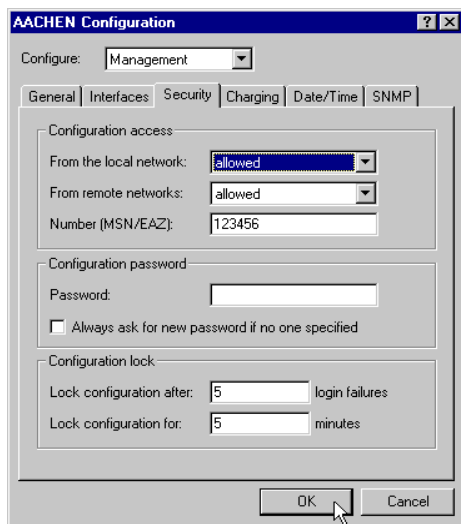


- ③ As the calling number in the 'Configuration access' area, enter a MSN or EAZ of your ISDN connection which is not used by the router, the *LANCAP1* or the a/b ports.

Alternatively, enter the following command:

```
set /setup/config-module/Farconfig (EAZ-MSN)
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.

3.5 New firmware with FirmSafe

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

3.5.1 This is how FirmSafe works

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

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

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

3.5.2 How to load new software

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

- *ELSA LANconfig* (recommended)
- Terminal programs
- TFTP



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

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

ELSA LANconfig



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

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

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

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

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

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

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

TFTP

With TFTP you can use the **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_1000u.130 writeflash
```

*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.

3.6

What's happening on the line?

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

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

3.6.1

ELSA LANmonitor

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

Installing *ELSA LANmonitor*

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

If *ELSA LANmonitor* is not yet installed on your computer, place the *ELSA LANCOM* in your CD drive. If the setup program does not start up automatically after insertion of the CD, start Windows Explorer, click on 'autorun.exe' on the *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.

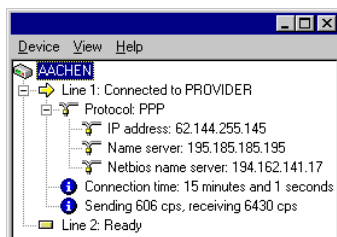
Checking your internet connection with *ELSA LANmonitor*

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 are 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.

3.7 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.

3.7.1 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

This parameter brings up the following display for the trace:
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.

3.8 Configuration using SNMP

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

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

4 Operating modes and functions

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

- Security for your configuration
- Security for your LAN
- Charge management
- ISDN connections
- PPP support
- IPX-Routing (only *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1100 Office*, *ELSA LANCOM 1000 Office*)
- IP routing
- Bridging (only *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1100 Office*, *ELSA LANCOM 1000 Office*)
- Automatic address administration with DHCP (except *ELSA LANCOM 800 Office*)
- DHCP-relay agent
- DNS server
- NetBIOS-Proxy (only *ELSA LANCOM 2000 Office*, *ELSA LANCOM 1100 Office*, *ELSA LANCOM 1000 Office*)
- Least-cost router
- *ELSA LANCAPI*
- Time check
- Telephone system (only *ELSA LANCOM 2000 Office*)
- 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.

4.1 Security for your configuration

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

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

4.1.1 Password protection

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

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

4.1.2 Login barring

The configuration in the *ELSA LANCOM 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)

4.1.3 Access control via TCP/IP

Access to the internal functions of the devices through TCP/IP can be restricted using a special filter list. Internal functions in this case means telnet or TFTP sessions to configure the *ELSA LANconfig*.

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

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

4.2 Security for your LAN

You certainly would not like any outsider to have easy access to or to be able to modify the data on your computers. The *ELSA LANCOM 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)

4.2.1 Security check

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

- All Calls are accepted from any remote station.
- Name: Only calls from those remote stations entered in the name list are accepted.
- Number: Only calls from those remote stations entered in the number list are accepted.

- 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 (Ppassword Authentication Protocol), CHAP (Cchallenge 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 a call is placed over an ISDN line, the caller's number is normally sent over the D channel before a connection is even made (CLI – Calling Line Identifier).

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

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

4.2.2

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.

4.2.3

The hiding place – IP masquerading (NAT, PAT)

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

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

IP masquerading provides a hiding place for every computer while connected with the Internet. Only the router module of the unit and its IP address are visible on the Internet. The 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.

4.3

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

4.3.1

Charge-based ISDN connection limits

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



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



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

4.3.2

Time-dependent ISDN Connection control

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

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



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

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



Only the router functions are protected by the charge and time monitoring functions! Connections via LANCAP1 or the a/b ports are not affected.

4.3.3

Settings in the charge module

The interface settings for the *ELSA LANconfig* can be found in the 'Management' configuration section on the 'Charges' tab, or under */Setup/Charge-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
- Router-units
All charges incurred through the unit
- Table-budget, Time-table
Tables with charges or times for the respective modules



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

4.4

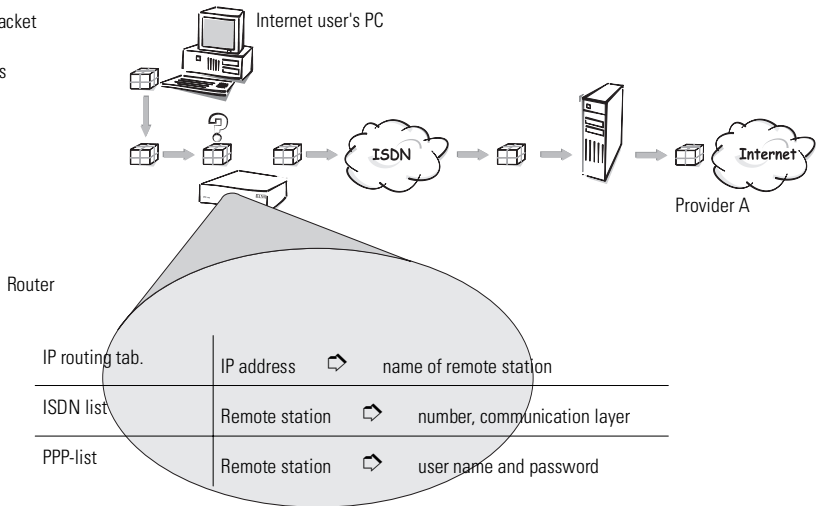
ISDN connections

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.

Data packet
with IP
address



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

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

4.4.1 ISDN name list

The name list in the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'Remote Stations' tab, or under `/Setup/WAN-module/ ISDN 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 station, 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

4.4.2 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.

4.4.3 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.

4.4.4 **LANCAPI interface settings**

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

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

- Subscriber numbers (MSN/terminal device selection numbers)

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

- Access to *LANCAPI*

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

- Transfer of own subscriber number

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

number entered in the 'Subscriber Number' field if no number has been specified in the CAPI application.

4.4.5

Layer list

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

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

- Layer name

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

- Encapsulation

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

- Layer-3

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

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

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

- Layer-2

Layer-2 protocol for the connection.

- Options

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

- Layer-1

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

4.4.6

Round-robin list

The round-robin list in the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'Remote Stations' tab, or under

`/Setup/WAN-module/Round-Robin List` during telnet or terminal sessions.

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

- Remote site
Name of the remote station as specified before in the name list.
- RoundRobin
Additional numbers for this remote station. 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.

4.4.7 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.

4.4.8 Call acceptance

The call acceptance settings for the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'Call Acceptance' tab, or under `/Setup/WAN-module/Security` 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.
- 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.
- 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.
- Name or number
The call will be accepted if one of the two checks was successful.

4.4.9

Number-list

The number list in the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'Call Acceptance' 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 station as specified in the name list. The remote station will be called back if so specified in the name list.

4.5

Automatic address administration with DHCP

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

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

In a smaller network, it is still conceivable that these addresses could be entered manually in all the computers in the network. In a larger network with

many workstation computers, however, this would simply be too enormous of a task.

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

4.5.1 The DHCP server

As a DHCP server, the *ELSA LANCOM 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
- Network mask
- Broadcast address
- 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.

4.5.2 DHCP – 'on', 'off' or 'auto'?

The DHCP server can be set to three different states:

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

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

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

The default state is 'auto'.

4.5.3

How are the addresses assigned?

IP address assignment

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

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

From the address used (IP or Intranet address) and the associated network mask, the DHCP server determines the first and last possible IP address in the local network as a start or end address for the address pool.

- If the router has neither an IP address of its own nor an Intranet address, the device has gone into a special operating mode. It then uses the IP address '10.0.0.254' for itself and the address pool '10.x.x.x' for the

assignment of IP addresses in the network. In this state, the DHCP server only assigns IP addresses and their validity to the computers in the network, but not the other information.

If only one computer in the network is 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.

Network mask assignment

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

Broadcast address assignment

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

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

DNS and NBNS assignment

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

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



Default gateway assignment

The 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' 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' entry for your network adapter and open **Properties**.

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

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

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

- new
The computer has made its initial request. The DHCP server verifies the uniqueness of the address that is to be assigned to the computer.
- unknown
While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the DHCP server has no means of obtaining additional information on this computer.
- status
A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.
- dynamic
The DHCP server assigned an address to the computer.

4.5.4

Configuring the DHCP server

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

- You have not yet configured a network or your existing local network does not use TCP/IP. The DHCP server in your new ELSA device lets you assign IP addresses to all of the computers in the network and to the 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 'ELSAlan' program group. When loading, the *ELSA LANconfig*, will detect an unconfigured router in the network and will launch the wizard for the basic settings.
 - If you have not previously used any IP addresses in your network, select the option 'Make all settings automatically' in this wizard and confirm your selection with **Finish** in the next window. The wizard assigns the IP address '10.0.0.1' with the netmask '255.255.255.0' to the router and enables the DHCP server. On the basis of this IP address, the device then determines the valid address pool for the DHCP assignment.
 - In the event that IP addresses were already in use in your network before converting to DHCP operation, select the option 'I would like to adjust the settings manually' in the wizard. In the next window, enter an unused IP address from the previously-used address range and activate the DHCP server.

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

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

Manual configuration

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

4.6

DNS

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

4.6.1

What does a DNS server do?

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

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

- a *ELSA LANCOM 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 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 Office* can also be used as an extremely convenient filter mechanism. Requests for domains can be prohibited throughout the LAN, for subnetworks, or even for individual computers—simply by specifying the domain name.

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

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

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

4.6.2 Setting up the DNS server

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

- ① Switch the DNS server on.

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

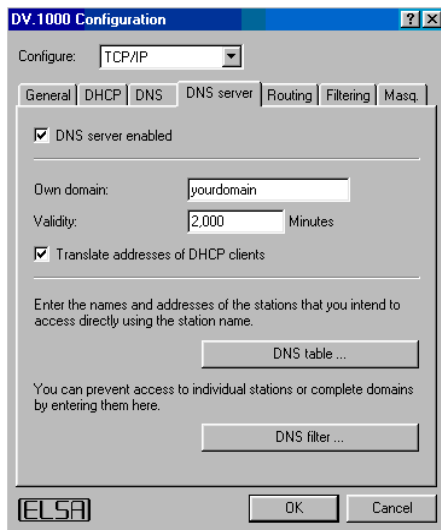
- ② Enter the domain in which the DNS server is located. The DNS server uses this domain to determine whether the requested name is located in the LAN. Entering the domain is optional.

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

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

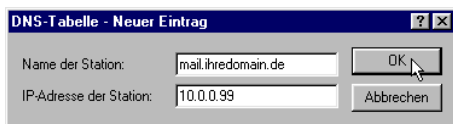
```
set setup/dns-module/dhcp-usage yes
```

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



- ④ The main task of the DNS server is to distinguish requests for names in the Internet from those for other remote stations. Therefore, enter all computers into the DNS table
- for which you know the name and IP address,
 - that are not located in your own LAN,
 - that are not on the Internet and
 - that are accessible via the router.

For example, if 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:

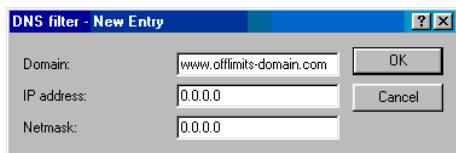


```
cd setup/dns-module/dns-table
set mail.yourdomain.com 10.0.0.99
```

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 .com domains, enter:

```
set 002 *.com 10.0.0.123 255.255.255.255
```

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

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

4.7

NetBIOS proxy

With the NetBIOS proxy function, a *ELSA LANCOM 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.

The feature is available only with the ELSA LANCOM 2000 Office, ELSA LANCOM 1100 Office and ELSA LANCOM 1000 Office models.



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

4.7.1

To the point: What is NetBIOS?

NetBIOS provides a simple, trouble-free means of networking multiple computers. An important example for NetBIOS networks is the Microsoft Network, with which several Windows 3.11, 9x and NT workstations can be networked simply by sharing the resources (drives or printers) of the individual computers with the other participants.

In a Microsoft Network, the computers are only addressed via their names. Multiple computers can be organized into groups, and multiple groups can be grouped further as Namenräumen 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 Office* offers such a billboard. The interconnection of Microsoft Networks is thus possible without a server as a result of this simple realization of the NBNS. The computers in the networks to be interconnected thus publicize their names and add them to the billboards in the respective remote networks.

4.7.2 Handling of NetBIOS packets

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

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

- In the NetBIOS module, it is possible to specify the remote stations to which the name information should be transferred via NetBIOS to ensure the routing of those packets that are actually required. After the NetBIOS module has been switched on and an unspecified waiting time has elapsed, a connection is established to the NetBIOS remote stations (insofar as these are not individual remote access workstations). The duration of the waiting period will be increased if the connection cannot be established. The following exchange of NetBIOS information then fills the billboard for the first time.
- In its proxy function, the unit answers queries to computers already known in the NetBIOS module (on the billboard) by proxy for those computers. After the initial exchange of information, no new connections are established as a result of queries to workstations in the local network, or to known workstations in the remote network.

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

4.7.3

Which preconditions must be fulfilled?

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

Installed components

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

- Network protocol

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



Unlike IX and PI, NetBEUI is not ratable and is thus only available in Microsoft Networks. If multiple Microsoft Networks are to be interconnected using routes, NetBIOS must be based on a ratable protocol in the ELSA LANCOM Office, such as IPA.

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

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

- Client

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

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

- Service

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

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

Windows Network settings

- Name and group designation

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

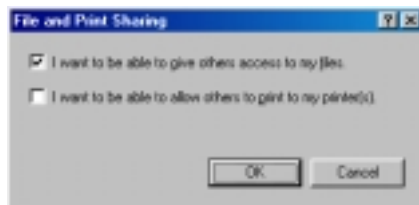


The name of the workstation must be unique. That applies to all Windows Networks, and all groups that you intend to connect using NetBIOS within these networks. Names also may not recur in different groups.

- 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.



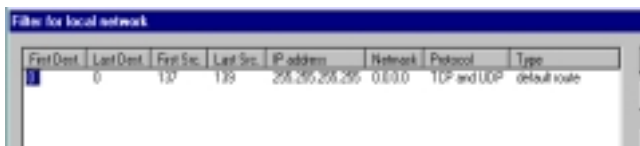
It's easy to check whether the Windows Network settings have been made correctly: the local computer must appear with its name in the Network Neighborhood.

4.7.4

Linking two Windows networks

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

- ① Set up both networks for a LAN-LAN interconnection via TCP/IP as described in the Workshop. We recommend using the convenient *ELSA LANconfig* wizard.
- ② Check the settings of the IP filter. This filter must capture all NetBIOS packets to be sent over the DEFAULT route to ensure that they do not lead the establishment of a connection on the DEFAULT route. This has been preset in the unit's factory defaults.



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



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.

4.7.5 Dial-up procedure for a remote access station

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

- ① The *ELSA LANCOM 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 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.

4.7.6

Search and Find: the Network Neighborhood

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

NetBIOS Routing via LAN-LAN Coupling

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

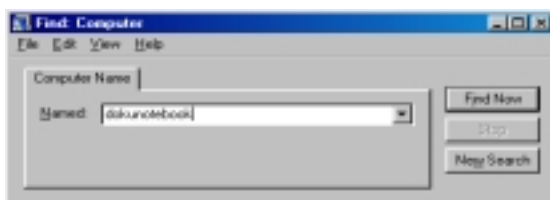
```
dir /Setup/NetBIOS-module/Host-list
```


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	192.168.100.1 62	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 Office* via Dial-Up Networking.

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

4.8 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 wide 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 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 *LANCAP!* etc).

4.8.1 Function of the *ELSA LANCOM* least-cost router

The LCR analyzes the digits dialed by the router or *LANCAP!*. The *ELSA LANCOM 2000 Office* also takes digits dialed by connected devices such as telephones or fax machines into account.

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:

Dialing 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 Munich (or other numbers with the prefix '089') on weekends will be made using the provider with the network prefix '01097'. 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 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. With this information on hand, you can now begin feeding your least-cost router...

4.8.2

Setting up the least-cost router

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

- Which operating modes of the *ELSA LANCOM 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:
 - ☐ Router
 - ☐ a/b ports (*ELSA LANCOM 2000 Office* only)
 - ☐ *LANCAPI*



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

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

Least-cost table - New Entry

Forward this prefix: 030

To Call-by-Call number: 01013

☒ Mondays
 ☒ Tuesdays
☒ Wednesdays
 ☒ Thursdays
☒ Fridays
 ☐ Saturdays
☐ Sundays
 ☐ Public holidays

Start time: 8 : 00 PM

End time: 12 : 00 PM

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

OK Cancel

- 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).

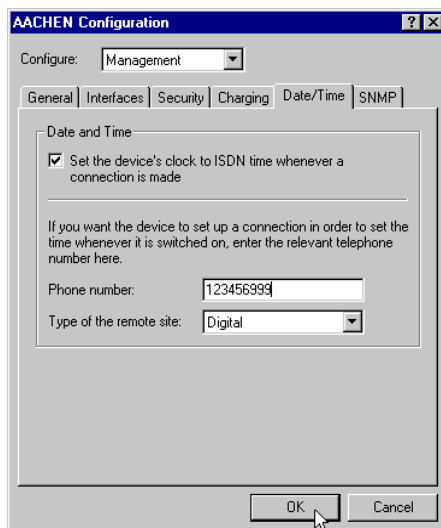
*Build the LCR table one step at a time and check your results. Open the ELSA LANmonitor, for example, and establish connections to the remote stations to be rerouted according to the table using the ELSA LANCAPI. Use the dialed number to verify whether the LCR settings suit your requirements. For router 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 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!

4.9 **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 Office*.

4.9.1 **Installation**

The *ELSA CAPI Faxmodem* can be installed from the CD setup. Always install the *ELSA CAPI Faxmodem* together with the current version of *ELSA LANCAPI*. After restarting, the *ELSA CAPI Faxmodem* will be available to your

system. Under Windows 95 or Windows 98, it can be found under **Start ► Control Panel ► Modems**.

4.9.2

Faxing with the *ELSA CAPI Faxmodem*

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



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

4.10

Office communications and *LANCAPi*

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

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

4.10.1

ELSA LANCAPi

What are the advantages of *LANCAPi*?

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

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

Installing the *LANCAPI* client

The *LANCAPI* is made up of two components, a server (in the *ELSA LANCOM 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.

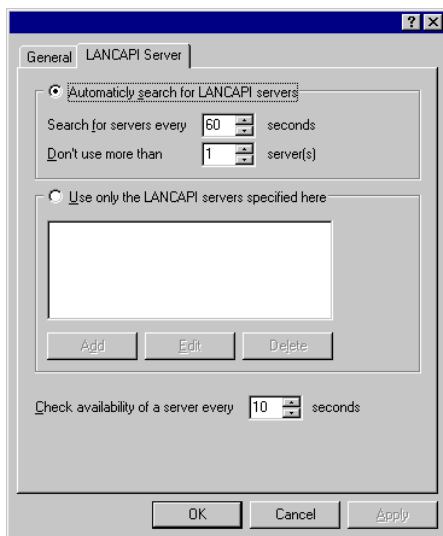
Configuring the *LANCAPI* client

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 Office* in your LAN as a *LANCAPI* server.

- ① Start the *LANCAPI* client in the 'ELSAIan' 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 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.



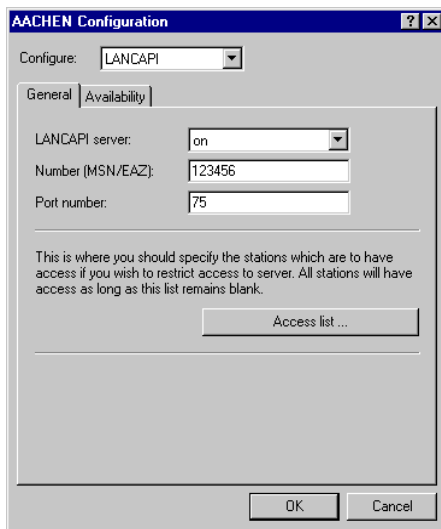
Configuring the *LANCAPi* server

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

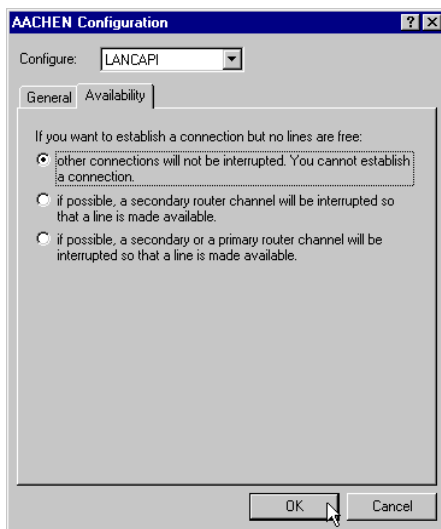


- ② Activate the *LANCAPI* server, or set it to permit outgoing calls only. In the latter case, the *LANCAPI* will not respond to incoming calls—to receive faxes, for example. Permitting outgoing calls only is useful if you do not have a specific call number available for the *LANCAPI*.
- ③ When the *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 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. The *LANCAPI* must wait if two router connections are established to separate remote stations (two main channels busy).
- 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'.

4.11 The Integrated Branch Exchange

When switching from analog lines to digital connections (ISDN), whether or not the existing analog terminal devices will still work often comes into question. Four integrated a/b ports in the *ELSA LANCOM 2000 Office* allow the connection of analog telephones, fax devices, answering machines and modems.

This allows you to use analog terminal devices at the workstation as well. This saves additional finances that would otherwise be invested in new digital terminal devices. Furthermore, the a/b ports of the *ELSA LANCOM 2000 Office* support modern, additional ISDN functions such as call forwarding, callback, brokering, holding and three-way conference calls.

You can also use the features of a small PBX when using the equipment connected to the a/b ports. For example, you can carry out internal calls, transfer an external call to another extension or alternate between internal and external callers.

Be sure to refer to the features of the least-cost router!

The PBX features are only available with the ELSA LANCOM 2000 Office!



4.11.1 Connecting analog terminal equipment

What devices can be used?

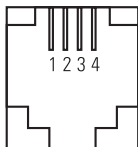
In principle, any analog terminal equipment can be connected to the a/b ports of the *ELSA LANCOM 2000 Office*:

- Telephones
- Class 3 fax machines
- Activating the answering machine

- Modem
- Combination units

Telephone adapter (RJ11)

ELSA provides the necessary adapters to ensure that you can continue to use your analog equipment (such as telephones, answering machines and fax machines).

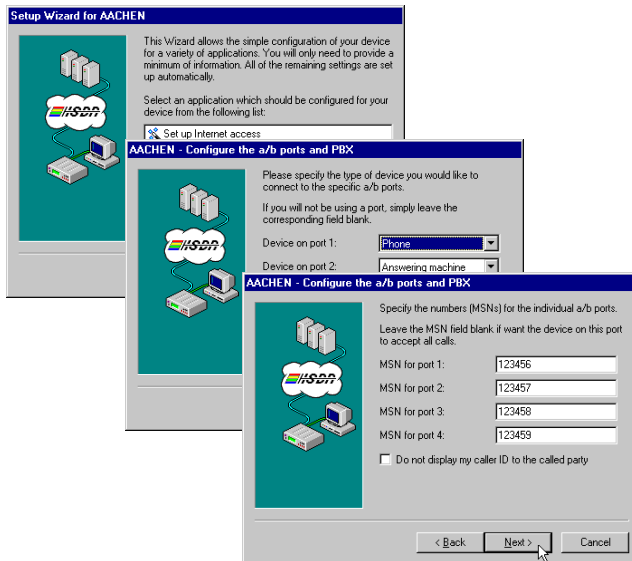


4.11.2

Configuration using *ELSA LANconfig* and the setup wizards

ELSA LANconfig includes a wizard for configuring the a/b ports and the PBX of the *ELSA LANCOM 2000 Office*, which makes all necessary settings in the *ELSA LANCOM* software environment for you. It only requires you to specify what device you have connected to which a/b port and which phone numbers you want assigned to the individual devices.

- ① Start the *ELSA LANconfig* from the 'ELSAIlan' program group.
- ② In the device list, select the *ELSA LANCOM* that you want to configure. Click **Extras ► Setup Wizard** and then select the 'Configure a/b ports and branch exchange' option.



- ③ In the steps to follow, specify what equipment you have connected to which port and assign call numbers to the a/b ports.
- ④ Finally select whether you want to use the *ELSA LANCOM* as a branch exchange system or continue using it as a normal telephone connection.
- ⑤ With this, you have completed the configuration. In the window that follows, click **Finish** to close the wizard and save the new settings in your *ELSA LANCOM*.

What exactly have you just achieved with the wizard? The result depends on the type of equipment you have selected for the ports. In addition to the configured call number and the default internal number, the following general settings apply:

- Telephone

If you connect a phone to an a/b port using this configuration, you will be informed of a second incoming call for this port during an existing call by call waiting.

- Activating the answering machine

For answering machines, second incoming calls are not indicated by call waiting, but instead can be dealt with by the call acceptance feature. If

the answering machine picks up the call faster than you can get to it, you can simply lift the receiver of another phone to take over the call.

- Fax and modem

For fax machines and modems, the wizard automatically disables the options described above, since neither call waiting nor call acceptance would be useful with these devices.

- External Calls

- If the *ELSA LANCOM 2000 Office* is configured as a PBX, when you lift the receiver you will be connected to the *ELSA LANCOM* at first. You can then make internal calls directly or dial 0 to get a dialing tone from the switching center for placing external calls.

If you have connected your ELSA LANCOM 2000 Office to a PBX, dialing 0 will connect you, as usual, to this, top-level system, from which you may have to dial 0 again for an external line!

When entering numbers in phone books or quick-dial lists for telephones, modems and other devices, be sure to include the preceding "0".

- If the *ELSA LANCOM 2000 Office* is set as a normal phone connection, you will hear the dial tone of the switching center (or the branch exchange to which you have connected the *ELSA LANCOM 2000 Office*) immediately upon lifting the receiver. With this configuration, internal calls via the *ELSA LANCOM 2000 Office* are not possible.

If the results of the configurations made using the wizards do not meet your requirements, you can, of course, change the settings at any other time as described in the following section.

4.11.3

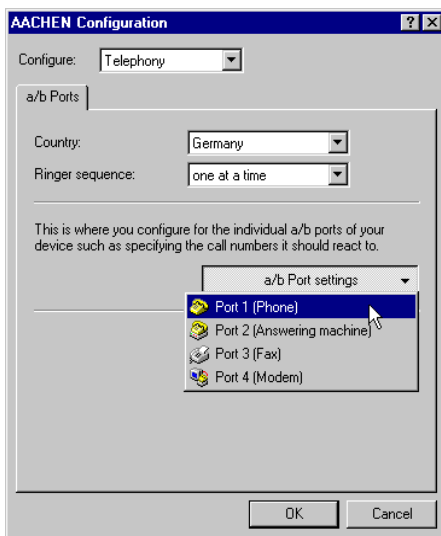
Manual configuration using *ELSA LANconfig*

You can manually configure exactly how each of the four a/b ports is to react to incoming and outgoing calls.

Select the 'Telephony' configuration section. First set the country in which you operate your *ELSA LANCOM 2000 Office* on the 'a/b Ports' page. You can also define here what is to take place for incoming calls to which several devices can react: Do you want all devices to ring individually, one after the other, in pairs or all at the same time?

Take into account the high current consumption, especially of old telephones. If several such units ring at the same time, the ELSA LANCOM power adapter

can become overloaded. If this might be the case, select 'individually' or 'in pairs':



Now use the pull-down list for the a/b port settings to open each port for configuration. The icon in front of each entry indicates what device type is connected to the port. Select the entry that you want to modify from the list.

General preferences

Customize the following settings on the 'General' page for every a/b port in use:

a/b Port settings - Port 1

General | Public exchange access | Class of service | Availability

Number (MSN/EAZ): 123456

Internal calling number: 11

Description: Phone

Capability: Telephony analog

☐ Don't ring on incoming calls (do-not-disturb service)

☐ Let hear knocking tone on incoming call during a conversation

☐ Generate metering pulse (for phones with charging display)

☐ Suppress transmission of own phone number to the remote site

☐ Allow automatic adoption of an established connection by another port (for answering machines)

☐ Automatically interconnect two external calls when hanging up

☐ Dial the following number whenever the phone is picked up:

Number: 123666

OK Cancel

- Assign a 'call number' to the connection: MSN (Multiple Subscriber Number) for multiple device terminals with DSS1 as D channel protocol, DDI (Direct Dial In) for system terminals or EAZ (terminal device selection number) for 1TR6 connections.
 - If the a/b port should react to more than one phone number, enter them separated by semicolons.
 - The first number specified will be displayed for calls from the switching center and the remote station.
 - If you do not enter any numbers, the a/b port reacts to all incoming calls and always sends the main number of your terminal to the switching center and the remote station.
- The preset internal call number is fixed and cannot be changed:
 - '11' for a/b-Port 1
 - '12' for a/b-Port 2
 - '13' for a/b-Port 3
 - '14' for a/b-Port 4
- Enter a description for the port. The description has no influence on the functions of the port or on the device connected to it. Its purpose is to make it easier to find which device is connected to which port. The following functions are available:
 - No description
 - Telephones

- Class 3 fax machines
- Activating the answering machine
- for the modem
- Combination units
- Select the service that the a/b port itself is to inform the remote station of while establishing a connection. This setting does not select the acceptance of incoming calls based on specific service attributes! Possible settings are:
 - Analog 3.1 kHz (default)
 - Language
 - Class 2/3 fax
- Enable or disable the following options to suit your needs:
 - 'No call signal ...' switches off ringing for the connected device.
 - 'Call ... signal with call waiting' allows the port to be informed of second incoming calls during an existing call.
 - The 'Generate call charge metering' feature generates a call charge pulse based on the ISDN call charge information and sends it to the device connected to the port. You can use this to monitor the costs of calls on analog phones that are equipped with a tariff display. Disable this option for ports to which fax machines or modems are connected, because the call charge pulse can corrupt or interrupt data transfer.



Call charge metering only functions correctly with connections having 'AOCD' (which enables the sending of charge information during the call). In the case of 'AOCE', the charge information is not sent until after the receiver is returned to its base, when the telephone is no longer able to detect all impulses.

- 'Display own number ... suppress' prevents the subscriber's number from being sent to the remote station, for example if you do not want the caller to be able to be identified based on his or her phone number. The subscriber number is always sent to the switching center. Thus it is possible for the telephone company to generate an itemized breakdown of the telephone charges based on subscriber numbers even if sending the numbers is suppressed.



The ability to "selectively suppress the call number" might have to be obtained separately from the telephone company.

- 'Automatic acceptance ...' allows a call to be accepted even though it has already answered by a device at another port. Generally, this option is applied only to ports with answering machines.
- 'External calls ...' allows external callers to be connected. If you are holding a call with two external callers, you can connect them simply by hanging up the receiver.



The feature for external call switching too might have to be obtained separately from the telephone company.

Note when using this type of call switching, that you will continue to be charged even though you are no longer participating in the call!

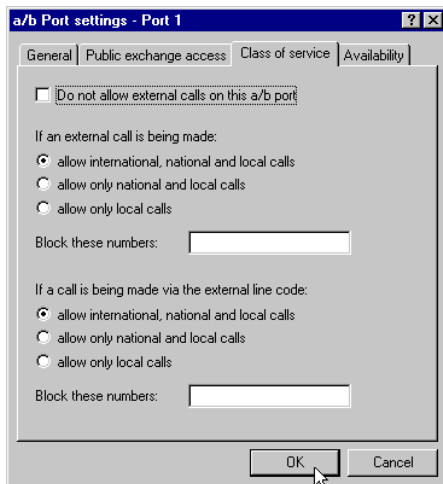
- 'Dial this number ... automatically:' Here, enter a call number to be used by the hotline feature. If this feature is enabled, the specified number will be dialed automatically five seconds after the receiver has been picked up if no other numbers have been dialed.



