

**ELSA LANCOM™ DSL Office series**

© 1999 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

Sonnenweg 11

Germany

[www.elsa.de](http://www.elsa.de)

Aachen, June 2001

# Preface

## Thank you for placing your trust in this ELSA product.

By selecting an *ELSA LANCOM DSL Office* you have chosen a router which you can use to connect local area networks or single workstations to the Internet with high speed.

## Model varieties

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

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

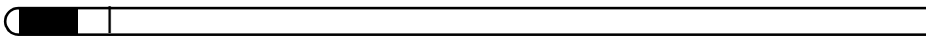
## Documentation

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.

If you should nevertheless find an error, or if you have any criticisms or suggestions with regard to this documentation, please send an e-mail directly to: [editorial@elsa.de](mailto:editorial@elsa.de)



*Our online services ([www.elsa.com](http://www.elsa.com)) are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. In the 'Support' file section you can find answers to FAQs (**F**requently **A**sked **Q**uestions) concerning your product. The KnowledgeBase offers a further large pool of information. Current drivers, firmware, tools and manuals can be downloaded at any time.*



# Contents

<b>1 Introduction</b>	<b>9</b>
1.1 What does a router do?	9
1.2 Typical applications	10
1.2.1 Internet on the LAN	10
1.2.2 LAN to LAN coupling	11
1.2.3 Telecommuting with remote access	11
1.2.4 Office communications	11
1.3 What does the <i>ELSA LANCOM DSL Office</i> offer?	12
1.3.1 All devices of the <i>ELSA LANCOM DSL Office</i> series	12
1.3.2 Additional functions <i>ELSA LANCOM DSL/I-10 Office</i>	15
<b>2 Introducing the <i>ELSA LANCOM DSL Office</i></b>	<b>19</b>
2.1 The front of the unit	19
2.2 The back of the unit	21
<b>3 Installation</b>	<b>23</b>
3.1 Package contents	23
3.2 System requirements	23
3.3 Hardware installation	24
3.4 Software installation	25
3.4.1 Starting ELSA Setup	25
3.4.2 Which software should you install?	26
3.5 In the next chapter...	27
<b>4 Basic settings</b>	<b>29</b>
4.1 Starting the setup wizard	29
4.1.1 Basic settings with <i>ELSA LANconfig</i>	29
4.1.2 Basic settings with <i>ELSA WEBconfig</i>	31
4.2 Set up access to the Internet	35
4.2.1 Start the wizard under <i>ELSA LANconfig</i>	35
4.2.2 Start the wizard under <i>ELSA WEBconfig</i>	35
4.2.3 Entering access data	35
4.3 Settings to workstation PCs	35
4.4 That's it!	36

<b>5 Configuration and management</b>	<b>37</b>
5.1 Configuration tools and approaches	37
5.2 Configuration software	38
5.2.1 Configuration using <i>ELSA LANconfig</i>	38
5.2.2 Configuration using <i>ELSA WEBconfig</i>	40
5.2.3 Configuration using Telnet	41
5.2.4 Configuration using SNMP	42
5.3 Remote configuration via Dial-Up Network	42
5.3.1 This is what you need for remote configuration	43
5.3.2 The first remote connection using a Dial-Up Network	43
5.3.3 The first remote connection using a PPP client and Telnet	44
5.3.4 Limiting remote configuration	44
5.4 <i>ELSA LANmonitor</i> —know what's happening	46
5.4.1 Extended display options	47
5.4.2 Monitor Internet connection	47
5.5 Trace outputs—Information for pros	48
5.5.1 How to start a trace	49
5.6 Saving and restoring the configuration	51
5.7 New firmware with ELSA FirmSafe	52
5.7.1 This is how ELSA FirmSafe works	52
5.7.2 How to load new software	53
<b>6 Security</b>	<b>55</b>
6.1 Protection for the configuration	55
6.1.1 Password protection	55
6.1.2 Login barring	57
6.1.3 Access control via TCP/IP	58
6.2 Protection for the LAN	58
6.2.1 The hiding place – IP masquerading (NAT, PAT)	58
6.2.2 Data packet filtering – Firewall	62
6.3 Protecting the ISDN connection	66
6.3.1 Identification control	66
6.3.2 Callback	68
6.4 The security checklist	69
<b>7 Server services for the LAN</b>	<b>73</b>
7.1 Automatic IP address administration with DHCP	73
7.1.1 The DHCP server	73
7.1.2 DHCP—'on', 'off' or 'auto'?	74
7.1.3 How are the addresses assigned?	75

7.2 DNS .....	78
7.2.1 What does a DNS server do? .....	79
7.2.2 DNS forwarding .....	80
7.2.3 Setting up the DNS server .....	81
7.3 Call charge management .....	85
7.3.1 Connection restriction for DSL and cable modem .....	85
7.3.2 Charge-based ISDN connection limits .....	87
7.3.3 Time-dependent ISDN connection control .....	87
7.3.4 Settings in the charges module .....	88
7.4 The SYSLOG module .....	88
7.4.1 Setting up the SYSLOG module .....	89
7.4.2 Example configuration with <i>ELSA LANconfig</i> .....	89
7.5 Office communications with <i>ELSA LANCAP</i> i .....	91
7.5.1 What are the advantages of <i>ELSA LANCAP</i> i? .....	91
7.5.2 Installing the <i>ELSA LANCAP</i> i client .....	92
7.5.3 Configuration of the <i>ELSA LANCAP</i> i clients .....	92
7.5.4 Configuring the <i>ELSA LANCAP</i> i server .....	94
7.5.5 How to use the <i>ELSA LANCAP</i> i .....	96
7.5.6 The <i>ELSA CAPI Faxmodem</i> .....	97

## **8 Routing and WAN connections ..... 99**

8.1 General information on WAN connections .....	99
8.1.1 Bridges for standard protocols .....	99
8.1.2 What happens in the case of a request from the LAN? .....	100
8.2 IP routing .....	101
8.2.1 The IP routing table .....	101
8.2.2 Local routing .....	103
8.2.3 Ddynamic routing with IP RIP .....	104
8.2.4 Policy Based Routing .....	108
8.2.5 SYN/ACK speedup .....	109
8.3 Configuration of remote stations .....	109
8.3.1 Name list .....	110
8.3.2 Layer list .....	111
8.4 Establishing connection with PPP .....	113
8.4.1 The protocol .....	114
8.4.2 Everything OK? Checking the line with LCP .....	116
8.4.3 Assigning IP addresses via PPP .....	116
8.4.4 Settings in the PPP list .....	118
8.5 Establishing DSL connection with PPTP .....	119
8.6 Permanent connection for flatrates – Keep-Alive .....	120

8.7	Callback functions .....	122
8.7.1	Callback using Microsoft CBCP.....	122
8.7.2	Fast callback using the ELSA process.....	123
8.7.3	Callback with RFC 1570 (PPP LCP extensions) .....	124
8.7.4	Overview of configuration of callback function .....	124
8.8	Channel bundling with MLPPP .....	125
<b>9</b>	<b>Technical data .....</b>	<b>129</b>
9.1	Performance data and specifications .....	129
9.2	Contact assignment .....	131
9.2.1	Ethernet ports 10/100Base-T (LAN) and 10Base-T (WAN).....	131
9.2.2	ISDN S <sub>0</sub> interface .....	131
9.2.3	Configuration interface(outband) .....	132
<b>10</b>	<b>Appendix .....</b>	<b>133</b>
10.1	Warranty conditions .....	133
10.2	Declaration of conformity European Union (CE) .....	134
<b>11</b>	<b>Index .....</b>	<b>135</b>



## 1

# Introduction

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

New technologies are eliminating the restrictions and are offering the user true broadband communications at significantly higher transfer speeds. An important criterion for the spread of these new access technologies is their availability in as many offices and private households as possible. One new technology is transmission by DSL, which covers the "last mile" over conventional copper wires. Domestic cable TV connections can also be used to realize a broadband connection to the Internet.

A *ELSA LANCOM DSL Office* can work with virtually any high-speed DSL or cable-TV Internet connection. The actual Internet access is always performed via a modem which is connected to the router.

## This chapter...

...will briefly introduce the functions and areas of application of routers. Next, you will receive an overview of the capabilities of your *ELSA LANCOM DSL Office*. 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.

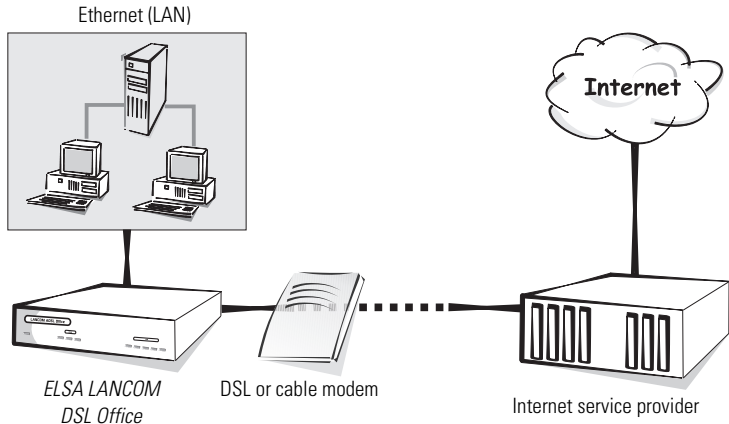
## 1.1

## 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.

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

With these performance values, an *ELSA LANCOM DSL Office* is especially suitable for high-speed Internet access. 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.



The router is incorporated into the network in the same way as any normal PC. Any data traveling on the network cable, therefore, is seen by the router too. It automatically determines whether or not the data needs to be transmitted to another network.

## 1.2 Typical applications

### 1.2.1 Internet on the LAN

Many companies are experiencing an increasing demand for Internet access from all workstations on the LAN. Online research, e-mail and file transfer 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 functions such as IP masquerading and Firewall filter shielding your network against access from the outside.

## 1.2.2

### LAN to LAN coupling

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

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

*ELSA LANCOM  
DSL/I-10 Office  
only*

A direct LAN-LAN coupling can be realized via ISDN using your *ELSA LANCOM DSL/I-10 Office*.

## 1.2.3

### Telecommuting with remote access

*ELSA LANCOM  
DSL/I-10 Office  
only*

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. Even with remote access an *ELSA LANCOM DSL Office* naturally enables a high degree of protection for your company's internal data stocks: the callback function uses the names and call numbers entered to provide access to specified users only. And telephone charges are calculated at head office, simplifying the billing process.

Remote access connections can be realized via the ISDN interface of the *ELSA LANCOM DSL/I-10 Office*.

## 1.2.4

### Office communications

*ELSA LANCOM  
DSL/I-10 Office  
only*

Faxing directly from within applications, answer-phone with different outgoing messages according to the time of day, banking without having to leave the office: these functions are made possible by using the *ELSA LANCAPI*.

The *ELSA 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.

The *ELSA LANCOM DSL/I-10 Office* provides office communications functions via its ISDN interface.

## 1.3

### What does the *ELSA LANCOM DSL Office* offer?

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

#### 1.3.1

### All devices of the *ELSA LANCOM DSL Office* series

#### Easy installation

- Connect the *ELSA LANCOM DSL Office* to the power supply
- Establish a link to the LAN
- Connect the device to the DSL or cable modem
- Connect the ISDN cable (*ELSA LANCOM DSL/I-10 Office* only)
- Switch it on
- Installing the ELSA software and basic configuration using the convenient wizards
- Go!

#### LAN connection

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

#### WAN connection

The *ELSA LANCOM DSL Office* can be connected to the Ethernet interface of a DSL or cable modem.

An *ELSA LANCOM DSL/I-10 Office* is also equipped with an ISDN connection, which is connected to the  $S_0$  port(s) of an ISDN (multi-device connection (point-to-multipoint configuration) or a system connection (point-to-point configuration)). The router automatically detects your ISDN port type and the D-channel protocol being used.

#### IP routing: Line connection and management

The router checks all IP packets 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.

### Security functions

The *ELSA LANCOM DSL Office* has powerful security functions to prevent intruders from accessing company networks. IP masquerading hides all of the workstations of a LAN behind a single public IP address. Their true identities remain masked. Firewall filters permit specific IP addresses, protocols and ports to be blocked. With MAC address filters it is also possible to specifically monitor the access of workstations in the LAN to the IP routing function of the device.

Login barring prevents any "brute force attacks" and denies access to the router after a configurable number of login attempts using an incorrect password. This measure effectively protects the configuration of the router against repeated attacks.

### DHCP

Your *ELSA LANCOM DSL Office* provides the following DHCP modes:

- DHCP server, to assign IP addresses
- DHCP relay agent, to forward DHCP requests

By default, the unit uses a sophisticated automatic mode that makes child's play of the installation of the *ELSA LANCOM DSL Office* in new and existing networks.

### 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 in the event of queries for known computer names.

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

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

### **ELSA LANmonitor**

Under Windows operating systems, this tool displays the status of the router on the screen at all times. The most important information for every device in the local network is displayed, such as:

- Connection status for each transmission channel (*ELSA LANCOM DSL/I-10 Office* only)
- Name of the remote site
- The device module (router, *ELSA LANCAP*) connected
- Connection duration and transmission rates
- Excerpts of the device statistics (e.g. PPP negotiation data)

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

### **Status displays**

LED indicators on the front of your device allow you to monitor all LAN and WAN connections, thus simplifying the process of diagnosing any systems failures.

### **Configuration**

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

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

Users of other operating systems use the HTML-based configuration tool with *ELSA WEBconfig*, an SNMP management system, Telnet or any other terminal program.

This means that you can access the device from the LAN, from the WAN, by remote configuration via ISDN (*ELSA LANCOM DSL/I-10 Office* only) or directly via the integrated configuration interface. For configurations from the LAN or WAN, the TFTP transfer protocol is also supported in addition to SNMP.

The integrated setup wizards from *ELSA LANconfig* and *ELSA WEBconfig* help you get the unit operating in a few steps.



## Firmware update

Your device has 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 ELSA homepage and can be loaded via the LAN, the WAN (*ELSA LANCOM DSL/I-10 Office* only) or the configuration interface.

## ELSA FirmSafe

There is no risk involved with loading the new firmware: The ELSA 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.

## Charge monitoring

The charges for Internet usage are calculated by the provider depending on the time used. To avoid unpleasant surprises at the end of the month, you can establish the amount of online time for your Internet connection within a given period (e.g. 600 minutes in 6 days) that will be permitted via the *ELSA LANCOM DSL Office*.

## Statistics

The comprehensive statistics function lets you keep track of your *ELSA LANCOM DSL 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.

## 1.3.2

## Additional functions *ELSA LANCOM DSL/I-10 Office*

The *ELSA LANCOM DSL/I-10 Office* features an ISDN connection, and therefore offers a series of additional functions.

### Multiprotocol router

In addition to IP, other protocols can also be routed via the ISDN interface. This permits the use of the IPX protocol for the coupling of Novell networks, for example.

ELSA routers offer a special feature for the coupling 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 unnecessary connections from being established.

### **Compatibility through PPP**

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

### **Remote configuration using PPP**

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

### **Security functions of the ISDN interface**

To secure the integrated ISDN interface, the *ELSA LANCOM DSL/I-10 Office* uses password protection and caller identification (CLIP) as well as the callback function to restrict connection establishment to previously specified ISDN subscriber numbers. Authentication mechanisms in the PPP round out the security concept.

### ***ELSA LANCAPI and ELSA CAPI Faxmodem***

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

Any workstation which has been integrated into the LAN (Local Area Network) can use *ELSA LANCAPI* to give unlimited access to office communication functions such as fax and eurofile transfer. 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.

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

### **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%.

### **Least-cost routing**

Even if there is a large selection of telecommunications service providers you can always use the cheapest ISDN lines using the least-cost router. You define once which providers have the most favorable charges for your purposes, and the router automatically selects the most economical provider for you, regardless of whether you are using the router or the *ELSA LANCAPI*.