You can also configure the hotline feature using the buttons on your telephone. Doing so overwrites the settings made in ELSA LANconfig.

Setting external calls

Switch to the 'External Calls' page to make settings such as how the a/b port should behave if the receiver is picked up and if the flash button is pressed. Here we use the phrase, "picking up the receiver", generally, meaning opening the port for dialing, such as done by a modem or fax machine.



You can choose one of three options for the behaviour when picking up the receiver:

- If you choose Option 1, picking up the receiver will connect you to the *ELSA LANCOM* only. You can then place internal calls, i.e. call a device connected to another a/b port. How to place external calls depends on your configurations:
 - If the *ELSA LANCOM* is connected directly to an ISDN terminal, dial '0' to get an outside line.
 - If you have connected the *ELSA LANCOM* to another, larger PBX, you may have to additionally dial the PBX code to place an external call.
- If you choose Option 2, picking up the receiver will connect you to the terminal to which your *ELSA LANCOM* is connected. This is equivalent to a connection to the *ELSA LANCOM* and having '0' dialed automatically. You then have the following options:
 - If the *ELSA LANCOM* is connected directly to an ISDN terminal, you can place external calls without having to dial any preceding number.
 - If you have connected the *ELSA LANCOM* to another, larger PBX, you may have to dial the PBX code to place an external call.
- If you choose Option 3, picking up the receiver will connect you to the terminal to which your *ELSA LANCOM* is connected and, after the internal connection is established to the *ELSA LANCOM*, a '0' is dialed automatically. In addition to this, the number entered in the field at the

bottom of the window is also dialed. With this configuration, you have, among others, the following options:

- If you have connected the *ELSA LANCOM* to another, larger PBX, you can have the PBX code for placing external calls dialed automatically so that you can get an external line directly, without having to dial any preceding code.
- If you only want to place a long-distance call using a specific telephone company based on the call-by-call method, enter in addition to the required line code the prefix for the operating company (e.g. 0101x). Then, each time you pick up the receiver, you automatically get a dial tone at your phone service provider.

The function of the flash button (R button)

Use the settings in the lower section of the 'External Calls' page to define the results of pressing the flash button.



The flash button on most phones is the callback or R button. Its function is usually configurable. Refer to the technical documentation provided with your telephone to find out how this button is configured by default and how to set it to the flash function. The ELSA LANCOM accepts flash signals of between 70 and 300 ms in length.

For the flash button, too, you can choose one of the three described options. These options are similar to those which control what happens when you pick up the receiver:

- If you choose Option 1, pressing the flash button will establish a connection to the internal PBX of the *ELSA LANCOM*. You can then place an internal call or dial '0' to establish a connection to your ISDN terminal (or, if connected, your external PBX).
- If you choose Option 2, pressing the flash button will connect you directly to the ISDN terminal (or, if connected, your external PBX).
- Option 3 automatically dials the preset external number when you press the flash button.

By combining the settings for picking up the phone handset and pushing the flash button, you can customize your PBX in the *ELSA LANCOM* to meet your needs.

- Your *ELSA LANCOM* is connected directly to an ISDN terminal. Enable the second option for picking up the receiver and the first option for the

flash button. You can now place an external call when you pick up the receiver and switch to an internal call by pressing the flash button.

- Your *ELSA LANCOM* is connected to a larger PBX. Enable the first option for picking up the receiver and the third option for the flash button. In the 'External prefix' field, enter the digit required by your PBX for obtaining an external line. Then, when you pick up the receiver, you can place an internal call and then press the flash button to dial automatically all required codes for initiating an external call.

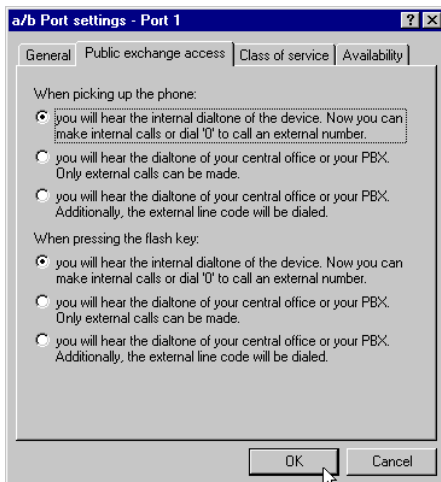
The flash button has special significance depending on whether there are any currently active connections, for which callbacks are being held, or whether a connection is currently being dialed. The following table illustrates what happens in these situations. Generally you may assume that you will achieve intuitively what you intend when you push the flash button.

In detail, the following takes place:

Connection	State	Flash Button Result
no active connection	- dial tone - incomplete call - timeout during call - remote station rings - timeout while ringing	The call or attempt to connect is canceled and the configured function is carried out.
active connection		The connection is placed on hold and the configured function is carried out.
connection on hold	- dial tone	You are returned to the call that you have placed on hold.
	- incomplete call - timeout during call	The call is canceled and the configured function is carried out.
	- remote station rings - timeout while ringing	The attempt to connect is canceled and you are returned to the call that you have placed on hold.
one active connection and one connection on hold or one call waiting connection pending		Flash + '0': held/call waiting connection is disconnected. Flash + '1': active connection is disconnected and you are switched to the held/call waiting connection. Flash + '2': you are switched from the active connection to the held/call waiting connection. Flash + '3': a three-way conference call is established.
three-way conference call active		Flash + '2': the three-way conference is held and split into one active and one held connection.

Setting direct outward dialing

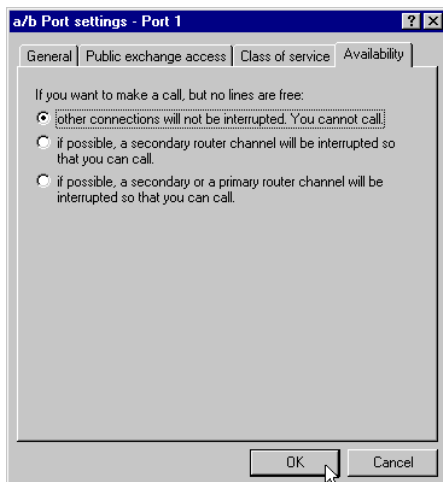
Use the 'Direct outward dialing' page to specify whether external calls are permitted for the devices connected to each a/b port.



Whether or not external calls are enabled, the call acceptance function always remains enabled. Outgoing calls, however, can be restricted to local calls and non-international long-distance calls. Specific phone numbers can be blocked as well.

Setting availability

Use the 'Availability' page to specify how the *ELSA LANCOM* behaves if a connection is to be established through the a/b ports (i.e. an incoming or outgoing call) while both B channels are busy (priority control). The available options are:



- Do not allow other connections to be disconnected. The connection cannot be established using the a/b port.
- Allow the use of secondary channels, for example for channel bundling. The connection through the a/b port can be established if a main channel is free.
- Allow main channels to be disconnected. A connection can always be established via through the a/b port; an existing router connection will be disconnected for the duration of the call if required. In other words, you can always be reached by phone.

For the ELSA LANCOM 2000 Office to be able to detect incoming calls even while other connections are active, call waiting must be enabled.



4.11.4

Operating the PBX by phone

With the *ELSA LANCOM 2000 Office*, you can use certain convenient services (like brokering) when making phone calls. This requires the use of a telephone with tone dialing (multi-frequency dialing) and a flash button.

If you do not know exactly whether your telephone uses tone or pulse dialing, you can usually find out simply by listening to the sounds produced in the telephone receiver when dialing: If you hear a sort of rattling sound for each dialed digit, your phone is using pulse dialing; if you hear various tones, it is using tone dialing.



Certain services (such as call waiting) are features which have to be applied for from the telephone service provider directly and include an additional charge.

Call waiting

With this feature, an audible signal lets you know if another call is coming in while you are already on the line. You can then choose to continue your present call or end it in order to take the second incoming call. To accept a call-waiting call, follow these steps:

- ① Check activation
 - To check whether this service is active, pick up the receiver and dial ***#43#**.
 - If you hear two bright tones, the feature is enabled. If you hear two dark tones, the feature is disabled.
 - ② Enable call waiting
 - Lift the receiver and wait for a dial tone.
 - Enter ***43#** on the number pad on your phone.
 - Wait for the announcement to end and then hang up the receiver.
 - ③ Accept a call-waiting call
 - Press the **R** button within 30 seconds after you hear the call-waiting signal tone through the receiver.
 - Then push the number **2**. The first call is now inactive and the second call active.
 - Press the **R** button followed by **2** to switch back and forth between callers (also called brokering).
 - ④ End the existing connection
 - Press the **R** button.
 - Then push the number **1** to terminate the active connection.
- Note that the receiver has to be hung up or the release button pressed for at least a half second between two calls.*
- ⑤ Disable call waiting
 - Lift the receiver and wait for a dial tone.
 - Enter **#43#** on the number pad on your phone.



- Wait for the announcement to end and then hang up the receiver.

Three-party conference call

Use this feature to carry on a call with two other callers at the same time. This function allows you to call the other two parties yourself or let a call-waiting caller into an existing call.



A conference may consist of two external and one internal callers. Two internal callers cannot hold a three-party conference call with one external caller!

To establish a three-party conference calls, follow these steps:

- ① Three-party conference with a call waiting party
 - Press the **R** button within 30 seconds after you hear the call-waiting signal tone through the receiver.
 - Then push the number **2**. The first call is now inactive and the second call active.
 - Press the **R** button again.
 - Then push the number **3** to initiate the three-party conference call.
- ② Three-party conference call with two independent connections
 - First establish a connection to one of the call parties.
 - Then push the **R** button. Depending on how external calls are configured, you then hear either an internal or external dial tone.
 - Dial the number of the second call party. The first call is now inactive and the second call active.
 - Then push the number **3** to initiate the three-party conference call.
- ③ End an active connection
 - Press the **R** button.
 - Then push the number **1** to terminate the active connection.
- ④ End both connections
 - You can terminate both connections of the three-way conference at the same time by hanging up the receiver.



Note the configuration of the 'Automatically connect external calls when receiver hung up' option for the corresponding a/b port. If this option is enabled, calls are not disconnected when the receiver is hung up. Instead

both external callers are connected with each other.

Note when using this type of call switching, that you will continue to be charged even though you are no longer participating in the call!

Callback/Brokering

This function lets you establish a second call parallel to an existing connection, for example to ask a colleague something. To initiate the callback, proceed as follows:

- ① Establish a second call
 - Press the **R** button.
 - Then dial the number of the second call party. The first call is now inactive and the second call active (callback)

You can place the second call either to an internal or external party.

- ② Brokering

- Press the **R** button followed by **2** to switch back and forth between callers (also called brokering).

- ③ Connections

- You can connect both call parties to each other by hanging up the receiver.

Note the configuration of the 'Automatically connect external calls when receiver hung up' option for the corresponding a/b port. If this option is enabled, you can also connect two external callers to each other.

- ④ End the existing connection

- Press the **R** button.
- Then push the number **1** to terminate the active connection.

If you disconnect the active call simply by hanging up the receiver, the telephone rings immediately after being hung up to remind you of the caller you placed in the inactive connection.

Call pickup

If you have telephones connected to more than one a/b port, you can use this feature to pickup an incoming call intended for another phone on your phone.

- ① Pick up your receiver when a call rings on another terminal.

- ② When you hear the internal dial tone of the *ELSA LANCOM 2000 Office*, dial the internal call number for the a/b port to which the call is being placed. If you do not hear the internal dial tone of the *ELSA LANCOM 2000 Office* right away, you may need to press the **R** button, based on the configuration, to establish a connection to the *ELSA LANCOM 2000 Office*.

- ③ Then push the number **8** to take over the call to the other terminal.



*If you are currently in the middle of a call, press, for example, the **R** button, based on the configuration of the *ELSA LANCOM 2000 Office*, in order to place the current caller on hold, and then pick up the second call using the internal call number followed by **8** on your telephone.*

Call forwarding

This function makes you available at your number at all times. You need only enter the relevant destination call number to have all calls automatically forwarded to this number. The call can be forwarded immediately, after 15 seconds or if busy. Proceed as follows:



*Before you can use this feature, you have to assign an MSN to the a/b port. Use *ELSA LANconfig* to assign the MSN.*

- ① Enable call forwarding
- Lift the receiver and wait for a dial tone.
 - Enter one of the following sequences on the number pad on your phone:
 - * 2 1 *** (for "immediate" call forwarding)
 - * 6 1 *** (for call forwarding "after 15 seconds")
 - * 6 7 *** (for "busy" call forwarding)
 - Enter the desired destination call number and press #.
 - If you hear two bright tones, the feature is enabled and you can hang up the phone receiver.



*If you have not assigned an MSN to the corresponding a/b port, you can enable call forwarding by entering the combination of *** x y * target call number * MSN of the a/b port #** and disable it by entering **# x y * MSN of the a/b port #** (where x y stands for the variable option 'immediately', 'after 15 seconds' or 'busy').*

*To check whether this service is enabled, pick up the receiver and dial **# * x***

y * MSN of the a/b port # at the dial tone. If you hear two bright tones, the feature is enabled. If you hear two dark tones, the feature is disabled.

② Disable call forwarding

- Lift the receiver and wait for a dial tone.
- Enter one of the following sequences on the number pad on your phone:

2 1 # (for "immediate" call forwarding)

6 1 # (for call forwarding "after 15 seconds")

6 7 # (for "busy" call forwarding)

- If you hear two bright tones, the feature was enabled, has been disabled and you can hang up the phone receiver. If you hear one low tone, the either the feature was disabled or you have specified an incorrect MSN.

No-dialing connection

This function enables you to automatically call a special calling number (such as an emergency number). If no call number is dialed within five seconds of lifting the receiver, this destination number is automatically dialed.

For example, if you go out for the evening you can enter the call number where you can be reached. Your child simply needs to lift the receiver and the number is dialed automatically.

You can also configure this feature using ELSA LANconfig. This will overwrite the settings you have made using the buttons on your phone.

Proceed as follows:

① Check activation

- To check whether this service is enabled, pick up the receiver and dial *** # 5 3 #** at the dial tone.
- If you hear two bright tones, the feature is enabled. If you hear two dark tones, the feature is disabled.

Note, depending on the configuration of 'External Calls' for the corresponding a/b port, that you may have to dial '0' first.

② Enable no-dialing connection

- Lift the receiver and wait for a dial tone.



- ☐ Enter ***53*** on the number pad on your phone.
- ☐ Enter the desired call number and press **#**.
- ☐ If you hear two bright tones, the feature is enabled and you can hang up the phone receiver.

③ Disable no-dialing connection

- ☐ Lift the receiver and wait for a dial tone.
- ☐ Enter **#53#** on the number pad on your phone.
- ☐ If you hear two bright tones, the feature is enabled and you can hang up the phone receiver.

*If you have enter a call number for the no-dialing connection once and then disabled the feature, the number remains stored and you can enable it any time for no-dialing connection by entering ***53#**.*

Enable a/b port for calls

Use this function to specify whether or not your telephone should ring for incoming calls. This feature is useful if you do not want to be disturbed. The caller simply hears a busy signal. Proceed as follows:

① Check activation

- ☐ To check whether this service is enabled, pick up the receiver and dial ***#99#** at the dial tone.
- ☐ If you hear two bright tones, the feature is enabled. If you hear two dark tones, the feature is disabled.

② Enable a/b port

- ☐ Lift the receiver and wait for a dial tone.
- ☐ Enter ***99#** on the number pad on your phone.
- ☐ If you hear two bright tones, the feature is enabled and you can hang up the phone receiver.

③ Disable a/b port

- ☐ Lift the receiver and wait for a dial tone.
- ☐ Enter **#99#** on the number pad on your phone.
- ☐ If you hear two bright tones, the feature is enabled and you can hang up the phone receiver.



Suppression of own subscriber number

Use this feature to suppress your own multiple subscriber number (MSN) from being sent to the remote station.

The ability to “selectively suppress the call number” might have to be obtained separately from the telephone company.

Proceed as follows:

- ① Check activation
 - To check whether this service is enabled, pick up the receiver and dial ***#310#** at the dial tone.
 - If you hear two bright tones, the feature is enabled. If you hear two dark tones, the feature is disabled.
- ② Enable call number suppression
 - Lift the receiver and wait for a dial tone.
 - Enter ***310#** on the number pad on your phone.
 - If you hear two bright tones, the feature is enabled and you can hang up the phone receiver.
- ③ Disable call number suppression
 - Lift the receiver and wait for a dial tone.
 - Enter **#310#** on the number pad on your phone.
 - If you hear two bright tones, the feature is enabled and you can hang up the phone receiver.

4.12 Accounting

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

The data collected include the following:

- User (name, IP address, MAC address)

The online times and data transfer volumes are assigned the MAC addresses of the system network interfaces in the LAN. The router can supply additional information regarding the assignments of MAC addresses and computer names from the DHCP or DNS server modules,

if available. In this case, online times can be assigned directly to computer names. If the assignment of MAC addresses to computer names is not possible, other existing information is recorded to identify the user, such as the IP address.

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

- Remote station to which the connection was established
- Type of connection
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.

4.12.1 Configuring accounting

Settings for accounting are found under `/Setup/Accounting`. 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.

4.12.2 Reading the accounting data

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



Accounting	Line	Remote Site	Type	Connections	Received	Transmitted	Total Online Time
LANCOM BOX Office	01A02	ELSA061	Dial-up (128K)	2	221 KB	41 KB	4 minutes, 47 seconds

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

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 station
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.

5 Appendix

5.1 Technical data

Hardware	
WAN connection	ISDN So (BRI), point-to-point and point-to-multipoint configuration, I.430 (auto-sensing)
LAN connection	<p><i>LANCOM 800 Office</i>: Ethernet IEEE 802.3, 10Base-T</p> <p><i>LANCOM 1000 Office</i>: Ethernet IEEE 802.3, 10Base-T, 10Base-2 (BNC), full duplex operation</p> <p><i>LANCOM 1100 Office</i>: Ethernet IEEE 802.3, 10/100Base-T (RJ45, node/hub switch), auto-sensing, 10Base-2 (BNC), full duplex operation</p> <p><i>LANCOM 2000 Office</i>: Ethernet IEEE 802.3, 10Base-T, 10Base-2 (BNC), full duplex operation</p>
CPU/Memory	32 bit RISC CPU (Hitachi SH3), 60 MHz, 2 MB Flash-ROM, 4 MB RAM
Power supply	12 VA with AC adapter for 230 V, 12 VA, LANCOM 2000: 24 VA
Dimensions and design	Rugged metal case, connections on rear panel; dimensions 158 x 40 x 125 mm (W x H x D)
Ambient conditions	Temperature: 5–40°C, humidity: 0–80%, non-condensing
Approvals	CE approvals, Switzerland and all other EU countries: D800109K, ICT D800110K, EN 50082 (Part 1), EN 55022 (Class B), EN 60950, NET3
Software	
Functions	<p>IP router, DHCP server, DHCP client, DNS server;</p> <p><i>LANCOM 1000/1100 Office</i> additional: IPX router, NetBIOS proxy, bridge</p> <p><i>LANCOM 2000 Office</i> additional: IPX router, bridge, NetBIOS proxy, PBX</p>
Network protocols	<p>IP router ARP, PROXY ARP, IP, ICMP, UDP, TCP, RIP-1, RIP-2, DHCP,</p> <p>IPX router: IPX, SAP, Novell NetBIOS, Novell burst mode</p>
ISDN protocols	<p>ISDN connection: ISDN So bus, point-to-point and point-to-multipoint configuration, I.430 (auto-sensing)</p> <p>D channel: DSS1 or 1TR6 (auto-sensing), optional leased line support</p> <p>B-chan. PPP (asynch./synch.), X.75, HDLC, MLPPP for channel bundling, CAPI 2.0 over <i>LANCAPI</i>, Stac compression</p>
Line control	Automatic callback with or without call establishment: Line-on-demand, dyn. short hold mode, channel-on-demand for channel bundling, round-robin dialing, fast callback, programmable priority switching, BACP
Telephony (a/b ports)	<p><i>LANCOM 2000 Office</i> only: 4 analog ports, RJ11-BAPT adapter,</p> <p>ISDN functions: internal calls, call forwarding, brokering, holding, callback, three-way conference calls, call acceptance, call charge metering, optional automatic external calls, priority switching, hotline</p>

Security and firewall functions	PAP and CHAP, MS-CHAP, PPP authentication mechanisms; filter options in IP mode (<i>LANCOM 1000/1100/2000 Office</i> also in IPX and bridge mode), protection of configuration using access lists and passwords, IP masquerading, ISDN security measures (CLIP, callback etc.), password protection, accounting
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
Operating security	Hardware watchdogs, regular self-testing, FirmSafe concept for remote software upgrades
Charge monitoring	Maximum charges or connection time for a preset period can be set
Accounting	Stores the number and lengths of connections
Management	TFTP configuration and firmware upload, SNMP management via SNMP v.1 or v.2, WAN or LAN access activated separately, diagnostic output for protocols and interfaces, diagnostic tools, status display <i>ELSA LANmonitor</i> , <i>LANconfig</i> , remote configuration via ISDN, configuration via HTML, <i>ELSA WebConfig</i> (<i>LANCOM 1000/1100/2000 Office</i> plus V.24/V.28 outband interface (8-pin mini-DIN))
Package contents	
Accessories	power adapter, ISDN line connection cable, two LAN twisted-pair cables, complete documentation and <i>ELSA LANCOM</i> CD-ROM <i>LANCOM 1000/1100 Office</i> additionally: cable for outband interface, BNC-T adapter <i>LANCOM 2000 Office</i> additionally: cable for outband interface, BNC-T adapter, 4 RJ11-BAPT adapters Software: <i>ELSA LANCAPI</i> , <i>ELSA LANtools</i> (<i>ELSA LANconfig</i> , <i>ELSA LANmonitor</i> for status display), <i>ELSA CAPI Faxmodem</i>
Service & Support	6 years warranty, via hotline and Internet

5.2

Declarations of conformity

EN



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

Geräteart: ISDN Router
 Type of Device:
 Typenbezeichnung: ELSA LANCOM 800 Office
 Product Name:
 EG-Baumusterprübscheinigungs Nr.: D800109K
 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)
 ISDN Richtlinie (97/346/EWG)
 ISDN Directive (97/346/EEC)
 EMV Richtlinie (89/336/EWG)
 EMC Directive (89/336/EEC)

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

EN 50082-1: 1992
 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, 29. Februar 2000
 Aachen, 29th February 2000

I.V. Stefan Kriebel
 Bereichsleiter Entwicklung
 VP Engineering



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

Geräteart: ISDN Router
 type of device
 Typenbezeichnung: ELSA LANCOM 1100 Office
 product name
 EG-Baumusterprüfbescheinigungs Nr.: D800109K
 Registration no.
 Benannte Stelle: CETECOM ICT Services GmbH
 Notified Body: **CE0682 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/EEG)

Low Voltage Directive (73/23/EEC)

ISDN Vorschrift (97/346/EG)

ISDN Directive (97/34/EC)

EMV Richtlinie (89/336/EEG)

EMC Directive (89/336/EEC)

Zur Beurteilung der Konformität wurden folgende Normen herangezogen:

The assessment of this product has been based on the following standards

EN 50082: 1992 Teil 1: EN 61000-4-2, 3, 4, 5, 6

EN 50081: 1992 Teil 1: 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, 8. Februar 1999
 Aachen, February 8th 1999

I.V. Peter Wieninger
 Bereichsleiter Entwicklung
 VP Engineering



KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

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

Geräteart:	ISDN Router
Type of Device:	
Typenbezeichnung:	ELSA LANCOM 1000/2000 Office
Product Name:	
EG-Baumusterprüfbescheinigungs Nr.:	D800109K
Registration No.:	
Benannte Stelle:	CETECOM ICT Services GmbH
Notified Body:	CE0682 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/EEG)
Low Voltage Directive (73/23/EEG)
ISDN Richtlinie (97/34/EEG)
ISDN Directive (97/34/EEG)
EMV Richtlinie (89/336/EEG)
EMC Directive (89/336/EEG)

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

EN 50082-1: 1992
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, 8. April 1998
Aachen, 8th April 1998

I.V. Peter Wieninger
Bereichsleiter Entwicklung
VP Engineering

5.3

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.

6 Index

Items with page numbers above 150 can be found on CD.

10 Mbit network	28
10/100Base-Tx	28
100 Mbit network	28
100BASE-T	232
10Base-2 (BNC)	28
10Base-T	28
1TR6	14, 224
802.2	234
802.3	234

● A

a/b port	103
a/b ports	13, 17
call number	108
configuration	104
description	108
internal call number	108
options	109
router connection	115
service attributes	109
acceptance	110
Access control	59
Access protection	15, 59
name	59
name or number	60
number	59
Access Type	87
Access-list	243
Accounting	19
Adapter	41
Adapter for configuration cable	21
additional ISDN functions	18
Address Administration	43
address administration	71
Address pool	73

address pool	78, 254
address ranges	246
Advice of charge	15
Aging-minute(s)	238, 240
Analog connections	13
analog end devices	17
analog terminal devices	103
Analog terminals	28
AOCD	15, 63
Apple Talk	147
APPP	228
ARP cache	244
ARP-aging-minute(s)	244
asynchronous PPP	228
Auth.	229
Authentication	15, 159, 163
auto mode	254
automatic synchronization	96
Availability	102
availability	114
Available workstations	91

● B

B channel	52
connection status	16
B channel protocol	60
Backoff	237
BACP	16
Barring	58
B-channel protocol	61
B-channel protocols	227
Binding	234
Boot system	266
branch exchange	13, 17, 103, 104
Bridge	
configuration	183
filtering data packets	184

bridge 183
 Broadcast address 149
 Broadcast transfer 152
 Brokering 13, 118
 brokering 18, 103
 Brute force 15, 58
 Buffers 232

C

Cable 145
 Cable network 148
 cache 244
 Call acceptance 105
 Call charge information 18, 63, 165
 Call charge limit 62
 Call charge management 62
 Call charge metering 13
 call charge metering 18
 Call charge units 165
 Call establishment 84
 Call forwarding 119
 call forwarding 18, 103
 Call number recognition 15
 call numbers 230
 Call pickup 13, 118
 Call redirection 13
 Call switching 13
 Call waiting 116
 call waiting 105
 Callback 59, 61, 112, 118, 225
 fast call back 61
 callback 12, 18, 103, 230, 232
 Callback function 15
 Callback options 226
 call-by-call 92, 93, 261
 Calling Line Identification Restriction 224
 Calls to the D2 mobile network 93
 CAPI Faxmodem 97
 CAPI interface 98
 CBCP 162
 CD 21
 Cells 145
 Challenge Handshake Authentication
 Protocol 60, 229
 Channel bundling 16, 165
 dynamic 165
 static 165
 channel bundling 16, 115, 228
 dynamic 16
 static 16
 CHAP 60, 229
 charge 226
 Charge monitoring 15
 Charge units 63
 Charges 239
 charges 92, 234
 charging information 225
 charging unit 225
 CLI 61, 230
 CLIP 15
 CLIR 224
 Common ISDN Application
 Programming Interface 98
 compatibility 227
 Compression 16
 Computer names 79, 83
 Config-aging-minute(s) 259
 Configuration 14
 methods 40
 SNMP 55
 Configuration call number 47
 Configuration interface 21, 40, 41
 configuration options 258
 Configure a/b ports and branch exchange
 104
 Connect 231
 Connect charges 84
 connect-charge structure 94
 Connection 93
 Connection control 63

connection limits	63
connection time-outs	225
Connections	28
Connector	232
Consultation hold	13
cost reduction	62

D

D channel	61
data compression	228
Data compression procedure	
LZS	165
Data packet	145
data transfer	165
Data transmission in an IPX network	168
data volume	19
days of the week	93
DDI numbers	227
Dedicated lines	12
default route	247
destination network	245
Destination port	248
destination ports	247
device names	225
Device-name	225
DHCP	71, 254
DHCP for WINS Resolution	76
DHCP mode	72
DHCP server	16, 43, 72, 79, 254
configuration	77
dial prefix	226
dialing prefix	93
Dial-up connection	12, 40, 44
Dial-Up Networking	60
Dialup-remote	225
digital terminal devices	103
Direct outward dialing	114
Disconnect	231
Distance of a route	173
DNS	79, 181, 243

DNS Forwarding	181
DNS forwarding	244
DNS forwarding mechanism	80
DNS queries	248
DNS server	17, 71, 74, 79
available information	80
filter list	82
filter mechanism	80
DNS-backup-IP-address	244
Documentation	21
Domain Name Service	181
Domain name service	79
Domains	79
DSS1	14, 224
Dst-address	249
Dst-netmask	249
dynamic assignment of the IP	
address	245
dynamic bundling	225
Dynamic channel bundling	165
dynamic channel bundling	16
Dynamic Host Configuration Protocol	72
dynamic IP routing table	251
Dynamic routing	172
dynamic short-hold	225

E

electronic documentation	21
ELSA CAPI Faxmodem	17
ELSA protocol	60
ELSA-RVS-COM	13
ELSA-ZOC	13
E-mail	12
Encaps	227
End address	73
End-address-pool	254
Ethernet	13, 227
10/100Base-T	14
10Base-2	13
10Base-T	13, 14

Fast Ethernet	14
Ethernet packet format	234
EuroFileTransfer	11, 17
Exclusion routes	174
exponential backoff	237
external call	103
External Calls	106, 110
External calls	110

F

Fast Call Back	61
fast callback procedure	226
Fast Ethernet	14
Fast-Ethernet	
10/100Base-T	14
Fax	11, 13, 17, 97
Fax Class 1	17, 97
Fax driver	17, 97
Fax transmission	98
Faxmodem	17
LANCAPi	98
File and printer sharing	86
File transfer	12
Filter	59
Filter mechanisms	12
Firewall	15
Firewall function	62
firewall function	248
FirmSafe	14, 48
firmsafe	265
Firmware	14, 264
Firmware upload	49
using TFTP	50
with LANconfig	49
with terminal program	50
firmware upload	264
Flash button	112
Flash ROM	48
flash ROM memory	14

G

Gateway	62, 71
gateway	75
Group table	257
Groups	83

H

HDLC packets	228
HDLC56K	228
HDLC64K	228
hierarchical IP addresses	150
High telephone costs	62
holding	18, 103
holidays	93
Home office	12
Host	79, 145
Host table	257
Hotline	110
hotline	18
Hyperterminal	41

I

IANA	149
ICMP	248, 250, 252
Identification	86, 222
Identifying the caller	60
Inband	40, 42
using Telnet	44
inband	40
inband configuration	40
Install software	48
Installation	13
Interface	145
Interface list	223
Interfaces	28
Internal calls	13
internal calls	18, 103
internal clock	96
international calls	92
Internet	12, 62, 147

- Internet access 161
 - Internet address 180
 - Internet service provider 11
 - Internetwork 147
 - Intranet 242
 - intranet address 180
 - Intranet-mask 242
 - inverse masquerading 251
 - IP 250
 - IP access list 42
 - IP address 42, 53, 62, 160, 242
 - IP addresses 148
 - IP broadcast 250
 - IP filter 84
 - IP header 250
 - IP masquerading 12, 15, 59, 62, 179, 45, 251
 - simple masquerading 181
 - supported protocols 181
 - IP multicast 250
 - IP network 147
 - IP routing
 - Filter 175
 - FTP 175
 - Telnet 175
 - IP routing table 172
 - IP-Adressen 16
 - IP-netmask 242
 - IP-routing-table 245
 - IPX 147
 - IPX routing
 - backoff 168
 - Binding 167
 - binding 168
 - exponential backoff 170
 - Filter 170
 - Hops 169
 - network 167
 - propagate 168
 - Propagate loop function 170
 - remote station 167
 - RIP and SAP tables 169
 - Tics 169
 - IPX routing table 167
 - IPX watchdogs 172
 - IPX-router 233
 - IPX-watchdog 234
 - ISDN cable 13
 - ISDN connection cable 21
 - ISDN connection charges 62
 - ISDN layers 227
 - ISDN network 148
 - ISDN time 15, 189
 - ISDN-S0 port 28
- **K**
- Key 159, 229
- **L**
- LAN 147, 152
 - LAN connection 13
 - LAN connection cable 21
 - LAN to LAN coupling 12
 - LANCAPi 11, 13, 17, 45, 98, 260
 - LANCAPi client 99
 - LANCAPi server 100
 - LAN-Coll 27
 - LANconfig 30, 40, 42, 43, 45, 49, 51
 - Wizards 43
 - LAN-configuration 259
 - LAN-filter-table 238, 240, 247
 - Langner openISDN config
 - Wizard 43
 - Language 259
 - LAN-Link 27
 - LANmonitor 16, 51, 96
 - LAN-Rx 27
 - LAN-Tx 27
 - layer name 225
 - Layer-name 227