### **Leased-line option**

Network couplings via leased ISDN lines can be realized using the leased-line option.



## 2

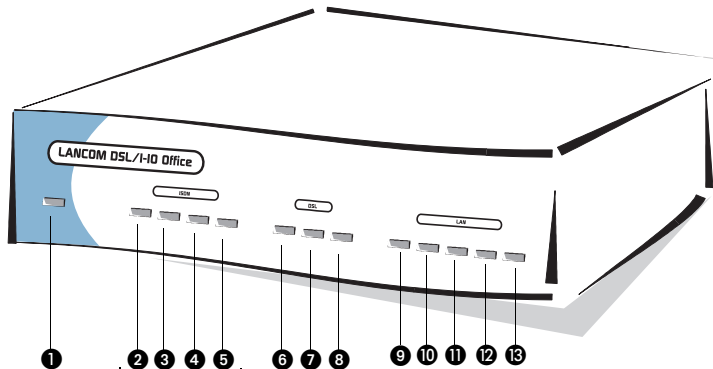
## Introducing the *ELSA LANCOM DSL Office*

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

## 2.1

### The front of the unit

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



these LEDs are only featured on the *ELSA LANCOM DSL/I-10 Office*

#### Meaning of the LEDs

- ❶ **Power/Msg** – The LED on the access point flashes once briefly when the power 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	indication of boot error (coded in flashing); continuous flashing also when time or charge budget limits reached
red		device ready for use

ELSA LANCOM  
DSL/I-10 Office  
only

**② ISDN S<sub>0</sub> status** – shows the condition of the ISDN S<sub>0</sub> connection:

off		not connected or no S <sub>0</sub> voltage (the S <sub>0</sub> voltage is often disabled at ISDN connections after certain length of inactivity)
green	flashing	initializing (establishing contact with the connection point)
green		operational (S <sub>0</sub> bus activated, TEI exists and D channel protocol checked)
green	power off	LED is on, but power LED is off: unit in boot monitor

ELSA LANCOM  
DSL/I-10 Office  
only

**③ ISDN Chan1** – status of the first logical ISDN B-channel (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

ELSA LANCOM  
DSL/I-10 Office  
only

**④ ISDN Chan2** – status of second logical ISDN B-channel (same meaning as for ISDN Chan1)

**⑤ ISDN 1+2** – indicates whether the current ISDN connection is static or using dynamic channel bundling.

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

**⑥ DSL Rx/Tx** – this yellow LED shows the movements of data on the WAN connection (via DSL or cable modem).

**⑦ DSL Link** – this green LED shows that the Ethernet connection between *ELSA LANCOM DSL Office* and the DSL or cable modem is operating properly.

**⑧ DSL Chan** – this LED indicates the status of the WAN connection (via DSL or cable modem) to the provider. The connection to the provider

generally requires a login with a user name and password. Charges are incurred during this time in the case of time-based connection billing. The details of the LED:

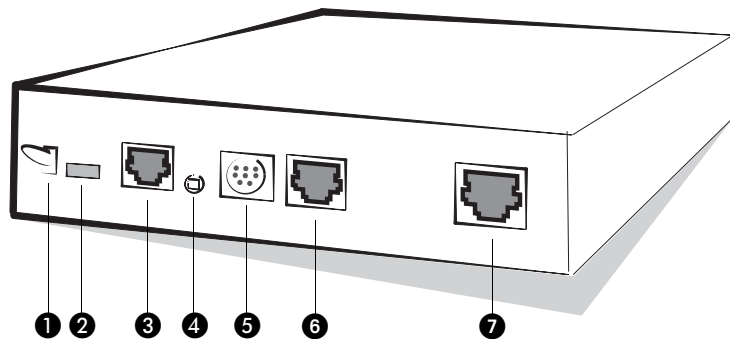
off	no login has been requested at the switching center
red	a login has been requested at the switching center; it is logging in
green	it has successfully logged in and is connected to the provider

- ⑨ **LAN Rx/Tx** – data packet sent from device to the LAN or from the LAN to the device
- ⑩ **LAN Coll** – transmission collision
- ⑪ **LAN Link** – the connection to the LAN has been established and is ready
- ⑫ **LAN FDpx** – the router is transmitting and receiving data simultaneously (full duplex mode)
- ⑬ **LAN Fast** – the device operates in the LAN in 100-Mbit mode

## 2.2

### The back of the unit

The connectors and switches can be found on the back of the device.



An ISDN connection is featured only on the *ELSA LANCOM DSL/I-10 Office*

- ① On/off switch
- ② Connection for power supply unit



*Use the supplied power supply unit only! Using an unsuitable power supply unit may cause damage or injury.*

- ③ 10/100Base-Tx for LAN connections. 10-Mbit and 100-Mbit connections are supported. The *ELSA LANCOM DSL Office* recognizes the network speed automatically (autosensing).
- ④ Node/hub switch – the transmit and receive lines of the LAN connection (③) can be crossed (hub setting) for the direct connection of a PC. The switch should be in the 'Node' position (default setting) when connecting the device to a hub or switch.
- ⑤ V.24 configuration interface
- ⑥ ISDN/S<sub>0</sub> connection (*ELSA LANCOM DSL/I-10 Office* only)
- ⑦ 10Base-T connection for DSL or cable modem

## 3 Installation

This chapter will assist you to install hardware and software as quickly as possible. First, check the package contents and system requirements. The device can be installed and configured quickly and easily if all prerequisites are fulfilled.

### 3.1 Package contents

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

- *ELSA LANCOM DSL Office*
- Power supply unit
- LAN connector cable, green plugs
- WAN connector cable for DSL or cable modem, dark blue plug
- ISDN line connection cable, light blue plug (*ELSA LANCOM DSL/I-10 Office* only)
- Cable for the serial configuration interface
- *ELSA LANCOM Office* CD with *ELSA LANtools* and additional software
- License sticker with software serial numbers
- Printed documentation

If anything is missing, please contact us using the address stated on the delivery slip of the unit.

### 3.2 System requirements

Computers that connect to an *ELSA LANCOM DSL Office* must meet the following minimum requirements:

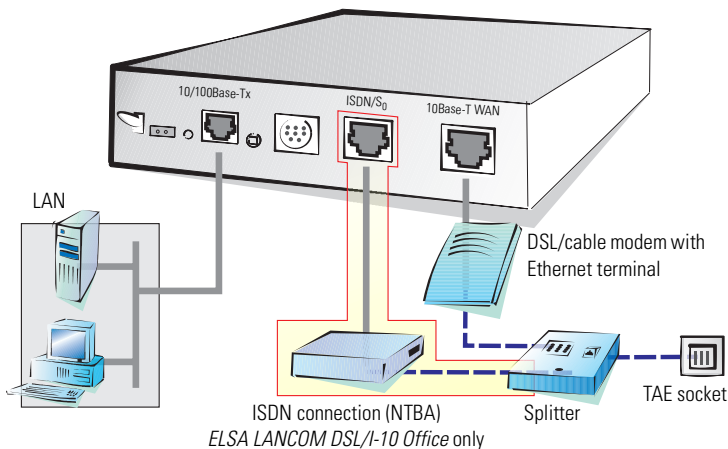
- Any operating system that supports TCP/IP, such as Windows Millennium Edition (Me), Windows 2000, Windows 98, Windows 95, Windows NT, Linux, Apple Mac OS, OS/2, BeOS.
- An Ethernet card must be installed.
- The TCP/IP protocol must be installed.
- A web browser should be installed.

*In addition, the ELSA LANtools and the functions of the ELSA LANCAPI (ELSA LANCOM DSL/I-10 Office only) require a Windows operating system.*



### 3.3 Hardware installation

- ① Connect your *ELSA LANCOM DSL Office* to the LAN. Plug the network cable supplied (green plugs) into the 10/100Base-Tx terminal of the device (③) and into a free network connector on your local network (or into a free socket on a hub in your LAN). Alternatively, you can also connect a single PC. In this case, switch the node/hub selector switch (④) to the 'Hub' position.



- ② Connect your *ELSA LANCOM DSL Office* to the DSL or cable TV network by inserting the WAN connector cable (dark blue plug) in the 10Base-T WAN connection (⑦) of the device. Then connect the other end to the DSL or cable modem.
- ③ Connect your *ELSA LANCOM DSL/I-10 Office* to the ISDN network. Insert one end of the supplied ISDN connector cable (light blue plugs) in the ISDN/S<sub>0</sub> connection (⑥) of the device and the other end in an ISDN/S<sub>0</sub> point-to-point or point-to-multipoint connection.

*ELSA LANCOM  
DSL/I-10 Office  
only*



*Please note that your DSL or cable modem must feature an Ethernet connection (10Base-T). The ELSA LANCOM DSL Office cannot be used with modems that only feature USB or ATM-F connections.*

- ④ Connect the AC adapter to the device and switch it on. After a short device self-test the 'Power/Msg' LED will be permanently lit. The 'LAN Link' LED indicates that your router is correctly connected to the LAN.





*If this LED does not light, actuate the node/hub selector switch (4) at the rear of the device. If the LED still does not light, there may be a problem with the network card or the wiring.*

## 3.4

## Software installation

This section covers the installation of the included ELSA software for Windows. Skip this section if you intend to use your *ELSA LANCOM DSL Office* exclusively with PCs running operating systems other than Windows. In this case, a software installation is not necessary.



*A number of your router's functions require a Windows operating system. These include monitoring with ELSA LANmonitor. In the case of the ELSA LANCOM DSL/I-10 Office, the ELSA LANCAPI functions for the ISDN interface also require a Windows operating system on the workstation PC.*

### 3.4.1

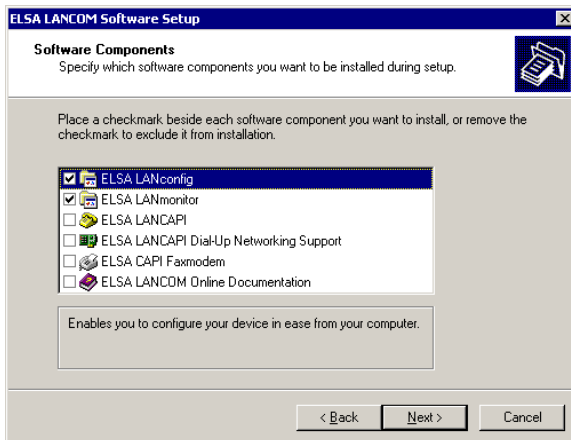
### Starting ELSA Setup

Place the *ELSA LANCOM Office* CD in your CD drive. The ELSA setup program will start automatically. The Autostart feature will not work under Windows NT: in this case, manually launch the AUTORUN.EXE file in the root folder of the CD.



*It will also be necessary to manually launch the AUTORUN.EXE file if you have disabled the CD Autostart function on your PC, or if the ELSA setup program does not start automatically for any other reason.*

In ELSA Setup select **Install LANCOM Software**. The following selection menus will appear on the screen:



### 3.4.2

## Which software should you install?

Not every application listed in the selection menu is required for the operation of your *ELSA LANCOM DSL Office*.

- **ELSA LANconfig** is the configuration program for all *ELSA LANCOM*. *ELSA WEBconfig* can be used alternatively or in addition via a Web browser.
- **ELSA LANmonitor** lets you monitor all *ELSA LANCOM* in the LAN.



*For the following three programs, you need a ELSA LANCOM with an ISDN interface. Of the ELSA LANCOM DSL Office series, only the ELSA LANCOM DSL/I-10 Office features an ISDN interface.*

- **ELSA LANCAPI** permits all Windows PCs in the LAN to use any ISDN software as if they had installed ISDN cards. In actual fact, the ISDN connection is realized centrally using the *ELSA LANCOM* with its ISDN interface.
- **ELSA LANCAPI Dial-Up Networking Support** lets you use the CAPI software interface on your Windows PC as a network adapter, for example for dial-up remote access to an *ELSA LANCOM*.
- The **ELSA CAPI Faxmodem** installs a fax modem driver on your Windows PC, permitting you to send faxes via the *ELSA LANCAPI*.

Select the appropriate software options and confirm your choice with **Next**. The software is automatically installed.

## 3.5

### In the next chapter...

...we will perform the basic configuration of the device. Only a few clicks of the mouse are required to set up your *ELSA LANCOM DSL Office* to provide all of the PCs in your LAN with high-speed Internet access.



## 4

# Basic settings

In this chapter we make the most important basic settings on your *ELSA LANCOM DSL Office*:

- Assignment of an IP address
- Activation of an integrated DHCP server (on request)
- Securing of the configuration access with a password
- Configuring the ISDN interface (only with *ELSA LANCOM DSL/I-10 Office*)
- Setting up the Internet access

## 4.1

### Starting the setup wizard

An unconfigured *ELSA LANCOM DSL Office* can be reached in two convenient ways:

- *ELSA LANconfig* finds an unconfigured *ELSA LANCOM* automatically and starts the setup wizard for the basic settings.
- With *ELSA WEBconfig*: You enter the IP address of the unconfigured *ELSA LANCOM DSL Office* in the address line of a web browser on a PC in the network. In certain network environments you also reach your *ELSA LANCOM DSL Office* by entering any name in the address line. More about this later.



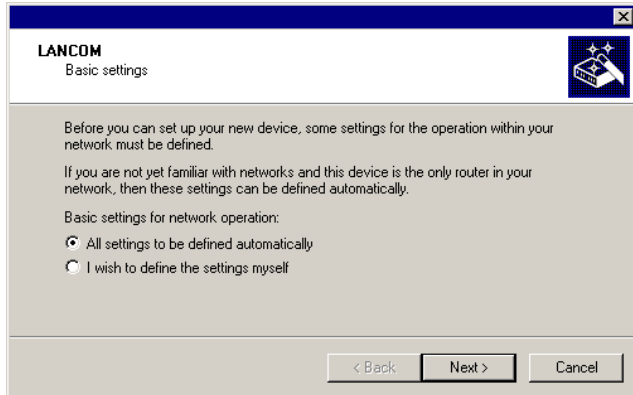
*There should never be several unconfigured ELSA LANCOM in a network. As all unconfigured ELSA LANCOM report under the same IP address (with the end numbers 254), address conflicts result with several devices. To prevent problems, several devices should only be configured consecutively and the respective device should immediately be provided with a unique IP address.*

### 4.1.1

#### Basic settings with *ELSA LANconfig*

- ① Start *ELSA LANconfig* by clicking **Start ► Programs ► ELSAan ► ELSA LANconfig**.

*ELSA LANconfig* automatically detects the new *ELSA LANCOM DSL Office* in the TCP/IP network. Then the setup wizard starts that will help you make the basic settings of the device or will even do all the work for you (provided the suitable network environment exists).



*Should the setup wizard fail to start automatically, please search manually for new devices in the network (**Device ► Find**).*

*This input window only appears when no DHCP server is active in your network and your PC has not been assigned an IP address manually. Otherwise, the wizard runs exactly as described for the entry 'I wish to define the settings myself' in ②.*

Make your selection after the following considerations:

### Select 'All settings to be defined automatically'...

...if you are **not** familiar with networks and IP addresses, and have not used IP addresses in your network up until now. The router as a DHCP server will automatically set and assign the IP addresses for all devices in the LAN.

### Select 'I wish to define the settings myself'...

...if you are familiar with networks and IP addresses and one of the following conditions applies:

- You have not yet used IP addresses in your network but would like to do so starting now. You wish to set the IP address for the router and assign it any 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 (if the DHCP server is enabled).
- You have previously used IP addresses for the computers in your LAN.

- ② If you want to make the IP settings yourself, then give the *ELSA LANCOM DSL Office* an available address from the IP address range used up until now. Confirm your choice with **Next**.
- ③ The IP settings to be made also include the setting as to whether or not the router is to operate as a DHCP server. Make your selection and confirm with **Next**.
- ④ In the following window you define the password for the configuration access. In addition, you specify whether the device is only to be configured from the LAN, or whether remote configuration via a WAN connection (via DSL/cable modem and with *ELSA LANCOM DSL/I-10 Office* also via ISDN) is permitted. Confirm your selection with **Next**.



*Please note that when the remote configuration is enabled, remote configuration from within the Internet also becomes possible. You should always make sure that the configuration access is suitably protected, e.g. with a password.*

- ⑤ The *ELSA LANCOM DSL/I-10 Office* enables the configuration of the ISDN interface now. Confirm your selection with **Next**.
- ⑥ If you want to set the ISDN settings for your *ELSA LANCOM DSL/I-10 Office*, specify a telephone number (as an MSN) under which the device is to accept calls. In addition, you can enter a trunk code for dialing into ISDN. Finally, you should specify whether or not the tariff information is to be transmitted at your ISDN connection. Confirm your choice with **Next**.
- ⑦ Complete the configuration with **Complete**.

## 4.1.2

### Basic settings with *ELSA WEBconfig*

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

There's only one precondition for accessing the router: You must know how to address the unconfigured router in the LAN. An unconfigured *ELSA LANCOM* always reacts to a certain IP address, and in some network configurations even to a name.

### Does my *ELSA LANCOM DSL Office* react to a name?

If you do not yet have a DHCP or DNS server on your LAN, the router reacts to any name (like 'LANCOM' or 'Router') that you specify in the URL address field of a Web browser.



*If you don't know whether IP addresses have been used in your network up until now, display the IP address of your own PC (see the following section). If the 'IP Address' field contains the value '0.0.0.0', the network adapter does not have an IP address yet.*

### What is the IP address of the *ELSA LANCOM DSL Office*?

The IP address of an unconfigured *ELSA LANCOM* results from the IP address of the calling PC by replacing the last number of this IP address (after the third dot) with 254.

For example, if your PC is assigned the IP address 10.0.0.17, then you will find an unconfigured *ELSA LANCOM* under the address 10.0.0.254. The IP address of your PC can be displayed (depending on the operating system) with the following command line commands (entry under Windows at the command prompt):

Operating system	Command in the command line
Windows 95, Windows 98, Windows Me	winipcfg
Windows NT 4.0, Windows 2000	ipconfig
Linux, UNIX	ifconfig

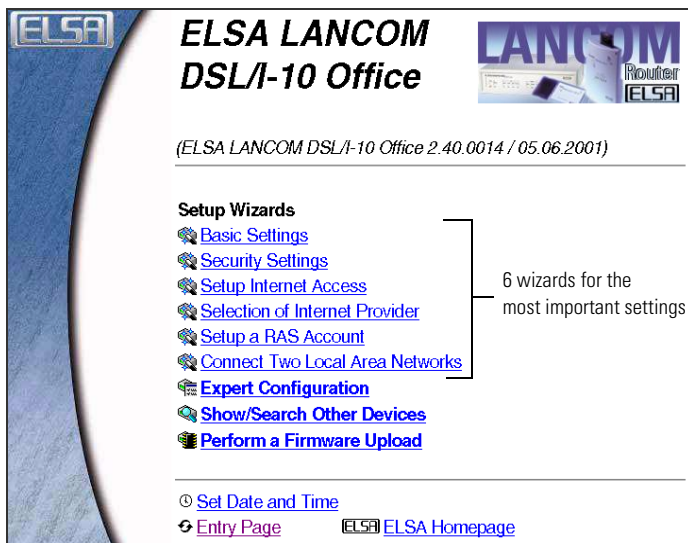
### Starting the wizards in *WEBconfig*

- ① Start your web browser (Internet Explorer, Netscape Navigator) and call the *ELSA LANCOM DSL Office* there:

`http://<IP address of the LANCOM>` (or with any desired name)

The following main menu will be displayed:





*The wizards are tailored to the respective ELSA LANCOM and therefore differ. As a result, your device may not offer all the wizards shown.*

- ② Select **Basic Settings**. The following window offers you the choice between 'Automatically specify IP parameters' and 'Specify IP parameters yourself'.



*This selection only appears if no DHCP server is active in your network and your PC has not been assigned an IP address. Otherwise, the wizard runs exactly as described from step ④.*

- ③ Make your selection after the following considerations:

#### **Activate 'Automatically specify IP parameters'...**

...if you are **not** familiar with networks and IP addresses, and have not used IP addresses in your network up until now. The router as a DHCP server will automatically set and assign the IP addresses for all devices in the LAN.

#### **Deactivate 'Automatically specify IP parameters'...**

...if you are familiar with networks and IP addresses and one of the following conditions applies:

- You have not yet used IP addresses in your network but would like to do so starting now. 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.x' 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 switched on).
- You have previously used IP addresses for the computers in your LAN. Assign the new device a free address from the previously used address range. Also specify whether or not the device is to operate as a DHCP server in the LAN.

- ④ If you want to make the IP settings yourself, then give the *ELSA LANCOM DSL Office* an available address from the IP address range used up until now. Also set whether or not it is to operate as a DHCP server. Confirm your entry with **Set**.
- ⑤ In the following window 'Security settings' you define the password for the configuration access. In addition, you specify whether the device is only to be configured from the LAN, or whether remote configuration via a WAN connection (via DSL/cable modem and with *ELSA LANCOM DSL/I-10 Office* also via ISDN) is permitted. Confirm your selection with **Set**.



*Please note that when the remote configuration is enabled, remote configuration from within the Internet also becomes possible. You should always make sure that the configuration access is suitably protected, e.g. with a password.*

- ⑥ The online help for *ELSA WEBconfig* is available for direct use at the ELSA website on the Internet. As an alternative, the contents of the online help can be copied to a file server in the LAN or locally to the configuration PCs as HTML files. The location of the online help is specified as a URL path.

If you accept the default path, the *ELSA LANCOM DSL Office* loads the help texts from the ELSA website as required. However, if you also want to access the help texts without an active Internet connection, then change the path accordingly. For additional information on this subject, see the section 'The ELSA WEBconfig help files (HTTP module)' on page 40.

With an *ELSA LANCOM DSL/I-10 Office* you have the possibility to configure the ISDN interface now. Confirm your selection with **Set**.

- ⑦ If you have requested the configuration of the ISDN connection, you will then be asked whether the tariff information is to be transmitted on your ISDN connection. Select DSS1 and confirm your choice by clicking **Set**.
- ⑧ When *ELSA WEBconfig* signals the acceptance of the entries, the basic configuration is complete.

## 4.2 Set up access to the Internet

A separate wizard is available for setting up the Internet access. It is started as follows:

### 4.2.1 Start the wizard under *ELSA LANconfig*

- ① Select your *ELSA LANCOM DSL Office* in the selection window.
- ② With the command **Extras ► Setup wizard** you open the menu with the available wizards. Select **Set up Internet access**.

### 4.2.2 Start the wizard under *ELSA WEBconfig*

The Internet access wizard is started directly in the main menu of *ELSA WEBconfig*.

### 4.2.3 Entering access data

The Internet access wizard will ask you step by step for all necessary data for connecting to the Internet. The connection data have been specified by your Internet Service Provider.

## 4.3 Settings to workstation PCs

Depending on the method with which IP addresses are assigned in your LAN, the following settings must be made on the PCs in the LAN for the Internet access:

- **DHCP assignment via the *ELSA LANCOM DSL Office* (normal case)**

The *ELSA LANCOM DSL Office* also transmits its own IP address as a standard gateway and DNS server to the PCs via DHCP. The workstation PCs must be configured so that they automatically obtain their own IP

address and the IP addresses of the standard gateway and DNS server (via DHCP).

- **DHCP assignment via a separate DHCP server**

The workstation PCs must be configured so that they automatically obtain their own IP address and the IP addresses of the standard gateway and DNS server (via DHCP). The IP address of the *ELSA LANCOM DSL Office* must be saved on the DHCP server so that the DHCP server transmits it to the PCs in the LAN as the standard gateway. In addition, the DHCP server should also specify the *ELSA LANCOM DSL Office* as a DNS server.

- **Manual IP address assignment**

If the IP addresses in the network are assigned statically, then the IP address of the *ELSA LANCOM DSL Office* must be set in the TCP/IP configuration as the standard gateway and as a DNS server.

*Additional information and assistance on the TCP/IP settings of your PC is contained in the documentation of your operating system.*



## 4.4

### That's it!

By clicking a few buttons, you have completed the configuration of the *ELSA LANCOM DSL Office* for Internet access. From now on all computers in your LAN can surf through the Internet at top speed...

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

Of course, you can also configure a large number of additional settings. For a detailed description of these options, please refer to the following chapters.

## 5

# Configuration and management

This section will show you the methods and routes you can use to access the device and specify further settings. You will find descriptions on the following topics:

- Configuration tools
- Monitoring and diagnosis functions of the device and software
- Backup and restoration of entire configurations
- Installation of new firmware in the device

## 5.1

### Configuration tools and approaches

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

An *ELSA LANCOM DSL Office* can be accessed via up to three different options:

- Through the configuration interface (config interface) on the rear of the router (also known as outband)
- Through the connected network (LAN as well as WAN—inband)
- Remote configuration via the ISDN connection (only with *ELSA LANCOM DSL/I-10 Office*)

#### What is the difference between these three possibilities?

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

On the other hand, whether or not you will need additional hardware and software: The inband configuration requires one of the computers already available in the LAN or WAN, as well as only one suitable software, such as *ELSA LANconfig* (see following section). In addition to the configuration software, the outband configuration also requires one of the computers (with a serial port). The preconditions are most extensive for remote configuration: In addition to the ISDN connection on the *ELSA LANCOM DSL Office* (only present on *ELSA LANCOM DSL/I-10 Office*), an ISDN card, an ISDN adapter or access via *ELSA LANAPI* to another *ELSA LANCOM* with an ISDN port is also required in the configuration PC.

## 5.2 Configuration software

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

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

- **ELSA LANconfig** – nearly all parameters of the *ELSA LANCOM DSL Office* can be set quickly and with ease using this menu-based application. Outband, inband and remote configuration are supported.
- **ELSA WEBconfig** – this software is permanently installed in the router. All that is required on the workstation used for the configuration is a web browser. *ELSA WEBconfig* is thus independent of operating systems. Inband and remote configuration are supported.
- **SNMP** – device-independent programs for the management of IP networks are generally based on the SNMP protocol. It is possible to access the *ELSA LANCOM DSL Office* inband and via remote configuration using SNMP.
- **Terminal program, Telnet** – a *ELSA LANCOM DSL Office* can be configured with a terminal program via the config interface (e.g. HyperTerminal) or within an IP network (e.g. Telnet).
- **TFTP** – the file transfer protocol TFTP can to a limited extent also be used within IP networks (inband and remote configuration).



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

### 5.2.1 Configuration using **ELSA LANconfig**

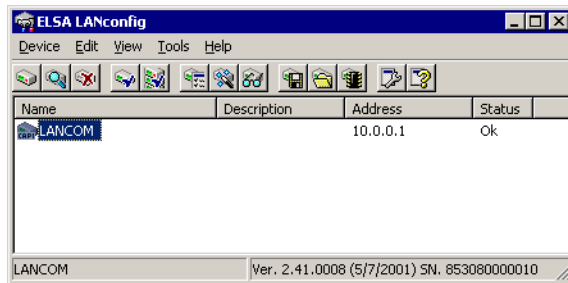
Start *ELSA LANconfig* e.g. via the Windows taskbar with **Start ► Programs ► ELSAan ► ELSA LANconfig**. *ELSA LANconfig* searches the local area network for devices. *ELSA LANconfig* will automatically launch the setup wizard if a device which has not yet been configured is found on the local area network. For the description of the basic configuration using the setup wizard, please refer to the section 'Basic settings with ELSA LANconfig' on page 29.

## Find new devices



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

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



## The expanded range of functions for professionals

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 integrated Help function

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



## 5.2.2

### Configuration using *ELSA WEBconfig*

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

#### Functions with any web browser

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

A LAN connection via TCP/IP (PPP for remote configuration) must be established to use *ELSA WEBconfig*. The *ELSA WEBconfig* is accessed via the IP address of the *ELSA LANCOM DSL Office* (or in a suitable network environment also via any name).

The section 'Basic settings with *ELSA WEBconfig*' on page 31 covers accessing an unconfigured device for the first time using *ELSA WEBconfig* and performing the basic configuration.

#### The *ELSA WEBconfig* help files (HTTP module)

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

This link points to help files in HTML format. In its default setting the Help link points to the *ELSA* web site.

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

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

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



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

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

- Specify the path only up to the directory containing the complete help files structure.

For example, if you have created the help files structure '500\2\1611\1' in the local directory 'C:\ELSA\HTMLRef', then specify 'file://C:/ELSA/HTMLRef' as the document root.

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

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

Instead of the placeholder <IP address>, either the valid IP address of the HTTP server in the format 'x.x.x.x' is expected, e.g. '128.7.9.155', or a server name, e.g. 'www.elsa.com'.

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



## 5.2.3

### Configuration using Telnet

Start configuration using Telnet, e.g. from the Windows command line with the command:

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

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

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

## TFTP

Certain functions cannot be run at all, or not satisfactorily, with Telnet. These include all functions in which entire files are transferred, for example the uploading of firmware or the saving and restoration of configuration data. In this case TFTP is used.

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

The syntax of the TFTP call is dependent on the operating system. With Windows 2000 and Windows NT the syntax is:

```
tftp -i <IP address host> [get|put] Source [Target]
```

*With numerous TFTP clients the ASCII format is preset. Therefore, for the transfer of binary data (e.g. firmware) the binary transfer must usually be explicitly selected. This example for Windows 2000 and Windows NT shows you how to achieve this by using the '-i' parameter.*



### 5.2.4

## 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.

There are a number of configuration and management programs that run via SNMP. Commercial examples are Tivoli, OpenView from Hewlett-Packard, SunNet Manager and CiscoWorks. In addition, numerous programs also exist as freeware and shareware.

Your *ELSA LANCOM DSL Office* can export a so-called device MIB file (**M**anagement **I**nformation **B**ase) for use in SNMP programs.

Configuration tool	Call
<i>ELSA WEBconfig</i>	Call SNMP device MIB (in main menu)
TFTP	tftp 10.0.0.1 get readmib file1

### 5.3

## Remote configuration via Dial-Up Network



*The entire section for remote configuration only applies to ELSA LANCOM with an ISDN interface. From the device series ELSA LANCOM DSL Office only the ELSA LANCOM DSL/I-10 Office meets this requirement.*

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

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

### 5.3.1

## This is what you need for remote configuration

- An *ELSA LANCOM DSL Office* with an ISDN connection
- A computer with a PPP client, e.g. Windows Dial-Up Network
- A program for inband configuration, e.g. *ELSA LANconfig* or Telnet
- A configuration PC with ISDN card, ISDN adapter or an *ELSA LANCOM* with an ISDN connection and *ELSA LANCAPi*.

### 5.3.2

## The first remote connection using a Dial-Up Network

- ① In the *ELSA LANconfig* program select **Device ► New**, enable 'Dial-Up Network' as the connection type and enter the calling number of the WAN interface to which the *ELSA LANCOM DSL/I-10 Office* is connected. If you wish, you can also enter the time period after which an idle connection is to be disconnected automatically.
- ② *ELSA LANconfig* now automatically generates a new entry in the Dial-Up Network. Select a device that supports PPP (e.g. the NDIS-WAN driver included with the *ELSA LANCAPi*) for the connection and press **OK** to confirm.
- ③ Then the *ELSA LANconfig* program will display a new device with the name 'Unknown' and the dial-up call number as the address in the device list.