LCP echo reply	160
LCP echo request	160
LCR	15, 63, 92, 261
LCR table	92
leased-line connection	227
Least-cost router	92
least-cost router	95
automatic fallback	95
connect-charge monitoring	95
operating modes	95
Least-cost routing	15, 63
LED	25
LED indicators	16
Line connection	18
Line Display	53
Line management	12, 18
Local Area Network	147
local calls	94
local network	147
Local-routing	235, 249
location	222
Lock-minutes	259
Login	49, 58
Login barring	58
log-in block	259
Login-errors	259
long distance calls	93
LOOP-propagate	236
Looser	226
LZS data compression	165

● M

MAC	152
MAC address	232
MAC addresses	153
MAC protocol	153
Mail server	82
main channels	115
manual connection	231
Masquerading	245, 251
masquerading	242
Masquerading table	252
Maximum number of simultaneous connections	259
Media Access Control	152
Medium	145
Medium Access Control	152
Microsoft Network	83
Microsoft Network client	85
MLPPP	16, 165
mobile telephones	93
Mode	72
Modem	17
modem operation	228
Monitoring	51
Multi-device terminal	14
Multilink PPP	157, 165
Multipoint cabling	152
Multiprotocol capability	153

● N

Name	222
Name and group designation	86
Name information	84
name server	243
name verification	230
Name-list	225
Namenräume	83
Names	83
Naming IP Addresses	167
NAT	59, 62, 179
NBNS	83, 244
NBNS server	71, 74, 76
NBNS-backup	244
neighboring local exchanges	94
NetBIOS	18, 80, 235
IP filter	88
LAN-LAN interconnection	88
network protocol	85
remote access	89

remote station	88
TCP/IP	85
NetBIOS name server	244
NetBIOS nameserver	83
NetBIOS networks	80
NetBIOS ports	84
NetBIOS propagated frames	236
NetBIOS proxy	83
NetBIOS remote stations	84
Netmask	148
NetWare server	234
Network	145, 234
Network adapter	145
Network address	148, 236
Network cable	145
Network connection	11
network connection	232
network identification prefix	92
Network Information Center	179
Network names	79
Network Neighborhood	90
network operators	92
Network protocol	147
NIC	179
No charge information	63
Node/hub selector switch	28
Node-ID	233
No-dialing connection	120
Novell	236
NT domain	256
number	225
Number list	230

● O

office communications	98
Online media	42
Online research	12
online time	19
Operating	233, 242, 245
Operating modes	57

options for saving telephone charges	94
Other	266
Outband	40, 41
Requirements	41
Outband configuration	41
outband configuration	40

● P

Package contents	21
Packet	145
PAP	60, 229
Password	47, 52, 59, 61
password	60, 243
Password Authentication Protocol	60, 229
Password protection	15, 58
Password-required	259
Passwords	87
PAT	59, 62, 179
PBX	103, 112
peer-to-peer networks	18
period	62
Period of validity	72
period of validity	75
physical medium	145
picking up the receiver	111
Point-to-multipoint configuration	14
Point-to-multipoint connection	146
Point-to-point configuration	14
Point-to-point connection	146
point-to-point protocol	228
port	101
Port number	181
Power	26
Power supply unit	21
PPP	18, 52, 60, 165, 228, 230
Assigning IP addresses	160
Callback functions	161
checking the line with LCP	159
PPP client	40, 44
PPP connection	40, 47

PPP LCP Extensions 164
 PPP list 60
 PPP negotiation 47, 242
 prefix 92
 preselection 92
 priority control 102, 114
 Priority switching 114
 Private address spaces 149
 Prohibited address ranges 246
 Prohibiting domains 82
 Propagated Frames 236
 Propagated frames 170
 protect 230
 Protocol 147
 providers 92
 Proxy 18
 proxy ARP 245, 246
 Proxy-ARP 249
 pulse dialing 115

R

R button 112
 R1-mask 251
 rate zones 94
 registered IP address 149, 242
 Remote Access 84, 249
 Remote access 12, 44, 160
 remote access 237
 Remote configuration 18, 40
 Remote connection 45
 remote station verifications 229
 Remote-table 256
 Reset system 266
 Ring 106
 RIP 168, 250
 RIP tables 169
 RIP-SAP-scaling 235
 RIP-type 250
 Round robin list 226
 round robin list 226

Round-Robin 227
 Router 145
 Router name 173
 Routes/FRM 238
 Routing 84, 150
 Routing Information Protocol 168
 Routing Microsoft Networks 83
 Routing table 150
 IP masquerading 174
 special entries 174
 Routing-table 236

S

S0 interface 14
 S0 status 26
 SAP 168, 239
 SAP services 240
 SAP tables 169
 scaling 235
 Scope ID 256
 Scopes 83
 Script list 230
 script processing 228, 230
 secondary channels 115
 Security 57, 59, 62
 Security features 12
 security procedure 229
 Security procedures 60
 semipermanent leased-line
 connection 226
 serial port 40
 server information 239
 Server list 258
 Server/FRM 240
 Service 79
 Service Advertising Protocol 168
 service information 240
 Service table 251
 Setup
 DHCP-module 254

IP-router-module	245
IPX-module	233
LAN-module	232
TCP-IP-module	241
WAN-module	222
Setup Wizard	41
Shared Medium	152
Shared medium	147
Shared resources	87
Sharing	87
Short-hold	225
Single user access	62
SNAP	234
SNMP	55, 253
Socket filter	171
Socket-Filter	235
Socket-filter	237
Software update	14
Source port	248
Spare-heap-blocks	233
special dialing characters	225, 226
special prefixes	94
speed	228
Split horizon	170
Spoofing	239, 241
SPX watchdogs	172
SPX-watchdog	235
Stac	165, 228
Stac data compression	16
Standard fax programs	97
Start address	73
Start-address-pool	254
static bundling	225
Static channel bundling	165
static channel bundling	16
static IP address	245
Static routing	172
Statistics	16
Status	187
Call-info-table	217, 218, 220, 221

Config-statistics	214
Connection-state	189
Connection-statistics	215
Delete values	221
Info-connection	216
IP-router-statistics	212
IPX-statistics	201
LAN-statistics	192
Layer-connection	217
operating time	189
PPP-statistics	193
Queue-statistics	214
SO-bus	219
TCP-IP-statistics	206
WAN-statistics	190
Status Displays	16
Subnet	150
Suppress the call number	109
Suppresses the outgoing MSN	224
Suppression of own subscriber number	122
System terminal	14
System-administrator	253
System-location	253

● T

Table-ARP	244
Table-RIP	237, 251
Table-SAP	239
TCP	248, 252
TCP max. connections	244
TCP/IP	30, 42, 147, 172
TCP/IP networks	79
TCP/IP stack	147
TCP-aging-minute(s)	244
Technical data	125, 127
Telephone	13
Telephone adapter	104
telephone company	261
Telephone functions	13

telephone provider 94
 Telephones 17
 teleworkers 249
 Teleworking 12
 Telix 41
 Telnet 14, 34, 45
 Telnet server 243
 Terminal program 14, 41
 TFTP 42
 TFTP server 243
 three-way conference call 117
 three-way conference calls 18, 103
 throughput 165
 Time 189, 229
 time 93, 96, 263
 Time budget 63
 Time check 15
 time in the ISDN 96
 time of day 93
 Time-dependent connection control ... 63
 Time-out 165
 Timeout 255
 tone dialing 115
 TOS 250
 Trace
 code and parameters 54
 Examples 55
 starting 53
 Trace outputs 53
 transfer costs 18
 Transmission rates 53
 Trap-IP 253
 Traps-active 253
 Troubleshooting 51
 trunk seizure 226
 Type of Service 182
 Type-of-service 250

U

Übertragungsraten 16

UDP 248, 252
 Upload 15, 48
 Upload-system 266
 User name 47, 61, 159
 Username 229

V

V.24 configuration interface 28
 Verbindungsdauer 16
 verification attempt 229
 Version-table 264
 Voice mail 13

W

WAN connection 14
 WAN-Chan1 27
 WAN-Chan2 27
 WAN-configuration 259
 WAN-filter-table 238, 240, 248
 WAN-update-minute(s) 239, 241
 watchdog 234
 Watchdogs 172
 Wildcards 82
 Windows Internet Name Service
 Server 83
 Windows network 76
 Windows Networking 90
 Windows networks 18
 winipcfg 31, 34
 WINS Address 76
 WINS server 83
 Wireless links 145
 WWW 62

X

X.75 data protection 228
 X.75 secured format 228

Y

Y connection 165

Y connections 224

Technical basics

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

Network technology



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

The network and its components

*Network,
transmission
medium,
interfaces*

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



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

*Packets
Cells*

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



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

Host

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

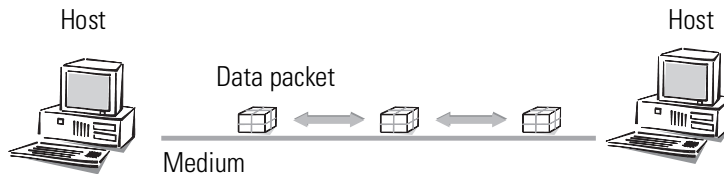
Router

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

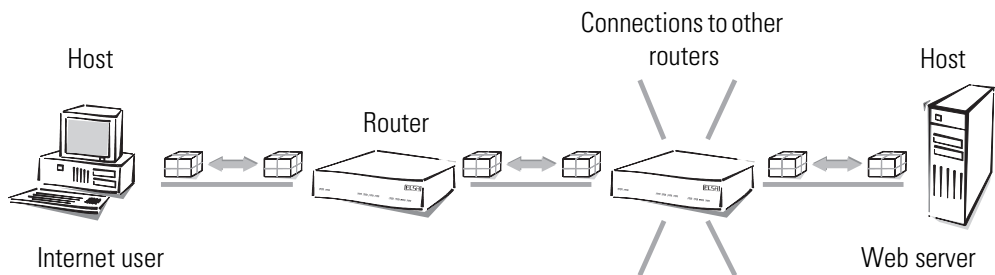
Connection modes

Point-to-point connection

The connection of exactly two hosts via a medium is called a “point-to-point connection”. In this case a host sends packets that can only be received by **one** specific recipient (unambiguous connection).



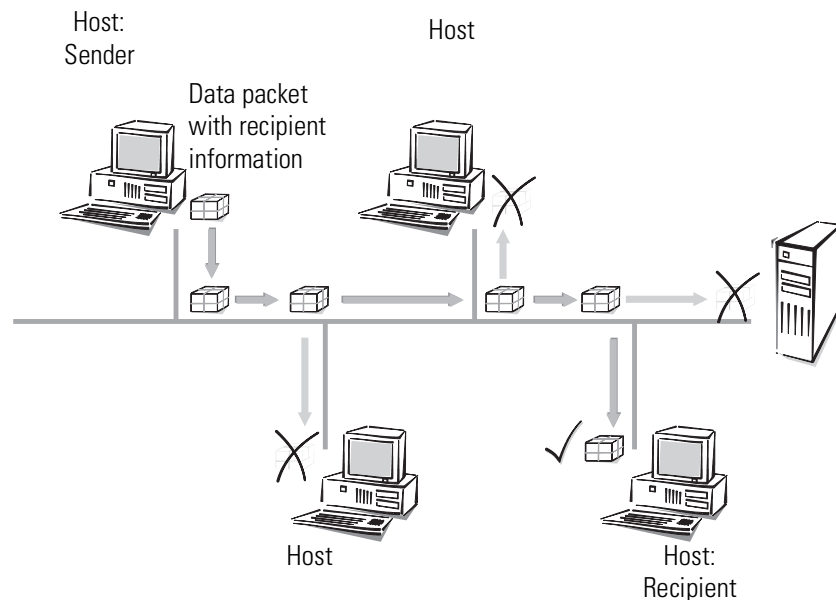
Access to the Internet is also established through point-to-point connections. Even though the data packets are sent from the host at the Internet user to the host at the Internet provider (server) via several routers, every data packet still has its own specific destination. Furthermore, the routers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



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

Point-to-multipoint connection

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



Kinds of networks

<i>Protocol</i>	An important prerequisite for communications between computers is a common language among the hosts. In the world of network technology this language is called "network protocol" or simply "protocol".
<i>TCP/IP</i>	The most broadly distributed network protocol is the TCP/IP (T ransmission C ontrol P rotocol/ I nternet P rotocol). It is used mainly in the Internet, but nowadays more and more company networks use it. Examples of other network protocols are IPX or Apple Talk. Because of its wide use, this chapter deals mainly with the TCP/IP.
<i>IP network</i>	All hosts wanting to communicate using the TCP/IP protocol have to be plugged into the same network and have to have the TCP/IP protocol (also known as TCP/IP stack) installed. Such a network is referred to as an IP network.
<i>Internetwork Internet</i>	The connection of multiple networks based on the IP protocol is referred to as an internetwork. The largest union of many small, public IP networks is the Internet.
<i>Local network (LAN)</i>	A network covering a limited area with hosts on the same hierarchical level and using the same medium (shared medium) is called a local network (L ocal A rea N etwork, LAN).

IP addressing

<i>Packet-oriented transfer</i>	In IP networks the communication between computers takes place in a packet-oriented fashion. This means that data or messages are packed together in packets of variable length and are as such sent from the source computer to the target computer. Apart from
-------------------------------------	--

the actual information to be transmitted (useful data), the data packet also contains address and control information.

IP address

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



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

Network address

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

Netmask

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

Examples:

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

The same IP address, this time with another netmask:

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

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

And you can also see that there are more bits available to identify the individual hosts in a connected network if there are fewer bits in a netmask that contain a one. While only 254 different addresses could be allocated in the first example with the netmask 255.255.255.0, the second example has as many as $254 \times 254 = 64516$ different addresses available! The first and the last digit of an address space are reserved for the network address and the broadcast address (addresses for packets to all hosts in an IP network). In the netmask 255.255.255.0 this is the '0' for the network address and the '255' for the broadcast address.

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

IP address management

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

Private address spaces

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

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

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

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

There are two considerations when using these IP addresses:

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

IP routing and hierarchical IP addressing

Routing

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

Routing-table

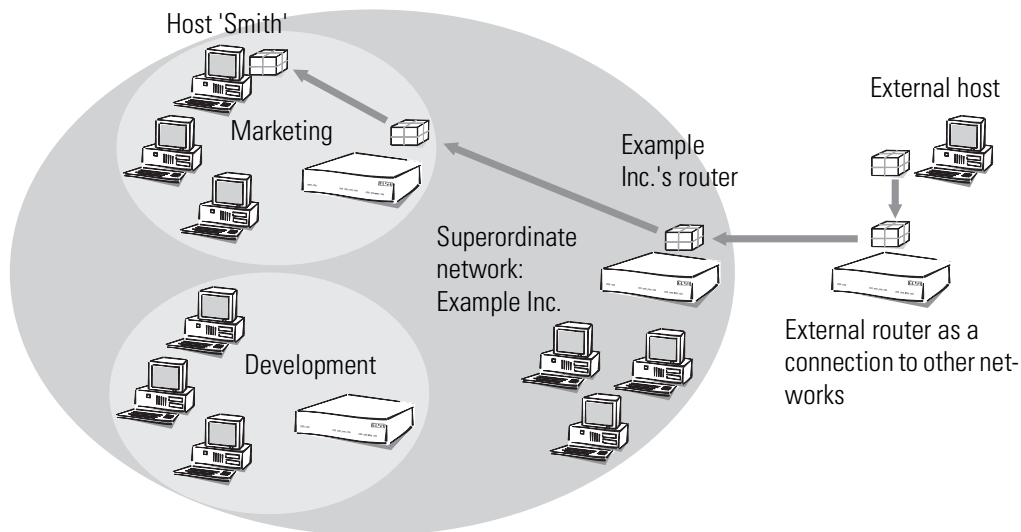
Every router manages a table (routing table). This table indicates the quickest interface connection to the host for every host in the network. You can imagine that, as they grow, these tables may exceed the capacity of the router—the Internet, as a worldwide linking up of publicly accessible IP computers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

Hierarchical IP addresses

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

The consequences of this hierarchical IP addressing:

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



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

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

- ① The sender gives the packet the destination address "host 'Smith' – Marketing – Example Inc.".
- ② All an external router that establishes the connections to other networks has to know is how to reach Example Inc. As soon as it receives a packet with the address for Example Inc., it passes the packet on to the router responsible for Example Inc.
- ③ The router at Example Inc. receives the packet and extracts from the address the information that it is directed at Example Inc. Since it is itself part of Example Inc., it takes a closer look at the address to find the name of the division. It then passes the packet on to the router in the marketing division.
- ④ The router in the marketing division receives the packet and extracts from the address the information that it is directed at the marketing division of Example Inc. Since it is itself part of this division, it takes a closer look at the address to find the name of the host. It then passes the packet on to the host of the employee Sam 'Smith'.

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

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

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

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

- ① If a host in the subnet of the development department wants to send a data packet to Mr. 'Smith', the sender attaches the destination address "Host 'Smith' – Marketing – Example Inc.".
- ② The router in the development division receives the packet and extracts from the address the information that it is directed at the marketing division of Example Inc. Since it is itself part of Example Inc., but not of the marketing division, it passes the packet on to the router in the superordinate network.
- ③ The router at the Example Inc. receives the packet and extracts from the address the information that it is directed at Example Inc. Since it is itself part of Example Inc., it takes a closer look at the address to find the name of the division. It then passes the packet on to the router in the marketing division, where the packet is passed on to the recipient.

Expansion through local networks

Media access control

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

LAN and IP network

The connection of all computers communicating through a shared medium using a MAC protocol is called a LAN. A LAN forms an independent network and is subordinate to the IP network, i.e. IP networks can use the physical connections of the LAN to establish connections between the hosts and the routers. LAN refers to a limitation of the area covered by the network, not a restriction of the number of workstations connected to it.

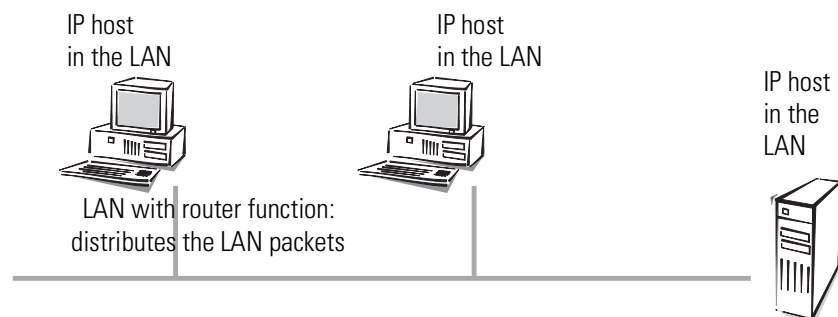
MAC address Specific LAN addresses hardwired into the interfaces by their manufacturers are used to manage the transfer in the LAN. Since the LAN addresses are used for communication via the MAC protocol, they are called MAC addresses. They can be thought of as the fingerprint of the interface hardware.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

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

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

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

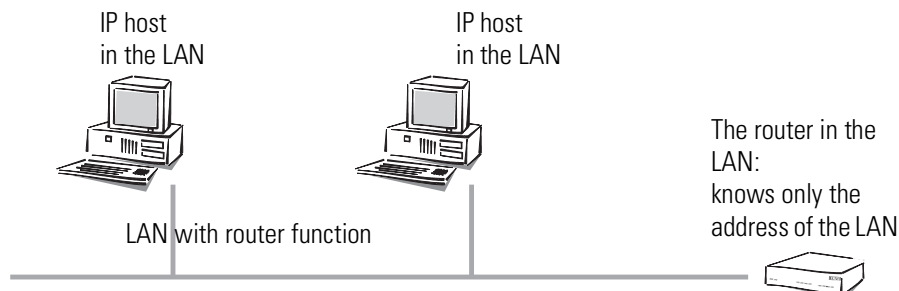
To an IP host, a LAN behaves as if it were an independent network with a router. The hosts gives the packets to the LAN which handles the further distribution of the data packets. This is why only IP addresses from the numerical space of the specific network should be used for the internal communication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



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

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

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



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

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

Data transfer within the LAN

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

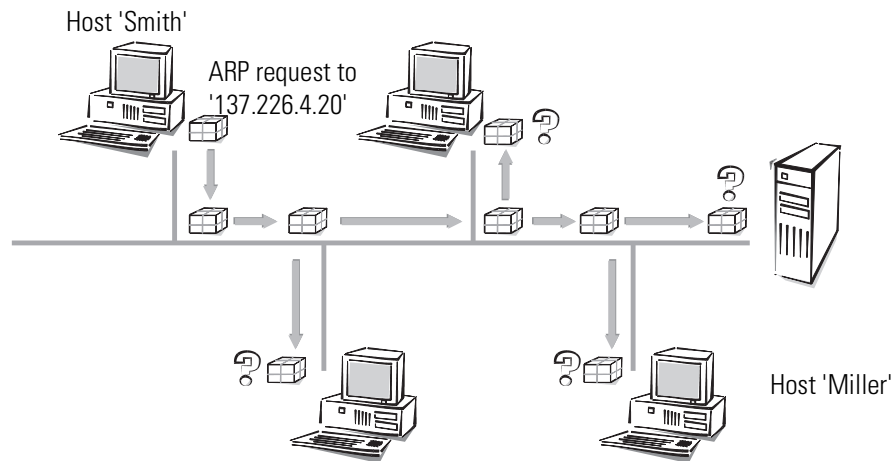
Imagine wanting to send an IP packet from host 'Smith' (with IP address '137.226.4.10' and MAC address '00-10-5A-31-20-DF') to host 'Miller' (with IP address '137.226.4.20' and MAC address '00-10-5A-31-20-EB'). Using the network address and the netmask, host 'Smith' recognizes that host 'Miller' is located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

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

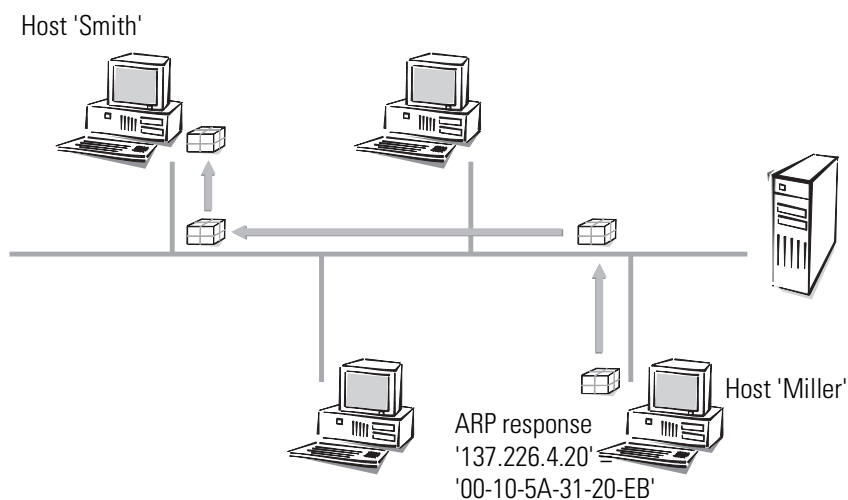
ARP

Therefore the LAN has a special mechanism that automates this process: the **A**ddress **R**esolution **P**rotocol, ARP. The table itself is called the ARP table. Whenever a host does

not find an entry in the table for a particular IP address (in our example '137.226.4.20'), it sends an ARP request packet to all hosts in the LAN (with the LAN broadcast address as a target address).



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



Then it can finally turn to its original task: sending the IP packet to host 'Miller'. It now finds the entry "IP address 137.226.4.20 corresponding to MAC address '00-10-5A-31-20-

EB'' in the ARP table and tells its LAN interface: "Send this IP packet to the computer with the MAC address '00-10-5A-31-20-EB'".

Data transfer from the LAN onto the Internet

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

LAN coupling on MAC basis

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

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

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

Point-to-point protocol

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

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

The protocol

What is PPP?

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

- Password protection according to PAP or CHAP
- Callback functions
- Negotiation of the network protocol to be used over the connection established (IP or IPX, for example). Included in this are any parameters necessary for these protocols, for example IP/IPX addresses. This process is carried out using IPCP and IPXCP (IP Control Protocol and IPX Control Protocol).
- Verification of the connection through the LCP (Link Control Protocol)
- Channel bundling (Multilink PPP)

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

What is PPP used for?

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

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

PPP as implemented in the *ELSA MicroLink Cable* can be used synchronously or asynchronously and over both a transparent HDLC connection and an X.75 connection.

The phases of PPP negotiation

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

- Establish phase

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

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

- Authenticate phase

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

There may also be negotiation on a callback using CBCP (Callback Control Protocol) during this phase.

- Network phase

The IPCP and IPXCP protocols have been implemented in the *ELSA MicroLink Cable*.

The IPCP and/or IPXCP network layers can be established following a successful transfer of the password.

IP and/or IPS packets can be transferred from the router modules to the opened line if the negotiation of parameters is successful for at least one of the network layers.

- Terminate phase

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

PPP negotiation in the *ELSA MicroLink Cable*

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

You can specify a custom definition of the PPP negotiation 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 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
Auth.	Security method used on the PPP connection ('PAP', 'CHAP' or 'none'). Your own router demands that the remote station observes this procedure. Not the other way round. This means that 'PAP' or 'CHAP' security is not useful when connecting to Internet service providers, who may not wish to provide a password. Select 'none' as the security attribute for connections such as these.
Password	Password transferred by your router to the remote 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 multiple of 10 seconds (i.e. 2 for 20 seconds, for instance). Simultaneously the time between two checks of the connection according to CHAP. This time is entered in minutes. The time must be set to '0' for remote stations using Windows 95, Windows 98 or Windows NT.
Retries	Number of retries for the check attempt. You can eliminate the effect of short-term line interference by selecting multiple retries. The connection will only be dropped if all attempts are unsuccessful. The time interval between two retries is 1/10 of the time interval between two checks. Simultaneously the number of the "Configure requests" that the router maximum sends before it assumes a line error and clears the connection itself.
Conf, Fail, Term	These parameters are used to affect the way in which PPP is implemented. The parameters are defined in RFC 1661 and are not described in greater detail here. You will find troubleshooting instructions in this RFC in connection with the router's PPP statistics if you are unable to establish any PPP connections. The default settings should generally suffice. These parameters can only be modified via SNMP or TFTP (using the <i>ELSA LANconfig</i> configuration program)!
Username	The name with which your router logs onto the remote station. The device name of your router is used if nothing is specified here.
Rights	Network protocols to be routed over this connection: IP, IPX, NTB (NetBIOS). NetBIOS always requires one of the other two protocols.

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. This may be found in the form of a backup line, for example.



We recommend that you switch off regular LCP queries in the case of remote access from individual workstation computers using Windows 95, Windows 98 or Windows NT since these operating systems do not respond 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 'Retries' 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 using TCP/IP as the network protocol, all participating computers require a valid and unique IP address. In the event that a remote station does not have an IP address of its own (e.g. an individual computer belonging to a teleworker), the *ELSA MicroLink Cable* can assign an IP address for the duration of the connection to permit communications.

This mode of assigning addresses is run during the PPP negotiation and is used only for connections over the WAN. The assignment of addresses via DHCP, on the other hand, is used only within the LAN.



Assignment of an IP address will only be possible if the ELSA MicroLink Cable can identify the remote sites by its call number or name when the call arrives, i.e. the authentication process has been successful.

- For example: Remote access

Address assignment is made possible by a special entry in the IP routing table. 255.255.255.255 is specified as the network mask as the IP address to be assigned to the remote station in the 'Router' field. In this case the router name is the name

the remote station uses to identify itself to the *ELSA MicroLink Cable*.

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

For the whole thing to work it follows that the remote station should be configured to take the IP address and the name servers (DNS and NBNS) from the *ELSA MicroLink Cable*. This can be done under Windows Dial-Up Networking, for example, using the 'TCP-settings' under 'IP-address' or 'DNS-configuration'. Enable the 'Server-assigned IP-address' and 'Server-assigned name server addresses' options.

■ For example: Internet access

The assignment of IP addresses can take place the other way round if the *ELSA MicroLink Cable* is used to provide access to the Internet for a local area network. In this case it is possible to configure the *ELSA MicroLink Cable* so that it has no valid Internet IP address of its own but has one assigned to it by the Internet provider for the duration of the connection. The *ELSA MicroLink Cable* also receives information on DNS servers at the provider in addition to the IP address during PPP negotiation.

The *ELSA MicroLink Cable* is only known by its internally valid intranet address on the local area network. This means that all workstation computers on the local area network can access the same Internet account and reach the same DNS server, for example.

Windows users can view the assigned addresses in the *LANmonitor*. In addition to the name of the remote station, the current IP address as well as the addresses of DNS and NBNS servers can be found there. Options such as channel bundling or the duration of the connection are also displayed.



The ELSA LANmonitor is generally installed automatically during the installation of the ELSA LANconfig. Its description can be found in the 'Configuration modes' chapter in the 'What's happening on the line?' section.

Callback functions

In addition to callback via the D channel and via the ELSA protocol, the *ELSA MicroLink Cable* also supports callback via CBCP as specified by Microsoft and via PPP in accordance with RFC 1570 (PPP LCP extensions). There is also the option of a particularly fast callback using a process developed by ELSA.

PCs running Windows 95, Windows 98 or Windows NT can only be called back through the CBCP. The following values have been made available to you in the name list for the

callback entry so that additional call number verification is also possible on the *ELSA MicroLink Cable*:

This entry is used to...	...to set the callback so that:
Off	No callback occurs.
Auto (not Windows 95, Windows 98 or Windows NT, see below)	If the remote station is found in the number list, it will be called back. The call is initially rejected and the return call placed as soon as the channel is free (approx. 8 seconds later). If the remote station is not found in the number list, the call is initially accepted as the DEFAULT remote station and the callback is negotiated during the callback protocol negotiation. A charge of one unit is incurred for this.
Name	A protocol negotiation is always performed before the return call is placed, even if the remote station is found on the number list (e.g. for computers using Windows that have dialed into the device). A charge of one unit is incurred for this.
ELSA	If the remote station is found in the number list, a fast callback is performed; i.e. the <i>ELSA MicroLink Cable</i> sends a special signal to the remote station and returns the call immediately once the channel is free. The connection is established in approx. 2 seconds. If the remote station does not cancel the call immediately upon receiving the signal, a fallback to the standard callback procedure is performed after 2 seconds (duration of call establishment approx. 8 seconds). This process is only available for DSS1 connections.
Looser	Use the 'Looser' option if a return call is being expected by the remote station. This setting simultaneously fulfills two tasks. It ensures that the call establishment is canceled locally for incoming calls from a remote station just called, as well as enabling the response to the fast-callback process. In other words, to take advantage of the fast callback, the caller must be in 'Looser' mode, while the station being called must be set to the 'ELSA'.



Greatest security is offered by the 'Name' setting if an entry exists in both the number list and the PPP list. The 'ELSA' setting ensures the fastest callback method between two ELSA routers.

*The 'Name' setting **must** be selected for Windows remote stations.*

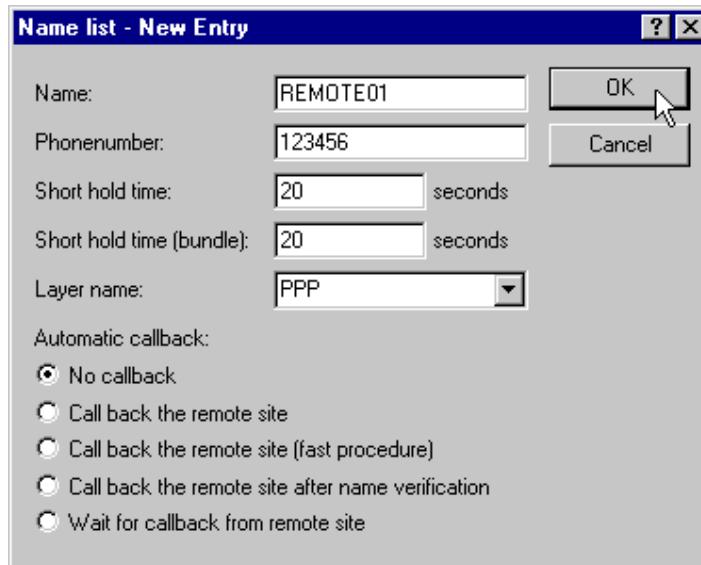
Microsoft CBCP callback

Microsoft CBCP provides a number of options to determine callback numbers:

- The party called does not call back.
- The party called allows the caller to specify the callback number itself.
- The party called knows the callback numbers and **only** calls these back.