*When an entry in the device list is deleted, the related connection in the Windows Dial-Up Network is also deleted.*



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

### 5.3.3

#### The first remote connection using a PPP client and Telnet

- ① Establish a connection to the *ELSA LANCOM DSL/I-10 Office* with your PPP client using the following details:
  - User name 'ADMIN'
  - Password as set on the *ELSA LANCOM DSL/I-10 Office*, factory default setting is no password
  - An IP address for the connection, only if required
- ② Open a Telnet session to the *ELSA LANCOM DSL/I-10 Office*. Use the following IP address for this purpose:
  - '172.17.17.18', if you have not defined an IP address for the PPP client. The *ELSA LANCOM DSL/I-10 Office* automatically uses this address if no other address has been defined. The calling PC then responds to the IP address '172.17.17.17'.
  - Raise the IP address of the PC by one, if you have defined an address. For example: If you have defined the IP address '10.0.200.123' for the PPP client, the *ELSA LANCOM DSL/I-10 Office* will respond to '10.0.200.124'. Exception: If the digits '254' are at the end of the IP address, the router responds to 'x.x.x.1'.
- ③ You can configure the *ELSA LANCOM DSL/I-10 Office* remotely just like all other devices.

### 5.3.4

#### Limiting remote configuration

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

You may, however, want to change the default layer for LAN-to-LAN connections, for example, to a different protocol after the first configuration run. Then the device will no longer take calls on the dial-up connection using the PPP settings. The solution to this is to agree upon a special calling number

for configuration access. If the device receives a call on this number, it will always use PPP, regardless of any other settings made on the router. Only a specific user name which is automatically entered by the *ELSA LANconfig* program during call establishment will be accepted during the PPP negotiations.

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

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

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

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

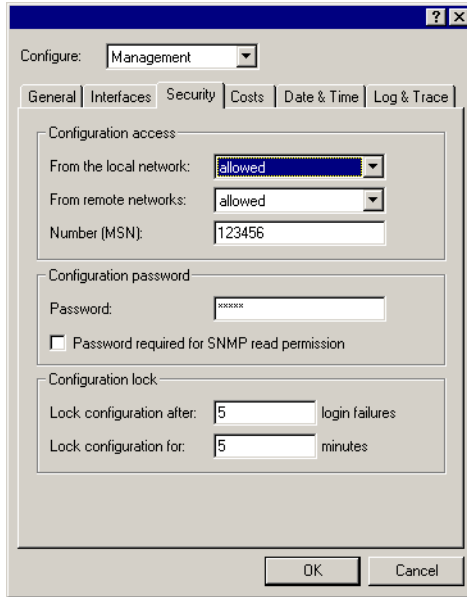
- ③ In the 'Configuration access' field, enter a calling number of your connection which is not used for other purposes as the calling number.

Alternatively, enter the following command:

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

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





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

```
passwd
```

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

## 5.4 ***ELSA LANmonitor***—know what's happening

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

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

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

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

functions are also available in the *ELSA LANmonitor*, such as the enabling of an additional charge limit.



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

## 5.4.1

### Extended display options

Under **View ► Display** you can activate and deactivate the following display options:

- Fault messages
- Diagnosis messages
- System information



*Many important details on the status of the ELSA LANCOM DSL Office are not displayed until the display of the system information is activated. These include, for example, the ports and the charge management. Therefore, we recommend that interested users activate the display of the system information.*

## 5.4.2

### Monitor Internet connection

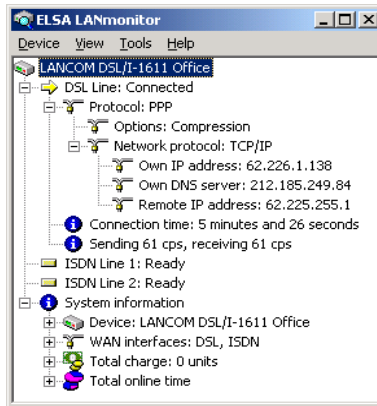
To demonstrate the functions of *ELSA LANmonitor*, we will first show you the types of information *ELSA LANmonitor* provides about connections being established to your Internet provider.

- ① Start up *ELSA LANmonitor* by clicking **Start ► Programs ► ELSA LAN ► 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 as well.

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

- ② *ELSA LANmonitor* automatically creates a new entry in the device list and initially displays the status of the transfer channels. Start your Web 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 communication channel entry indicates that further information on this channel is available. Click on the plus sign to open a tree structure in which you can view various information.



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

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

- ③ To break the connection manually, click on the active channel with the right mouse button. You may be required to enter a configuration password.
- ④ 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.

## 5.5 Trace outputs—Information for pros

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





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

## 5.5.1

### How to start a trace

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

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

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

This code...	... in combination with the trace causes the following:
?	Displays a help text
+	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
IPX-router	IPX routing
PPP	PPP protocol negotiation
SAP	IPX Service Advertising Protocol
IPX-watchdog	IPX watchdog spoofing
SPX-watchdog	SPX watchdog spoofing
LCR	Least-cost router
Script	Script negotiation
RIP	IPX Routing Information Protocol
IP router	IP routing
IP RIP	IP Routing Information Protocol

This parameter...	... brings up the following display for the trace:
ARP	Address Resolution Protocol
ICMP	Internet Control Message Protocol
IP masquerading	Processes in the masquerading module
DHCP	Dynamic Host Configuration Protocol
NetBIOS	NetBIOS management
DNS	Domain Name Service Protocol
Packet dump	Display of the first 64 bytes of a package in hexadecimal form
D-channel dump	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

This code...	... in combination with the trace causes the following:
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

## 5.6

### Saving and restoring the configuration

The current configuration of an *ELSA LANCOM DSL Office* can be saved as a file and reloaded in the device (or in another device of the same type) if necessary.

#### Backup copies of configuration

With this function you can create backup copies of the configuration of your *ELSA LANCOM DSL Office*. Should your *ELSA LANCOM DSL Office* (e.g. due to a defect) lose its configuration data, you simply reload the backup copy.

#### Convenient series configuration

However, even when you are faced with the task of configuring several *ELSA LANCOM DSL Office* of the same type, you will come to appreciate the function for saving and restoring configurations. In this case you can save a great deal of work by first importing identical parameters as a basic configuration and then only making individual settings to the separate devices.

## Running function

Configuration tool	Run command
<i>ELSA LANconfig</i>	Edit ► Save configuration as file Edit ► Restore configuration from file
<i>ELSA WEBconfig</i>	Save configuration/ load configuration (in main menu)
TFTP	tftp 10.0.0.1 get readconfig file1 tftp 10.0.0.1 put file1 writeconfig

## 5.7

## New firmware with ELSA FirmSafe

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

### 5.7.1

### This is how ELSA FirmSafe works

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

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

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

- 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.

## 5.7.2

### How to load new software

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

- *ELSA LANconfig*
- *ELSA WEBconfig*
- Terminal program
- TFTP



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

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

#### ***ELSA LANconfig***



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

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

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

### ***ELSA WEBconfig***

Start *ELSA WEBconfig* in your web browser. On the starting page, follow the **Upload new Firmware** link. In the next window you can browse the folder system to find the firmware file and click **Upload** to start the installation.

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

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

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

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

### **TFTP**

TFTP can be used to install new firmware on *ELSA LANCOM DSL Office*. This can be done with the command (or target) **writeflash**. For example, to install new firmware in a *ELSA LANCOM DSL Office* with the IP address 10.0.0.1, enter the following command under Windows 2000 or Windows NT:

```
tftp -i 10.0.0.1 put Lc_16xxu.240 writeflash
```

## 6 Security

This chapter covers an important topic: safety. The description of the security settings is divided into the following sections:

- Protection for the configuration
  - Password protection
  - Login-lock
  - Access verification
- Protection for the LAN
  - IP masquerading
  - Data packet filtering
- Protection of the ISDN connection (only *ELSA LANCOM DSL/I-10 Office*)

At the end of the chapter you will find the most important security settings as a checklist. With it you can be quite sure that your *ELSA LANCOM DSL Office* is excellently protected.

### 6.1 Protection for the configuration

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

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

#### 6.1.1 Password protection

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

##### Tips for proper use of passwords

We would like to give you a few tips here for using passwords:

- **Keep a password as secret as possible.**  
Never write down a password. For example, the following are popular but completely unsuitable: Notebooks, wallets and text files in computers. It

sounds trivial, but it can't be repeated often enough: don't tell anyone your password. The most secure systems surrender to talkativeness.

- **Only transmit passwords in a secure manner.**

A selected password must be reported to the other side. To do this, select the most secure method possible. Avoid: Unprotected e-mail, letter, fax. It is better to convey a password personally while alone with the other person. The maximum security is achieved when you personally enter the password at both ends.

- **Select a secure password.**

Use random strings of letters and numbers. Passwords from common language usage are not secure. Special characters such as '&'?'#-\*+\_:;,!'°' also make it more difficult for attackers to guess your password and increase the security of the password.

- **Never use a password twice.**

If you use the same password for several purposes, you reduce its security effect. If the other end is not secure, you also endanger all other connections for which you use this password at once.

- **Change the password regularly.**

Passwords should be changed as frequently as possible. This requires effort, however considerably increases the security of the password.

- **Change the password immediately if you suspect someone else knows it.**

If an employee with access to a password leaves the company, it is high time to change this password. A password should also always be changed when there is the slightest suspicion of a leak.

If you comply with these simple rules, you will achieve the highest possible degree of security.

## Entering the password

The field for entering the password is located in *ELSA LANconfig* in the 'Management' configuration area on the 'Security' tab. Under *ELSA WEBconfig* you run the wizard **Security settings**. In a terminal or Telnet session you set or change the password with the command `passwd`.

Configuration tool	Run command
<i>ELSA LANconfig</i>	Management ► Security ► Password
<i>ELSA WEBconfig</i>	Security settings
Terminal/Telnet	<code>passwd</code>



## Protecting the SNMP access

At the same time you should also protect the SNMP read access with a password. For SNMP the general configuration password is used.

Configuration tool	Run command
<i>ELSA LANconfig</i>	Management ► Security ► Only permit SNMP read access with password
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► SNMP module ► Passw. required for SNMP read access
Terminal/Telnet	setup/SNMP module/passw. prompt

### 6.1.2

## Login barring

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

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

If barring is activated on one port, all other ports are automatically barred as well.

The following entries are available in the configuration tools to configure Login barring:

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

Configuration tool	Run command
<i>ELSA LANconfig</i>	Management ► Security
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► Config module
Terminal/Telnet	Setup/config module

### 6.1.3

## Access control via TCP/IP

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

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

Configuration tool	Run command
<i>ELSA LANconfig</i>	TCP/IP ► General ► Access list
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► TCP/IP-module ► Access list
Terminal/Telnet	/setup/TCP-IP-module/access list

## 6.2

## Protection for the LAN

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

- IP masquerading (also known as NAT/PAT)
- Data packet filtering – firewall

### 6.2.1

## 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, for example, the WWW from his workstation and be able to fetch bang up-to-date information for his work.

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

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

### 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 any new port 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.

### Configuration of IP masquerading

The use of IP masquerading is set individually for each route in the routing table. The routing table can be reached as follows:

Configuration tool	Run command
<i>ELSA LANconfig</i>	IP router ► Routing ► Routing table
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► IP-router-module ► IP-routing-tab
Terminal/Telnet	/setup/IP-router-module/IP-routing-tab

### 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 **Masquerading** option in the routing table to inform the router which of the two addresses to use when transferring the packets.

- 'Off': No masquerading.
- 'Dynamic': This entry requests a random IP address valid in the Internet from your provider which is then used for the connection and masquerading.
- 'Static': This entry requests a specific IP address from your provider which is then used for the connection and masquerading. You enter the desired IP address in the following field:

<i>ELSA LANconfig</i>	TCP/IP ► General ► Internet IP address
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► TCP/IP-module ► IP-address
Terminal/Telnet	/Setup/TCP/IP-module/IP-address

### Unmasked Internet access for individual devices

If a certain address is requested by the provider (masquerading option 'stat'), there are two methods for 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 incomplete network mask, e.g. 255.255.255.248 (for 4 IP addresses): 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.

Example: You are assigned the IP network address 123.45.67.0 with the net mask 255.255.255.248 by the provider. Then you can distribute the IP addresses as follows:

IP address	Meaning/use
123.45.67.0	Network address
123.45.67.1	<i>ELSA LANCOM DSL Office</i> as a router for the LAN
123.45.67.2	Additional device in the LAN which is to receive unmasked access to the Internet, e.g. web server
123.45.67.3	Broadcast address

All other computers and devices in the LAN have no public IP address, and therefore appear with the IP address of the *ELSA LANCOM DSL Office* (123.45.67.1) in the Internet.

### Simple and inverse masquerading

This masquerading operates in both directions: The local network behind the IP address of the router is masked if a computer from the LAN sends a packet to the Internet (simple masquerading).

If, on the other hand, a computer sends a packet from the Internet to, for example, an FTP server on the LAN, from the point of view of this computer the router appears to be the FTP server. The router reads the IP address of the FTP server in the LAN from the entry in the service table. The packet is forwarded to this computer. All packets that come from the FTP server in the LAN (answers from the server) are hidden behind the IP address of the router.

The only small difference is that:

- Access to a service (port) in the intranet from outside must be defined in advance by specifying a port number. The destination port is specified with the Intranet address of, for example, the FTP server, in a service table to achieve this.
- When accessing the Internet from the LAN, on the other hand, the router itself makes the entry in the port and IP address information table.

The table concerned can hold up to 2048 entries, that is it allows 2048 **simultaneous** transmissions between the masked and the unmasked network.

After a specified period of time, the router, however, assumes that the entry is no longer required and deletes it automatically from the table.

## Configuration of the inverse masquerading

Configuration tool	Run command
<i>ELSA LANconfig</i>	IP-router ► Masq. ► Service-table
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► IP-router-module ► Masquerading ► Service table
Terminal/Telnet	/Setup/IP-router-module/masquerading/ service table

### Which protocols can be transmitted using IP masquerading?

Naturally, only those which also communicate using ports. Protocols working without port numbers or using ports above IP in the OSI model cannot be masked without special treatment.

The current version of router implements masquerading for the following protocols:

- TCP (and all protocols based on it such as FTP, HTTP, etc.)
- UDP
- ICMP

## 6.2.2

### Data packet filtering – Firewall

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

#### What can be filtered?

The source and target filters for individual ports or the port ranges are important. In addition, individual protocols or any combinations of protocols (TCP/UDP/ICMP) can be filtered. IP address ranges or entire IP networks are also suitable objects.

In addition to these objects, stations in the LAN can also be selected via their MAC address on the IP level. "MAC" stands for **M**edia **A**ccess **C**ontrol and is the heart of all communication within a LAN. A MAC address is permanently stored in each network adapter. MAC addresses are unique worldwide and unmistakable, similar to serial numbers of devices. The PCs in the LAN can be reliably selected via the MAC addresses in order to grant or deny them specific rights on the IP packet level. MAC addresses are frequently applied



on the outside of the network devices in hexadecimal format (e.g. 00:A0:57:01:02:03).

*Filtering only concerns IP router operation. The access of PCs in the LAN to the ELSA LANCOM (e.g. to the configuration data) cannot be restricted with the firewall rules.*

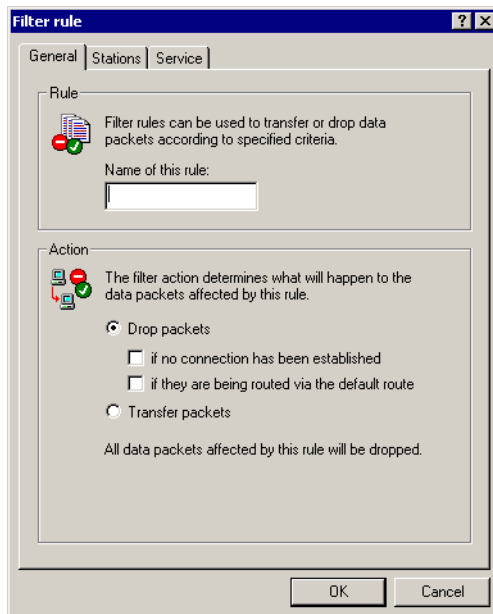
## Setting up the filter

The firewall filters will be configured in the following menus and lists:

Configuration tool	Run command
<i>ELSA LANconfig</i>	IP router ► Filtering ► Add
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► IP router module ► Firewall
Terminal/Telnet	/setup/IP router module/firewall

## Setting up filters under *ELSA LANconfig*

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



- 'General'  
The name of the filter service and what should happen with the data packets (action) are specified here.
- 'Stations'  
The stations for which the filter rule should apply as sender or receiver of the packets are specified here.
- 'Service'  
The IP protocols, source and destination ports to which the filter rule should apply are specified here.