It is possible to use the CBCP from a PC running Windows 95, Windows 98 or Windows NT to establish a connection to the *ELSA MicroLink Cable* have it call you back.

The callback entry and the call numbers entry in the name list are used to select these three possible settings.



The dialog box 'Name list - New Entry' contains the following fields and options:

- Name:** Text box containing 'REMOTE01'
- Phonenumber:** Text box containing '123456'
- Short hold time:** Text box containing '20' followed by 'seconds'
- Short hold time (bundle):** Text box containing '20' followed by 'seconds'
- Layer name:** Dropdown menu showing 'PPP'
- Automatic callback:** A group of five radio buttons:
 - ☒ No callback
 - ☐ Call back the remote site
 - ☐ Call back the remote site (fast procedure)
 - ☐ Call back the remote site after name verification
 - ☐ Wait for callback from remote site
- Buttons:** 'OK' and 'Cancel' buttons on the right side.

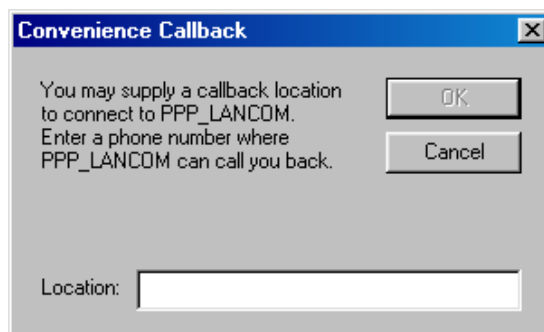
No callback

For this setting, the callback entry must be set to 'Off' during configuration with a terminal program or via telnet.

Choose select callback number

The remote station is called back after the name has been verified. The callback entry must have the value 'Name' for this setting and **no** call number may be specified in the name list.

Following the authentication process, the dialog box below will appear in Windows 95 in which the user can specify his call number:



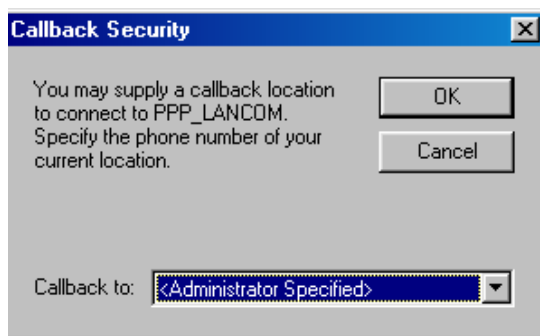
The dialog box 'Convenience Callback' contains the following elements:

- Title:** 'Convenience Callback'
- Text:** 'You may supply a callback location to connect to PPP_LANCOM. Enter a phone number where PPP_LANCOM can call you back.'
- Buttons:** 'OK' and 'Cancel' buttons.
- Location:** A text box for entering the callback location.

Callback number specified by the *ELSA MicroLink Cable*

The remote station is called back after the name has been verified. The callback entry of the appropriate remote station must have the value 'Name' for this setting and **one** call number must be specified in the name list.

Following the authentication process, the message below will appear in Windows 95 which the user can only confirm:



Callback to a Windows 95, Windows 98 or Windows NT workstation is initiated approximately 15 seconds after the connection is dropped. This delay is specified by Windows and cannot be shortened.

Fast ELSA callback

This fast, ELSA-specific process is ideal if two *ELSA MicroLink Cable* are to communicate with one another via callback.

- The caller who would like to be called back sets 'Wait for callback from remote site' in the name list ('Looser' when configuring via a terminal program or Telnet).
- The return caller selects 'Call back the remote site (fast procedure)' in the name list and sets the number ('ELSA').

Callback as specified in RFC 1570 (PPP LCP extensions)

There are five methods of demanding a callback specified in RFC 1570. All versions are accepted by the *ELSA MicroLink Cable*. All versions will be processed in the same way, however:

The *ELSA MicroLink Cable* drops the connection to the remote station after authentication and then calls it back three seconds later.

Channel bundling with MLPPP

If you are establishing an ISDN connection to a party supporting PPP you can really speed up your data: You can compress the data and/or use several B channels for the transfer (channel bundling).

Connections using channel bundling differ from "normal" connections inasmuch as they use not only one, but several B channels in parallel for transmitting the data.

MLPPP (Multilink PPP) is used for channel bundling. Of course, this procedure is only available if PPP is being used as the B-channel protocol. MLPPP is ideal, for example, for accessing the Internet via a provider which also supports MLPPP on its dial-up nodes.

■ Static channel bundling

If a connection is established with static channel bundling, the router tries to establish the number of B channels specified as 'Minimum' in the channel list. Either the channels specified in the channel list or random free channels are used.

■ Dynamic channel bundling

In the case of dynamic channel bundling, the router initially establishes the number of B channels specified as 'Minimum' in the channel list and starts the data transfer. If the router determines that the throughput stays above a certain threshold for a given period of time, it will attempt to add further channels until the number specified as 'Maximum' in the channel list has been reached. Either the channels specified in the channel list or random free channels are also used in this case.

If the dynamic channels are established and the data throughput rate drops below the threshold value, the router waits for the set B2 timeout period and then automatically closes the channels again. Any partly used call charge units are used up fully if call charge information is transmitted during the connection. Therefore, the router only uses the dynamic channels if and as long as it really needs them.

How to configure channel bundling

Three settings are required to configure a channel-bundled connection:

- ④ Create an entry in the name list for the connection to be established with channel bundling. Select a layer which has set the bundling in the layer-2 options.
 - **compr.** When using the LZS data compression procedure (Stac), the data volume is reduced provided it was not already compressed before. This process is also supported by routers from other manufacturers and by ISDN adapters under Windows operating systems.
 - **bundle** uses several B channels per connection. The channel bundling method is determined by the configuration of the layer 2 options in the layer list, the timeouts in the names list, the setting for the Y connection in the interface table and the setting for the channel table.

- **bnd+compr** uses both compression and channel bundling and therefore provides maximum possible transmission performance.
- ⑤ Enter the holding times for this connection in the name list as well. Please observe the following rules:
- Depending on the application, the B1 holding time should be long enough to ensure that the connection is not prematurely terminated by the brief absence of data packets. Experience has shown that values between 60 and 180 seconds are a good basis which can be adapted as required during operation.
 - The B2 hold time determines the delay time after which the dynamic channels are terminated once the data throughput drops below the threshold value.
- ⑥ Use the channel list to determine the number of channels to be used for the connection. You may also specify the channels to be used, thus keeping certain channels free for dial-up connections via RAS, for example.

The channel list entry determines whether static or dynamic channel bundling will be used (see above). More than one minimum channel results in static bundling, whereas a difference between the minimum and maximum number of channels permits dynamic channel bundling.

- ⑦ Use the entry for the Y connection in the interface list to determine what should happen if an additional connection to a different remote station is requested during an existing connection using channel bundling, but no further B channels are available.
- Y connection **On**: The router interrupts the bundled connection on this interface to establish a connection to the other remote station. When the channel is free again, the originally bundled connection automatically takes the channel back (always in the case of static bundling, only as required when using dynamic bundling).
 - Y connection **Off**: The router holds the existing bundled connection on this interface, the other connection must try a different interface or wait if none of the interfaces with active channel bundling permit a channel to be terminated.

IPX routing

The IPX router transmits data from networks using IPX/SPX as the network protocols (e.g. Novell networks). A remote network is notified to the computers in the local network by its entry in the IPX routing table. A maximum of 16 different networks can be entered in the routing table.

Naming IPX addresses

A complete IPX network address comprises three parts: A network number, the MAC address of the network adapter and the socket number.

- The network number can be freely selected. It must, however, be unique on all the addressable IPX networks to ensure correct assignment.
- The MAC address is burnt into each network component. A different address is only used inside the network in special cases.
- An IPX network uses the socket numbers to address a specific service on a computer rather than just the computer itself. Socket numbers identify the various services uniquely.

Information about the LAN

Several separate LANs required at one location do not necessarily need to have their own cabling. Different logical networks can share one cable. They use different formats for the Ethernet packets to ensure that the data belonging to the various networks does not clash and that one network remains invisible to the others. These formats are determined by the binding belonging to a unique network number on this cable.

You must provide the router with the network number and the binding associated with it to ensure that it too now knows which network it belongs to. If we leave the network address at the default setting '00000000', the router provides the address and the binding itself. It does this by searching on the attached cable for the network from which it receives the most SAP replies.

IPX routing table

Use the IPX routing table to determine which remote stations (i.e. which other routers or computers) can be reached by the local network and to give it some parameters for connection purposes. The table, which can hold up to 16 entries has the following structure:

Remote site	Network	Binding	Propagated	Backoff
BRANCH01	00000245	802.3	Route	On
BRANCH02	00000320	SNAP	Filt.	On
HEAD OFFICE	00000420	802.2	Filt.	Off

- Remote site:
The name of the remote station registered as the device name in the corresponding router on the remote side.
- Network:

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

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

■ Binding:

This is where you set which Ethernet binding is to be used on the WAN. This entry is only effective if the layer for this connection supports Ethernet encapsulation. 802.3 is assumed if the entry is missing.

■ Propagated:

A filter for type 20 IPX packets (NetBIOS propagated frames). The Network Basic Input/Output System was originally developed for IBM, and has since also been used by Microsoft in a modified form. This protocol provides services such as name resolution, data protection and correct packet sequencing (secure protocol) in layers 3 and 4 of the OSI model. NetBIOS packets have a special packet type and socket (propagated packets). NetBIOS is primarily used to exchange data between stations on a local network (LAN).

These IPX packets can be excluded from transmission or routed using the 'Filter' property. The 'Route' property transmits the packets if a connection to the remote station concerned is active or a free channel is available for the establishment of an additional connection. The propagated frames are rejected if all the lines to other remote stations are busy.

■ Backoff:

The IPX router uses a special algorithm (exponential backoff) to keep the connection costs arising in the case of erroneous configurations as low as possible.

The backoff function should be switched off if there is no server available on the remote station network (e.g. in the case of remote access from a workstation) (see also exponential backoff).

The default setting is 'On'.

What happens when data is transmitted on an IPX network?

When a device logs on to an IPX network, it first sends a request for the Service Advertising Protocol (SAP) and locates the nearest available server (get nearest server request) in the network numbered '00000000'. A router or server located on this network responds to this request and sends the correct network number.

The servers also regularly transmit information regarding which services they offer and which other networks they can reach. They use the special data packets complying with the Service Advertising Protocol or the Routing Information Protocol (RIP).

Once the IPX router is fully configured and is ready for operation, it proceeds to establish connections to all remote stations which can be reached via the routing tables and then exchanges SAP and RIP information with these networks. The router saves this data to its internal SAP and RIP tables.

RIP and SAP tables

RIP and SAP information is sorted alphabetically in the relevant tables. RIPs are thus only ordered by network and SAPs by service type first, then by server name.

The RIP and SAP tables are updated with each new RIP or SAP packet. The router only incorporates in its table SAP information for which it also has a corresponding RIP entry to ensure that only those services are offered (SAP) which can also be reached (RIP). The entries on the tables indicate, in addition to the information on reachable routes and services, how many routers the path to the destination (hops) passes through or how much time a data packet needs in the destination network (tics = approx. 1/18 of a second), for instance. The router selects the path with the fewest tics and the lowest hop count from the tables and stores only this route if the RIP information offers several different routes to a destination network, for instance.

RIP tables can hold 64 entries and SAP tables 128. If each new packet updates the tables, it stands to reason that the old entries must also disappear at some stage. Entries are artificially aged to do this. The age of all entries on RIP/SAP tables derived from local data transfers is incremented by 1 point every 60 seconds. A new RIP or SAP packet for an entry resets the age to zero. The route or service can be designated unreachable (down) once a selectable age of between 1 and 60 is reached. The entry is deleted when this elapsed time doubles. Additionally, any RIP and SAP information related to this remote station is deleted from the tables and replaced with new information when a connection is established.

So many routers around here...

If the establishment of simultaneous network connections to a greater number of remote stations is required than the number of B channels available, then it's time for a second (third...) router. The same entries are made in the routing tables for all routers to ensure that the brothers function in perfect harmony with each other and that the network really can always find a contact. The same routing information is then sent in the RIP packets to each router, albeit with a higher tic and hop count (`Setup/IPX-module/LAN-config/RIP-SAP-scal . activate`). This marks these routes as a sort of stand-by in the event that all channels are busy on the device addressed.

Redundant routes

A router receiving information in a RIP packet relating to routes with the same tic and hop counts as its own routes (redundant routes) does not, of course, have to reannounce

these routes itself to the sender. Therefore, it only sends these routes to the routers which did not propagate the route. This procedure is known as a "split horizon".

The Propagate loop (`Setup/IPX-module/LAN-Config/LOOP-Prop.`) can be used if it is nevertheless necessary to notify redundant routes to the local network. The routes learned in this way are then flagged in the RIP table with 'LOOP'. Although the propagation of redundant routes is not prohibited by the Novell specification, it should still be avoided as much as possible. Therefore, the default setting is 'Off'.

Exponential backoff

When switched on, the unit's IPX router attempts to establish suitable connections to receive routing information (RIP and SAP information) required for operation from the remote IPX stations. If this is not possible, due perhaps to a faulty configuration of the IPX router, the exponential backoff algorithm prevents connections constantly being established and thus saves charges.

The router will attempt to reach a remote station again with ever increasing wait times if the first attempt is unsuccessful. The wait time for this is determined as follows:

- The first attempt takes place after $10 + x$ seconds. x being a number from 0 to 10.
- The second attempt will be made $10 + x$ seconds after the first attempt has failed. x now standing for a number from 0 to 20 seconds.
- The higher value for x will now be doubled with each repeated attempt. The router finally gives up after the 16th unsuccessful attempt. The continual increase in the wait time means that 16 attempts will take a maximum of one day.

The route will be blocked if all attempts to call the remote station are unsuccessful. You can then only make further attempts at connection by amending the entry in the routing table.



The time to the next attempt and the number of attempts to establish a connection can be found in the network statistics using (`Status/IPX-module/IPX-router/Networks`).

IPX packet filters

The entries in the routing table determine which other networks will be accessible. However, they are then also accessible for data packets which are not actually required in the network of the remote station. These packets can also lead to unwanted connections being established which cost money.

Suitable filters are therefore required. These enable you to exclude from transmission over the WAN or at least restrict data packets which are only used in internal network communications, for example:

- Propagated frames

These special data packets use protocols which cannot in fact be routed. This data is encapsulated in normal IPX packets and sent as broadcast so that they can nevertheless participate in common routing.

These packets are sometimes not desirable in routing. For this reason, you can specify explicitly whether this type of packet is to be routed or filtered.

■ Socket filter

Every packet in an IPX network contains destination and source sockets along with destination and source addresses. Sockets identify the processes for which the data in the packet is intended.

There is a filter table each for sockets from local and remote networks containing the filters which can be used to exclude individual or entire groups of destination sockets. Certain sockets which are known frequently to be the cause of unwanted connections have already been entered in the socket filter table as default settings.

■ RIP and SAP information

A router uses the RIPs to inform the other routers of all the routes (paths to the other networks) known to it using the split horizon principle. This includes the entries from its own routing table and all routes which the router has derived from other routers. It gets its information for this purpose from routers on both local and remote networks. The router enters all available routing information in its internal RIP table.

The servers offer their services in the SAP information. The various services are represented within the SAP information as numbers. Each service (e.g. file server or print server) has a unique number. The router incorporates the information on the services available in its internal SAP table and registers which service is available on which network at which MAC address. At the same time it also establishes whether the service offered is located in a local or remote network and whether it can propagate the service without first establishing a connection.



You can look at the RIP and SAP tables and their current values in the IPX module (setup/IPX-module/RIP-config or SAP-config) of the router.

RIP and SAP information are extremely important for devices communicating on a network, which is why there are various different options for setting up the transmission of these packets.

- A LAN and WAN filter table can be used to tell the router not to include information on routes to particular networks or on certain available services in internal or external tables. The affected routes are thus not used, information on them is not provided and the services are not offered in the local network.
- RIP and SAP packets are always transmitted, i.e. no filters are used. These packets, however, must occupy a part of the connection.

- RIP and SAP packets will only be sent if the information they contain has been modified in some way.
- RIPs and SAPs can be transferred at regular, selectable intervals. Information is usually sent out in one minute intervals. The time interval between blocks can be stretched to up to 60 minutes.
- The most economical handling of RIP and SAP packets involves transmitting the information only once, when a connection is established.

■ IPX and SPX watchdogs:

These data packets are used by the server to determine whether workstation computers, for example, are still active or if they can be logged off. To ensure that these "Are you there?" packets for computers on a remote network do not continually result in connections being established, you can set the responses to these requests as follows:

- IPX watchdogs receive no response. The computers are logged off after a time specified on the server.
- IPX and SPX watchdogs can be responded to locally. This procedure is known as spoofing. The router responds in place of the computers addressed, which are then never logged off. It is also recommended that a time is set on the server after which the devices in question are always logged off.
- IPX and SPX watchdogs may of course be routed as normal but this frequently results in a connection being established.



Further information on IPX, the IPX router and the associated parameters can be found in 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 "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 'TCP/IP' configuration section on the 'Routing' tab, or in the `/Setup/IP-router-module/IP-routing-table` menu. This, then, is how an IP routing table might look:

IP address	Netmask	Router	Dis- tance	Mask.
192.168.120.0	255.255.255.0	GLASGOW	2	On
192.168.125.0	255.255.255.0	LONDON	3	Off
192.168.130.0	255.255.255.0	191.168.140.123	0	Static

What do the various entries on the list mean?

■ IP addresses and Network

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.

■ Router

The router transmits the appropriate data packets to the IP address and network mask to this remote station. A name is entered at this point if the remote station is a router in another network or an individual workstation computer. This is where the IP address of another router which knows the path to the destination network is entered if the router on the network cannot address the remote station itself.

■ 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 is established to a destination network are propagated with a distance of 1.

- All non-connected networks are propagated with the distance entered in the routing table (but with a minimum distance of 2) as long as a free transmitting channel is still available.
- The remaining networks are propagated with a distance of 16 (= unreachable) if there are no longer any channels available.
- Remote stations connected using Proxy ARP are an exception to this. These "Proxy hosts" are not propagated at all.

■ Mask.

Use the '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.

■ Following entries have a special meaning:

- IP address 255.255.255.255 with a network mask of 0.0.0.0: This is the default route. Any data packets which cannot be routed by other routing entries are transmitted to the remote station listed here.
- Network mask 255.255.255.255: Entries with completed network masks frequently only identify individual workstation computers (remote access) and not actual networks. A network which is only visible by a single IP address using IP masquerading may sometimes be concealed behind this.
- Router name 0.0.0.0: 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.

Examples with explanatory notes:

IP address	Netmask	Router	Dist.	This is what happens:
192.168.1.9	255.255.255.255	FIELD SERVICE	2	The FIELD SERVICE remote station can be reached at IP address 192.168.1.9.
192.168.120.0	255.255.255.0	Router01	2	All data packets with destination IP addresses 192.168.120.x are transmitted to ROUTER01.

IP address	Netmask	Router	Dist.	This is what happens:
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 router with the IP address 192.168.140.123.
10.0.0.0	255.0.0.0	0.0.0.0	0	Excludes transmission of all data packets to networks using private address spaces.
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 remote station. 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 IP 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 'Filtering' tab, or in the /Setup/IP-router-table/WAN-filter-table or LAN-filter-table menus.

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 'Use Proxy ARP' option (in LANconfig in the 'TCP/IP' configuration section on the 'Routing' tab or in the /Setup/IP-router-module menu for other configuration modes).

The router becomes a proxy for the teleworker with the following entry in the routing table:

IP address	Netmask	Router	Dis- tance	Mask
192.168.110.123	255.255.255.255	Teleworker01	0	off

Proxy hosts are not propagated in an RIP packet because the router responds to an ARP request for the proxy computer with its own MAC address. The distance is set to '0' on the routing table to indicate this clearly.

The router now responds to the request for the MAC address to the IP address 192.168.110.123 with its own MAC address. This ensures that all packets in the LAN for the teleworker are now automatically sent to the router, and that data is sent on to the computer at the other end of the ISDN connection.

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 network. 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 'TCP/IP' configuration section on the 'Routing' tab or in the `/Setup/IP-router-module/Local-routing` menu). This is how you tell the router to send the data packet to the other 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.

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 routers with RIP in a local network 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 running 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 '16' stands for "This route is not available at the moment". If a router cannot establish a connection, in addition to the present one, this 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).
 - The existing connection is using all B channels (channel bundling).



To take advantage of this function, enable the 'IP RIP' option (in ELSA LANconfig in the 'TCP/IP' configuration section on the 'Router' tab or in the Setup/IP Router-module menu for other configuration modes).

Routers with RIP capabilities dispatch the RIP packets approximately every 30 seconds. The router is only set up to send and receive RIPs if it has a unique IP address. The IP RIP module is deselected in the default setting using the IP address XXX.XXX.XXX.254.

Which information does the router take from received IP RIP packets?

When the router receives such IP RIP packets, it incorporates them in its dynamic routing table, which looks something like this:

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

What do the entries mean?

IP addresses and network masks identify the destination network, the distance is taken from the RIP information, the final column indicates the router which announced 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 router notifies the degradation of its own static routing table in this way (e.g. releasing a connection increases the distance from 1 to 2), 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.

The interaction of 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, 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. 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').

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 intranet, from the point of view of this computer the router appears to be the FTP server. The router knows the intranet address of the server from the entry in the service table (in *ELSA LANconfig* in the 'TCP/IP' 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 intranet, 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:

- FTP
- TCP
- 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: "Which IP address belongs to `www.domain.com`?" If the router has been specified as the DNS server in the workstations, the request is handled as follows:

- 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 connects to this server and retrieves the information required.
- 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.
- If no connection exists, the default route is established and a search is then carried out there for the DNS server.

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 router 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.

Policy Based Routing

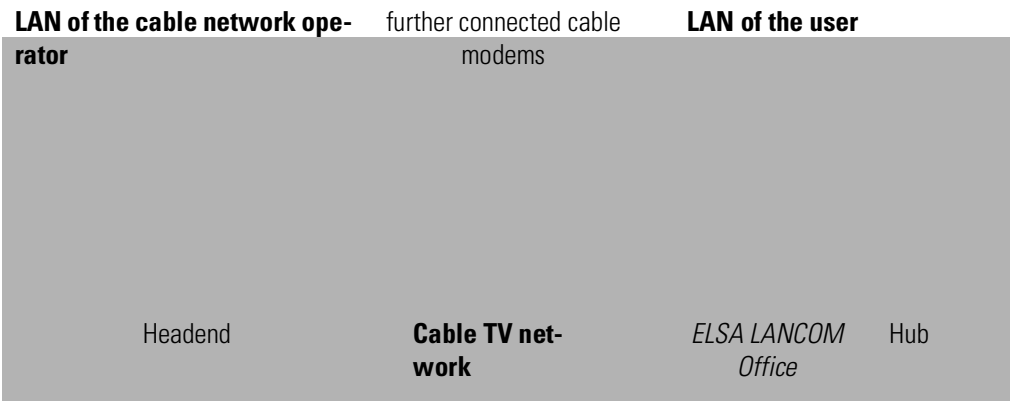
Policy-based routing describes a process in which particular data packets are given preferential treatment. This requires evaluation of a special field within the IP data packet, known as the Type of Service (TOS) field. This preferential treatment of a number of data packets can, for example, simplify 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'.

Bridging

A bridge connects two or more LANs in such a way that they appear to be a single large network. When bridging via cable modems, the LAN of the cable network operator with the headend is on one side and the LAN of the network participants with the cable modem and the local workstations on the other.



In the bridge operating mode, the *ELSA LANCOM Office* transfers all data to computers without locally assigned MAC addresses, between the local network or another local area network (LAN) or a workstation on one side and the cable network on the other side.

The bridge thus learns on its own which MAC addresses are located on its own network and which are located on the other side. After a very high level of data traffic that occurs during the initial negotiations between the two LANs, the network load drops sharply. In this case, the connection will no longer be established so frequently. When receiving data from the cable network, the bridge in the cable modem uses the MAC addresses to determine whether the data is destined for its own LAN. The bridge will only accept data packets that are addressed to MAC addresses in its LAN.

The bridge connects the two participating computers as if they were in fact located in one network. For this reason, however, only those computers which can also theoretically be integrated into a network should be connected. This means that both networks and the network and workstation computer must have the same network addresses.

The bridge is not dependent on the protocol used in layer 3. It operates only with Ethernet addresses (MAC addresses). Please, therefore, ensure that you only use those B-channel protocols in the layer list which have the setting ETHER in the ENCAPS column. Use a protocol other than PPP on layer 3, as this protocol is not supported for the bridge.



It is not possible to use the bridge via 2 B channels, as MLPPP is used for channel bundling.

What do you need to configure the bridge?

First establish which subscriber numbers the *ELSA MicroLink Cable* should listen to and which it should itself transfer externally (Setup/WAN-Module/Interface).

An entry which includes name and subscriber number must exist in the name list for *ELSA MicroLink Cable* to reach the remote station (Setup/WAN-Module/Name-List).

You should specify the correct remote station to the bridge (Setup/Bridge-Module/Remote-ID) since additional remote stations may be entered in the *ELSA MicroLink Cable* over time. This is because the bridge can only connect precisely two

networks together, while one router can manage several remote stations. You should also set (Setup/Bridge-Module/Operating:On) so that the bridge can function.

The process is now completed. The bridge now sets to work transferring all the data packets for non-local MAC addresses to the remote station set.



You can find more instructions on how to configure the ELSA MicroLink Cable as a bridge in the appropriate section of 'Workshop' and in the detailed description of the individual menus in the reference section of the manual.

What are the filter options?

You may not always wish to transfer all data. Much of the data which is bouncing around in the LAN is of no interest to remote networks or computers. For this reason, you can block transfer of the following data packets or only transfer them if the line has been established already: You can thus block transfer of the following data packets via the bridge:

- Broadcast packets: Data directed at all devices accessible in a network (Setup/Bridge-Module/LAN-config/Broadcast).
- Multicast packets: Data which is transferred to all devices accessible in a group (Setup/Bridge-Module/LAN-config/Multicast).
- Unicast packets: This is data directed only at a specific device (meaning a fixed MAC address).

Special filter lists which exclude certain addresses from a transmission or only allow certain addresses can be set up to handle this data. The bridge filters differentiate here between destination and source addresses. You can first establish for both address types whether the associated table contains the addresses to which data is to be transmitted (Setup/Bridge-Module/LAN-config/Dest.-address/Filter-type/pos) or the addresses to be excluded (.../Filter-type/neg). You then enter the MAC addresses to be filtered into the table itself.



This method of filtering by entering the exact MAC address naturally demands a certain degree of maintenance effort. Should the addresses change, when a network adapter is changed for example, the new addresses must be entered to ensure that the bridge continues to function.

Description of the menu options

The menu tree for *ELSA LANCOM* configuration is divided up into status information, setup parameters, firmware information and 'other'.

In order to help you familiarize yourself with the system, you will first be given an overview of the menu structure.

A complete list of all the menu options will be followed by a detailed description of all displays, menus and actions along with their associated parameters, default settings and input options.



Some of the features described in this Reference Manual apply only to specific models in the *ELSA LANCOM* family. Restrictions with regard to specific models are indicated by the symbol shown here.







You can access the menus when configuring via Telnet or terminal programs and via SNMP (also see 'Configuration Modes').

When configuring with *ELSA LANconfig*, you are provided with an integrated help system that gives you brief descriptions of the individual parameters.





















































All channel-related statistics and menus in this documentation refer to two channels only, even if more than two channels are available to the specific devices. Interface-related information is also provided for a single interface only. The information is equally applicable to the additional channels and interfaces.

Symbols

	Menu	Indicates a further submenu.
	Info	Indicates a value that cannot be modified.
	Value	Indicates a value that can be modified.
	Table	Indicates a table whose entries can be modified.
	Info table	Indicates a table whose entries cannot be modified.
	Action	Performs an action.

Overview of the menus






	Setup		Status
	Name		Connection
	WAN-module		Current-time
	Charges-module		Operating-time
	LAN-module		WAN-statistics
	IPX-module		LAN-statistics
	TCP-IP-module		PPP-statistics
	IP-router-module		IPX-statistics
	SNMP-module		TCP-IP-statistics
	DHCP-module		IP-router-statistics
	NetBIOS-module		Config-statistics
	Config-module		Queue-statistics
	LANCAPI-module		Conn.-statistics
	LCR-module		Info-connection
	DNS module		Layer-connection
	Time-module		Call-info-table
	Firmware		Remote-statistics
	Version-table		S ₀ -bus
	Table-firmsafe		Channel-statistics
	Mode-firmsafe		Time-statistics
	Timeout-firmsafe		LCR-statistics
	Test-firmware		Delete-values
	Firmware-upload		Other
			Manual-dialing
			Boot-system
			Reset-system
			Upload-system

Status

The Status menu contains information on the current status and the internal sequences of operations in the LAN and WAN, which can relate to the data transmission route (e.g. dialing or connection) or to statistics (e.g. number of calls received or data blocks transmitted). The statistics displays are an important aid for verifying correct functioning and optimizing parameter settings. In addition, they provide valuable information for error analysis when malfunctions occur.

Most status displays are continually updated and can be deleted with a **value** or set to 0 in the current menu.

The menu has the following layout:

Status		Running status displays
Connection		Status of the WAN route
Current-time		Current time in device
Operating-time		Period of time the device has operated since it was last switched on
WAN-statistics		Displays WAN statistics
LAN-statistics		Displays LAN statistics
PPP-statistics		Point-to-point-protocol statistics
IPX-statistics		Statistics from the IPX and IPX router area
TCP-IP-statistics		Statistics from the TCP/IP area
IP-router-statistics		Statistics from the IP router
Config-statistics		Remote configuration statistics
Queue-statistics		Statistics relating to the packets in the queues of the individual modules
Connections-statistics		Connection information for each interface
Info-connection		Information on the last connection for each interface
Layer-connection		Information on the B-channel protocol used for each interface
Call-info-table		Information on the last 100 calls received
Remote-statistics		Statistics on the last 100 connections
S ₀ -bus		Status of the S ₀ interface
Channel-statistics		Information of the status of the individual channels.
Time-statistics		Time module information
LCR-statistics		Least-cost router information
Delete-values		Deletes all values except tables with substatistics.

Display and keyboard

The display shows status information and error messages issued by the device. The following display modes are available:

- B channel overview (one character per channel)
- B channel status (one line per channel)
- Device status / Device error messages

A total of six keys are available (cursor keys + "Mode" + "Clr"), as well as a two-line display with 40 characters per line, of which 16 characters each are currently displayed. Depending on the devices settings, the text information is displayed in German or English.

B-channel-overview

In the B channel overview the channels are displayed in the form of a table. The individual fields of the table have the following significance:

P : x (status of port 1, first B channel)	P : X	P : X	P : X
1 : x (status of port 1, second B channel)	2 : x	3 : x	4 : x

The following symbols are used for the channel status (shown by x in the table):

.	Channel idle (disabled)
-	Channel idle (enabled)
E (flashing)	An error has occurred on the channel
A (flashing)	Outgoing call
A	Connected (outgoing)
P (flashing)	Incoming call
P	Connected (incoming)
N (flashing)	Negotiation

The cursor keys have no function in this mode.

B channel status display

The B channel status display shows an excerpt from a table with an entry for each B channel. In the event of changes to the status of a channel, the table will jump to the current entry if no cursor key has been used for at least 5 seconds. The status of the channel is displayed in plain text, e.g.:

CH11: Connection LC_PPP

CH12: Remote station LC_PPP not responding

Error messages are retained for 60 seconds. Information with regard to the enabling and disabling of S₀ interfaces is also displayed.

The up and down cursor keys can be used to scroll through the individual lines; use the left and right cursor keys to navigate within the line itself. Although a width of only 16 characters is available, the display has a total width of 40 characters (the visible section can be moved). The display returns to the start 5 seconds after the last horizontal movement.

Device status and device error messages

Channel-independent device status messages and especially error messages (with simultaneous flashing Power/Msg LED) are displayed in this mode. The unit automatically switches to this mode in the event of an error.


The up and down cursor keys permit scrolling through all available messages. The model number (e.g. "Model 4100") and the firmware version always appear as the final message. This display also appears immediately after switching the unit on, before changing to the last current display mode. The error messages in this mode can also be up to 40 characters long.