### Setting up filters under *ELSA WEBconfig* or Terminal/Telnet

Configuration via *ELSA WEBconfig* or via a terminal/Telnet connection is somewhat more difficult than in *ELSA LANconfig*.

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

*The filter list cannot be created directly. It is automatically generated from the entries in the object and control table.*



### The object table

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

- protocols
- single computers
- whole networks
- services

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

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



## The rules table

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

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

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

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

all computers:           %A0.0.0.0

all services:            %S0

all protocols:           %P0

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

*During configuration via the console (Telnet or terminal program) the combined parameters (port, destination, source) must each be enclosed in quotation marks (inch marks – ").*

## The filter list

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



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

## 6.3

## Protecting the ISDN connection

For a device with an ISDN connection basically any ISDN subscriber can dial into your *ELSA LANCOM*. To prevent undesired intruders, you must therefore pay particular attention to the protection of the ISDN connection.



*Of the devices of the series ELSA LANCOM DSL Office only the ELSA LANCOM DSL/I-10 Office is equipped with an ISDN connection. The explanations of this section therefore only refer to this device.*

The protection functions of the ISDN connection can be divided into two groups:

- Identification control
  - Access protection using name and password
  - Access protection via caller ID
- Callback to defined call numbers

### 6.3.1

### Identification control

For identification monitoring either the name of the partner or the so-called caller ID can be used. The caller ID is the telephone number of the caller that is normally transmitted to the partner with the call with ISDN.

Which "Identifier" is to be used to identify the caller is set in the following list:

Configuration tool	Run command
<i>ELSA LANconfig</i>	Communication ► Call acceptance
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► WAN module ► Protection
Terminal/Telnet	setup/WAN-module/protection

You have a choice of the following:

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

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

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

### Verification of name

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

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

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

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

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

The PPP list can be found as follows:

Configuration tool	Run command
<i>ELSA LANconfig</i>	Communication ► Protocols ► PPP list
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► WAN module ► PPPI list
Terminal/Telnet	/setup/WAN-module/PPP-list

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



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

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.

### 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 – **C**alling **L**ine **I**dentifier).

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

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

## 6.3.2

### 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.

Configuration tool	Run command
<i>ELSA LANconfig</i>	Communication ► Remote stations ► Name list (ISDN)
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► WAN module ► ISDN name list
Terminal/Telnet	/setup/WAN-module/ISDN-name-list

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

- The router can refuse to call back.
- It can call back using a preset call number.

- First the name can be checked and then a preset telephone number can be called back.
- The caller can opt to specify the call number to be used for callback.

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

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

*For additional information on the callback function, see the section 'Callback functions' on page 122.*



## 6.4

### The security checklist

In the following checklist you will find an overview of the most important security functions. That way you can be quite sure not to have overlooked anything important during the security configuration of your *ELSA LANCOM DSL Office*.

#### ☐ **Have you assigned a password for the configuration?**

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 field for entering the password is contained in *ELSA LANconfig* in the 'Management' configuration area on the 'Security' tab. It is particularly advisable to assign a password to the configuration if you want to allow remote configuration.

#### ☐ **Have you permitted remote configuration?**

If you do not require remote configuration, then deactivate it. If you require remote configuration, then be sure to assign a password protection for the configuration (see previous section). The field for deactivating the remote configuration is also contained in *ELSA LANconfig* in the 'Management' configuration area on the 'Security' tab.

○ **Have you provided the SNMP configuration with a password?**

Also protect the SNMP configuration with a password. The field for protection of the SNMP configuration with a password is also contained in *ELSA LANconfig* in the 'Management' configuration area on the 'Security' tab.

○ **Have you allowed remote access?**

If you do not require remote access, deactivate call acceptance by deactivating a 'call acceptance by number' and leaving the number list blank in *ELSA LANconfig* in the 'Communication' configuration area on the 'Call acceptance' tab.

○ **Have you activated the callback options for remote access and is CLI activated?**

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 – **C**alling **L**ine **I**dentifier). 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 (this callback via the D-channel is not supported by the Windows dial-up network). If the *ELSA LANCOM DSL Office* is set to provide security using the telephone number, any calls from remote stations with unknown numbers are denied access.

○ **Have you activated IP masquerading?**

IP masquerading is the hiding place for all local computers for connection to 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. The router separates Internet and intranet, as if by a wall. The use of IP masquerading is set individually for each route in the routing table. The routing table can be found in the *ELSA LANconfig* in the 'IP router' configuration section on the 'Routing' tab.

○ **Have you closed critical ports with filters?**

The firewall filters of the *ELSA LANCOM DSL Office* devices offer filter functions for individual computers or entire networks. Source and target filters can be set for individual ports or for ranges of ports. In addition, individual protocols or any combinations of protocols (TCP/UDP/ICMP) can be filtered. It is particularly easy to set up the filters with *ELSA LANconfig*. The 'Filter' tab under 'IP-Router' can assist you to define the filter rules.

*ELSA LANCOM  
DSL/I-10 Office  
only*

*ELSA LANCOM  
DSL/I-10 Office  
only*

○ **Have you excluded certain stations from access to the router?**

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

○ **Is your saved LANCOM configuration stored in a safe place protected from unauthorized access?**

Protect the saved configurations against unauthorized access in a safe place. A saved configuration could otherwise be loaded in another device by an unauthorized person, enabling, for example, the use of your Internet connections at your expense.





# 7

## Server services for the LAN

An *ELSA LANCOM DSL Office* offers a number of services for the PCs in the LAN. These are central functions that can be used by workstation computers. They are in particular:

- Automatic address administration with DHCP
- Name management of computers and networks with DNS
- Logging of network traffic with SYSLOG
- Recording of charges
- Office communication functions with *ELSA LANCAPI* (only *ELSA LANCOM DSL/I-10 Office*)

### 7.1

### Automatic IP address administration with DHCP

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

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

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

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

#### 7.1.1

#### The DHCP server

As a DHCP server, the *ELSA LANCOM DSL 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
- Netw mask
- Broadcast address
- Standard gateway
- DNS server

- NBNS
- 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.

## 7.1.2

### 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 servers within the local network. This search can be recognized by the LAN-Rx/Tx LED flashing momentarily after activation.
  - The device then disables its own DHCP server if at least one other DHCP server is 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'.

### 7.1.3

## 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.

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

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



### Netmask assignment

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

### Broadcast address assignment

In general, 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!*

### Standard gateway assignment

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

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

### 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.

### Period of validity for an assignment

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

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

- **Maximum lease time in minutes**

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

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

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

- **Default lease time in minutes**

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

### **Priority for the DHCP server—request assignment**

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

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

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

### **Priority for computer—overwriting an assignment**

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

Under Windows 98, 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.

### Checking of IP addresses in the LAN

Configuration tool	Run command/Table
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► DHCP module ► Table-DHCP
Terminal/Telnet	setup/DHCP module/DHCP table

The DHCP table provides a list of the IP addresses in the LAN. This table contains the assigned or used 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.
- 'dyn.'  
The DHCP server assigned an address to the computer.

## 7.2

### 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.

## 7.2.1

### 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 is possible to immediately go to the correct remote station for all of the names with known IP addresses. In principle, the DNS server can be a separate computer in the network. However, the following reasons speak for locating the DNS server directly in the *ELSA LANCOM DSL Office*:

- *ELSA LANCOM DSL Office* can automatically distribute IP addresses for the computers in the local network when in DHCP server mode. In other words, the DHCP server already knows the names and IP addresses of all of the computers in its own network that were assigned IP addresses via DHCP. With the dynamic address assignments of a DHCP server, an external DNS server might have difficulties in keeping the associations between the names and IP addresses current.
- When routing Microsoft Networks via NetBIOS, the *ELSA LANCOM DSL Office* also knows the computer names and IP addresses in the other connected NetBIOS networks. In addition, computers with fixed IP addresses can also enter themselves in the NetBIOS table and thus be known by their names and addresses.
- The DNS server in the *ELSA LANCOM DSL 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.

*ELSA LANCOM  
DSL/I-10 Office  
only*

### How does the DNS server react to the request?

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.
- Finally, the DNS server checks whether the request to another DNS server is to be forwarded to another DNS server via a WAN interface (special DNS forwarding via the DNS destination table).

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 general DNS forwarding mechanism, or returns an error message to the requesting computer.

## 7.2.2

### DNS forwarding

If it cannot serve the request from its own DNS tables, the DNS server forwards the request to other DNS servers. This process is called DNS forwarding.

Here a distinction is made between

- Special DNS forwarding  
Requests for certain name areas are forwarded to certain DNS servers.
- General DNS forwarding  
All other names not specified in detail are forwarded to the "higher-level" DNS server.

#### Special DNS forwarding

With special DNS forwarding name areas can be defined for the resolution of which specified DNS server are addressed.

A typical application for special DNS forwarding results for a home workstation: The user wants to be able to connect to the company intranet and directly to the Internet at the same time. The requests sent into the intranet must be routed to the company DNS server, and all other requests to the DNS server of the provider.

#### General DNS forwarding

All DNS requests that cannot be resolved in another way are forwarded to a DNS server. This DNS server is determined according to the following rules:



- Initially the router checks whether a DNS server has been entered in its own settings. If it is successful there, it obtains the desired information from this server. Up to two higher-level DNS servers can be specified.

<i>ELSA LANconfig</i>	TCP/IP ► Addresses ► First DNS server / second DNS server
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► TCP/IP-module ► DNS-default / DNS-backup
Terminal/Telnet	/setup/TCP-IP-module/DNS-default /setup/TCP-IP-module/DNS-backup

- If no DNS server is entered in the router, it will attempt to reach a DNS server over a PPP connection (e.g. from the Internet provider) to get the IP address assigned to the name from there. This can only succeed if the address of a DNS server is sent to the router during PPP negotiation.
- The default route is established and the DNS server searched for there if no connection exists.

This procedure does not require you to have any knowledge of the DNS server address. Entering the Intranet address of your router as the DNS server for the workstation computers is sufficient to enable you obtain the name assignment. This procedure also automatically updates the address of the DNS server. Your local network always receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

## 7.2.3

### Setting up the DNS server

The settings for the DNS server are contained in the following menu or list:

Configuration tool	Run command/Table
<i>ELSA LANconfig</i>	TCP/IP ► DNS-server
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► DNS module
Terminal/Telnet	cd /setup/DNS module

Proceed as follows to set the DNS server:

- Switch the DNS server on.

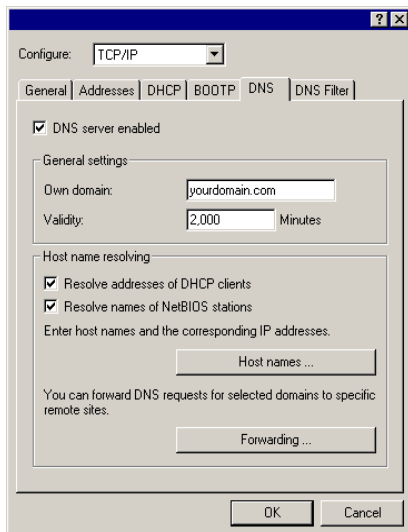
<i>ELSA WEBconfig</i>	... ► Operating
Terminal/Telnet	set operating on

- 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.

<i>ELSA WEBconfig</i>	... ► Domain
Terminal/Telnet	set domain yourdomain.com

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

<i>ELSA WEBconfig</i>	... ► DHCP-usage ... ► NetBIOS-usage
Terminal/Telnet	set DHCP-usage yes set NetBIOS-usage yes



Activated DNS server  
in the TCP-IP configuration

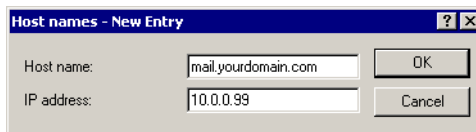
- ④ The main task of the DNS server is to distinguish requests for names in the Internet from those for other remote stations. Therefore, enter all computers in the Station name table,
- for which you know the name and IP address,
  - that are not located in your own LAN,
  - that are not on the Internet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

- that are accessible via the router.

With the following commands you add stations to the Station name table:

<i>ELSA LANconfig</i>	TCP/IP ► DNS ► Station name ► Add
<i>ELSA WEBconfig</i>	... ► DNS table ► Add
Terminal/Telnet	cd setup/DNS module/DNS table set mail.yourdomain.com 10.0.0.99

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:



Stating the domain is optional but recommended.

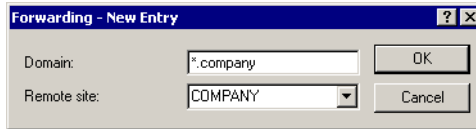
When you now start your mail program, it will probably automatically look for the server 'mail.yourdomain.com'. The DNS server thereupon returns the IP address '10.0.0.99'. The mail program will then look for that IP address. With the proper entries in the IP routing table and name list, a connection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

- ⑤ To resolve entire name areas of another DNS server, add a forwarding entry consisting of a name area and remote station:

<i>ELSA LANconfig</i>	TCP/IP ► DNS ► Forwarding ► Add
<i>ELSA WEBconfig</i>	... ► DNS destination table ► Add
Terminal/Telnet	cd setup/DNS module/destination table set *.intern COMPANY

When specifying the name areas, the wildcards '?' for individual characters and '\*' for multiple characters may be used.

To reroute all domains with the ending '\*.intern' to a DNS server in the LAN of the remote station 'COMPANY', create the following entry:



*The IP address of the DNS server must automatically be transmitted by the remote station via PPP. It is not possible to manually specify the IP address of this DNS server.*

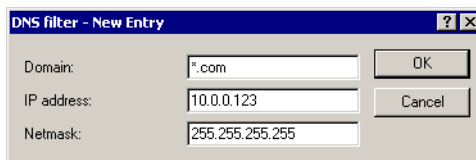
- ⑥ Finally, use the filter list to specify the users that cannot access certain names or domains.

To block the Domain (in this case the web server) 'www.blocked.com' for all computers in the LAN, the following commands and entries are required:

ELSA LANconfig	TCP/IP ► DNS filter ► DNS filter ► Add
ELSA WEBconfig	... ► Filter list ► Add
Terminal/Telnet	<pre>cd setup/DNS module/filter list set 001 www.blocked.com 0.0.0.0 0.0.0.0</pre>



The index '001' in the console command can be selected as desired and is used only for clarity. The wildcards '?' (stands for exactly one character) and '\*' (for a random number of characters) are valid when entering the domain. To only block the access of a certain computer (e.g. with IP 10.0.0.123) to COM domains, enter the following values:



In the console mode the command is:

```
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.

## 7.3

### Call charge management

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

To reduce these costs, the software provides various options:

- The available online minutes can be restricted to a specific period.
- For ISDN connections a charge or time limit can be assigned to a specific period.

*ELSA LANCOM  
DSL/I-10 Office  
only*

## 7.3.1

### Connection restriction for DSL and cable modem

Even if a DSL or cable modem connection acts like a fixed connection for which no connection must be established and therefore neither a start nor an end to the connection can be recognized), the costs are calculated based on time depending on the provider.



*In the further course of this section, we will only talk about DSL connections. However, the descriptions also apply to any other connection that is made via the 10Base-T-WAN line of the ELSA LANCOM DSL Office, for example for cable modem connections.*

The telephone charges can be controlled by limiting the maximum connection time. For this purpose a time limit is agreed upon for DSL connections for a certain period. In the delivered state the DSL connections may, for example, be used for a maximum of 600 minutes within six days.

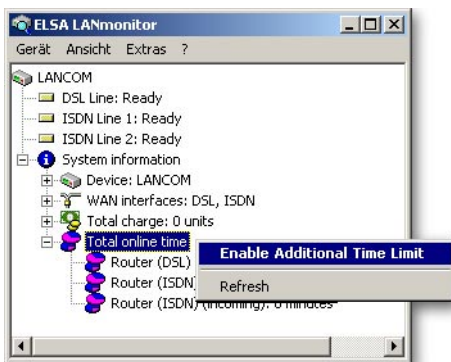


*When the limit of a budget is reached, all open DSL connections will be shut down automatically. The budgets will not be reset to permit the*

*establishment of connections until the current period has elapsed. Needless to say, the administrator can reset the budgets at any time if required!*

If you want to extend the online budget for one-time actions, e.g. to download a very large file from the Internet, you do not necessarily have to change the time limit. You can specify an additional limit for such cases that can be activated separately.

In *ELSA LANmonitor* you activate the additional limit via the context menu of the total connection time (press right mouse button on "Total connection time"):



*If you do not see the system information in ELSA LANmonitor, activate the corresponding display with **View ► Display ► System information**.*

In *ELSA WEBconfig* and in the console the commands for enabling the additional time limit are:

Configuration tool	Run command
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► Charges module ► Activate reserve
Terminal/Telnet	cd /setup/charges module do Activate reserve

When the additional time limit is activated, it is enabled for the current period. In the next period the normal time limit applies again.

## 7.3.2

### 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!*

## 7.3.3

### 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 ELSA LANCAP1 are not affected.*

## 7.3.4

## Settings in the charges module

Configuration tool	Run command/table
<i>ELSA LANconfig</i>	Management ► Costs
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► Charges module
Terminal/Telnet	<code>cd /setup/charges module</code>

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

- Day(s)/period  
The duration of the monitoring period in days can be specified here.
- Budget units, DSL/ISDN minutes budget  
The maximum number of ISDN units or DSL/ISDN online minutes in a monitoring period



*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.*

## 7.4

## The SYSLOG module

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

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

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

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



## 7.4.1

## Setting up the SYSLOG module

Configuration tool	Run command/table
<i>ELSA LANconfig</i>	Management ► Log & Trace
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► SYSLOG module
Terminal/Telnet	cd /setup/SYSLOG module

## 7.4.2

Example configuration with *ELSA LANconfig*

## Create SYSLOG client

- ① Start *ELSA LANconfig*. Under 'Management', choose the 'Log & Trace' tab.
- ② Turn the module on and click **SYSLOG clients**.
- ③ In the next window click **Add...**
- ④ First enter the IP address of the SYSLOG client, and then set the sources and priorities.

**SYSLOG clients - New Entry**

IP address: 10.1.0.160

Source:

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

Priority:

☒ Alert      ☒ Error  
☒ Warning      ☒ Information  
☐ Debug

OK Cancel

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

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

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

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

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

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

### Facilities

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

*Example*

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

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

writes all outputs of the *ELSA LANCOM DSL Office* to the file '/var/log/lancom.log'.

## 7.5

### Office communications with *ELSA LANCAP*



*Of the devices of the series ELSA LANCOM DSL Office only the ELSA LANCOM DSL/I-10 Office is equipped with an ISDN connection. The explanations of this section therefore only refer to this device.*

*ELSA LANCAP* 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 section briefly introduces the *ELSA LANCAP* and its use for office communications tasks.

### 7.5.1

#### What are the advantages of *ELSA LANCAP*?

The main advantages of using *ELSA LANCAP* are economic. *ELSA LANCAP* provides all Windows workstations integrated in the LAN (local-area network) with unlimited access to office communications functions such as fax machines, answering machines, online banking and eurofile transfer. All functions are supplied via the network without the necessity of additional hardware at each individual workstation. This does away with the cost of equipping workstations with ISDN adapters or modems. All you need do is install the office communications software on the individual workstations.



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

*Please note: All ELSA LANCAPI-based applications access the ISDN directly and do not run across the router of the device. The connect-charge monitoring and firewall functions are thus disabled!*

## 7.5.2

### Installing the **ELSA LANCAPI** client

The *ELSA LANCAPI* is made up of two components, a server (in the *ELSA LANCOM DSL/I-10 Office*) and a client (on the PCs). The *ELSA LANCAPI* client must be installed on all computers in the LAN that will be using the *ELSA LANCAPI* functions.

- ① Place the *ELSA LANCOM Office* CD in your CD-ROM drive. If the setup program does not automatically start when you insert the CD, simply click 'autorun.exe' in the main directory of the *ELSA LANCOM Office* 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 *ELSA LANCAPI* is then ready to accept all jobs from the office communications software. After successful installation, an icon for *ELSA LANCAPI* will be available in the Start menu. A double-click on this icon opens a status window that permits current information on the *ELSA LANCAPI* to be displayed at any time.

## 7.5.3

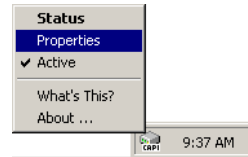
### Configuration of the **ELSA LANCAPI** clients

The configuration of the *ELSA LANCAPI* clients is used to determine which *ELSA 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* in your LAN as a *ELSA LANCAPI* server.

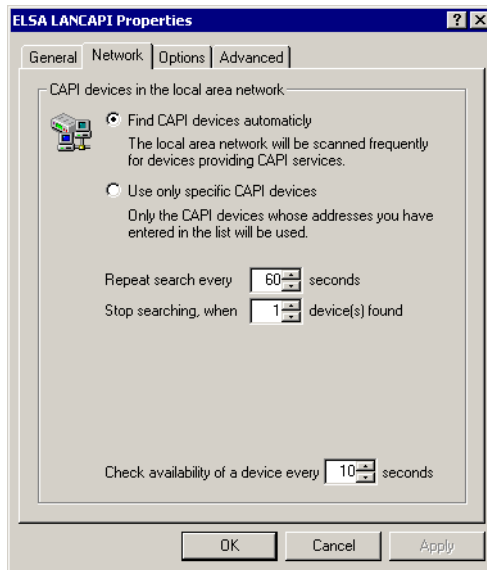
- ① Start the *ELSA LANCAPI* client in the 'ELSAlan' program group. Information regarding the drivers for the available service can be found on the 'General' tab.



You can also run the *ELSA LANCAPi* client from the Windows taskbar. To do this, simply click with the right mouse button on the *ELSA LANCAPi* symbol in the Windows taskbar next to the clock and select **Properties**.



- ② In the *ELSA LANCAPi* client, change to the **Network** tab. First, select whether the PC should find its own *ELSA LANCOM* 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* in your LAN as *ELSA 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.



## 7.5.4

Configuring the *ELSA LANCAPI* server

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

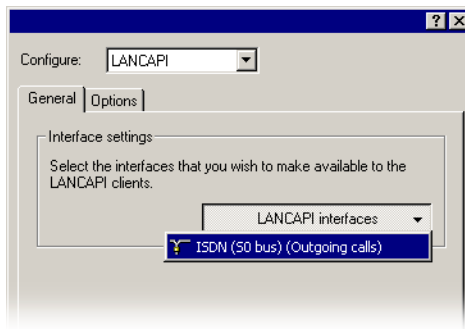
- What call numbers from the telephone network should *ELSA LANCAPI* respond to?
- Which of the computers in the local network should be able to access the telephone network via *ELSA LANCAPI*?

The *ELSA LANCAPI* server is configured in the following menus:

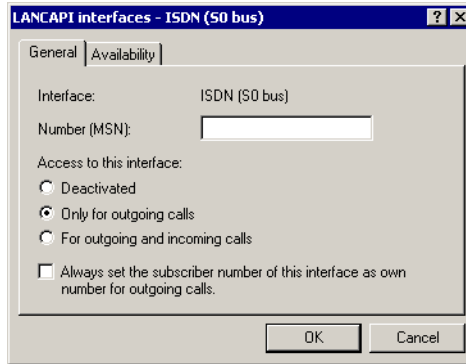
Configuration tool	Run command/menu
<i>ELSA LANconfig</i>	LANCAPI
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► LANCAPI module
Terminal/Telnet	<code>cd /setup/LANCAPI module</code>

Example configuration with *ELSA LANconfig*

- ① Open the configuration of the router by double-clicking on the device name in the list and select the **LANCAPI** section.
- ② Select the ISDN port you want to set.



- ③ Activate the *ELSA LANCAPI* server for the outgoing and incoming calls, or allow only outgoing calls.

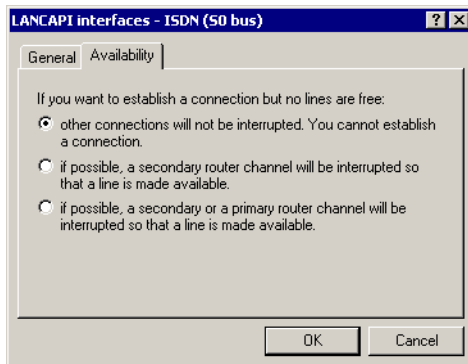


- ④ In the latter case, the *ELSA LANCAPi* will not respond to incoming calls—to receive faxes, for example. Permitting outgoing calls only is useful if you do not have a specific call number available for the *ELSA LANCAPi*.
- ⑤ When the *ELSA LANCAPi* server is activated, enter the call numbers to which the *ELSA LANCAPi* should respond in the 'Number (MSN/EAZ)' 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 *ELSA LANCAPi*.
- ⑥ *ELSA LANCAPi* is preset to use IP 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.
- ⑦ If you do not wish all the computers in the local network to be able to access the *ELSA LANCAPi* functions, you can define all the authorized users (by means of their IP addresses) by entering them in the access list.



*If you enter more than one call number for the ELSA 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.*

- ⑧ Switch to the 'Availability' tab. Here you can determine how the *ELSA LANCOM DSL/I-10 Office* should respond if a connection is to be established via the *ELSA LANCAPi* (incoming or outgoing) when both B-channels are already busy (priority control).



The meaning of the options offered here:

- The connection cannot be established via the *LANC API*. A fax program using the *LANC API* will then probably attempt to send again at a later time.
- The connection via the *ELSA LANC API* 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 *ELSA LANC API* must wait if two router connections are established to separate remote stations (two main channels busy).
- A connection via *ELSA LANC API* can always be established; an existing router connection will be terminated for the duration of the call if required. This can be used to ensure the permanent availability of the fax function, for example.

## 7.5.5

### How to use the *ELSA LANC API*

Two options are available for the use of the *ELSA LANC API*:

- You may use software which interacts directly with a CAPI (in this case, the *ELSA LANC API*) 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 *ELSA LANC API*, select the entry 'ISDN WAN Line 1'.



## 7.5.6

### The *ELSA CAPI Faxmodem*

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

#### Installation

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

#### Faxing with the *ELSA CAPI Faxmodem*

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



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



## 8 Routing and WAN connections

This chapter describes the most important protocols and configuration entries used for WAN connections. It also shows ways to optimize WAN connections via DSL, a cable modem or ISDN.

### 8.1 General information on WAN connections

WAN connections are used for the following applications.

- Internet connection via DSL, cable modem or ISDN
- LAN to LAN coupling via ISDN
- Remote access via ISDN

#### 8.1.1 Bridges for standard protocols

WAN connections differ from direct connections (for example, via the *ELSA LANCAP*) in that the data in the WAN are transmitted via standardized network protocols also used in the LAN. On the other hand, direct connections operate with proprietary processes that have been specially developed for point-to-point connections.

Via WAN connections a LAN is extended, and with direct connections only one individual PC establishes a connection to another PC. WAN connections form a kind of bridge for the communication between networks (or for connecting individual computers to the LAN).

#### Which protocols are used in WAN connections?

On WAN connections via the high-speed connection (for DSL and cable modem connections) packets according to the IP standard are transferred. In addition to IP, the *ELSA LANCOM DSL/I-10 Office* also supports IPX on its ISDN interface.

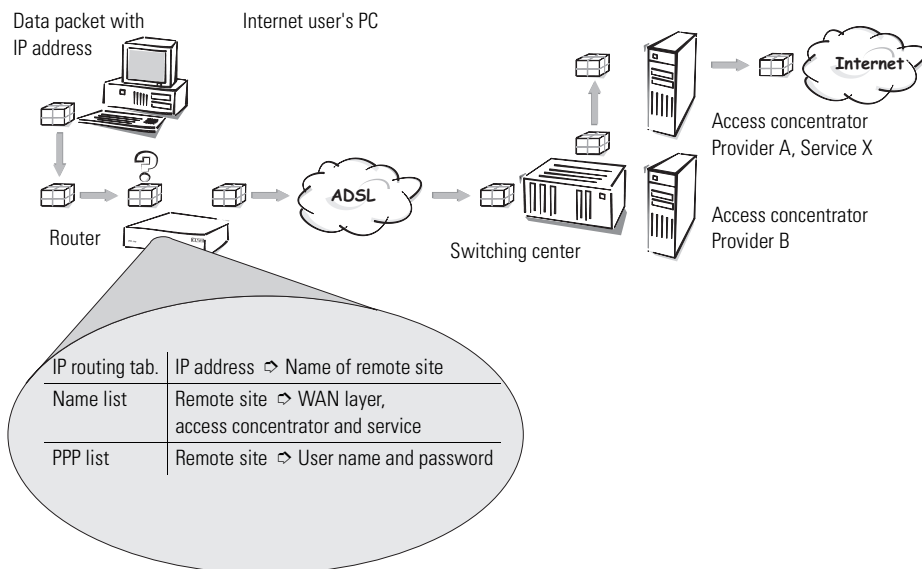
#### Close cooperation with router modules

Characteristic of WAN connections is the close cooperation with the router modules in the *ELSA LANCOM*. The router modules (IP and with *ELSA LANCOM DSL/I-10 Office* also IPX) ensure the connection of LAN and WAN. They make use of the WAN modules to meet requests from PCs from the LAN for external resources.

## 8.1.2 What happens in the case of a request from the LAN?

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

A simplified example (on ADSL) will clarify this process. Here we assume that the IP address of the computer being searched for is known in the Internet.



### ① Selecting the correct route

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. The router determines the remote station in its IP routing table via which the target IP address can be reached, e.g. 'Provider\_A'.

### ② **Authentication data for the remote station**

Using this name, the router then checks the name list and locates the names of the accompanying access concentrators and service, which should be claimed at this AC. The router also obtains the user name and password required for login to provider A from the PPP list.

### ③ **Establishment of WAN connection**

The router can then establish a connection on the ADSL line and indicate that it wants a connection to the access concentrator of Provider A and to use Service X there. It authenticates itself with a user name and password.

### ④ **Forwarding data packet**

Once the connection has been established, the router can forward the data packet to the Internet over the ADSL line.

## 8.2

## 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 section explains the structure of the IP routing table of an ELSA router, as well as the additional functions available to support IP routing.

### 8.2.1

### The IP routing table

Use the IP routing table to tell the router which remote station (which other router or computer) it should send the data for particular IP addresses or IP address ranges to. This type of entry is also known as a "route" since it is used to describe the path of the data packet. This procedure is also called "static routing" since you make these entries yourself and they remain unchanged until you either change or delete them yourself. Naturally, "dynamic routing" also exists. 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 256 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.

### Configuration of the routing table

Configuration tool	Call
<i>ELSA LANconfig</i>	IP router ► Routing ► Routing table
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► IP-router-module ► IP-routing-tab.
Terminal/Telnet	cd /setup/IP-router/IP-routing-tab.

An IP routing table can, for example, look like this:

IP address	IP net mask	Router	Distance	Mask.
192.168.120.0	255.255.255.0	MAIN	2	On
192.168.125.0	255.255.255.0	NODE1	3	Off
192.168.130.0	255.255.255.0	191.168.140.123	0	Static

What do the various entries on the list mean?

- IP addresses and netmasks

This is the address of the destination network to which data packets may be sent and its associated network mask. The router uses the network mask and the destination IP address of the incoming data packets to check whether the packet belongs to the destination network in question.

The route with the IP address '255.255.255.255' and the network mask '0.0.0.0' is the default route. All data packets that cannot be routed by other routing entries are sent over this route.

- Router

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

The router name indicates what should happen with the data packets that match the IP address and network mask.

Routes with the router name '0.0.0.0' identify exclusion routes. Data packets for this "zero route" are rejected and are not routed any further. That way routes which are forbidden on the Internet (private address spaces, e.g. '10.0.0.0'), for example, are excluded from transmission.

If an IP address is input as router name, this is a locally available router, which is responsible for transfer of the relevant data packets.

● Distance

Number of routers between your own and the destination router. This value is often equated with the cost of the transmission and used to distinguish between inexpensive and expensive call paths for wide-area connections. The distance values entered are propagated as follows:

- All networks which can be reached while a connection exists to a destination network are propagated with a distance of 1.
- All non-connected networks are propagated with the distance entered in the routing table (but with a minimum distance of 2) as long as a free transmitting channel is still available.
- The remaining networks are propagated with a distance of 16 (= unreachable) if there are no longer any channels available.
- Remote stations connected using proxy ARP are an exception to this. These "proxy hosts" are not propagated at all.

● Mask.

Use the 'Masquerading' option in the routing table to inform the router which IP addresses to use when transferring the packets.

For further information see section 'The hiding place – IP masquerading (NAT, PAT)' on page 58.

## 8.2.2

### Local routing

You know the following behavior of a workstation within a local network: The computer searches for a router to assist with transmitting a data packet to an IP address which is not on its own LAN. This router is normally introduced to the operating system with an entry as standard router or standard 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 this way you instruct the router itself in your device to send the data packet to other routers. In addition, in this case no more ICMP redirects will be sent. The setting is made under:

Configuration tool	Call
<i>ELSA LANconfig</i>	IP router ► General ► Forward packets in local network
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► IP-router-module ► Loc.-routing
Terminal/Telnet	set /setup/IP-router/Loc.-routing on

Local routing can be very helpful in isolated cases, however, it should also only be used in isolated cases. For local routing leads to a doubling of all data packets to the desired target network. The data is first sent to the default router and is then sent on from here to the router which is actually responsible in the local network.

## 8.2.3

### Dynamic routing with IP RIP

In addition to the static routing table ELSA routers also have a dynamic routing table containing up to 128 entries. Unlike the static table, you do not fill this out yourself, but leave it to be dealt with by the router itself. It uses the Routing Information Protocol (RIP) for this purpose. All devices that support RIP use this protocol to exchange information on the available routes.

#### What information is propagated by IP RIP?

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



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

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

- If the router has established a connection to a remote station, it propagates all the networks which can be reached via this route in the RIPs with the distance '1'. Other routers in the LAN are thus informed by these means that a connection to the remote station has been established on this router which they can use. The establishment of additional connections by routers with dial-up connections can be prevented, thus reducing connection costs.
- If this router cannot establish a further connection to another remote station, all other routes are propagated with the distance '16' in the RIPs. The number '16' stands for "This route is not reachable at the moment." A router may be prevented from establishing a connection in addition to the present one may be due to one of the following causes:
  - Another connection has already been established on all the other channels (also via the *ELSA LANCAP*).
  - Y connections for the  $S_0$  port have been explicitly excluded in the interface table.
  - The existing connection is using all B-channels (channel bundling).
  - The existing connection is a leased-line connection. Only a few ISDN providers enable a dial-up connection to be established on the second B-channel in addition to a permanent connection on the first B-channel.

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

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

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

### What do the entries mean?

IP address and network mask identify the destination network, the distance shows the number of routers between the transmitter and receiver, the last column shows which router has revealed this route. This leaves the 'Time'. The dynamic table thus shows how old the relevant route is. The value in this column acts as a multiplier for the intervals at which the RIP packets arrive. A '1', therefore, stands for 30 seconds, a '5' for about 2.5 minutes and so on. New information arriving about a route is, of course, designated as directly reachable and is given the time setting '1'. The value in this column is automatically incremented when the corresponding amount of time has elapsed. The distance is set to '16' after 3.5 minutes (route not reachable) and the route is deleted after 5.5 minutes.

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

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



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

### Interaction: static and dynamic tables

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

## Routers without IP RIP support

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

## Scaling with IP RIP

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

## Configuration of IP-RIP function

Configuration tool	Menu/table
<i>ELSA LANconfig</i>	IP router ► General ► RIP options
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► IP-router-module ► RIP configuration
Terminal/Telnet	setup/IP-router-module/RIP-configuration

- In the field 'RIP support' (or 'RIP type') the following selection is possible:
  - 'Off': IP-RIP is not used (default).
  - 'RIP-1': RIP-1 and RIP-2 packets are received but only RIP-1 packets are sent.
  - 'RIP-1 compatible': RIP-1 and RIP-2 packets are received. RIP-2 packets are sent as an IP broadcast.
  - 'RIP-2': Same as 'RIP-1-compatible' except that all RIP packets are sent to the IP multicast address 224.0.0.9.
- The entry under 'RIP-1 mask' (or 'R1 mask') can be set to the following values:
  - '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.
- 'Class+Address': 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.



*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.*

## 8.2.4

### 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.

Policy based routing can be activated and deactivated as follows:

Configuration tool	Menu/table
ELSA LANconfig	IP router ► General ► Take Type-of-service field into account
ELSA WEBconfig	Expert configuration ► Setup ► IP router module ► Routing method ► Routing method
Terminal/Telnet	cd /setup/IP router module/routing method set routing method TOS (on) set routing method NORMAL (off)

## 8.2.5

### SYN/ACK speedup

The SYN/ACK speedup method is used to accelerate IP data traffic. With SYN/ACK speedup IP check characters (SYN for synchronization and ACK for acknowledge) a given preference within the transmission buffer over simple data packets. This prevents the situation that check characters remain in the transmission queue for a longer time and the remote station stop sending data as a result.

The greatest effect occurs with SYN/ACK speedup with fast connections when data quantities are transferred in both directions at high speed.

The SYN/ACK speedup is activated at the factory.

### Switching off in case of problems

Due to the preferred handling of individual packets, the original packet order is changed. Although TCP/IP does not ensure a certain packet order, problems may result in a few isolated applications. This only concerns applications that assume a certain order that differs from the protocol standard. In this case the SYN/ACK speedup can be deactivated:

Configuration tool	Menu/table
<i>ELSA LANconfig</i>	IP router ► General ► Forward TCP SYN and ACK packets with preference
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► IP router module ► Routing method ► SYN/ACK speedup
Terminal/Telnet	<code>cd /setup/IP router module/routing method</code> <code>set SYN/ACK speedup OFF</code>

## 8.3

### Configuration of remote stations

Remote stations are configured in two tables:

- In the name list(s) all information is set that applies individually to only one remote station.
- Parameters for the lower protocol levels (below IP or IPX) are defined in the communication layer table.



*The configuration of the authentication (protocol, user name, password) is not covered in this section. Information on authentication is contained in the section 'Establishing connection with PPP' on page 113.*

## 8.3.1

## Name list

The available remote stations are created in the name list with a suitable name and additional parameters.

Devices of the type *ELSA LANCOM DSL/I-10 Office* have two name lists - one for DSL (or cable modem) and another for ISDN remote stations. *ELSA LANCOM DSL Office* routers without an ISDN connection have only the DSL name list.

Configuration tool	Menu/table
<i>ELSA LANconfig</i>	Communication ► Remote stations ► Name list (DSL) Communication ► Remote stations ► Name list (ISDN)
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► WAN module ► DSL name list or ISDN name list
Terminal/Telnet	cd /setup/WAN module set DSL name list [...] set ISDN name list [...]

- The following parameters are required for a DSL remote station:

Name list	Parameter	Meaning
DSL	Name	This name is used to identify the remote station in the router modules. Once the router module has used the IP address to find which remote station can be used to reach the desired destination, the associated connection parameters can be determined from the name list.
	Time out	This period indicates how long the connection will remain active after no more data are transferred. If a zero is given as time out, the connection will not be automatically terminated. With a holding time of 9,999 seconds, disconnected connections are automatically reestablished (see 'Permanent connection for flatrates – Keep-Alive' on page 120).
	Access concentrator	The access concentrator (AC) represents the server that can be accessed over this connection. If more than one provider is available over your ADSL terminal, select the one that is responsible for the IP address group of this remote station with the name of the AC. The value for the AC will be supplied by your provider. If a value for the AC is not entered, every AC that offers the requested service will be accepted.

Name list	Parameter	Meaning
	Service	Enter the service that you wish to use with your provider. This can be simple Internet browsing, video downstream or other. The value for the service will be supplied by your provider. If a value for the service is not entered, every service that offers the requested AC will be accepted.
	Layer name	Select the communication layer which should be used for this connection. The configuration of this later is described in the following section.
ISDN	Name	As in the DSL name list.
	Phone number	A telephone number is only required when the remote stations is to be called. The field can be left blank when calls are only to be answered. Several telephone numbers for the same remote station can be entered in a roundrobin list.
	Time out	As in the DSL name list.
	Holding time for bundling	The second B-channel in a bundle is disconnected if it has not been used for the set duration.
	Layer name	As in the DSL name list.
	Automatic callback	The automatic callback function enables a reliable connection and reduces the costs for the caller. For details, see section 'Callback functions' on page 122.



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

## 8.3.2

### Layer list

With a layer, a collection of protocol settings are defined, which should be used when connecting to specific remote stations. The list of the communication layers can be found under:

Configuration tool	List
<i>ELSA LANconfig</i>	Communication ► General ► Communication layer
<i>ELSA WEBconfig</i>	Expert Configuration ► Setup ► WAN module ► Layer list
Terminal/Telnet	cd /setup/WAN-module/ set layer list [...]

In the communication layer list the common protocol combinations are already predefined. Changes or additions should only be made when remote stations are incompatible to the existing layers. The possible options are contained in the following list:

Parameter	Meaning
Layer name	The layer is selected in the name list under this name.
Encapsulation	The data packets can also be encapsulated as Ethernet packets above layer 3 of the OSI model. This setting is required for communication with older <i>ELSA LANCOM</i> devices. In the 'Transparent' setting the packets are not specially encapsulated.
Layer-3	The following options are available for the switching layer or network layer:
	'Transparent' No additional header is inserted.
	'PPP' The connection is established according to the PPP protocol (in the synchronous mode, i.e. bit-oriented). The configuration data are taken from the PPP table.
	'AsyncPPP' Like 'PPP', only the asynchronous mode is used. This means that PPP functions character-oriented.
	'... with script' All options can be run with their own script if desired. The script is specified in the script list.
	'ELSA' ELSA's own process for negotiating connections.
	'DHCP' Assignment of the network parameters via DHCP.



Parameter	Meaning	
Layer-2	In this field the upper section of the security layer (Data Link Layer) is configured. The following options are available:	
	'Transparent'	No additional header is inserted.
	'X.75LAPB'	Connection establishment according to X.75 and LAPM (Link Access Procedure Balanced).
	'PPPoE'	The PPP negotiation runs via Ethernet. The PPP packets are encapsulated in Ethernet frames for this purpose. This process is frequently used for DSL connections.
Options	Here you can activate the compression of the data to be transmitted and the bundling of channels. The selected option only becomes active when it is supported by both the ports used and the selected Layer-2 and Layer-3 protocols. For further information see section 'Channel bundling with MLPPP' on page 125.	
Layer 1	In this field the lower section of the security layer (Data Link Layer) is configured. The following options are available:	
	'ETH-10'	Transparent 10-Mbit Ethernet as per IEEE 802.3.
	'HDLC'	Securing and synchronization of the data transfer as per HDLC (in the 7 or 8-bit mode).
	'V.110'	Transmission as per V.110 with a maximum of 38,400 bits/second.

## 8.4

### Establishing connection with PPP

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.

## 8.4.1

### The protocol

#### What is PPP?

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

- Password protection according to PAP, CHAP or MS-CHAP
- Callback functions (only *ELSA LANCOM DSL/I-10 Office*)
- Negotiation of the network protocol to be used over the connection established (IP or IPX, for example). Included in this are any parameters necessary for these protocols, for example IP/IPX addresses. This negotiation runs via the IPCP protocol (IP Control Protocol).
- Verification of the connection through the LCP (Link Control Protocol)
- Bundling of several ISDN channels (multilink PPP – only *ELSA LANCOM DSL/I-10 Office*)

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

#### What is PPP used for?

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

- for reasons of compatibility when communicating with external routers, for example
- Remote access of remote workstations with ISDN adapters (only *ELSA LANCOM DSL/I-10 Office*)
- Internet access (when sending addresses)

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

#### The phases of PPP negotiation

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

- Establish phase

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

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

- Authenticate phase

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

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

- Network phase

In the *ELSA LANCOM DSL Office* the protocols IPCP and IPXCP (the latter only in the *ELSA LANCOM DSL/I-10 Office*) are implemented.

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

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 LANCOM*

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

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