The Mode key switches between the display modes described above.

The Clr key clears the errors displayed in the device status and device error message display modes.

Status/Connection

The **Status/Connection** menu option displays the status messages for the individual channels.

/Connection-state	Running status displays	
Connection		CH01: Ready; CH02: Ready

Status/Current-time

This displays the current device time, used, e.g., for the least-cost-router calculations or certain statistics. The time can be read from the ISDN (ISDN time, see also Setup/time module) or set manually (with the 'time' command).










Status/Operating-time

The operating time of the router since it was last started is displayed here in days hours, minutes and seconds.

Status/WAN-statistics

This option allows you to display the various statistics parameters for the WAN port. A large number of values related to the data volume transferred provide you with useful information on WAN port utilization, errors that have occurred, and the internal resources of the devices that are available in the current operating state.

The WAN statistics are maintained on an interface-specific basis, i.e. separate statistics in which the transferred data and errors are recorded are available for each interface. The **Status/WAN-statistics** menu has the following layout:

/WAN-statistics		Running status displays
Byte-transport-statistics		Statistics on bytes transferred
Packet-transport-statistics		Statistics on data packets transferred
Error-statistics		Statistics on data errors that have occurred
WAN-tx-discarded		Number of packets discarded due to an error/lack of resources
WAN-heap-packets		Number of buffers in use
WAN-queue-packets		Number of buffers available
WAN-queue-errors		Number of packets discarded due to a lack of buffers
Throughput-statistics		Statistics for bytes transferred on every channel
Delete-values		Deletes WAN statistics

Byte-transport-statistics

The menu item **Status/WAN-statistics/Byte-transport-statistics** contains statistics of the bytes transferred over an interface for every available interface. The table maintained here has the following layout:

Ifc	CRx-bytes	Rx-bytes	Tx-bytes	CTx-bytes
Ch01	0	0	0	0
Ch02	0	0	0	0

Below is a detailed description of the meaning of each field:

Ifc	Designates the associated channel.
CRx-bytes	Number of bytes received (compressed)
Rx-bytes	Number of bytes received (uncompressed)
Tx-bytes	Number of bytes sent (uncompressed)
CTx-bytes	Number of bytes sent (compressed)

Packet-transport-statistics

For each available interface, the **Status/WAN-statistics/Packet-transport-statistics** menu option provides statistics on the data packets transferred via this interface. The table maintained here has the following layout:

Ifc	Rx	Tx-total	Tx-normal	Tx-reliable	Tx-urgent
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0

Below is a detailed description of the meaning of each field:

Ifc	Designates the associated channel.
Rx	Number of packets received
Tx-total	Number of packets sent (data and protocol packets)
Tx-normal	Number of normal data packets sent
Tx-reliable	Number of data packets transferred with secured handling
Tx-urgent	Number of data packets transferred with priority handling (urgent queue)

Error-statistics

For each available interface, the **Status/WAN-statistics/Error-statistics** menu option provides statistics on the transmission errors that have occurred on this interface. The table maintained here has the following layout:

Ifc	Rx-l1-error	Rx-l2-error	Rx-l3-error	Stack-error	Tx-error
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0

Below is a detailed description of the meaning of each field:

Ifc	Designates the associated channel.
Rx-l1-error	Number of layer-3 errors in data received (i.e., the protocol header of layer-3 is incorrect)
Rx-l2-error	Number of layer-2 errors in data received (i.e., similar to the layer-3 errors, e.g. defective PPP header)
Rx-l3-error	Number of layer-1 errors in data received (similar to layer-3 errors)
Stack-error	Number of transmission errors that occurred while sending
Tx-error	Number of stack errors for data received. Stack errors are caused when frames are received that cannot be assigned to an internal processing procedure (e.g. IP router).

Throughput-statistics

The menu item **Status/WAN-statistics/Throughput-statistics** contains statistics of bytes transferred over this interface for both channels. The table maintained here has the following layout:













lfc	Rx/s current	Tx/s current	Rx/s average	Tx/s average
Ch01	0	0	0	0
Ch02	0	0	0	0











Below is a detailed description of the meaning of each field:

lfc	Designates the associated channel.
Rx/s current	Throughput on the channel in the last second in the receiving direction
Tx/s current	Throughput on the channel in the last second in the transmission direction
Rx/s average	Average throughput on the channel in the receiving direction
Tx/s average	Average throughput on the channel in the transmission direction

Status/LAN-statistics










Similarly to the previous menu option, this option allows you to display the statistics relating to the LAN port. The **Status/LAN-statistics** menu has the following layout:





/LAN-statistics	Running status displays	
LAN-rx-packets		Number of data packets received
LAN-tx-packets		Number of data packets sent
LAN-rx-errors		Number of data packets incorrectly received
LAN-tx-errors		Number of data packets incorrectly sent
LAN-stack-errors		Number of packets without a suitable receive module (bridge/router)
LAN-NIC-errors		Number of data packets discarded by the NIC
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
LAN-queue-errors		Number of packets discarded due to a lack of buffers
LAN-collisions		Number of collisions during a send procedure
Link-active		Display of correct Ethernet connection (data transfer possible). Corresponds to the 'Link' LED on the device.
Negotiation done		The negotiation of the transfer mode between the router and the remote station is complete. This is only relevant if Setup/LAN/Connection is set to 'Auto'.

/LAN-statistics	Running status displays	
Connector		This item shows the connection type currently being used on the Ethernet connection: 10B-TX: 10 MBit, half-duplex FD10B-TX: 10 MBit, full-duplex 100B-TX: 100 MBit, half-duplex FD100B-TX: 100 MBit, full-duplex If 'Auto' is set under Setup/LAN, then this is the connection type the two units have negotiated. This corresponds to the 'Fast' and 'FDpx' LEDs on the unit. If, on the other hand, a fixed transfer mode has been set, this value will be the same as the one in Setup/LAN/Connection.
LAN-rx-bytes		Number of bytes received from the LAN
LAN-tx-bytes		Number of bytes sent to the LAN
LAN-rx-broadcasts		Number of broadcast packets received from the LAN
LAN-rx-multicasts		Number of multicast packets received from the LAN
LAN-rx-unicasts		Number of directly addressed packets received from the LAN
LAN-tx-broadcasts		Number of broadcasts received from the LAN
LAN-tx-multicasts		Number of multicasts received from the LAN
LAN-tx-unicasts		Number of unicasts received from the LAN
Delete-values		Deletes LAN statistics

Status/PPP-statistics

Within the PPP statistics, the states of individual subprotocols of the PPP are managed separately for each interface. However, statistics relating to the frames transmitted for individual subprotocols are maintained only in joint statistics. Consequently, the **Status/PPP-statistics** menu has the following layout:

/PPP-statistics	Running status displays	
PPP-phases		Statistics relating to the status of PPP protocol negotiation for each interface
LCP-statistics		Displays PPP/LCP statistics
PAP-statistics		Displays PPP/PAP statistics
CHAP-statistics		Displays PPP/CHAP statistics
CBCP-statistics		Displays PPP/CBCP statistics
IPXCP-statistics		Displays PPP/IPXCP statistics
IPCP-statistics		Displays PPP/IPCP statistics
CCP-statistics		Displays PPP/CCP statistics
ML-statistics		Displays PPP/ML statistics

/PPP-statistics		Running status displays
BACP-statistics		Displays PPP/BACP statistics
Rx-options		Displays the LCP, IPCP and IPXCP information received
Tx-options		Displays the LCP, IPCP and IPXCP information sent
Delete-values		Deletes PPP statistics.

The PPP statistics provide detailed information on the phases of a PPP negotiation, particularly in the event of connection problems with external products. It provides important information for error diagnosis.

PPP-phases

For each available interface, the **Status/PPP-statistics/PPP-phases** option provides a list of the current states of PPP protocol negotiation. The table maintained here has the following layout:

Ifc	Phase to	LCP	IPCP	IPXCP	CCP
Ch01	DEAD	Initial	Initial	Initial	Initial
Ch02	DEAD	Initial	Initial	Initial	Initial

Below is a detailed description of the meaning of each field:

Ifc	Designates the associated channel.
Phase to	Indicates the current phase of the PPP. The possible values are AUTHENTICAT , NETWORK and TERMINATE .
LCP	Status of the 'Link Control Protocol' subprotocol. The possible values are: Initial , Starting , Stopping , Stopped , Closing , Closed , ReqSent , AckRcvd , AckSent and Opened .
IPCP	Similarly to 'LCP', displays the status of the 'IP Control Protocol' subprotocol.
IPXCP	Similarly to 'LCP', displays the status of the 'IPX Control Protocol' subprotocol.
CCP	Similarly to 'LCP', displays the status of the 'Compression Control Protocol' subprotocol.

The current PPP phases are shown under **Status/PPP-statistics/PPP-phases**. As specified above, these phases are the idle (Dead), ready (Establish), access parameter verification (Authenticate) and network phase (Network). In the substatistics, the frames exchanged are encrypted separately by type and quantity.

Status/PPP-statistics/LCP-statistics

The **LCP** (Link Control Protocol) negotiates the basic features of the PPP connections. The LCP frames exchanged during PPP negotiation are recorded in statistics and displayed by type and quantity. If the LCP does not change to the OPEN state for a connection, these statistical values provide information on errors that occurred during the initial phase of

PPP negotiation. Below is a detailed description of the meanings of the parameters for these statistics:

Rx-errors	Number of faulty PPP packets received
Rx-discarded	Number of PPP packets discarded
Rx-config-request	Number of configure request packets received for LCP
Rx-config-ack.	Number of configure acknowledge packets received for LCP
Rx-config-nak.	Number of configure negative acknowledge packets received
Rx-config-reject	Number of configure reject packets received for LCP
Rx-terminate-request	Number of terminate request packets received for LCP
Rx-terminate-ack.	Number of terminate acknowledge packets received for LCP
Rx-code-reject	Number of code reject packets received for PPP
Rx-protocol-reject	Number of protocol reject packets received for PPP
Rx-echo-request	Number of echo request packets received for LCP
Rx-echo-reply	Number of echo response packets received for LCP
Rx-discard-request	Number of discard request packets received for LCP
Tx-config-request	Number of configure request packets sent for LCP
Tx-config-ack.	Number configure acknowledge packets sent for LCP
Tx-config-nak.	Number of configure negative acknowledge packets sent
Tx-config-reject	Number of configure reject packets sent for LCP
Tx-terminate-request	Number of terminate request packets sent for LCP
Tx-terminate-ack.	Number of terminate acknowledge packets sent for LCP
Tx-code-reject	Number of code reject packets sent for PPP
Tx-protocol-reject	Number of protocol reject packets sent for PPP
Tx-echo-request	Number of echo request packets sent for LCP
Tx-echo-reply	Number of echo response packets sent for LCP
Tx-discard-request	Number of discard request packets sent for LCP
Delete-values	Deletes LCP statistics

Status/PPP-statistics/PAP-statistics

The **PAP** (Password Authentication Protocol) is one of two common procedures for verifying remote stations in the PPP. When a connection is established, it checks the remote station password and enables the connection only after a successful exchange of passwords (refer also to Chapter 'Point-to-Point Protocol'). Below is a detailed description of the meanings of the parameters for these statistics:

Rx-discarded	Number of PAP packets discarded
Rx-request	Number of PAP request packets received
Rx-success	Number of PAP success packets received

Rx-failure	Number of PAP failure packets received
Tx-retry	Number of times PAP request packets resent
Tx-request	Number of PAP request packets sent
Tx-success	Number of PAP success packets sent
Tx-failure	Number of PAP failure packets sent
Delete-values	Deletes PAP statistics

Status/PPP-statistics/CHAP-statistics

The **CHAP** (Challenge Authentication Protocol) is the second option for verifying the remote station under PPP. The password is checked as the connection is established and again at adjustable intervals during the connection (refer also to Chapter 'Point-to-Point Protocol'). Below is a detailed description of the meanings of the parameters for these statistics:

Rx-discarded	Number of CHAP packets discarded
Rx-challenge	Number of CHAP challenge packets received
Rx-response	Number of CHAP response packets received
Rx-success	Number of CHAP success packets received
Rx-failure	Number of CHAP failure packets received
Tx-retry	Number of times the CHAP challenge packets were resent
Tx-challenge	Number of CHAP challenge packets sent
Tx-response	Number of CHAP response packets sent
Tx-success	Number of CHAP success packets sent
Tx-failure	Number of CHAP failure packets sent
Delete-values	Deletes CHAP statistics

Status/PPP-statistics/IPXCP-statistics

When IPX is used, the **IPXCP** (Internet Exchange Protocol Control Protocol) indicates the status of the protocol and the packets exchanged in the negotiation. Below is a detailed description of the meanings of the parameters for these statistics:

Rx-discarded	Number of IPXCP packets discarded
Rx-config-request	Number of configure request packets received for IPXCP
Rx-config-ack.	Number of configure acknowledge packets received for IPXCP
Rx-config-nak.	Number of configure negative acknowledge packets received
Rx-config-reject	Number of configure reject packets received for IPXCP
Rx-terminate-request	Number of terminate request packets received for IPXCP
Rx-terminate-ack.	Number of terminate acknowledge packets received for IPXCP
Rx-code-reject	Number of code reject packets received for IPXCP
Tx-config-request	Number of configure request packets sent for IPXCP
Tx-config-ack.	Number of configure acknowledge packets sent for IPXCP
Tx-config-nak.	Number of configure negative acknowledge packets sent
Tx-config-reject	Number of configure reject packets sent for IPXCP
Tx-terminate-request	Number of terminate request packets sent for IPXCP

Tx-terminate-ack.	Number of terminate acknowledge packets sent for IPXCP
Tx-code-reject	Number of code reject packets sent for IPXCP
Delete-values	Deletes IPXCP statistics

Status/PPP-statistics/IPCP-statistics

When IP is used, the **IPCP** (Internet Protocol Control Protocol) indicates the status of the protocol and the packets exchanged in the negotiation.

Rx-discarded	Number of IPCP packets discarded
Rx-config-request	Number of configure request packets received for IPCP
Rx-config-ack.	Number of configure acknowledge packets received for IPCP
Rx-config-nak.	Number of configure negative acknowledge packets received
Rx-config-reject	Number of configure reject packets received for IPCP
Rx-terminate-request	Number of terminate request packets received for IPCP
Rx-terminate-ack.	Number of terminate acknowledge packets received for IPCP
Rx-code-reject	Number of code reject packets received for IPCP
Tx-config-request	Number of configure request packets sent for IPCP
Tx-config-ack.	Number of configure acknowledge packets sent for IPCP
Tx-config-nak.	Number of configure negative acknowledge packets sent
Tx-config-reject	Number of configure reject packets sent for IPCP
Tx-terminate-request	Number of terminate request packets sent for IPCP
Tx-terminate-ack.	Number of terminate acknowledge packets sent for IPCP
Tx-code-reject	Number of code reject packets sent for IPCP
Delete-values	Deletes IPCP statistics

Status/PPP-statistics/CBCP-statistics

The **CBCP** (Callback Control Protocol) shows the protocol status when the IP is in use and the packets exchanged during negotiation.

Rx-request	Number of CBCP request packets received
Rx-discarded	Number of CBCP packets discarded
Rx-acknowledge	Number of CBCP acknowledge packets received
Tx-request	Number of CBCP request packets sent
Tx-response	Number of CBCP response packets sent
TX-acknowledge	Number of CBCP acknowledge packets sent
Request-discarded	Number of CBCP request packets discarded

Response-discarded	Number of CBCP response packets discarded
Ack.-discarded	Number of CBCP acknowledge packets discarded
Delete-values	Deletes CBCP statistics

Status/PPP-statistics/CCP-statistics

The statistics of the Compression Control Protocol (CCP) show the packets exchanged for data compression during the PPP negotiation.

Rx-discarded	Number of all CCP packets discarded
Rx-config-request	Number of CCP queries received
Rx-config-ack.	Number of CCP queries accepted
Rx-config-nak.	Number of CCP queries rejected because query parameters were not accepted.
Rx-config-reject	Number of CCP rejected for other reasons.
Rx-terminate-request	Number of CCP queries after releasing the compression.
Rx-terminate-ack.	Number of confirmed CCP queries after releasing the compression.
Rx-code-reject	Number of CCP queries rejected because the remote station will not or cannot apply compression.
Rx-reset-request	Number of CCP queries after synchronizing the compression (e.g. after transfer errors)
Rx-reset-ack.	Number of confirmed CCP queries after synchronizing the compression
Tx-config-request	Number of CCP queries sent
Tx-config-ack.	Number of CCP queries accepted by the remote station
Tx-config-nak.	Number of CCP queries rejected by the remote station because of parameters not being accepted.
Tx-config-reject	Number of CCP queries rejected by the remote station for other reasons.
Tx-terminate-request	Number of CCP queries sent after releasing the compression.
Tx-terminate-ack.	Number of CCP confirmations sent for releasing the compression.
Tx-code-reject	Number of CCP queries rejected because the <i>ELSA LANCOM</i> does not wish to use compression (by layer list settings).
Tx-reset-request	Number of CCP queries sent after synchronizing the compression (e.g. after transfer errors)
Tx-reset-ack.	Number of CCP confirmations sent for synchronizing the compression
Delete-values	Deletes CCP statistics

Status/PPP-statistics/ML-statistics

The MLPPP statistics mostly provide information on how the remote station handled the individual packets during a bundled PPP connection.

Bundle-connections	Number of connections that used the MLPPP.
Rx-Seq-loss	Number of packets in which an error occurred in the sequence of sequence numbers.
Rx-Seq-repeat	Number of packets in which the sequence of sequence numbers came late.
Rx-Mrru-exceeded	Number of packets in which a violation of the MRRU negotiated in the PPP negotiation was found after assembly (maximum received reassembled unit).
Rx-Header-error	Number of packets with header errors.
Rx-discarded	Number of all discarded MLPPP packets.
Rx-Frag-start	Number of packets with a start flag set (first part of a fragmented packet).
Rx-Frag-mid	Number of packets with set mid flag (middle part of a fragmented packet).
Rx-Frag-end	Number of packets with set end flag (last part of a fragmented packet).
Rx-not-fragmented	Number of packets with set start and end flag (unfragmented packets).
Delete-values	Delete ML statistics

Status/PPP-statistics/Rx- and Tx-options

The PPP statistics options show what information was exchanged during the negotiation over LCP, IPCP or IPXCP.




Rx-options

This shows information on what the remote station requested (LCP) or what was assigned to the router (IPCP and IPXCP).

Tx-options

This shows information on what the router requested from the remote station (LCP) or what it assigned to it (IPCP and IPXCP).

The two submenus have the same layout:

/Rx- and Tx-options	Display	
LCP		Information on packet sizes, control characters, security procedures and callback
IPXCP		Information on addresses and routing procedures in the IPX network
IPCP		Information on addresses in the IP network

The LCP table has separate listings for every channel:

MRU	M aximum R eceive U nit designates the maximum packet size that the remote station can receive
ACCM	A synchronous C ontrol C haracter M ap designates the character in the asynchronous data flow that is interpreted as the control character
Authent.	Authentication procedure used (PAP/CHAP)
Callback	Callback negotiation type

The IPXCP table shows the negotiated IPX option separately for every channel:








Network	Network number of the WAN network
Node-ID	The Rx options show the node ID assigned to the <i>ELSA LANCOM</i> (generally 000000000000 or the MAC address of the router). The Tx options show the node ID of the remote station (also 000000000000 or the MAC address of the remote station)
Routing-method	The routing protocol in use is given here (RIP/SAP or nothing), in the Rx what the remote station has assigned to us and in the Tx the one that the <i>ELSA LANCOM</i> assigns to the remote station.

Finally, IPCP has the negotiated IP options, again separated according to the channel:

IP-address	Again the Rx options have the addresses that were assigned by the remote station and the Tx options have those that the <i>ELSA LANCOM</i> assigned to the remote station (e.g. the IP address of the dial-up node at the Internet provider can easily be read in the Tx options).
DNS-default	
NBNS-default	

Status/IPX-statistics

The statistics from the IPX area are grouped here and classified by type, socket and router information. The IPX statistics contain the following parameters:

/IPX-statistics	Statistics from the IPX and IPX router area	
MAC-statistics		Statistics from the IPX packet media access control
Watchdog-statistics		Statistics for watchdog packets
Propagate-statistics		Statistics for IPX propagated packets (IPX type 20)
RIP-statistics		Statistics for NetWare RIP
SAP-statistics		Statistics for NetWare SAP
IPX-router-statistics		Statistics on the remote IPX router
Delete-values		Deletes IPX statistics

The substatistics then provide you with further parameters for the individual menus.

Status/IPX-statistics/MAC-statistics

These statistics include the following values:

IPX-LAN-rx	Number of IPX packets received from the LAN
IPX-LAN-rx-broadcasts	Number of broadcast IPX packets received from the LAN
IPX-LAN-rx-multicasts	Number of multicast IPX packets received from the LAN
IPX-LAN-rx-unicasts	Number of directly addressed IPX packets received from the LAN
IPX-LAN-tx	Number of IPX packets sent to the LAN
IPX-WAN-rx	Number of IPX packets received from the WAN
IPX-WAN-rx-broadcasts	Number of broadcasts received from the WAN
IPX-WAN-rx-multicasts	Number of multicasts received from the WAN
IPX-WAN-rx-unicasts	Number of directly addressed IPX packets received from the WAN
IPX-WAN-tx	Number of IPX packets sent to the WAN
Delete-values	Deletes MAC statistics

Status/IPX-statistics/Watchdog-statistics

These statistics include the following values:

IPX-watchdog-LAN-rx	Number of IPX watchdog packets received from the LAN
IPX-watchdog-LAN-tx	Number of IPX watchdog packets sent to the LAN
IPX-watchdog-WAN-rx	Number of IPX watchdog packets received from the WAN
IPX-watchdog-WAN-tx	Number of IPX watchdog packets sent to the WAN
SPX-watchdog-LAN-rx	Number of SPX watchdog packets received from the LAN
SPX-watchdog-LAN-tx	Number of SPX watchdog packets sent to the LAN
SPX-watchdog-WAN-rx	Number of SPX watchdog packets received from the WAN
SPX-watchdog-WAN-tx	Number of SPX watchdog packets sent to the WAN
Delete-values	Deletes watchdog statistics

Status/IPX-statistics/Propagate-statistics

These statistics include the following values:

Propagate-LAN-rx	Number of IPX propagated packets received from the LAN
Propagate-LAN-filters	Number of IPX propagated packets from the LAN that were received/filtered
Propagate-LAN-tx	Number of IPX propagated packets sent to the LAN
Propagate-LAN-socket-errors	Number of IPX propagated packets from the LAN filtered by socket filter

Propagate-LAN-hop-errors	Number of IPX propagated packet filtered from the LAN by hop count
Propagate-LAN-backroute-errors	Number of IPX propagated packets to be backrouted from the LAN
Propagate-LAN-contention	Number of packets to be routed from the LAN during a defective connection
Propagate-WAN-rx	Number of IPX propagated packets received from the WAN
Propagate-WAN-filters	Number of IPX propagated packets from the WAN that were received/filtered
Propagate-WAN-tx	Number of IPX watchdog packets sent to the WAN
Propagate-WAN-socket-errors	Number of IPX propagated packets filtered from the WAN by socket filter
Delete-values	Deletes IPX propagated packet statistics

Status/IPX-statistics/RIP-statistics

These statistics include the following values:

RIP-LAN-rx	Number of RIP packets received from the LAN
RIP-LAN-errors	Number of RIP packets with defective content received from the LAN
RIP-LAN-tx	Number of RIP packets sent to the LAN
RIP-WAN-rx	Number of RIP packets received from the WAN
RIP-WAN-errors	Number of RIP packets with defective content received from the WAN
RIP-WAN-tx	Number of RIP packets sent to the WAN
Delete-values	Deletes RIP statistics
Table-RIP	Displays RIP table

Table-RIP

There are 256 entries with RIP information in the **RIP table**. It has the following layout:

Network	Hops	Tics	Node ID	Time	Flags
Network address	Number of routers to be passed on the path to the other network	Time required for this route in tics	MAC address of the server	Number of table updates until the entry is deleted	Local, remote, loop or down

Status/IPX-statistics/SAP-statistics

These statistics include the following values:

SAP-LAN-rx	Number of SAP packets received from the LAN
SAP-LAN-errors	Number of SAP packets with defective content received from the LAN
SAP-LAN-tx	Number of SAP packets sent to the LAN
SAP-WAN-rx	Number of SAP packets received from the WAN
SAP-WAN-errors	Number of SAP packets with defective content received from the WAN

SAP-WAN-tx	Number of SAP packets sent to the WAN
Table-SAP	Number of SAP packets received from the LAN
Delete-values	Deletes SAP statistics

Table-SAP There are 512 entries with SAP information in the **SAP table**. It has the following layout:

Type	Server-name	Network	Node ID	Socket	Hops	Time	Flags
Service SAP no.	Server computer name	Network address	MAC address of the server	Socket for the service	Number of routers to the destination network	Number of table updates until the entry is deleted	Local, remote, loop or down

Status/IPX-statistics/IPX-router-statistics

These statistics include the following values:

IPXr-LAN-rx	Number of IPX packets to be routed from the LAN
IPXr-LAN-tx	Number of IPX packets routed to the LAN
IPXr-LAN-hop-errors	Number of IPX packets filtered by hop count to be routed from the LAN
IPXr-LAN-socket-errors	Number of IPX packets filtered by socket filter to be routed from the LAN
IPXr-LAN-net-errors	Number of packets from the LAN to be routed to incorrect networks
IPXr-LAN-backroute-errors	Number of IPX packets to be backrouted from the LAN
IPXr-LAN-contention	Number of packets to be routed from the LAN during a defective connection
IPXr-LAN-down-errors	Number of IPX packets to be routed from the LAN to logged-off networks
IPXr-WAN-rx	Number of IPX packets to be routed from the WAN
IPXr-WAN-tx	Number of IPX packets routed to the WAN
IPXr-WAN-hop-errors	Number of IPX packets filtered by hop count to be routed from the WAN
IPXr-WAN-socket-errors	Number of IPX packets filtered by socket filter to be routed from the WAN
IPXr-WAN-net-errors	Number of packets from the WAN to be routed to incorrect networks
IPXr-WAN-backroute-errors	Number of IPX packets to be backrouted from the WAN
IPXr-WAN-down-errors	Number of IPX packets to be routed from the WAN to logged-off networks
IPXr-intern-rx	Number of packets from internal modules to the IPX router
Networks	Table of networks in the IPX routing table with node IDs
Establish-table	Table of the last 20 packets that required a connection
Delete-values	Deletes IPX router statistics

Establish-table The **establish table** is a further submenu option within router statistics. It contains the last 20 entries, which provide information on the system time, the IPX destination address, and the IPX source address of the data packets that have caused a connection to be established.

An IPX establish table might have the following appearance:

Time	Destination	Source
1T; 16:45:01	00000081 ffffffff 0453	00000001 00a05702000a 0453
1T; 10:45:10	00000081 ffffffff 0452	00000001 00a05702000a 0452

The 'Time' is displayed as the device operating time or the ISDN real time (if this is available from the ISDN terminal). The destination address 'fffffff' might refer, for example, to a broadcast packet. The destination and source addresses both consist of the network number, MAC address and the socket number (all hexadecimal values).

Networks

The **network statistics** are also a submenu option within the IPX router statistics. This table provides more extensive information on a static route (remote station). It has the following layout:

Remote-ID	Network	Binding	Propagate	Backoff	Time	Node-ID
Logical remote station	Network address	Binding	Route/Filter	Connection counter	Time remaining until next connection	Node-ID of remote station










The different entries have the following meaning:

Remote-ID	Logical name of the remote station as it is entered in the routing table. An entry for the LAN link is also present; it is located in the first position in the table and has the name "LAN".
Network	Address of the network in which the remote station is located. For remote WAN stations, this corresponds to the entry in the routing table. If the autodetect function is configured in the IPX routing table (/SETUP/IPX-MODULE/LAN-CONFIGURATION/NETWORK), the network that was detected is displayed here.
Binding	Ethernet binding to which the remote station is linked. For remote WAN stations, this corresponds to the entry in the routing table. If the autodetect function is configured in the IPX routing table (/SETUP/IPX-MODULE/LAN-CONFIGURATION/NETWORK), the binding that was detected is displayed here.
Propagate	Filter flag for IPX type 20 (propagated) frames. For remote WAN stations, this corresponds to the entry in the routing table. For the LAN, a route is always entered here.

Backoff	Connection counter for the exponential backoff algorithm. When the connection counter reaches a value of 16, no more attempts are made, meaning that the route is deactivated (also possible for the LAN).
Time	Time remaining (specified in seconds) until the next connection attempt is made by the exponential backoff algorithm. When a connection has been successfully established, the remaining time is set to zero, thus activating the route.
Node ID	Node ID of the responsible router in the WAN network. The node ID of the router is entered here for the LAN entry.

Status/TCP-IP-statistics

The TCP/IP-related statistics are shown here, broken down according to the various TCP/IP sub-protocols. The TCP/IP statistics contain the following parameters:

/TCP-IP-statistics		Statistics from the TCP/IP area
ARP-statistics		Statistics from the ARP area
IP-statistics		Statistics from the IP area
ICMP-statistics		Statistics for ICMP packets
TFTP-statistics		Statistics for TFTP operations
TCP-statistics		Statistics for TCP packets from TCP sessions to the router
DCHP-statistics		Statistics from the DCHP server
Delete-values		Deletes TCP/IP statistics
NetBIOS-statistics		NetBIOS module statistics
DNS-statistics		Statistics from the DNS server

The substatistics then provide you with further parameters for the individual menus.

Status/TCP-IP-statistics/ARP-statistics

These statistics include the following values:

ARP-LAN-rx	Number of ARP requests and responses received from the LAN
ARP-LAN-tx	Number of ARP requests and responses sent to the LAN
ARP-LAN-errors	Number of ARP requests incorrectly received from the LAN
ARP-WAN-rx	Number of ARP requests and responses received from the WAN
ARP-WAN-tx	Number of ARP requests and responses sent to the WAN
ARP-WAN-errors	Number of ARP requests incorrectly received from the WAN
Table-ARP	Displays ARP table
Delete-values	Deletes ARP statistics

Table-ARP

There are 128 entries with ARP information in the **ARP table**. It has the following layout:

IP-address	Node-ID	Last-access	Connect
IP address that has previously been found by ARP request	Associated MAC address	Time since the last access in tics	Local or remote

Status/TCP-IP-statistics/IP-statistics

These statistics include the following values:

IP-LAN-rx	Number of IP packets received from the LAN
IP-LAN-tx	Number of IP packets sent to the LAN
IP-LAN-checksum-errors	Number of IP packets incorrectly received from the LAN
IP-LAN-service-errors	Number of IP packets received from the LAN for an incorrect service
IP-WAN-rx	Number of IP packets received from the WAN
IP-WAN-tx	Number of IP packets sent to the WAN
IP-WAN-checksum-errors	Number of IP packets incorrectly received from the WAN
IP-WAN-service-errors	Number of IP packets received from the WAN for an incorrect service
IP-WAN-rx-disconnect	Number of packets from the WAN discarded by timeout
Delete-values	Deletes IP statistics

Status/TCP-IP-statistics/ICMP-statistics

These statistics include the following values:

ICMP-LAN-rx	Number of ICMP packets received from the LAN
ICMP-LAN-tx	Number of ICMP packets sent to the LAN
ICMP-LAN-checksum-errors	Number of ICMP packets incorrectly received from the LAN
ICMP-LAN-service-errors	Number of non-supported ICMP packets received from the LAN
ICMP-WAN-rx	Number of ICMP packets received from the WAN
ICMP-WAN-tx	Number of ICMP packets sent to the WAN
ICMP-WAN-checksum-errors	Number of ICMP packets incorrectly received from the WAN
ICMP-WAN-service-errors	Number of non-supported ICMP packets received from the WAN
Delete-values	Deletes ICMP statistics

Status/TCP-IP-statistics/TCP-statistics

These statistics include the following values:

TCP-LAN-rx	Number of TCP packets received from the LAN
TCP-LAN-tx	Number of TCP packets sent to the LAN
TCP-LAN-tx-repeats	Number of TCP packets repeatedly sent to the LAN
TCP-LAN-checksum-errors	Number of TCP packets incorrectly received from the LAN
TCP-LAN-service-errors	Number of TCP packets received from the LAN for an incorrect port
TCP-LAN-connections	Current number of TCP connections from the LAN
TCP-WAN-rx	Number of TCP packets received from the WAN
TCP-WAN-tx	Number of TCP packets sent to the WAN
TCP-WAN-tx-repeats	Number of TCP packets repeatedly sent to the WAN
TCP-WAN-checksum-errors	Number of TCP packets incorrectly received from the WAN
TCP-WAN-service-errors	Number of TCP packets received from the WAN for an incorrect port
TCP-WAN-connections	Current number of TCP connections from the WAN
Delete-values	Deletes TCP statistics

Status/TCP-IP-statistics/TFTP-statistics

These statistics include the following values:

TFTP-LAN-rx	Number of TFTP packets received from the LAN
TFTP-LAN-rx-read-request	Number of TFTP read requests received from the LAN
TFTP-LAN-rx-write-request	Number of TFTP write requests received from the LAN
TFTP-LAN-rx-data	Number of TFTP data packets received from the LAN
TFTP-LAN-rx-ack.	Number of TFTP acknowledges received from the LAN
TFTP-LAN-rx-option-ack.	Number of TFTP option acknowledges received from the LAN
TFTP-LAN-rx-errors	Number of TFTP error packets received from the LAN
TFTP-LAN-rx-bad-packets	Number of unknown TFTP packets received from the LAN
TFTP-LAN-tx	Number of TFTP packets sent to the LAN
TFTP-LAN-tx-data	Number of TFTP data packets sent to the LAN
TFTP-LAN-tx-ack.	Number of TFTP acknowledges sent to the LAN
TFTP-LAN-tx-option-ack.	Number of TFTP option acknowledges sent to the LAN
TFTP-LAN-tx-errors	Number of TFTP error packets sent to the LAN
TFTP-LAN-tx-repeats	Number of TFTP packets repeatedly sent to the LAN
TFTP-LAN-connections	Number of TFTP connections established to the LAN
TFTP-WAN-rx	Number of TFTP packets received from the WAN
TFTP-WAN-rx-read-request	Number of TFTP read requests received from the WAN

TFTP-WAN-rx-write-request	Number of TFTP write requests received from the WAN
TFTP-WAN-rx-data	Number of TFTP data packets received from the WAN
TFTP-WAN-rx-ack.	Number of TFTP acknowledges received from the WAN
TFTP-WAN-rx-option-ack.	Number of TFTP option acknowledges received from the WAN
TFTP-WAN-rx-errors	Number of TFTP error packets received from the WAN
TFTP-WAN-rx-bad-packets	Number of unknown TFTP packets received from the WAN
TFTP-WAN-tx	Number of TFTP packets sent to the WAN
TFTP-WAN-tx-data	Number of TFTP data packets sent to the WAN
TFTP-WAN-tx-ack.	Number of TFTP acknowledges sent to the WAN
TFTP-WAN-tx-option-ack.	Number of TFTP option acknowledges sent to the WAN
TFTP-WAN-tx-errors	Number of TFTP error packets sent to the WAN
TFTP-WAN-tx-repeats	Number of TFTP packets repeatedly sent to the WAN
TFTP-WAN-connections	Number of TFTP connections established to the WAN
Delete-values	Deletes TFTP statistics

Status/TCP-IP-statistics/DHCP-statistics

These statistics include the following values:












DHCP-LAN-rx	Number of DHCP packets received from the LAN
DHCP-LAN-tx	Number of DHCP packets sent to the LAN
DHCP-WAN-rx	Number of DHCP packets received from the LAN
DHCP-discard	Number of DHCP packets discarded
DHCP-rx-discover	Number of discover messages received
DHCP-rx-request	Number of request messages received
DHCP-rx-decline	Number of decline messages received
DHCP-rx-inform	Number of inform messages received
DHCP-rx-release	Number of release messages received
DHCP-tx-offer	Number of offer messages sent
DHCP-tx-ack.	Number of DHCP packets acknowledged
DHCP-tx-nak.	Number of DHCP packets not acknowledged
DCHP-server-err.	Number of DHCP packets received that were not intended for this server
DHCP-assigned	Number of addresses currently assigned
DHCP-MAC-conflicts	Number of assignments rejected because IP addresses were in use
Table-DHCP	Table containing assignments of IP addresses to MAC addresses
Delete-values	Deletes DHCP statistics

Table-DHCP There are entries with DHCP information in the **DHCP table**. It contains 16 entries (or multiples of 16). The table adapts dynamically to the given requirements and grows or shrinks accordingly. It has the following layout:

IP-address	Node-ID	Timeout	Hostname	Type
IP address assigned via DHCP	Associated MAC address	Duration of assignment validity in minutes	Computer name	Assignment type

Status/TCP-IP-statistics/NetBIOS

Additional information about the NetBIOS module can be found in the /Status/TCP-IP-statistics/NetBIOS-statistics menu. This menu has the following structure:

LAN-Rx, WAN-Rx		Number of NetBIOS packets received by the LAN or WAN
LAN-Tx, WAN-Tx		Number of NetBIOS packets sent to the LAN or WAN
Registers		Number of name registrations performed
Conflicts		Number of detected name conflicts. As the NetBIOS module is only a billboard to which each computer attaches its name, it also does not verify the consistency of the data. The counter is thus only incremented if a host determines a conflict and broadcasts a message to the network to this effect.
Releases		Number of name shares performed
Refreshs		Number of name renewals performed
Timeouts		Number of names dropped due to aging
B-Nodes		Number of currently active B nodes (broadcast) in the network
P-Nodes		Number of currently active P nodes (peer-to-peer) in the network
M-Nodes		Number of currently active M nodes (mixed-mode) in the network
W-Nodes		Number of currently active W nodes (hybrid) in the network

B-Nodes Broadcast nodes. A B node performs name negotiations exclusively via broadcasts. Such a computer is not visible over a router connection, since broadcasts may not be routed.












P-Nodes Point-to-point nodes. For name negotiations, a P node requires a NetBIOS nameserver (NBNS) as well as a NetBIOS datagram distribution server (NBDD) to transfer datagrams over a router.

M-Nodes Mixed nodes. This type is a mixture of B and P nodes. It acts as a B node in the local network; if the required partner can't be found in the local network, it attempts to locate it using an NBNS query (P node behavior).

W-Nodes This type of node is not permissible according to RFC, but was introduced nevertheless by Microsoft as a hybrid node.

Status/TCP-IP-statistics/DNS-statistics

The DNS statistics provide supplementary information about the DNS module. This menu has the following structure:

LAN-Rx		Number of DNS packets received by the LAN
LAN-Tx		Number of DNS packets sent on the LAN
WAN-Rx		Number of DNS packets received by the WAN
WAN-Tx		Number of DNS packets sent on the WAN
Forwarded		Number of requests that could not be fulfilled and were thus forwarded
Errors		Number of invalid requests
DNS-access		Indicates the number of names that were looked up from the DNS table
DHCP-access		Indicates the number of names that were looked up from the DHCP table
NetBIOS-access		Indicates the number of names that were looked up from the Net-BIOS tables
Hit-list		This table contains the 16 most popular requests. These may then be prohibited via the filter list if desired.
Delete values		Deletes DNS statistics

The hit list has the following structure:

Domain	Requests	Time	IP-address
www.elsa.com	1	00.00.0000 00:00:29	10.0.0.123






















The individual fields of this list have the following significance:

Domain	Name of the requested computer
Requests	Total number of requests for this name since its appearance in the table
Time	Time of the last request
IP-address	Address of the computer that last requested this name

This list is sorted according to the frequency of requests. When the table is full, the names that have not been requested for the longest period will be deleted to make room for new entries.

Status/IP-router-statistics

This menu groups together the statistics from the IP router module.

/IP-router-statistics	Statistics from the IP router area	
IPr-LAN-rx		Number of data packets to be routed from the LAN
IPr-LAN-tx		Number of data packets routed to the LAN
IPr-LAN-local-routings		Number of packets received from the LAN and routed to the LAN
IPr-LAN-network-errors		Number of LAN packets that were not routed
IPr-LAN-routing-errors		Number of LAN packets that must be sent to another router
IPr-LAN-ttl-errors		Number of LAN packets with an expired time-to-live value
IPr-LAN-filters		Number of LAN packets filtered by the filter table
IPr-LAN-discards		Number of LAN packets discarded
IPr-WAN-rx		Number of data packets to be routed from the WAN
IPr-WAN-tx		Number of data packets routed to the WAN
IPr-WAN-network-errors		Number of WAN packets that were not routed
IPr-WAN-ttl-errors		Number of WAN packets with an expired time-to-live value
IPr-WAN-filters		Number of WAN packets filtered by the filter table
IPr-WAN-discards		Number of WAN packets discarded
IPr-WAN-type-errors		Number of packets from the WAN without an IP router ID
IPr-ARP-errors		Number of unsuccessful accesses to the ARP cache
Delete-values		Deletes IP router statistics
Establish-table		Table of the last 20 packets that required a connection
Protocol-table		Table of routed packets arranged by protocol
RIP-statistics		Statistics from the IP/RIP area
Delete values		Deletes IP-router statistics

Establish-table The **establish table** contains the last 20 entries, which provide information on the system time, destination and source addresses, IP protocol, destination port and source port of the data packets that should have caused a connection to be established.

An IP router establish table might have the following appearance:

Time	Dest.-address	Src.-address	Prot.	D-port	S-port
1T; 16:45:01	192.120.131.40	192.120.130.10	tcp	23	4711
1T; 10:45:10	192.120.131.50	192.120.130.10	udp	53	8123

The 'Time' is displayed as either the device operating time or the system time of the ISDN (if provided by the ISDN terminal). The destination and source addresses are IP addresses. The protocol might refer, for example, to tcp, udp, or the like; the destination and source ports provide a more detailed description of the relevant services (e.g. Telnet via TCP and D-port 23, name server via UDP and D-port 53).

Protocol-table

The protocol table also supplies valuable information on the volume of packets transferred to the LAN or WAN. These values are encrypted as per the various IP protocols, such as ICMP, TCP, UDP.

A protocol table might have the following appearance:

Protocol	LAN-Tx	WAN-Tx
tcp	14	30
udp	15	50
icmp	60	40

Status/IP-router-statistics/RIP-statistics

This option allows you to display the IP-RIP packets received by the device. These substatistics provide you with the following entries:

RIP-rx	Number of IP-RIP packets received
RIP-request	Number of IP-RIP request packets received
RIP-response	Number of IP-RIP response packets received
RIP-discards	Number of IP-RIP packets discarded
RIP-errors	Number of defective IP-RIP packets
RIP-entry-errors	Number of defective entries in IP-RIP packets
RIP-tx	Number of IP-RIP packets sent
Table-IP-RIP	Routing table of routes learned through RIP broadcast
Delete values	Deletes RIP-statistics

Table-RIP












The associated RIP table contains all of the routes learned from the network. The router itself maintains this table; you cannot modify it manually.

An IP-RIP table might have the following appearance:

IP-address	IP-netmask	Time	Distance	Router
223.245.254.0	255.255.255.0	1	1	192.38.9.100
223.245.257.0	255.255.255.0	1	1	192.38.9.200










Status/Config-statistics




















This menu allows you to display the statistics from the remote configuration area. It allows you to retrieve information on the number of past and present configuration sessions at any time. Encryption is performed by LAN, WAN and outband port.

/Config-statistics	Remote configuration statistics	
LAN-active-connections		Current number of active configuration connections from the LAN
LAN-total-connections		Total number of configuration connections from the LAN up until the present
WAN-active-connections		Current number of active configuration connections from the WAN
WAN-total-connections		Total number of configuration connections from the WAN up until the present
Outband-active-connections		Current number of active outband configuration connections
Outband-total-connections		Total number of previous outband configuration connections up until the present
Outband-bitrate		Bit rate of the last outband configuration session
Login-errors		Total number of defective logins
Login-locks		Number of login locks
Login-rejects		Number of login attempts while the login lock was active
Delete-values		Deletes the config statistics

Status/Queue-statistics

These statistics allow you to observe the flow of the individual packets through the various modules of the *ELSA LANCOM*.

/Queue-statistics	Statistics on the queue	
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
WAN-heap-packets		Number of buffers available
WAN-queue-packets		Number of buffers in use
Bridge-internal-queue-packets		Number of bridge packets from the LAN
Bridge-external-queue-packets		Number of bridge packets from the WAN
ARP-query-queue-packets		Number of ARP packets in the query queue
ARP-queue-packets		Number of ARP packets in the normal queue
IP-queue-packets		Number of IP packets in the normal queue

/Queue-statistics		Statistics on the queue
IP-urgent-queue-packets		Number of IP packets in the secured queue
ICMP-queue-packets		Number of ICMP packets
TCP-queue-packets		Number of TCP packets
TFTP-queue-packets		Number of TFTP packets
SNMP-queue-packets		Number of SNMP packets
IPX-queue-packets		Number of IPX packets
RIP-queue-packets		Number of RIP packets
SAP-queue-packets		Number of SAP packets
IPX-watchdog-queue-packets		Number of watchdog-packets
SPX-watchdog-queue-packets		Number of SPX watchdog packets
IPX-router-queue-packets		Number of IPX router packets
Prot-heap-packets		Number of prot heap packets
IPr-queue-packets		Number of packets remaining to be processed by the IP router.
DHCP-server-queue-packets		Number of packets in the receive queue of the DHCP server.
IPR-RIP-queue-packets		Number of packets in the receive queue of the IP-RIP module (for RIP queries, RIP propagations...).
DNS-Tx-queue-packets		Number of packets to be forwarded to DNS or NBNS servers.
DNS-Rx-queue-packets		Number of packets that come from DNS or NBNS servers and are to be forwarded to the host.
IP-Masq.-Tx-queue-packets		Number of packets to be sent masked (to the Internet).
IP-Masq.-Rx-queue-packets		Number of packets received from the Internet and have to be demasked.

Status/Connection-statistics

This menu allows you to display connection times, all charges incurred and other useful information related to ISDN port utilization.

For each available interface, the **Status/Conn.-statistics** menu option provides statistics on the connections established via this interface. The table maintained here has the following layout:

Ifc	Connection	Active	Passive	Errors	Con.-Time	Charge
Ch01	0	0	0	0	No connection	0
Ch02	0	0	0	0	No connection	0

Below is a detailed description of the meaning of each field:

Ifc	Designates the associated channel.
Connection	Indicates the number of connections to the particular channel.
Active	Indicates the number of connections actively established for the channel.
Passive	Indicates the number of connections established for the channel by incoming calls.
Errors	Indicates the number of connection errors.
Con.-Time	Indicates the period of time the current connection has existed. If no connection exists, "No-connection" is output.
Charge	Indicates the amount of charges for the current connection. This value is reset to zero when a new connection is established.

The total charges incurred are not displayed directly. However, the charges are totaled internally in order to permit the management of the charges budget (also see **Setup/Charges-module**).

Status/Info-connection

The menu item **Status/Info-connection** has additional information on the current connection status (logical remote station etc.) for every available interface. The table maintained here has the following layout:

Ifc	Status	Mode	Dialup-remote	Device-name	B1-DT	B2-DT
Ch01	Ready				0	0
Ch02	Ready				0	0

Below is a detailed description of the meaning of each field:

Ifc	Designates the associated channel.
Status	Indicates the status of the particular connection. The possible values are: Init , Setup WAN , Ready , Dial , Incoming call , Protocol , Connection , Callback , Bundle and Reserved . The Bundle status is indicated in the display <i>ELSA LANCOM Business 4100</i> by the addition of a "/2" in columns 15 and 16 of the associated display line. Bundle is displayed for the second interface either when a bundle connection has been activated via the first interface or when a leased-line connection with two B channels has been set. Reserved is displayed for the second interface when a connection exists to the first B channel and the Y connection has been deactivated.
Mode	Reflects the type of establishment. The following are possible: Active (active call establishment = dialing) Passive (passive call establishment = call acceptance) CB (call establishment via callback)

Dialup-remote	Indicates the call number of the remote station from the name list.
Device-name	Indicates the logical name of the remote station (if it can be detected). The device name is also displayed on the appropriate display line as soon as a logical connection is established.
B1-DT	Indicates the short timeout for the connection.
B2-DT	Indicates the short timeout for bundled channels for this connection.

Status/Layer-connection

The menu item **Status/Layer-connection** has information on the B-channel protocol used on the interface for every available interface. The entries in this table correspond to those in the layer list **Setup/WAN-module/Layer-list** in the WAN module. An additional entry exists for the interface itself. The menu has the following layout:

Ifc	WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
Ch01	DEFAULT	ETHER	ELSA	X.75ELSA	compr.	HDLC64K
Ch02	PPPHDLC	TRANS	TRANS	PPP	none	HDLC64K

Status/Call-info-table

This table displays the last ten incoming calls, regardless of whether the router answered these calls.

This allows you, for example, to determine the internal MSN used when the system is operated in connection with a PBX. The table has the following layout:

System-Time	Ifc	CLIP-Caller	Dial-Caller	Capab.	B-chan.
OT; 00:20:57	S ₀	5678	1234	HDLC64K	2
OT; 00:20:46	S ₀	4321	1234	HDLC64K	1
OT; 00:19:47	S ₀	4321	1234	HDLC64K	1
OT; 00:11:33	S ₀	5678	1234	HDLC64K	1
OT; 00:01:13	S ₀	4321	1234	HDLC64K	2
OT; 00:01:02	S ₀	4321	1234	HDLC64K	1
OT; 00:00:06	S ₀	5678	1234	HDLC64K	1

The different entries have the following meaning:

System-time	Time when the call came. Either the device operating time or the system time of the ISDN is displayed (if made available from the ISDN terminal).
Ifc	Designates the associated interface.
CLIP-Caller	Call number (CLIP) of the caller

Dial-Caller	The MSN/EAZ dialed by the caller
Capab.	The service requested by the caller. Possible values are HDLC64K, HDLC56K and unknown. An analog call is displayed as unknown here.
B-chan.	The B channel used. A value of 0 means that all channels have already been seized, i.e. call waiting is activated.

A tip for those using a router in a PBX: Following a call to any ISDN device under the number of the ISDN bus, the MSN/EAZ displayed under 'Dial-Caller' is exactly the entry that must be entered in the router at /SETUP/WAN-MODULE/ROUTER-INTERFACE-LIST/MSN-EAZ in order for a call to be correctly answered from an external station.

Status/Remote-statistics

This table shows the last hundred connections of the *ELSA LANCOMs* with information on the remote station.

The table has the following layout:

Conn.-start	Remote-ID	Mode	Ifc	Conn.-time	Charge
OT; 00:20:57	LONDON	Active	Ch01	50	5
OT; 00:20:46	MANCHESTER	Passive	Ch02	230	10



The different entries have the following meaning:

Conn.-start	Time at which the connection was established. Either the device operating time or the system time of the ISDN is displayed (if made available from the ISDN terminal).
Remote-ID	Logical remote station name
Mode	Type of connection establishment: Active – the connection was actively established by the device Pas. – The device received a call CB – The device called the remote station back
Ifc	Interface, over which the connection is made (Ch01, Ch02).
Conn.-time	Duration of the connection in seconds
Charge	Charges for this connection in units

A connection remains in the table for at least as long as it is established. Every new connection fills the table from top to bottom. If an existing connection is the lowest entry in the table, an already released connection will be deleted from the table instead if necessary.

Status/S₀-bus

This option allows you to display the current status of the S₀ interface. The statistics have the following layout:

/S ₀ -bus		Running status displays
D-info		Overview of the D channel status
D2-statistics		Breakdown of the Layer-2 information of the D channel for the B channels.

D-info

This table shows general information related to the D channel:

Channel	B-channel identification.
Protocol	D-channel protocol. Either the protocol fixed in the interface table or the protocol detected in the 'Auto' settings at the ISDN terminal.
Layer-2	Activation of layer 2 of the D channel ('Yes' or 'No')
TEI	TEI assigned ('Yes' or 'No')
S ₀ -activation	Displays activation status ('Yes' or 'No')

D2-statistics

This table shows layer 2 information for the individual B channels:

Channel	B-channel identification.
TEI	T erminal E quipment I dentifier assigned by the switching center.
L2-activation	Activation of layer 2 of the D channel ('Yes' or 'No').
Connections	Number of connections made over the displayed TEI.

Status/Channel-statistics

This table shows information on the current status of the two B channels. The information from this table is primarily used for output via *ELSA LANmonitor*. Therefore, some values are shown simply as bits with no further explanation.

The table has the following layout:

Channel	State	App	Mode	Cause	Dialup-remote	Sub-address	Charge	Conn.-time	Extra	ISDN-display
S ₀ -1-ERR	00000000	Router	active	0000	0241123456	00000000	3	0		
S ₀ -1-B1	00000000	a/b	active	0000	0241123457	00000000	2	20		
S ₀ -1-B2	00000000	LAN-CAPI	passive	0000	0241123458	00000000	4	180		





Below is a detailed description of the meaning of each field:

Channel	Channel for the entry is valid. Only the latest status of a channel is ever displayed. A dedicated "channel" is maintained for error messages on channels.
State	The status of a channel is shown here as, e.g., 'ready'.
App	Application that occupies the channel: Router, <i>LANCAPI</i>
Mode	Types of last connection establishment: active or passive
Cause	Last error
Dialup-remote	Remote station call number: with active establishment the number dialed, with incoming calls the number sent.
Subaddress	Addition to application that, e.g., indicates the logical channel for the router for the <i>LANCAPI</i> , e.g., the IP address of the client that is using the CAPI.
Charge	Number of charging units incurred for this connection.
Conn.-time	Duration of the last connection on this channel
Extra	Additional information on the connection, e.g. the name of the remote station for router connections.
ISDN-display	Information from the switching center, e.g. error messages, if connected to the PBX possibly also the caller's name, etc.

Status/Time-statistics

This menu has information on the current time in the device and on the path over which the *ELSA LANCOM Office* has obtained the time.

The menu has the following layout:

/Time statistics		Time module statistics
Current-time		Current device time.
Source		Time output source. The possible values are: 'ISDN' for time taken from the ISDN, 'Manual' for the manual setting of the time with the 'time' command, 'RAM' for time imported from the device RAM after booting.
Setup		Number of time imports from one of the above sources.
ISDN		Additional information on time import from the ISDN

Status/Time-statistics/ISDN







These statistics include the following values:

Connection	Number of attempts to read time information from the ISDN
Information	Number of time updates received from the ISDN
Info-error	Number of erroneous time updates received from the ISDN
Units	
Delete values	Deletes ISDN statistics

Status/LCR-statistics

This menu has information on the current time in the device and on the path over which the *ELSA LANCOM Office* has obtained the time.

The menu has the following layout:

/LCR-statistics		Least-cost router statistics
Total calls		Total number of LCR calls
Found-events		Number of calls in which the router found a suitable rule in its tables and successfully rerouted the connection.
Not-found-errors		Number of calls in which the router did not find a suitable rule in its tables and thus could not reroute the connection.
Missing time-errors		Number of calls in which the LCR could not become active due to lack of time
Provider-statistics		A table with all providers used (or their prefixes), the number of successful and unsuccessful calls
Delete values		Deletes LCR statistics









Status/Delete-values








With the exception of the tables, this option allows you to delete all the values in the substatistics. To do so, enter the following command:

```
do delete-values
```

Setup

This menu allows you to query and modify all the system parameters that are necessary to the functioning of the devices.

/Setup		System configuration
Name		Entering the device name
WAN-module		WAN settings
Charges-module		Charge management settings
LAN-module		LAN settings
IPX-module		IPX module (IPX router) settings
TCP-IP-module		TCP/IP module settings
IP-router-module		IP router module settings
SNMP-module		Settings for configuration via SNMP

/Setup		System configuration
DHCP-module		DHCP server settings
NetBIOS-module		Settings for the NetBIOS proxy
Config-module		Configuration module settings
LANCAPI-module		<i>ELSA LANCAP</i> i settings
LCR-module		Least-cost router settings
DNS module		DNS server settings
Time-module		Time module settings

Name

Here you can enter the device name (maximum 16 characters). The set of characters available includes uppercase and lowercase letters as well as some special characters. You can display the full range of available characters during a configuration session by entering the following command:

```
set \setup\name ?
```

In the default configuration, no name is entered.







The device name is required for identification purposes; it is a prerequisite for any connection via the IPX or IP router module, since the routers can exchange data only with known remote stations, and is also required for the unambiguous identification of a remote bridge station.







In the case of PPP connections, either the user name with the password from the PPP list or the device name is transferred to the remote station as a device ID during a verification by PAP or CHAP.

In addition, the device names you assign must be unique. For example, you might match the device names to the location (e.g. Glasgow, London, Provider, etc.).

Setup/WAN-module

This menu groups together all the settings necessary for starting up the WAN interface and controlling connections to logical remote stations.

/WAN-module		WAN settings
Interface-list		S ₀ interface settings
Router-interface-list		Router module settings
Channel-list		Settings for the use of the available channels
Name-list		Remote station settings
RoundRobin-list		Settings for different remote station numbers
Layer-list		Settings for the layer combinations used

/WAN-module		WAN settings
PPP-list		Parameter settings for PPP connections
Number-list		Settings for call numbers with access authorization
Script-list		Dial script settings
Manual-dialing		Settings for manual connection control
Protect		Protection for answering incoming calls
CB-attempts		Number of callback attempts when the remote station is busy
Backup-delay-seconds		

Interface-list

This table contains the interface settings, which apply to all operating modes (modules) of the devices.

Ifc	Protocol	LL-B-chan.	Dial-prefix
S0	Auto	1	0

Additional, special interface settings are also available for the various modules, e.g. the call numbers to which a module should react, see also

`Setup/WAN-module/Router-interface-list`

`setup/lancapi-module`

Below is a detailed description of the meaning of each field:

Ifc	Designates the associated interface.
Protocol	D-channel protocol setting. The possible values are: Auto : automatic detection of the D-channel protocol DSS1 : Euro-ISDN 1TR6 : National ISDN GRP0 : Leased-line connection group 0 P2P-DSS1 : Point-to-point connection
LL-B-chan.	B-channel settings for a leased-line connection. The possible values are: none : Leased-line connection not assigned to a specific channel. 1 or 2 : Leased-line connection operates over the assigned B channel. Please refer to the information on setting these parameters in the fixed connection description.
Dial-prefix	Global dialing prefix for all modules of the devices. The digits entered here (maximum 8) are automatically prefixed to the selected call number in every call. Use this prefix when, for example, the router is connected to a PBX.

*Router-
interface-list*

This table contains the interface settings that apply to the router modules of the *ELSA LANCOM*.

Ifc	MSN/EAZ	YC.	CLIP
S0	123456	Off	On

Below is a detailed description of the meaning of each field:

Ifc	Designates the associated interface.
MSN-EAZ	<p>If your device is connected to an ISDN port with 1TR6, enter the EAZ to which the interface is to respond.</p> <p>If your device is connected to an ISDN port with DSS1, enter the MSN to which the interface is to respond. If you wish the interface to respond to several different MSNs, enter them here separated by semicolons. A '#' in the list enables any number of incoming MSNs.</p> <p>For outgoing calls, the first MSN in this list will be reported to the remote station. If no MSN is entered, the switching center sends the main MSN of the terminal.</p>
YC.	<p>This entry can be used to control the interface's ability to establish Y connections. Possible settings are:</p> <p>On: Y connection is supported; a number of connections can be established simultaneously (default). A channel bundling connection is broken off when a second connection to another remote station has to be established.</p> <p>Refer also to the settings for the availability of the <i>LANCAP</i>.</p> <p>Off: Y connection not supported; only one connection can be established. The second connection is blocked. If a connection to an additional remote station is to be established, this establishment is rejected. A channel bundling connection is not affected.</p>
CLIP	<p>Calling Line Identification Protocol: Suppresses the outgoing MSNs.</p> <p>Possible values:</p> <p>Yes: Activate CLIR, do not send MSN.</p> <p>No: Deactivate CLIR, send MSN to remote station.</p> <p>Please note: The "selective suppression of call number transmission" may be a service feature that will have to be obtained from the telephone company.</p>

Channel list

The channel list specifies the number and sequence of the channels to be established.

Device-name	Min	Mx	Order	Backup
LONDON	2	2	1-1;1-2	1
INTERNET	2	2	1-1;1-2;2-1;2-2	0
DEFAULT	1	2	0	

Below is a detailed description of the meaning of each field:

Device-name	Name of the remote station that is also used in the name and PPP lists.
Min	Number of static channels. These channels are used during every call establishment to the remote station.

Mx	The maximum number of channels to be used for this remote station. The Max-Min difference is the number of dynamic channels.
Order	This defines which channels are to be established on which S ₀ bus. Syntax: [<BusNo>-<ChannelNo>];<BusNo>-<ChannelNo>]... Possible values: 1 to 4 for the busses, 1 or 2 for the channel. If no entry has been made, a random channel on a random bus will be used. If one or more leased lines are to be used, an entry must be available for each leased line.
Backup	Number of possible backup connections. These connections will be established in the event that all valid leased-line channels are down. Backup connections always use a random channel on a random bus.

Name-list

The names entered in the name list are needed by the router to determine the correct remote station and corresponding layer name. The name list is also used for the callback function.

The name list can contain 64 different device names and might, for example, have the following appearance:

Device-name	Dialup-remote	B1-DT	B2-DT	WAN-layer	Callback
GLASGOW	875463	180	0	PPPHDL	On
LONDON	040785647	20	20	DEFAULT	Off

Below is a detailed description of the meaning of each field:

Device-name	In the Device Name column, you can enter an original remote station name, which you must then assign to the relevant remote station via the Name option in the Setup menu.
Dialup-remote	In this column, you can store the number to be called and, if applicable, supplement it with special dialing characters (see above, default: None).
B1-DT	In this column, you can define appropriate connection time-outs (in seconds) for the first B channel. If no data is being transmitted when this time expires, the connection on this channel is released (default: 20). If charging information is transmitted over the ISDN network during the connection, the <i>ELSA LANCOM</i> will make full use of every charging unit and will only terminate the connection just before the beginning of the next unit. This function is also referred to as dynamic short-hold.
B2-DT	In this column, you can define appropriate connection time-outs for the second B channel (same as B1-DT, default: 20). The B2 hold time controls the bundling behavior during a channel bundling. Values of 0 or 9999 identify static bundling, values between them dynamic bundling.
WAN-layer	In this column, a name is stored that must also be entered in the layer list. This establishes the transfer protocol required for this connection.
Callback	In this column, you can define whether a callback is to be made for the relevant remote station (Off/Name/Auto/Looser/ELSA; default: Off).

■ Callback options

Off	No callback is made.
Looser	The router stops attempting to establish a connection when there is a call from this remote station (reciprocal call establishment). This setting must be used when a callback from the remote station is expected.
Auto (not applicable to Windows 9x or Windows NT)	The connection will be rejected and a direct callback will be initiated if the remote station is specified in the number list. This means that the caller is not charged. If the remote station is not specified in the number list, a callback will be negotiated in a protocol negotiation (ELSA or PPP). A charge of one unit is incurred for this.
Name	This setting forces a protocol negotiation. This enables call number protection to be set in the number list and also a callback to be started using the protocol negotiation. A charge of one unit is incurred for this.
ELSA	This setting enables a particularly fast callback procedure. The called-back remote station must use the 'looser' setting.

- The special dialing characters in the table below can be entered along with the call number in the name list, round robin list, or logical dial prefix. They control the line access, the use of a semipermanent leased-line connection or determine the interface to be used for the connection:

#	Trunk seizure (only with some PBXs).
F	The remote station can be reached via the leased-line connection only. Syntax: F[channel:][subscriber number] The channel and subscriber number are both optional. In the case of several leased lines, the channel specifies the B channel to be used. Depending on the setting in the channel list, the subscriber number indicates whether a dynamic channel bundling or backup line is to be realized over the dial-up connection.

When **S** or **S2** is appended to the call number, the semipermanent connection (SPV) is activated for the D-channel protocol 1TR6.

You must subscribe to an SPV through your telephone company for a fixed payment.

*If you forget to append an **S** or **S2**, the SPV will behave like a standard dial-up line and your charges will be unnecessarily high. The telecommunications provider then charges you the fixed charges and the dial-up line charges incurred during the time the line was used.*

RoundRobin-list The round-robin list enables a remote station to be reached with several call numbers. It has the following layout:

Device-name	RoundRobin	Head
GLASGOW	4321-5555-6666	Last

Below is a detailed description of the meaning of each field:

Device-name	In the device name column, you can enter a remote device name from the name list. If one line in the Round Robin list is insufficient for all desired call numbers, the line can be extended as shown below: The # character and a unique index are added to the device name (e.g. GLAS-GOW#1) and it is entered on the next line.
Round-Robin	The DDI numbers of all possible remote stations are entered here under their corresponding device names. The individual DDI numbers must be separated by hyphens.
Head	In the Head column, the following entries are possible: Last: The next connection to be established will begin with the DDI that was successfully used for establishing the last connection (default). First: The next connection to be established will always begin with the first DDI. For a logical remote station, this field can be modified only by means of its first entry in the table. The field is automatically updated when other entries are made for this remote station.