```
trace + ppp
```

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

*ELSA LANCOM  
DSL/I-10 Office  
only*

## 8.4.2

**Everything OK? Checking the line with LCP**

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

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

What happens when there is no reply? First a few retries will be initiated to exclude the possibility of any short-term line interference. The line will be dropped and an alternative route sought if all the retries remain unanswered. If, for example, the high-speed connection refuses to work, an existing ISDN port can open the way to the Internet as a backup.



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



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

## 8.4.3

**Assigning IP addresses via PPP**

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



This type of address assignment is carried out during PPP negotiation and implemented only for connections via WAN. In contrast, the assignment of addresses via DHCP is (normally) used within a local network.

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

## Examples

### ● Remote access

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

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

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

### ● Internet access

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

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

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

#### 8.4.4 Settings in the PPP list

You can specify a custom definition of the PPP negotiation for each of the remote sites that contact your net.

Configuration tool	List
<i>ELSA LANconfig</i>	Communication ► Protocols ► PPP list
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► WAN module ► PPP list
Terminal/Telnet	<code>cd /setup/WAN-module/ set PPP list [...]</code>

The PPP list may have up to 64 entries and contain the following values:

In this column of the PPP list...	...enter the following values:
Remote site (Device name)	Name the remote site uses to identify itself to your router.
User name	The name with which your router logs onto the remote site. The device name of your router is used if nothing is specified here.
Password	Password transferred by your router to the remote site (if demanded). An asterisk (*) in the list indicates that an entry is present.
Checking the remote station (Authentication)	Security method used on the PPP connection ('PAP', 'CHAP' or 'none'). Your own router demands that the remote site observes this procedure. Not the other way round. This means that 'PAP', '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.

In this column of the PPP list...	...enter the following values:
Time	<p>Time between two checks of the connection with LCP (see the following section). This is specified in multiple of 10 seconds (i.e. 2 for 20 seconds, for instance).</p> <p>The value is simultaneously the time between two checks of the connection according to CHAP. This time is entered in minutes. The time must be set to '0' for remote sites using a Windows operating system.</p>
Repetitions (Rep)	<p>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.</p> <p>Simultaneously the number of the "Configure requests" that the router maximum sends before it assumes a line error and clears the connection itself.</p>
Conf, Fail, Term	<p>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.</p> <p>The default settings should generally suffice.</p> <p>These parameters can only be modified via <i>ELSA LANconfig</i>, <i>SNMP</i> or <i>TFTP</i>!</p>

## 8.5

### Establishing DSL connection with PPTP

An increasing number of DSL providers enable dialing in not only via PPPoE, but also via PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol). This PPTP is a protocol extension of PPP that was primarily developed by Microsoft.

PPTP enables "Tunnels" to be established to a remote station via IP networks. A tunnel is a logically shielded connection that is intended to protect the transmitted data from access by unauthorized third parties. The encoding algorithm RC4 is used for this purpose.

#### Configuration of PPTP

In the *ELSA LANCOM DSL Office* all necessary PPTP parameters are requested from the Internet connection wizard as soon as the Internet connection via PPTP is selected. In addition to the entries that are also

requested with a normal PPPoE connection, only the IP address of the PPTP gateway must be specified. The PPTP gateway is usually the DSL modem. Contact your DSL provider for details.

Changes to the configuration are made in the PPTP list:

Configuration tool	List
<i>ELSA LANconfig</i>	Communication ► Protocols ► PPTP list
<i>ELSA WEBconfig</i>	Expert configuration ► Setup ► WAN module ► PPTP list
Terminal/Telnet	<code>cd /setup/WAN-module/ set PPTP list [...]</code>

The PPTP configuration consists of three parameters:

- 'Remote station' – The designation from the DSL name list.
- 'IP address' – IP address of the PPTP gateway, usually the address of the DSL modem
- 'Port' – IP port via which the PPTP protocol runs. In accordance with the protocol standard, port '1.723' should always be specified.

## 8.6 Permanent connection for flatrates – Keep-Alive

The term 'Flatrates' is used to refer to all-inclusive connection rates that are not billed according to connection times, but instead as a flat fee for fixed periods. With flatrates there is no longer any reason to disconnect. On the contrary: New e-mails should be reported directly to the PC, the home workplace is to be continuously connected to the company network and users want to be able to reach friends and colleagues via Internet messenger services (ICQ etc.) without interruption. This means it is desirable to continuously maintain connections.

With the *ELSA LANCOM DSL Office* the Keep-Alive function ensures that connections are always established when the remote station has disconnected them.

### Configuration of Keep-Alive function

The Keep-Alive function is configured in the name lists (for DSL and with the *ELSA LANCOM DSL/I-10 Office* also for ISDN).



If the holding time is set to 0 seconds, the inactive connection is disconnected by the *ELSA LANCOM DSL Office*. The automatic disconnection of connections over which no data has been transmitted for a longer time is deactivated with a holding time of 0 seconds. However, interrupted connections are not automatically reestablished with this setting.

With a holding time of 9,999 the connection is always reestablished when it has originally been established by the user's own side and has been disconnected by the remote station.

## 8.7

## Callback functions



The *ELSA LANCOM DSL/I-10 Office* supports automatic callback via its ISDN port.

*Of the ELSA LANCOM DSL Office series, only the ELSA LANCOM DSL/I-10 Office features an ISDN connection. The descriptions in this section therefore only apply to this device.*

In addition to callback via the D-channel, the CBCP (**C**allback **C**ontrol **P**rotocol) specified by Microsoft and callback via PPP as per RFC 1570 (PPP LCP Extensions) are also offered. In addition, it is possible for a rather quick callback to occur via a procedure developed by ELSA. PCs with Windows operating system can be called back only via the CBCP.

## 8.7.1

## Callback using Microsoft CBCP

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

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

Via CBCP, it is possible to establish connection to *ELSA LANCOM DSL/I-10 Office* from a PC with Windows operating system and also to be called back by this PC. Three possible settings are selected in the ISDN name list via the callback entry as well as the calling number entry.

### Do not carry out any callbacks

For this setting, the callback entry must be set to 'Off' when configuring via *ELSA WEBconfig* or in the console.

### Callback number specified by caller

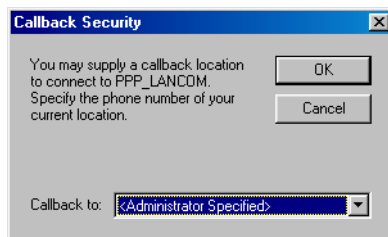
For this setting the callback entry must be set to 'Call back remote station after checking name' (or must have the value 'Name' in *ELSA WEBconfig* or in the console). In the name list **no** telephone number may be specified.

After the Authentication an input window appears on the caller's screen in Windows that requests the ISDN telephone number of the PC.

### The calling number is determined in the *ELSA LANCOM DSL/I-10 Office*

For this setting the callback entry must be set to 'Call back remote station after checking name' (or must be set to the value 'Name' in *ELSA WEBconfig* or in the console). In the name list **a** telephone number must be specified.

Some Windows versions (especially Windows 98) prompt the user to confirm the callback to the telephone number stored in the *ELSA LANCOM DSL/I-10 Office* ('Administrator Specified') with an input window. Other Windows versions only inform the user that the PC is waiting for the callback from the *ELSA LANCOM DSL/I-10 Office*.



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

## 8.7.2

### Fast callback using the *ELSA* process

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



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

*For fast callback using the ELSA method, the number list for answering calls must be kept up to date at both ends.*

### 8.7.3

## Callback with RFC 1570 (PPP LCP extensions)

The callback as per 1570 is the standard method for calling back routers of other manufacturers. This protocol extension describes five possibilities for requesting a callback. All versions are recognized by *ELSA LANCOM DSL/I-10 Office*. The same applies to all options:

The *ELSA LANCOM DSL/I-10 Office* drops the connection after authenticating the remote station and then calls back the station a few seconds later.

### Configuration

For callback as per PPP you select the option 'Call back remote station' in *ELSA LANconfig* or 'Auto' with configuration via *ELSA WEBconfig*, terminal program or Telnet.



*For callback as per PPP the number list for answering calls in the ELSA LANCOM DSL/I-10 Office must be up to date.*

### 8.7.4

## Overview of configuration of callback function

In the ISDN name list the following options are available for the callback entry under *ELSA WEBconfig* and terminal program/Telnet:

With this entry...	...the callback is thus entered:
'Off'	No callbacks.
'Auto' (not with Windows operating systems, see below)	The remote station will be called back if so specified in the name list. At first, the call is denied and as soon as the channel is clear again, it is called back (duration is approx. 8 seconds). If the remote station is not found in the numerical list, it is first accepted as the DEFAULT remote station, and the callback is negotiated during the protocol negotiation. Thus a one-unit charge is applied.

With this entry...	...the callback is thus entered:
'Name'	Before a callback occurs, a protocol negotiation is always carried out even when the remote station was found in the numerical list (e.g. for computers with Windows having direct dialing on the device). Here only minor charges result.
'ELSA'	When the remote station is found in the numerical list, a quick callback is carried out, i.e., the <i>ELSA LANCOM DSL Office</i> sends a special signal to the remote station and calls back immediately when the channel is clear again. After approx. 2 seconds, the connection is established. If the remote station does not take back the call immediately after the signal, then after two seconds the situation reverts back to normal callback procedures (duration is once again approx. 8 seconds). This procedure is only available with DSS1 connections.
'Looser'	Use the 'Looser' option when a callback is expected from the remote station. This setting carries out two functions simultaneously. On the one hand, it ensures that a custom connection setup is taken back when there is an incoming call from the called remote station, and on the other hand, the function is activated with this setting to be able to react to the rapid callback procedure. In other words, in order to be able to use rapid callback, the caller must be in the 'Looser mode' while the party being called must discontinue callback with 'ELSA'.



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



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

## 8.8

### Channel bundling with MLPPP

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



*Of the *ELSA LANCOM DSL Office* series, only the *ELSA LANCOM DSL/I-10 Office* features an ISDN connection. The descriptions in this section therefore only apply to this device.*

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

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

## Two methods of channel bundling

### ● Static channel bundling

If a connection is established with static channel bundling, the *ELSA LANCOM DSL/I-10 Office* tries to establish the second B-channel immediately after setting up the first B-channel. If this does not work because, for example, this channel is already taken by another device or a different connection within the *ELSA LANCOM DSL/I-10 Office*, the connection attempt is automatically and regularly repeated until the second channel is available for it.

### ● Dynamic channel bundling

In the case of a connection with dynamic channel bundling, the *ELSA LANCOM DSL/I-10 Office* first only establishes one B-channel and begins transmitting data. If, during this connection, it determines that the throughput rate lies above a certain threshold value, it tries to add the second channel.

If the second channel is established and the data throughput rate drops below the threshold value, the *ELSA LANCOM DSL/I-10 Office* waits for the set B2 timeout period and then automatically closes the channel again. Any partly used call charge units are used up completely if call charge information is transmitted during the connection. Therefore, the *ELSA LANCOM DSL/I-10 Office* only uses the second B-channel if and as long as it really needs it.

## Channel bundling is thus established

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

- ① Select a communication layer for the remote station from the layer list that has bundling activated in the Layer-2 options. Select from the following Layer-2 options:

- **data compr** according to LZS data compression procedures (Stac) reduces the data volume when the data has not yet been compressed. This procedure is also supported by routers of other manufacturers and by ISDN adapters under Windows operating systems.
  - **bundle** uses two B-channels per connection.
  - **bnd+cmpr** uses both (compression and channel bundling) and provides the maximum possible data transmission performance.
- ② Now create a new entry in the ISDN name list. When doing so, watch the holding times for the connection. Please note the following points:
- Depending on the type of application, the B1 hold time should be increased to such a level so that the connection is not dropped prematurely because of packets not being transmitted for a short time. Customarily, values between 60 and 180 seconds are a good base to begin with which one can continue to adjust during operation.
  - The B2 holding time determines whether static or dynamic channel bundling will be used (see above). A B2 holding time of '0' or '9999' ensures that the bundling will be static; values in between permit dynamic channel bundling. The B2 holding time defines how long the data throughput may lie below the threshold for dynamic channel bundling without the second B-channel automatically being disconnected.
- ③ Use the entry for the Y connection in the Router interface list to determine what should happen if a second connection to a different remote station is requested during an existing connection using channel bundling.

*ELSA WEBconfig*

Expert configuration ► Setup ► WAN module ►  
Router interface list

Terminal/Telnet