Layer-list

In the layer list, you can freely define the different B-channel protocols by combining various ISDN layers. This enables compatibility to devices from other manufacturers that use different B-channel protocols to be set.

The following table below is provided as an example and also shows the default settings for an *ELSA LANCOM Office*:

WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	TRANS	PPP	TRANS	bnd+cmpr	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	none	HDLC64K
MLPPP	TRANS	PPP	TRANS	bnd+cmpr	HDLC64K
RAWHDL	TRANS	TRANS	TRANS	none	HDLC64K

Below is a detailed description of the meaning of each field:

WAN-layer	In this column, you can enter an original name designating the layer combination that you use. These names can then be used in the name list 'layer name' column depending on their spelling to set the protocol. If an entry with the name DEFAULT is defined in this column, the settings stored there are always used when no layer name can be assigned (e.g. a caller does not transmit his or her call number). This entry is also used when a group 0 leased-line connection is established. If the DEFAULT entry is not present, a B channel protocol developed by ELSA is used as the default. The user may delete or change any of the layers predefined here.				
Encaps.	Additional information regarding the data to be transmitted may be specified in the Encaps column. The following entries are possible:				
	ETHER	The data is provided with an Ethernet header. This setting is required for communication with older <i>ELSA LANCOM</i> devices.			
	TRANS	No Ethernet header is sent in this setting. Only "pure" IP data packets are transferred, for example. This setting provides the greatest possible effective data throughput.			

Lay-3	In the lay-3 column, you can define additional headers for data transmission in ISDN. You can select from among the following settings:	
	TRANS	No additional header is inserted (higher data throughput). Always select this setting if the remote station sends the data transparently via ISDN layer 3 (e.g. transparent HDLC, transparent X.75LAPB).
	PPP	A negotiation is performed according to the point-to-point protocol.
	APPP	A negotiation is performed as per the asynchronous PPP. APPP is then used when synchronous PPP is not possible because the connection does not permit a synchronous transmission (e.g. for analog modem operation).
	SCPPP	Following completion of script processing, a synchronous PPP negotiation is initiated.
	SCAPPP	Following completion of script processing, an asynchronous APPP negotiation is initiated.
	SCTTRANS	Following completion of script processing, a connection exists to the remote station. No further protocol negotiation is performed.
Lay-2	In this column, you can select the protocol for ISDN layer 2:	
	TRANS	The data is packed directly in HDLC packets. Always select this setting if communication is to take place via transparent HDLC.
	X.75LAPB	The data is exchanged in X.75 secured format. Always select this setting if the remote station is to work with X.75 data protection.
L2-Opt.	The L2-opt. enables the setting of an option for the data transfer setting under Lay-2 with an additional <i>ELSA LANCOM</i> .	
	none	No data compression or channel bundling is performed.
	compr.	Stac data compression will be used. Compression as per Stac (Hi/fn) must be used in connection with PPP or multilink PPP. Stac compression may also be used in connection with Windows remote stations.
	bundle	Channel bundling is performed via several B channels. Channel bundling is only possible for the Lay-2 settings of 'PPP'.
	bnd+cmpr	Channel bundling and data compression takes place over two B channels.
Lay-1	The lay-1 column allows you to define the speed at which the data is sent in ISDN.	
	HDLC64K	The data is transmitted at 64,000 bps.
	HDLC56K	The data is transmitted at 56,000 bps. This setting is especially important for connections in the USA.
	V110_9K6	Data is transferred at 9,600 bps in a V.110 connection, when connecting to GSM mobile phones, for example.
	V110_19K2	Data is transferred at 19,200 bps in a V.110 connection.
	V110_38K4	Data is transferred at 38,400 bps in a V.110 connection.

To link to devices from other manufacturers, please check with that manufacturer for the data format used (PPP is almost universally supported).

For Internet and remote access, PPP is generally specified.

PPP-list

The router needs the device names contained in the PPP list in order to determine the security procedure settings suitable for the connection and to determine the PPP parameters. It contains a maximum of 64 entries and is structured as follows:

Device-name	Auth.	Key	Time	Try	Conf	Fail	Term	Username	Rights
GLASGOW	CHAP	*****	0	5	10	5	2	ELSA	IP

Not all parameters can be reached via the telnet configuration. Use *ELSA LANconfig* so far as possible.

Below is a detailed description of the meaning of each field:

Device-name	In the Device-name column, you can enter the name with which the remote station logs onto the router. In the case of connections via the data transmission network, this is the name entered as "Username". For remote access via the data transmission network, the 'Username' field (see below) is not evaluated! Entries are not case-sensitive!	
Auth.	In this column, you can enter the security procedure to be used for verification of the remote station. Default: PAP	
	None	The router does not negotiate authentication with the remote station when establishing a connection. However, the remote station can itself require authentication from the router. This is the case when dialing up a connection to an ISP, for example.
	PAP	The remote station is checked as per the Password Authentication Protocol.
	CHAP	The remote station is checked as per the Challenge Handshake Authentication Protocol.
Key	A password may be entered in this column. Its presence is indicated by the symbol * and it is used to check the remote station. It may consist of 95 characters (7-bit ASCII, including spaces). Default: None. The <code>set ?</code> command shows a list of the allowable characters.	
Time	In this column, you can enter the period of time between two remote station verifications specified in minutes. The CHAP protocol must be set here. Default: 0	
Try	In this column, you can specify the number of times the verification attempt is to be repeated. If verification fails, the connection is immediately terminated. Default: 5	
Conf, Fail and Term	These parameters may be used to influence the operation of the PPP. They are defined and described in RFC 1661. The default values are sufficient for most remote stations. If nothing is entered here, the values 0,0,0 appear in the display but the default values 10, 5, 2 are still used. These parameters can only be changed via SNMP or TFTP (using the <i>ELSA LANconfig</i> configuration program)!	
Username	The user name (max. 64 characters) transmitted to the remote station during PPP negotiation. The router identifies itself to the remote station with it. If no user name is entered, the device name serves as the user name. Entries are case-sensitive here.	
Rights	Network protocols to be routed over this connection: IP, IPX, NTB (NetBIOS). NetBIOS always requires one of the other two protocols. The routing of IP or NetBIOS via PPP always requires a suitable route (in the IP routing table for IP or in the remote-station table for NetBIOS).	

Number-list

Under this option, a number list is managed in which you can enter 64 different call numbers with their associated device names. This list can be used to assign the call numbers (CLI) transferred by remote stations to the remote station names.

The entries in the number list for the two calling devices GLASGOW and LONDON might appear as in the table below, thus permitting the name to be derived from the call number supplied and, if applicable, permitting a callback to be initiated via the name list:

Dialup-remote	Device-name
875463	GLASGOW
040785647	LONDON

This number list is required for passive connection establishment. The remote station call numbers must be entered without leading zeros.

The D-channel protocol that is currently activated is then used for a call number test.

If the 'Protect number' setting is selected and a call is received from a remote station, the remote station call number sent is compared to the entries in the number list. If the station number sent is identical to an entry in the list, the caller is authorized and the connection is established.

If the 'Protect no./name' setting is selected and a call is received from a remote station, the remote station call number sent is compared to the entries in the number list. If the call number sent is identical to an entry in the list, the caller is authorized to establish the connection. In addition, it is possible to derive the name of the remote station from the number list and, therefore, the layer that is to be used for this connection. The connection is then established using this layer and name verification is initiated using the layer detected (or using the default layer if no layer is detected).

If the name of the remote station (and thus the layer to be used) cannot be determined using the number list, the call will be accepted using the default layer and the name list will be checked for a suitable entry after the protocol (PPP) negotiation.

Script-list

Some Internet providers (e.g. CompuServe) conduct a script-controlled log-on procedure before a PPP negotiation. In order to be able to establish this type of connection as well, a simple script processing procedure is also implemented in the *ELSA LANCOM* (see 'Script processing').

In this table, the scripts are defined and assigned to the remote stations. The table has the following layout:




Device-name	Script
CSEVERE	<>[Host]<CIS>[User]\$U[Password]\$P[PPP]\$C

The entries in the script list have the following meaning:

- Device name: Name of the logical remote station
- Script: All commands to be executed—a maximum of 58 characters per line is available. If the required command sequence is longer, an additional entry for the logical remote station may be added as in the round-robin list. The syntax for this is: Device name followed by '#' and a number. The entries are processed from top to bottom.

Setup/WAN-module/Manual-dialing

This option can be used for manual connection control for testing purposes.

/Manual-dialing		Settings for manual connection control
Connect		Establishes a connection.
Disconnect		Termination of connections
State		Displays the current connection status.

Connect

Parameter: Remote station's device name (via remote configuration only).

You can use the command

Do /Setup/WAN-module/Manual-dialing/Connect to remote station

to initiate the manual establishment of a connection via remote configuration. The remote station's device name specified as a parameter must also be entered in the name list with a call number.

When the function is activated by the keyboard of the *ELSA LANCOM*, the error message 'No remote station' is displayed, because a name cannot be entered here. Therefore, this function must not be used from the keyboard of the *ELSA LANCOM*. If you attempt to establish a connection to a logical remote station for which no call number is specified in the name list, the 'No number' error message is displayed.

Disconnect

This command allows you to release an existing connection. If a connection is released manually, the name of a remote station may also be entered in the remote configuration. In this case, only the connection to the remote station specified is released. If a connection to the remote station specified does not exist, there is no further response. However, if a remote station name is not entered, all existing connections will be released.

Setup/WAN-module/protection

This option allows you to select the conditions under which incoming calls are to be answered at the transmission module.

- If 'Protect' is set to 'none', all pending calls are answered provided that the remote end supports the connection protocol.

- If this option is set to 'name', calls are accepted only from remote stations for which an entry is found in the name list. This verification provides additional protection. This verification is only available when using PPP.
- If this option is set to 'number', calls are accepted only from remote stations that are entered in the number list as authorized remote stations.
- The 'no./name' setting allows you to select combined protection using a name list and number list. First a verification that there is an entry in the number list is made. If this is not possible, the router will attempt to determine the name using the protocol negotiation.

Setup/WAN-module/CB-attempts




This option allows you to set the number of times (from 1 to 9) a callback is to be attempted when the remote station is busy. For international connections, you should enter a value from 3 to 5 in order to optimize the callback functionality. The default setting is 3.

Setup/WAN-module/Backup-delay-seconds

The backup start time indicates the number of seconds to elapse before the first backup attempt is started after determining that the leased line is down. If the value 0 is entered, no backup connection will be established actively.

Setup/LAN-module

This menu allows you to select the settings needed for the local network. The menu has the following layout:

/LAN-module	LAN settings	
Connector		Selection of the network connection
Node-ID		MAC layer address of the device
Spare-heap		Buffers that receive data packets from the local network

Connector

This option allows you to select from among the following network connections:

Connect	Meaning
Auto	Default setting; enables the Autosense function of the network chip. This automatically sets the router to the port in use without requiring manual configuration of this item.
10BTX	10BASE-T in half-duplex mode
FD10BTX	10BASE-T in full-duplex mode
100BTX	100BASE-T in half-duplex mode
FD100BTX	100BASE-T in full-duplex mode

When making settings for the fast-Ethernet operation, please note that the selected transfer mode must also support the additional terminals.







When the system is switched off and on again, the last port to be selected remains activated.

Node-ID This option allows you to display the router's own Ethernet address. The value displayed here was set at the factory and cannot be changed. The Ethernet address is displayed as a 12-digit hexadecimal value, with the first six digits '00a057' standing for an ELSA device.

Spare-heap The spare heap blocks for the local network affect the number of buffers that are always available for receiving frames from the local network. The default value is 10, which ensures that, e.g., four Telnet sessions can be activated via the local network at any time.

Setup/IPX-module

This menu allows you to enter settings for the IPX module, particularly for the IPX router. The menu has the following layout:

/IPX-module	IPX module (IPX router) settings	
Operating		Activates or deactivates the IPX module.
IPX-router		Activates or deactivates the IPX router.
LAN-config		Settings for the LAN side
WAN-config		Settings for the WAN side
RIP-config		RIP settings
SAP-config		SAP settings

Operating This option allows you to activate or deactivate the IPX module. In the default configuration, the IPX module is activated.










Remote configuration via DOS/IPX and the IPX router can be used only if the IPX module is activated. For local configuration via a LAN, the router does not have to be activated.

IPX-router This option allows you to activate or deactivate the IPX router. In the default configuration, the IPX router is deactivated.

When the IPX router is activated, the IPX module is also activated. The IPX router can be activated only if different, permissible network addresses are entered under LAN-configuration and WAN-configuration.

Setup/IPX-module/LAN-configuration

Settings for the LAN data packets may be made here. The menu has the following layout:

/LAN-configuration		Settings for the LAN side
Network		Logical IPX network number of the LAN port
Binding		Ethernet frame type setting for the LAN port
IPX-watch		Settings for IPX watchdog management
SPX-watch		Settings for SPX watchdog management
NetBIOS-watch		Settings for NetBIOS watchdog management
Socket-filter		Filter table for destination socket filtering
Loc.-routing		Activates or deactivates local routing.
RIP-SAP-scal.		Activates or deactivates RIP-SAP scaling.
LOOP-prop.		Activates or deactivates propagation of redundant routes.

Network

The NetWare network number of the network (8-digits, hexadecimal) that is connected to the LAN port under the binding (see below) may be entered here. If there is a NetWare server in the local network, the router can automatically detect the network number and the binding.

The default value is '00000000' and means that the router should automatically detect the network number.

Binding

This option allows you to select the Ethernet packet format (Auto, II, 802.3, 802.2, SNAP) for the LAN port. This format must match the Ethernet format used in the local network under the above-mentioned network number.

The default is 'auto' and means that the router should automatically detect the binding (only if there is a NetWare server in the local network).

IPX-watch

This option allows you to define the type of management used for IPX watchdog packets.

- **Filt.** means that the IPX watchdog packets are neither answered nor transferred locally. Users are always logged off after the period of time set in the NetWare server.
- **Route** causes the watchdog packets to be transferred and, consequently, also causes a regular establishment of connections by means of the server's watchdog packets.
- **Spoof** (default) ensures that IPX watchdog packets are answered locally by the router and therefore that users are no longer automatically logged off. This setting is especially economical but steps must be taken in the server to ensure that users are logged off at specific times in order to prevent the usage of too many user licenses.

- SPX-watch* This option allows you to define the type of management used for SPX watchdog packets.
- **Route** causes the SPX watchdog packets to be transferred and, consequently, also causes a regular establishment of connections by means of the server's SPX watchdog packets.
 - **Spoof** (default) causes SPX watchdog packets to be answered locally. This setting is especially economical.

NetBIOS-watch This item specifies how NetBIOS watchdog packets should be treated. NetBIOS watchdog packets occur, e.g., if Windows networks are connected by IPX. The same options are available as with IPX or SPX watchdog packets (filter, route, spoof).

Socket-filter The socket filter table permits the selective filtering of LAN packets to specific ranges of destination sockets. Filtering is performed for both single IPX packets and propagated IPX packets. The following sockets (which are periodically sent in the network and, therefore, would result in connections being established too frequently) are already entered in the LAN filter table as default values (for details, also see FAQs on the 'IPX router').

Start-socket	End-socket
0455	0457
0550	0555
1401	1402
1480	1481
83ba	83ba
900F	9010

Loc.-routing This setting supports the scaling of multiple routers in a local network. When all the channels for one router are already seized and packets for other remote stations are still being received at this router, other routers in the LAN may still have free channels.

If the 'Loc.-routing' option is activated, the router forwards the packets in the local network to a router that has propagated a route to the remote station desired. The router has saved this route, although it is less efficient than its own, and marked it with the 'reserve' flag in the RIP table.

The default setting for this option is 'Off' since an IPX client sends a RIP request for the relevant route after a timeout, thus automatically finding a different router through which it can access the destination network.

RIP-SAP-scal. Another option for supporting scaling is to propagate every route to which there is an active connection with a somewhat better tic count than the actual one. This will ensure that all clients will send their packets for these routes to the router that has the connection. In addition, in the event that all channels are busy, the routes that are no longer available will be propagated as 'DOWN'. Because one or more broadcasts are

sent on the LAN by this procedure every time a connection is established and released (which may require other routers for additional broadcasts and may result in a high network load), this feature can be activated and deactivated. The default setting is 'Off'.



LOOP-prop.

Redundant routes, i.e. routes with the same tic and hop count, are only sent to the remote station by which they were not received (split horizon). When the 'LOOP-prop.' function is activated, these routes can still be propagated. Redundant routes are identified in the RIP table by means of the LOOP flag.

Although the propagation of redundant routes is not prohibited by the Novell specification, it should still be avoided as much as possible. Therefore, the default setting is 'Off'.

Setup/IPX-module/WAN-configuration

This option allows you to maintain the data packet settings for the WAN port. The menu has the following layout:

/WAN-configuration		Settings for the WAN side
Routing-table		Routing table for IPX network and remote station assignment
Socket-filter		Filter table for destination socket filtering

Routing-table

The routing table can hold up to 16 remote stations and destination networks. It contains the following entries:

Remote-ID	Network	Binding	Propagate	Backoff
Name of the IPX remote station	Network address	802.3, II, 802.2, SNAP	Route / Filter	On / Off

The columns have the following meanings:

- **Remote-ID:** Name of the logical remote station (as specified in /Setup/WAN-module/Name-list).
- **Network:** Address of the network on the WAN side. A standalone network must be used, but it must be same for both of the participating routers!
- **Binding:** The Ethernet binding to be used on the ISDN route. This setting is taken into account only if Ethernet encapsulation is set in the layer used. If no binding is specified, a value of 802.3 is assumed.
- **Propagate:** This entry indicates how IPX type-20 packets (NetBIOS propagated frames) are to be handled. The possible settings are Route and Filter. With **Filter**, no propagated frames are routed to the remote station. If the entry has the value **Route**, the packets are forwarded to all currently available remote stations, i.e., there must be a connection to the remote station, or there must be at least one channel available for establishing a connection the remote station.

If no connection or channel is available, the packet is discarded. As a result, the maximum number of remote stations that can receive propagated frames corresponds to the number of possible simultaneous connections. The default setting is 'Filter'.

- **Backoff:** The IPX router uses a special algorithm (exponential backoff) to keep the connection charges as low as possible in the event of erroneous configurations (see below).

If there is no server in the remote network (e.g. with remote access from a workstation), the router cannot detect this and the corresponding remote station will be deactivated after a day at the latest. In order to prevent this from happening, the exponential backoff algorithm can be deactivated for these remote stations.

The default setting is 'On'.

Socket-filter

The socket filter table permits the selective filtering of WAN packets to specific ranges of destination sockets. Filtering is performed for both single IPX packets and propagated IPX packets.

Setup/IPX-module/RIP-configuration

This option allows you to store settings for RIP data packets (router information). The menu has the following layout:








/RIP-configuration		RIP settings
Table-RIP		Displays the RIP table.
LAN-filter-table		Filter ranges for IPX network addresses (LAN)
WAN-filter-table		Filter ranges for IPX network addresses (WAN)
Routes/Frm		Max. no. of RIP entries per RIP frame sent
Aging-minute(s)		Aging period in update units
Spoofing		Sets RIP spoofing procedure
WAN-update-min.		RIP update period; effectiveness depends on spoofing

Table-RIP

This option allows you to display the entries in the current RIP table. The table contains a maximum of 256 entries.

The entries in the RIP table might, for example, look like the entries shown below with the networks 00000001, 00000002, 00000010, 00000081, where these networks can be accessed via different routers. The flags can be used to determine where these networks are located with relation to the particular router (**local** or **remote**). The entry **direct** indicates whether this network is directly the local or remote network. **DOWN** indicates

a network that is known but is not currently available. The table is sorted by the network numbers.

Network	Hops	Tics	Node-ID	Time	Flags
00000001	0	1	00a05702000a	0	local, direct
00000002	1	2	00608c70ab56	1	local
00000010	2	7	00A057020014	1	local, DOWN
00000081	1	6	00a05702000b	0	remote, direct

LAN-filter-table The LAN filter table permits the selective filtering of routes that are 'learned' via the local network. Filtered routes do not appear in the IPX-RIP table.

A LAN filter table for filtering routes in the range from 00001000 to 00001fff might, for example, have the following appearance:

Start-net	End-net
00001000	00001fff

WAN-filter-table The WAN filter table permits the selective filtering of routes that are 'learned' via the wide-area network. Filtered routes do not appear in the IPX-RIP table.

A WAN filter table for filtering routes in the range from 00002000 to 00002fff might, for example, have the following appearance:

Start-net	End-net
00002000	00002fff

Routes/FRM This parameter sets the maximum number of routes that can be included in a RIP frame. The specified value originally defined by Novell is 50. Today, however, it is common practice to pack a higher number of routes in each frame in order to reduce network utilization. If all participating devices in the network support a higher number, this value can be raised as high as 182.

Aging-minute(s) This option allows you to set the number of times the RIP table will be updated until an entry in the RIP table ages, i.e. until the route recorded there is marked as 'not reachable (down)'. You can enter a value from 1 to 60; the default value is 3.

Spoofing

This option allows you to determine how the router will handle RIP packets.

- If you select **Off**, RIP packets are handled in the WAN in precisely the same manner as in local networks. RIP data are sent to the remote side in the event of new information and at intervals of one minute, i.e. a connection is established.
- With the **Trig** setting, the RIP data is sent to the remote end any time changes are detected.
- With the **Time** setting, the RIP data is sent to the remote end at selectable intervals (see below).
- **pBack** (default) is the most economical setting. In this case, the RIP data is sent to the remote end only when a connection is activated.

*When spoofing is set to **pBack**, entries in the RIP table age only when a new connection is established and an entry has been explicitly marked as 'not reachable'.*

WAN-update-min.

The periodic transfer interval for a spoofing time control in which RIP data can be transferred to the remote side is given here. You can enter a value from 1 to 60 minutes; the default value is 5.

Setup/IPX-module/SAP-configuration

This option allows you to store settings for SAP data packets (server information).








/SAP-configuration		SAP settings
Table-SAP		Displays the SAP table.
LAN-filter-table		Filter ranges for IPX service addresses (LAN)
WAN-filter-table		Filter ranges for IPX service addresses (WAN)
Server/Frm		Max. no. of SAP entries per SAP frame sent
Aging-minute(s)		Aging period in update units
Spoofing		Sets SAP spoofing method.
WAN-update-min.		SAP update period; effectiveness depends on spoofing.

Table-SAP

This option allows you to display the entries in the current SAP table. The table contains a maximum of 512 entries. It is sorted first by service type and then by server name. A SAP table might, for example, have the following appearance:

Type	Server-name	Network	Node-ID	Socket	Hops	Time	Flags
0004	Y	000000c1	000000000001	0451	1	1	local
0047	X	00000001	0000c0123456	8060	1	0	local
0107	Z	000000c1	000000000001	8104	2	1	local

Different SAP types are stored in the table. The server name, the applicable network, the server MAC address (000000000001 for internal server networks), the socket number and information on the location of the server must be read.

LAN-filter-table Entries in the LAN filter table make it possible to exclude specific service information ranges of a Novell network from being included in the SAP table and therefore to make better use of the resources of the IPX router. This also prevents unwanted connections from being established by these SAPs (services).

None of the service information located within a range of filters entered in the LAN filter table is transferred by the local network to the IPX router's SAP table. They are also not transferred to the remote station of the IPX router and therefore are also not available there.

For example, the service information for the printer server is often unnecessary for the remote station of the IPX router. If this information is to be excluded from the SAP table by means of the LAN filter table, the following entry is required:

Start-service	End-service
030c	030c

For a list and description of SAP services, please refer to the section entitled 'Novell SAP Numbers'.

WAN-filter-table As with the LAN filter table, you can use the WAN filter table to prevent ranges of service information from being transferred from the WAN to the SAP table.

Therefore, the blocked services have resulted in the establishment of a connection to the remote station before the destination router could filter them on the WAN side.

The layout and function of the WAN filter table are exactly the same as that of the LAN filter table. A WAN filter table for filtering file services might, for example, have the following appearance:

Start-service	End-service
0004	0004

Server/FRM This parameter sets the maximum number of services that can be included in a SAP frame. The specified value originally defined by Novell is 7. Today, however, it is common practice to pack a higher number of services in each frame in order to reduce network utilization. If all participating devices in the network support a higher number, this value can be raised as high as 22.

Aging-minute(s) This option allows you to set the number of times the SAP table will be updated until an entry in the SAP table ages, i.e. until the service recorded there is marked as "not reachable (down)". You can enter a value from 1 to 60; the default value is 3.

Spoofing

This option allows you to determine how the router will handle SAP packets.

- If you select **Off**, SAP packets are handled in the WAN in precisely the same manner as in local networks. SAP data are sent to the remote side in the event of new information and at intervals of one minute, i.e. a connection is established.
- With the **Trig** setting, the SAP data is sent to the remote end any time changes are detected.
- With the **Time** setting, the SAP data is sent to the remote end at selectable intervals (see below).
- **pBack** (default) is the most economical setting. In this case, the SAP data is sent to the remote end only when a connection is activated.















*When spoofing is set to **pBack**, entries in the RIP table age only when a new connection is established and an entry has been explicitly marked as 'not reachable'.*



WAN-update-min.

The periodic transfer interval for a spoofing time control in which SAP data can be transferred to the remote side is given here. You can enter a value from 1 to 60 minutes; the default value is 5.

Setup/TCP-IP-module

This menu allows you to enter settings for the TCP/IP module. The menu has the following layout:

/TCP-IP-module	TCP/IP module settings	
Operating		Activates or deactivates the TCP/IP module.
IP-address		Local IP address
IP-netmask		Local network's matching IP network mask
Intranet addr.		Local Intranet address
Intranetmask		Local network's matching Intranet network mask
Access-list		Restricts access to internal functions via TCP/IP.
DNS-default		Domain name server
DNS-backup		Backup domain name server
NBNS-default		NetBIOS name server
NBNS-backup		Backup NetBIOS name server
Table-ARP		ARP table for mapping an IP address onto a MAC address
ARP-aging-min.		Dwell time for entries in the ARP table
TCP-aging-min.		Time limit for configuration connections that are inactive
TCP-max.-conn.		Max. number of simultaneous configuration connections to the <i>ELSA LANCOM</i>

- Operating* The TCP/IP module of the router may be activated or deactivated here. In the default configuration, the TCP/IP module is activated.
- Configuration via TCP/IP using Telnet and the IP router is possible only if the TCP/IP module is activated.*
- IP address* The IP address for the router may be entered here. The default address on delivery is '0.0.0.0'.
- If IP masquerading is used, this address takes on a special meaning in connection with the Intranet address:
- If the IP address is assigned to the router by the Internet provider by PPP, all computers in the network linked by IP address and IP network mask are normally routed. These computers can then also be accessed directly from the Internet.
- IP-netmask* The network mask belonging to the IP address must be entered here. The default setting is 255.255.255.0 (class C network). A network mask of 255.255.255.255 means that there is only one computer in this network (the router itself). This setting (an IP address registered in the Internet with a fully assigned network mask) can be used for masquerading via a raw IP access, such as that offered by the provider of the individual network. With such an access an IP address is not assigned to the router by a PPP negotiation, but it must have a fixed IP address registered in the Internet.
- Intranet-address* A second IP address for the router may be entered here. This enables the router to be used as a router for two logical IP networks and also this address has a specific meaning with the use of IP masquerading:
- In this case, all computers that are in the network linked by Intranet address and Intranet mask are hidden behind the address assigned by the provider (or the Internet address (IP address)).
- The default address on delivery is '0.0.0.0'.
- Intranet-mask* The network mask belonging to the IP address must be entered here. The default setting is 255.255.255.0 (class C network).
-  *If neither an IP nor an Intranet address has been specified, the device responds to a default IP address, the first three digits of which are identical to the first three digits of the sending device XXX.XXX.XXX.YYY. The device can then be reached by dialing the IP address XXX.XXX.XXX.254.*
- In the event that such an address already exists in the network, a different address must be entered via outband configuration (terminal program).*
-  *If both an IP address and an Intranet address have been entered, the network defined by an IP address and IP network mask must contain only workstations (i.e. no routers).*

Access-list

The access to “internal functions” of the router may be controlled by an access list in TCP/IP applications.



The configuration data of the device are protected by a password, however this is always transferred in plain text, making it possible in principle to detect it and for any computer to read the configuration or to delete it. In order to prevent this from happening, the access list can be used to determine which computers or which networks can access the configuration.

For reasons of consistency, the access control is based on all “internal functions” of the router. The term “internal functions” refers to the following:

- Telnet server: the configuration interface based on the Telnet protocol
- TFTP server: the configuration interface based on the TFTP protocol
- SNMP: the configuration interface based on the SNMP

Each of the maximum of 16 entries in the access list has the following structure:

IP-address	IP-netmask
IP address of the authorized user (or user circle)	IP network mask of the user circle

Once an IP workstation with its IP address and the network mask 255.255.255.255 is entered into the list, the internal functions of the router can only be accessed from this computer. Any requests from devices with different IP addresses are ignored.

If a complete network has access enabled to an *ELSA LANCOM*, this can be done as follows for a class C network:

IP-address	IP-netmask
192.234.222.0	255.255.255.0

With this entry all IP addresses in the class C network 192.234.222.0 are authorized to use internal functions of the router.

DNS-default

The entry **DNS** (Domain Name Server) is required to announce the name server responsible for their own network for computers that have direct access via PPP to the router.

If the router is configured for access to the Internet via an Internet Service Provider, the DNS server is usually given by the provider. There are then two possible settings in the router:

- '0.0.0.0' is entered as the address of the DNS server. All computers in the local network can then use the provider's DNS server.
- The router's own IP address is entered as the DNS server. Then he uses the DNS information from the provider not only for its own local network but also forwards this information (DNS forwarding). Remote stations such as computers that dial in via remote access can then also access the provider's DNS server. This procedure is also referred to as DNS forwarding.

DNS-backup With the entry **DNS-Backup** a second name server can be named, which is used if the DNS fails.

NBNS-default The entry **NBNS-default** (NetBIOS Name Server) is required to announce the NBNS responsible for their own network for computers that have direct access via PPP to the router.

NBNS With the entry **NBNS-Backup** a second name server can be named, which is used if the NBNS fails.

Table-ARP This option allows you to display the ARP table (ARP cache), which is managed automatically for the purpose of mapping IP addresses onto physical terminal addresses. Individual entries can be removed from this table but no new entries can be entered manually.

The entries in the ARP table might, for example, have the following appearance if different devices with different IP addresses (192.168.139.20, 192.168.130.30) communicated with the router:

IP-address	Node-ID	Last-access	Connect
192.168.130.20	0000c0717860	6780443 tics	local
192.168.130.30	0800091eebf4	6214514 tics	local












ARP-aging-min. This option allows you to enter a time (from 1 to 99 minutes) at the end of which the ARP table is automatically updated, i.e. all IP addresses that have not been accessed since the last automatic update are removed. The default setting is 15 minutes.

TCP-aging-min. If data transfer stops during a TCP connection to the router, e.g. if the user does not enter any more data during the remote configuration, it will automatically release the TCP connection on expiry of the time entered here. Possible settings are from 1 to 99 minutes; The default setting is 15 minutes.

TCP-max.-conn. The maximum number of allowable connections possible at the same time can be set here. DEFAULT setting is '0', meaning the same as "any number".

Setup/IP-router-module

This menu allows you to enter settings for the IP router module. The menu has the following layout:

/IP-router-module		IP router module settings
Operating		Activates or deactivates the IP router module.
IP-routing-table		Router table for IP network and remote station assignment
LAN-filter-table		Negative/connect filter table for the TCP/UDP destination ports of LAN packets
WAN-filter-table		Negative filter table for the TCP/UDP destination ports of WAN packets
Proxy-ARP		Activates/deactivates the proxy ARP function
Loc.-routing		Activates/deactivates local routing
Start-WAN-Pool		Start of the address pool for dynamic address assignment for remote access
End-WAN-Pool		End of the address pool.
Routing-method		Routing method for IP packets
RIP-config		Settings for IP-RIP operation
Masquerading		Settings for IP masquerading

Operating

This option allows you to activate or deactivate the IP router module. In the default configuration, the IP router module is activated.

Activating the IP router module also activates the TCP/IP module.

IP-routing-table

The routing table can contain a maximum of 128 entries of destination network addresses or direct IP addresses with netmasks, and the names or IP addresses of other local routers. Alternatively, you can enter a setting by means of which packets to specific destination IP addresses are discarded and are not answered by proxy ARP. This is done by entering 0.0.0.0 for the name of the responsible router.

The 'Masquerade' field indicates whether the route should be masked or not. The following options are offered here:

- **On:** IP masquerading is switched on and functions with dynamic assignment of the IP address by the remote station. In this procedure the router queries the IP address '0.0.0.0' at the remote station and is assigned a random IP address by the remote station, which is then used for further processing.
- **Off:** Masquerading is switched off.
- **Static:** IP masquerading is switched on and functions with assignment of a static IP address previously assigned by the remote station. In this procedure the router queries the IP address entered under 'Setup/TCP-IP-module' at the remote station

and is assigned this address by the remote station. Use this setting when the remote station (e.g. your Internet provider) has assigned you a fixed IP address in the access data. Of course, this procedure will only function when this address has also been entered in the router as the IP address.

The IP routing table is generally sorted as shown below:

- The longest network mask is placed on top.
- For network masks of equal length, the one with the smallest IP address is placed on top.

In order to identify the correct remote station, the router searches the routing table from top to bottom using the destination IP address received. If a matching entry is found, the router name found is used for establishing the connection.

Address ranges that are prohibited in the Internet are excluded from transmission by preset entries in the IP routing table (the router name 0.0.0.0 means that packets to these addresses are not transmitted). The IP routing table below is provided by way of example and also shows the default settings:

IP-address	IP-netmask	Router-name	Distance	Masquerade
192.168.0.0	255.255.0.0	0.0.0.0	0	Off
172.16.0.0	255.240.0.0	0.0.0.0	0	Off
10.0.0.0	255.0.0.0	0.0.0.0	0	Off
224.0.0.0	224.0.0.0	0.0.0.0	0	Off

However, if these addresses are required for Intranet use, for example, it is possible to delete the predefined entries at any time. If the routing table contains no entries with the router name 0.0.0.0, the router processes all IP addresses with valid routes.

- Example
 - The local network address is 192.120.130.0.
 - Three terminal units must be available via proxy ARP with the IP addresses 192.120.130.10, 192.120.130.11 and 192.120.130.12 via an *ELSA LANCOM* 'Leeds'.
 - Two destination networks 192.120.131.0 and 192.120.132.0 can be accessed by the remote stations 'GLASGOW' and 'LONDON'.
 - Data packets for the destination network 193.140.300.0 are to be sent to another local router with the IP address 192.120.130.200.
 - Absolutely nothing is to be transmitted to the destination network 193.140.200.0.
 - All other non-local data packets must be sent to the router 'PROVIDER' at the Internet service provider.

In this example, the router table would contain the following entries:

IP-address	IP-netmask	Router-name	Distance	Masquerade
192.120.130.10	255.255.255.255	LEEDS	0	Off
192.120.130.11	255.255.255.255	LEEDS	0	Off
192.120.130.12	255.255.255.255	LEEDS	0	Off
192.120.131.0	255.255.255.0	GLASGOW	0	Off
192.120.132.0	255.255.255.0	LONDON	0	Off
193.140.200.0	255.255.255.0	0.0.0.0	0	Off
193.140.300.0	255.255.255.0	192.120.130.200	0	Off
255.255.255.255	0.0.0.0	PROVIDER	0	On

If the connection to the selected remote station is to be realized via a PPP connection, the IP rights must be enabled for the corresponding entry in the PPP table.

The last line is an entry for the "default route". The IP address 255.255.255.255 means the same as 0.0.0.0 (for technical reasons, 0.0.0.0 cannot be entered in the first column). Because it contains the IP network mask 0.0.0.0, this line is always appropriate after the rest of the table has been searched. Therefore, the router sends everything that it cannot transfer over other routes and should not discard or that comes from a WAN terminal and is not local to the router at the provider.

LAN-filter-table This table allows you to filter specific ranges of destination ports. In addition, you can determine how the packets are to be filtered. If packets with the entered ports are received from the LAN side, they will not be forwarded (always filter) unless a connection is currently in place (connect filter) or unless they can be routed over other than the DEFAULT route (I-Net filter).

The LAN port filters are defined in a table with the following layout:

Idx.	D-st.	D-end	S-st.	S-end	Src.-addres	Src-netmask	Prot	Type
WIN	0	0	137	139	255.255.255.255	0.0.0.0	TCP and UDP	Always s-filt.

The table fields have the following meaning:

■ **Idx.**

Unique index. This entry is required to enable the filters to be distinguished. The index may be four characters long and selected as desired.

- **D-st., D-end**
Destination port range that is to be filtered. A range of 0 to 0 means that no destination port is affected by this filter.
- **S-st., S-end**
Source port range that is to be filtered. A range of 0 to 0 means that no source port is affected by this filter.
- **Src-address, Src-netmask**
A subnetwork of the local network for which the filter is valid can be entered here. A source address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).
- **Prot**
Protocol that is to be filtered. Possible entries are **TCP**, **UDP**, **ICMP** and **all**.

The setting **all** filters out every packet from the specified source network or to the destination network.
- **Type**
Filter type. The possible values are Always-filt., Connect-filt. and Internet-filt.
 - **Always** filter: The packet is discarded.
 - **Connect** filter: The packet is discarded if there is no connection to the remote station.
 - **Internet** filter: The packet is discarded if its destination can be accessed only via the default route.

The default filter is entered in the above table. It suppresses the unwanted and cost-intensive connections in Windows networks on IP. These networks regularly send items such as DNS queries to the local network, which are routed to the Internet without this filter.

WAN-filter-table

This table allows you to enter specific ranges of destination ports. If packets with the entered ports are received from the WAN side, they will not be forwarded (firewall function).

The WAN port filters are defined in a table similar to the LAN filter table:

Idx.	D-st.	D-end	S-st.	S-end	Dst.-address	Dst-netmask	Prot
WIN	53	53	137	139	0.0.0.0	0.0.0.0	TCP and UDP

The fields in the table have the same meaning as in the LAN filter table, with the following exception:

■ Dst-address, Dst-netmask

A subnetwork of the local network for which the filter is valid can be entered here. A destination address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).

The table entries are sorted in a similar fashion to the IP router table:

- Longest network mask is placed on top.
- For two network masks of equal length, the one with the smaller IP address is placed on top.

Network masks and IP addresses of 0.0.0.0 can be used as "wildcards". Specified computers and networks may be simultaneously subjected to targeted filtering while others pass the router unfiltered.

The tables are processed from top to bottom. As soon as a matching filter is found, the packet is handled accordingly.

Proxy-ARP This option allows you to activate or deactivate the proxy ARP mechanism (default: 'Off'). This function permits data to be transmitted to IP addresses within the same logical network as the sender, e.g. when linking individual workstation computers (teleworkers) to the corporate network via TCP-IP.

Loc.-routing Local routing enables the router to forward data packets via the local network. The local routing is necessary if the router, as the default gateway for the workstations receives packets for destination networks to which it cannot establish a connection itself. If the router cannot return the address of the appropriate router to the workstation via IMCP, it will forward the data to the corresponding router itself (see also 'Local Routing'). Since this setting increases network utilization in the LAN, the default setting is 'Off'.

Start-address-pool Start of the address pool used for the dynamic assignment of IP addresses for devices dialing in. This function is also known as IP pooling and can be used for remote access by several field staff members, for example.

The address pool should be in the same address range as the router. If possible, ensure that the address pool is large enough that an IP address can be assigned to every device dialing in (e.g. one address for each of the available B channels).



If the device dialing in can initially establish a connection, only to have it terminated again during the protocol negotiation, this is a sign of insufficient free IP addresses in the IP pool.

End-address-pool End of the address pool for IP pooling.

Setup/IP-router-module/Routing-method

The router offers two methods for IP routing, which can be separately set for IP and ICMP packets. Both methods are based on the evaluation of the field 'Type-of-service' in the IP header.

The menu has the following layout:

/Routing-method		Routing method settings
Routing-method		Routing method for IP packets
ICMP-routing-method		Routing method for ICMP packets

Routing-method This option allows you to define the routing method used for IP packets:

- If you select 'Normal', all IP packets are handled in the same way as per the routing specifications of the Internet protocol.
- If you select 'Type-of-service', IP packets are placed in the urgent queue or reliable queue, depending on the contents of the 'Type-of-service' field. All other packets are placed in the normal send queue. In this way, transmission is guaranteed, provided that it is possible.




ICMP-routing-method

This option allows you to define the routing method used for ICMP packets:

- If you select 'Normal', the ICMP packets are handled like any other IP packets as per the routing specifications of the Internet protocol.
- If you select 'Reliable', all ICMP packets received are placed in the reliable queue.

Setup/IP-router-module/RIP-configuration

This option allows you to enter settings for the management of IP-RIP packets. The menu has the following layout:

/RIP-configuration		Settings for IP-RIP operation
RIP-Type		RIP compatibility switch
R1-mask		Management of network masks
Table-IP-RIP		Dynamic IP routing table

RIP-type

This option allows you to select the method to be used for handling the IP-RIP packets. The different settings have the following meaning:

- **Off:** IP-RIP is not supported (default).
- **RIP-1:** RIP-1 and RIP-2 packets are received but only RIP-1 packets are sent.
- **R1-comp:** RIP-1 and RIP-2 packets are received. RIP-2 packets are sent as an IP broadcast.
- **RIP-2:** Same as **R1-comp** except that all RIP packets are sent to the IP multicast address 224.0.0.9.

R1-mask

If **RIP-1** is set, this option allows you to influence the management of network masks. Therefore, these settings are required only for subnetting under **RIP-1**. The different settings have the following meaning:

- **Class** (default): The network mask used in the RIP packet is derived directly from the IP address class, i.e. the following network masks are used for the network classes:
 - Class A: 255.0.0.0
 - Class B: 255.255.0.0
 - Class C: 255.255.255.0
- **Address**: The network mask is derived from the first bit that is set in the IP address entered. This and all high-order bits within the network mask are set. Thus, for example, the address 127.128.128.64 yields the IP network mask 255.255.255.192.
- **Cl+Addr**: The network mask is formed from the IP address class and a part attached after the address procedure. Thus, the above-mentioned address and the network mask 255.255.0.0 yield the IP network mask 255.128.0.0.

Table-IP-RIP






This option allows you to display the entries in the current dynamic IP routing table.

An IP-RIP routing table might, for example, have the following appearance:

IP-address	IP-netmask	Time	Distance	Router
223.245.254.0	255.255.255.0	1	1	192.38.9.100
223.245.257.0	255.255.255.0	1	1	192.38.9.200

Setup/IP-router-module/Masquerading

This menu allows you to enter settings for the masking function. The menu has the following layout:

/Masquerading	Settings for IP masquerading	
TCP-aging-second(s)		Time in seconds after which a TCP masking becomes invalid
UDP-aging-second(s)		Time in seconds after which a UDP masking becomes invalid
ICMP-aging-second(s)		Time in seconds after which an ICMP masking becomes invalid
Service-table		Static masquerading table
Table-masquerading		Dynamic masquerading table

Service-table

The use of inverse masquerading makes 'services' (e.g. a file server) selectively visible in the Internet by entering specified ports in the service table in the IP network, while all other services and computers remain invisible from the local network (see also 'IP Masquerading (NAT, PAT)').

The service table (also called the static masquerading table) can contain up to 16 entries and has the following layout:

D-port	Intranet addr.
20	10.1.1.10
21	10.1.1.10

The different columns have the following meaning:

- D-port: Destination port for the particular entry
- Intranet-addr.: Destination IP address for the computer in the local network

Through this assignment, it is possible, for example, to address the relevant service directly via telnet. Enter the IP address of the router and attach the port number, separated by a double point, to the address.

You can use the command

```
telnet 192.38.50.100:27
```

to connect directly to a news server that can be reached via a router with the IP address 192.38.50.100.

*Table-
masquerading*

With IP masquerading, the IP addresses of computers in the local network are rendered invisible to external devices by means of a conversion of addresses and ports in the router. The dynamic masquerading table displays the IP addresses from the local network that the router is currently masking. The dynamic masquerading table can contain up to 2048 entries and has the following layout:








Intranet addr.	S-port	Protocol	Timeout
10.1.1.10	1234	TCP	10

The different columns have the following meaning:

- Intranet-addr.: IP address of the computer in the local network
- S-port: Source port for this entry
- Protocol: Protocol used (TCP/UDP/ICMP)
- Timeout: Time in seconds until the entry is removed from the table

Setup/SNMP-module

This menu allows you to enter settings for configuration of the router via SNMP. The menu has the following layout:

/SNMP-module	SNMP module settings	
Send-Traps		Switch for issuing SNMP traps
IP-Trap-Table		Table with 20 destination addresses for trap messages
Administrator		Device administrator
Location		Device location
Register-monitor		Command to set a destination address to which the traps are to be sent
Delete-monitor		Command to delete an address that was set with 'Register-monitor'
Monitor-table		Table with all currently active destination addresses that were set with 'Register-monitor'

Send-Traps This entry controls trap output (No/Yes).

IP -Trap-Table Enters the IP addresses to which the trap messages will be sent.

Administrator Administrator's name

Location Device location

You can also query the last two parameters via SNMP (MIB-2).

Register-monitor This command logs on applications with the router to retain targeted trap information. The *ELSA LANmonitor*, for example, queries the channel statistics in this way and converts them to a graphic display (under Windows).

In principle, any SNMP manager can use this command to obtain information from the router. The syntax

```
register-monitor IP-address:port mac address timeout
```

is used to direct the router to enter the given address in the monitor table and to send traps to it. If the traps are not received within the set hold time, the address will be automatically deleted from the table. A hold time of '0' permanently retains the entry in the table.

Delete-monitor This command removes the entries from the monitor table.









Monitor-table The monitor table has the following structure:

IP-address	Port	MAC-Address	Timeout
10.0.0.53	1057	0080c76da46e	1

This entry indicates, for example, that an *ELSA LANmonitor* has logged on to the router.

Setup/DHCP-module

This menu allows you to enter settings for the DHCP server. The menu has the following layout:

/DHCP-server-module	DHCP server settings	
Operating		Switch for activating the DHCP module
Start-address-pool		Start address for the address pool
End-address-pool		End address for the address pool
Netmask		Network mask for the address pool
Broadcast-address		Broadcast address for the LAN
Max.-lease-time-minute(s)		Maximum period of validity for the address assignment via DHCP
Default-lease-time-minute(s)		Default period of validity for the address assignment via DHCP
Table-DHCP		Table of current assignments via DHCP

Operating

On: The device operates as a DHCP server

Off: The device does not operate as a DHCP server

Auto: The device regularly checks whether there is another DHCP server in the LAN. If not, it operates as a DHCP server and issues IP addresses to local clients.



If there is no IP or Intranet address entered in the TCP/IP module (e.g. delivery status), the router will issue IP addresses from the address range 10.0.0.2 - 10.0.0.253 to all DHCP clients in auto mode.

*Start-address-pool
End-address-pool*

The IP address assigned is 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 device will determine the appropriate addresses (start or end) from the settings under 'Setup/TCP module'. The procedure is as follows:

- 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.
- The start address of the pool is either the address given in the DHCP module or the first valid address in the local network.
- The end address of the pool is either the address given in the DHCP module or the last valid address in the local network.

A valid address is then taken from the pool for the 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 that is to be assigned to the computer is unique in the local network. It does this by issuing an ARP request to the address. If the ARP request is answered, the DHCP server begins the procedure again with a new address. As soon as the uniqueness of an address has been established, the requesting computer is assigned the address found.

Netmask The network mask is assigned in the same way as the address:

The system either assigns the network mask entered in the DHCP module or uses the network mask that belongs to the local network (determined during address assignment).

Broadcast The broadcast mask is assigned in the same way as the address:

The system either assigns the broadcast address entered in the DHCP module or uses the broadcast address that belongs to the local network (determined during address assignment).

Max.-lease-time-minute(s) Here you can enter the maximum period of validity that the DHCP server assigns a host. The DEFAULT value of 6000 minutes equals approximately 4 days.

Default-lease-time-minute(s) Here you can enter the period of validity that is assigned if the host makes no request. The DEFAULT value of 500 minutes equals approximately 8 hours.

Table-DHCP In the DHCP module, the 'Table-DHCP' option allows you to verify (or look up) the assignment of IP addresses to the relevant computers. This table has the following layout:

IP-address	Node-ID	Timeout	Hostname	Type
10.1.1.10	00a0570308e1	500	ELSA	new

- IP-address: IP address assigned
- Node-ID: Computer's Ethernet address
- Timeout: Time remaining until the assignment becomes invalid
- Hostname: Computer's name in plain text if it was transmitted in the request
- Type: This field contains additional information on the 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.

- **unkn.:** 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.
- **stat.:** A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.
- **dyn.:** The DHCP server assigned an address to the computer.

Setup/NetBIOS-module

The Setup/NetBIOS-module menu contains the settings for the NetBIOS module. The menu has the following structure:

Operating		On or off
Scope-ID		NetBIOS scope in which the router is located.
NT-Domain		Workgroup/domain in which the router is located.
Remote-table		All remote stations with which NetBIOS information is to exchanged must be entered in the remote-station table.
Group-list		All workgroups known to NetBIOS are recorded in the group list.
Host-list		All computer names known to NetBIOS are recorded in the host list.
Server-list		All servers that have logged onto the network are recorded in the server list.
Watchdogs		
Update		
WAN-Update-Min.		

Scope-ID

The Scope-ID menu item can be used to specify the NetBIOS scope in which the device is located. It then sees only those NetBIOS packets originating in the same NetBIOS scope; all other packets are automatically rejected. The scope ID is only used in conjunction with Windows name servers (WINS). This entry can generally be left blank.

NT-Domain

A workgroup/domain can be specified in the NT domain item to trigger the search procedure when starting the NetBIOS module. This is required if the network does not contain any computers running Windows 95 or Windows 98.

Remote-table

All remote stations that are to provide or receive NetBIOS information must be entered in the remote-table. When the NetBIOS module is switched on, NetBIOS packets from remote stations other than those specified will be rejected automatically. The remote-table has the following structure:

Name	Type
GLASGOW	Router or workstation

If the connection to the selected remote station is to be realized via a PPP connection, the NetBIOS rights must be enabled for the corresponding entry in the PPP table.

Type The 'Type' field specifies whether the remote station is a router or a workstation. In the case of a workstation, all of the known names and servers in the local network and all other connected routers are logged off and deleted from their respective tables as soon as the connection to the remote station is closed.

Host table The host table has the following structure:

Name	Type	IP-address	Remote station	Timeout	Flags
REMOTE	00	10.0.1.100	GLASGOW	5000	xx20
WORKSTATION	00	10.0.0.10		5000	xx00

Group table The group table thus looks like this:

Group/Domain	Type	IP-address	Remote station	Timeout	Flags
WORKGROUP	1e	10.0.0.10		5000	xx00
WORKGROUP	1e	10.0.1.100	GLASGOW	5000	xx20

The fields of the table have the following significance:

Name	Name of the host in the host table.
Group/Domain	Name of the group or domain in the group list. Groups and NT domains are handled in the same manner from the NetBIOS point of view.
Type	WINS type of the host. The type is not relevant for NetBIOS, but Microsoft Networks assign certain properties to the name on the basis of the type.
IP-address	IP address of the owner of the name. The same name can be assigned to multiple IP addresses in the group list.
Remote station	Name of the remote station for which the name became known.
Timeout	Time until the name is no longer valid. The time-out is also associated with an aging counter in the flags.
Flags	The flags contain additional information pertaining to the name.

Flags The flags have the following significance:

0x0003	This counter increments up each time the validity expires. The entry will be deleted if the name is not refreshed after the second expiration at the latest.
0x0004	This identifies an entry that still needs to be transferred.
0x0008	This identifies an entry that is queued for deletion, i.e. the name has not yet been refreshed after the establishment of a connection.
0x0010	Reserved

0x0020	This identifies a remote station.
0x0040	Reserved
0x0080	Reserved

The server list has the following structure:

Host	Group/ Domain	UPD	IP-address	OS- Ver	SMB- Ver	Server- type	Remote station	Time- out	Flags
REMOTE	WORKGROUP	00	10.0.1.100	0400	010f	0004140b	GLASGOW	13	0020
WORKSTATION	WORKGROUP	07	10.0.0.10	0400	0415	00452003		31	0000






Unlike the host and group lists, this table fills gradually, as the NetBIOS module depends on messages from the servers themselves.





The individual fields have the following significance:

Host	Name of the server
Group/Domain	Workgroup or domain in which the server is located.
UPD	Update counter: indicates the number of times that the server has already propagated itself
IP-address	Address of the server
OS-Ver	Operating system version number
SMB-Ver	Version number of the SMB protocol used
Server-type	Bit mask in which the services of the server are coded
Remote station	Name of the remote station from which the server was announced
Timeout	Time until the entry loses its validity (for entries from the LAN) or time until the router propagates a remote entry.
Flags	Corresponds to the flags in the host or group tables.

Setup/Config-module

This menu allows you to enter settings for router configuration options. The menu has the following layout:

/Config-module		Configuration module settings
LAN-config		Switch for configuring from the LAN side
WAN-config		Switch for configuring from the WAN side
Password-required		Password required on/off if there is no password
Farconfig-(EAS-MSN)		Subscriber number for remote configuration via PPP
Maximum-connections		Maximum number of simultaneous connections

/Config-module		Configuration module settings
Config-aging-minute(s)		Time limit for remote configuration connections
Login-errors		Number for failed log-in attempts before the log-in block is activated
Lock-minutes		Duration of block and period until old log-in errors are forgotten
Display contrast		
Language		Configuration language

LAN-config This option allows you to define whether remote configuration from the LAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting for this option is **On**.

WAN-config This option allows you to define whether remote configuration from the WAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting for this option is **Off**.

Password-required This specifies whether a new password should be requested every time a remote configuration is begun (**On**), or the password request should be suppressed (**Off**). The default setting for this option is **On**.

Farconfig-(EAZ-MSN) This subscriber number permits remote configuration via PPP. If no number is specified here, remote-configuration calls will be accepted on all numbers.

Maximum connections This option allows you to display the maximum number of remote configuration sessions that can occur simultaneously for the device.

Config-aging-minute(s) If data transmission halts during a remote configuration session, e.g. because the user is no longer entering data, the device automatically releases the connection at the end of the time period specified here. Possible settings are from 1 to 99 minutes; the default setting is 5 minutes.

Login-errors This entry specifies the number of failed attempts allowed before the log-in block is activated. An empty password (simply pressing <ENTER> at the password prompt) is not considered an attempt and therefore does not activate the block.



The default value is 5. A lower value may cause the log-in block to be activated with only one access on an older ELSA LANconfig! In this case obtain an updated ELSA LANconfig version over our online media.

Lock-minutes This entry has two meanings. It indicates how long the access is blocked if the log-in block has been activated. It also sets the period after which the device forgets all prior login errors.





Language This option allows you to select whether you will use the German or English version of the software for performing the configuration.

Setup/LANCAPI-module

Configuring *LANCAPI* basically involves answering two questions:

- 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*?
- Via which UDP port do the *LANCAPI* server and *LANCAPI* clients communicate?

The *LANCAPI* module has the following layout:

/LANCAPI-module		LANCAPI settings
Access-list		List of computers allowed to use the <i>LANCAPI</i>
Interface-list		Activation of the <i>LANCAPI</i> for the various interfaces and specification of the various subscriber numbers to which the <i>LANCAPI</i> should respond.
Priority-list		Priority for the <i>LANCAPI</i> versus router connections
UDP-port		UDP port for communication between the <i>LANCAPI</i> server and clients

Access-list

This option allows you to limit the circle of computers permitted to use the *LANCAPI*. This table can have a maximum of 16 entries. If the table is empty, all computers can access the *LANCAPI*.

Interface-table

The interface table appears as follows:

lfc	Operating	EAZ-MSN(s)	Force-Out-MSN
S0-1	Outgoing	123456	no

The fields of the table have the following significance:

lfc	Designates the associated interface
Operating	This item determines whether <i>LANCAPI</i> operation is permitted on this interface for outgoing calls, incoming and outgoing calls (On) or whether <i>LANCAPI</i> operation is disabled completely (Off).
EAZ-MSN(s)	Enter the EAZs or MSNs on which the <i>LANCAPI</i> should respond to incoming calls here; these EAZs/MSNs will also be displayed to the exchange during outgoing calls.
Force-Out-MSN	If no outgoing MSN has been configured for the CAPI application, this item can be used to determine whether the <i>LANCAPI</i> transfers the first EAZ/MSN on the list.

Priority-table

The priority for a port controls the option for breaking outgoing connections via the *LANCAPI* router connections. Option '1' does not break router connections, the setting '2' breaks only auxiliary connections of a router connection with channel bundling, the selection '3' also breaks main channels of a router connection.

Setup/LCR-module

Enter the following information when setting the least-cost router:

- For which modules in the device should the LCR functions be active?
- Which area codes should be diverted when via which call-by-call provider?

The LCR module has the following layout:

/LCR module		Least-cost router settings
Router-usage	<input type="checkbox"/>	Activate LCR for the router modules, On or Off
Lancapi-usage	<input type="checkbox"/>	Activate LCR for the <i>LANCAPI</i> , On or Off
Timetable	<input type="checkbox"/>	Call forwarding table
Celebration-day-table	<input type="checkbox"/>	List of holidays affecting the timetable.

Timetable

The table has 256 entries and the following structure:

Index	Prefix	Days	Start	Stop	Number-list	Fallback
1	0171	192	0:00	23:59	01013;01070	On

The individual entries have the following meaning:

Index	Continuing index of entries in the table.
Prefix	Area code to be diverted.
Days	Validity of the entry for week days and holidays shown in an 8-bit mask: Bit 0 represents Monday, bit 7 holidays. The entry '31' therefore designates all business days, '192' Sundays and holidays.
Start	Beginning time for the validity of the entry on the defined days.
Stop	Termination time for the validity of the entry on the defined days.
Number-list	Network identification number of the call-by-call providers.
Fallback	Automatic fallback to your own telephone company if all call-by-call numbers are busy.

Example:

`set 1 02 31 1:00 11:59 01030;01090;01070 On` diverts all long-distance calls to region '02' between one and twelve o'clock to the provider with the network identification number '01030'. If this number is busy, the network identification numbers '01090' and '01070' will be attempted. If they are also not available, the connection will be made via the normal telephone company.

Celebration-day-table

The celebration-day-table has 256 entries and the following structure:








Index	Date
1	01010000
2	01050000
3	03100000
4	25120000
5	26120000
6	02041999
7	13051999

The individual entries have the following meaning:

Index	Continuing index of entries in the table
Date	Dates of holidays. Enter the index and the date in full without separators, e.g. 'set 8 13041999' for April 13, 1999 as the eighth entry in the list. Enter '0000' as the year for annually occurring holidays.

Setup/DNS-module

The settings for the DNS server can be modified here as required. The menu contains the following items (incl. their default settings):

Operating		On (default) or off
Domain		Own domain, optional, 32 characters max.
DHCP-usage		Yes (default) or no
NetBIOS-usage		Yes (default) or no
DNS-table		Static DNS table for the manual association of IP addresses to names, 64 entries
Filter-list		Filter list for the exclusion of prohibited domains, 64 entries
Leasetime		Specifies the name validity information to be given to a requesting computer. Default: 2000

DNS-table

The DNS table contains a simple association of local names to IP addresses. The table is sorted alphabetically by names.

The table is restricted to 64 entries, as large networks are configured more effectively using the DHCP server, which can also be used to handle name requests. The table has the following layout:

Hostname	IP-address
Host10	10.0.0.10

The name is restricted to a maximum of 32 characters. Longer names are not necessarily practical in a local network.

Filter-list

The filter list contains the entries for prohibited domains. In addition, it is possible to specify for whom a given domain will be prohibited. This is set using an IP address/netmask pair. An IP address of 0.0.0.0 prohibits this domain for all computers. A subnet mask of 0.0.0.0 prohibits the domain for all networks. The table has the following layout:

Idx.	Domain	IP-Address	Netmask
F001	*xxx*	0.0.0.0	0.0.0.0

Clear IDs can be freely selected and assigned to the filters in the 'Idx.' field.

Enter the name of the domain to be prohibited in the 'Domain' field. Wildcards such as '?' and '*' may be used. The wildcard '?' replaces exactly one character, while '*' can stand for a random number of characters. Multiple instances of the wildcard '*' can be used. For example, *xxx* filters all names containing the letters xxx in any position within the name.

The IP address and subnet mask fields can be used to specify the subnet for which the domain will be prohibited.

The filter table is sorted according to the subnet masks in descending order (the longest at the top); entries with identical subnet masks are sorted according to the IP addresses in ascending order. In the event of identical IP addresses, the entries are sorted in ascending order according to the domain to be prohibited.

The table is searched from top to bottom and an error message is returned to the requesting computer in the event of a match.





Setup/Time-module

The least-cost router in the device requires correct time information to calculate the call number diversions via call-by-call provider. Precise time information is also desirable for some statistics.

The time may be set manually (with the 'time' command) or automatically read from the ISDN network.







For automatic time comparison when the module is switched on, a previously specified remote station is called directly and the time information is taken from the ISDN network. So long as the time module is switched on, the time will be taken from the ISDN every time the router establishes a connection.

The time module has the following layout:

/Time-module	Time module settings	
Operating		Activating the module: On, Off
Current-time		Displays the current time in the device.
Time-call-number		Call number to which a connection must be established to receive time information from the ISDN.
Call-attempts		Number of possible attempts to receive time information

Firmware

The various firmware parameters can be called up and a firmware upload started from this menu:

/Firmware	Display and keyboard settings	
Version-table		Displays hardware releases and serial numbers for the router
Table-firmsafe		Information on the two firmware versions stored in the device and on the bootloader.
Mode-firmsafe		Firmware activation mode
Timeout-firmsafe		Time in minutes required to test new firmware
Test-firmware		Tests the inactive firmware
Firmware-upload		Initiates a firmware upload

Version table

The version table displays the firmware version and serial number of the device.

lfc	Module	Version	Serial-number
lfc	LANCOM Business 4100	1.60.0012 / 30.06.1999	8427.000.020

Table firmsafe This table provides the following details for the two firmware versions stored in the device: the position in memory (1 or 2), status information (active or inactive), the version number, the date, the size and the index (sequential number).

Position	Status	Version	Date	Size	Index
1	Inactive	1.60	23061999	690	6
2	Active	1.60	30061999	692	7
3	<loader>	1.60	07061999	64	0

Enter the following command to activate an inactive firmware version:





```
set <position number> active.
```

Mode-firmsafe Only one of the firmware versions stored in the device can be active at any one time. When new firmware is loaded the inactive firmware is overwritten. You can decide which firmware will be activated after the upload:

- 'immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
 - The new firmware is successfully loaded and then operates as desired. Everything is then in order.
 - However, if the new firmware does not operate correctly, it may not be possible to communicate with the device after the restart. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots the device.
- 'login': To prevent problems caused by defective firmware, the second option will load the firmware and start it immediately.
 - In contrast to the first option, the firmsafe will wait until it has successfully logged on over outband or inband (by telnet). In contrast to the first option, the firmsafe will wait until it has successfully logged on (by telnet). The new firmware will only be permanently activated when the login occurs successfully within the time set under 'Timeout firmsafe'.
 - If the device no longer responds and it is therefore impossible to log in, the firmware automatically loads the previous firmware version and reboots the device with it.
- 'manual': The third option allows you to set a period (Timeout firmsafe) beforehand for testing the new firmware. 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.

Other

The **Other** menu allows you to manage the following functions:

/Other	Various functions	
Manual-dialing		Connection testing
Boot-system		Boots the device.
Reset-system		Resets to factory settings.
Upload-system		Loads new firmware.

Other/Manual Dialing

Select this option when you wish to establish a connection manually for testing purposes.

Boot-system

This option allows you to reboot the device.
Before executing the command all open connections (ISDN or TCP) will be released or closed.

Reset-system

This option resets all the settings that have been entered. The device is reset to the delivery version.

For safety's sake, the system asks you to enter the configuration protection password in order to ensure that you have not mistakenly selected this command instead of the `Boot-system` command. If no password has been assigned, you must press Enter a second time.

Upload-system

This option starts a firmware upload (refer to chapter 'How to set up new software').

The flash ROM technology permits flexible and service-friendly handling of the system software by allowing different firmware versions to be read in. It also allows devices can be retrofitted for all future options.