```
cd /setup/WAN-module
set router-interface-list [...]
```

- Y connection **On**: The router interrupts the bundled connection to establish a connection to the other remote station. When the second 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 maintains the existing bundled connection; the establishment of the new connection must wait.



*Please note that if channel bundling is used, the cost of two connections is charged. Here no additional connections via the ELSA LANCAP1 are possible! So you should only use channel bundling if the double transmission capacity can really be used in full.*



# 9 Technical data

## 9.1 Performance data and specifications

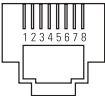
	<b><i>ELSA LANCOM DSL Office</i></b>
Functions	all devices: IP router, DNS server, DHCP server; simultaneous operation of all functions possible  additional for <i>ELSA LANCOM DSL/I-10 Office</i> : IPX router, CAPI server, least-cost router for router and CAPI connections
10Base-T WAN connection	Ethernet IEEE 802.3, 10Base-T (RJ45) with PPP-over-Ethernet (PPPoE) or PPTP as communication protocol
ISDN interface ( <i>ELSA LANCOM DSL/I-10 Office</i> only)	Connection: ISDN S <sub>0</sub> bus, point-to-point and point-to-multipoint configuration, I.430; D channel: 1TR6, Euro-ISDN (DSS1), autosensing, optional fixed connection support Group 0 (D64S, D64S2, D64SY); B-channel: PPP (asynch./synch.), MLPPP, X.75, HDLC, V.110, CAPI 2.0 via <i>ELSA LANCAPI</i> , Stac data compression
LAN connection	Ethernet IEEE 802.3, 10/100Base-Tx (RJ45, node/hub switch), auto-sensing, full duplex
Network protocols	all devices: IP router ARP, Proxy ARP, DHCP server, IP, ICMP, UDP, TCP, RIP-1, RIP-2, Proxy DNS  additional for <i>ELSA LANCOM DSL/I-10 Office</i> : Proxy NetBIOS/IP IPX router: IPX, SPX, RIP, SAP, Novell NetBIOS, Novell burst mode
Security functions	all devices: PAP, CHAP and MS-CHAP for authentication under PPP; filtering options in router mode; configuration protected by access lists and passwords; accounting for recent connection information; IP masquerading  additional for <i>ELSA LANCOM DSL/I-10 Office</i> : Evaluation of the telephone number of the remote station (CLIP); automatic call-back via ISDN;
Filter possibilities (fire-wall)	all devices: IP router Source and target filters for networks, protocols and ports; MAC address filter  additional for <i>ELSA LANCOM DSL/I-10 Office</i> – IPX router: RIP, SAP, IPX and SPX watchdog, sockets, routes, propagated packets
IP masquerading	Translation of internal IP addresses and ports to an external IP address; static/dynamic IP address assignment via PPP; masking of TCP, UDP, ICMP and FTP; DNS forwarding; inverse masquerading of intranet services such as web server (DMZ)
Spoofing ( <i>ELSA LANCOM DSL/I-10 Office</i> only)	IPX router: RIP and SAP packets; IPX and SPX watchdogs, Novell NetBIOS, keep-alive-packets

	<b><i>ELSA LANCOM DSL Office</i></b>
CAPI server ( <i>ELSA LANCOM DSL/I-10 Office</i> only)	Virtual CAPI 2.0 for Windows operating systems, NDIS-WAN drivers, fax class 1
Line control, transfer optimization	all devices: Keep-Alive on WAN connections, Policy Based Routing, SYN/ACK speedup  additional for <i>ELSA LANCOM DSL/I-10 Office</i> – automatic callback via ISDN with or without connections establishment; Line-on-demand (dynamic channel bundling), short-hold mode, round-robin selection, fast callback, dial-backup for fixed connections
Charge monitoring	Maximum online time or charges per period
Management	all devices: Via LAN or V.24, <i>ELSA LANconfig</i> <i>ELSA LANmonitor</i> for Windows management software, configuration via SNMP v. 1, TFTP, Telnet or terminal  additional for <i>ELSA LANCOM DSL/I-10 Office</i> – via ISDN (teleservice)
Operating security	Hardware watchdogs, regular self-testing, <i>ELSA FirmSafe</i> concept for remote software upgrades
Statistics	Separate counter for LAN/WAN; packets, errors, connections and online time; logging of connection control and online time with <i>ELSA LANmonitor</i> and SYSLOG; accounting of connections, online time, volume per IP with <i>ELSA LANmonitor</i> ; trace of protocols for diagnostic purposes
Display/operation	LEDs for power, WAN and LAN status; node/hub switch
Power supply	12 V AC with AC adapter for 230 V, 12 VA
Environmental conditions	Temperature: 5–40°C, humidity: 0–80%, non-condensing
Dimensions and design	Rugged metal case, connections on rear panel; dimensions 230 x 38 x 228 mm (W x H x D)
Package contents	Power supply unit, cable for outband port, ISDN connection cable ( <i>ELSA LANCOM DSL/I-10 Office</i> only), two LAN twisted-pair cables, detailed documentation and <i>ELSA LANCOM Office</i> CD; <i>ELSA LANconfig</i> , <i>ELSA LANmonitor</i> , <i>ELSA LANCAPI</i> , <i>ELSA CAPI</i> Faxmodem, office communications software <i>ELSA-RVS-COM</i> , LapLink Pro
Approvals	For Germany, Switzerland and all other EU countries
Service and warranty	6 years warranty
Support	via hotline and Internet

# 9.2 Contact assignment

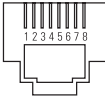
## 9.2.1 Ethernet ports 10/100Base-T (LAN) and 10Base-T (WAN)

8-pin RJ45 sockets as per ISO 8877, EN 60603-7

Connector	RJ45 pin	Line
	1	T+
	2	T-
	3	R+
	4	–
	5	–
	6	R-
	7	–
	8	–

## 9.2.2 ISDN S<sub>0</sub> interface

8-pin RJ45 socket as per ISO 8877, EN 60603-7

Connector	RJ45 pin	Line	IAE
	1	–	–
	2	–	–
	3	T+	2A
	4	R+	1A
	5	R-	1b
	6	T-	2b
	7	–	–
	8	–	–

## 9.2.3

## Configuration interface(outband)

8-pin mini-DIN socket



Connector	Mini-DIN, 8-pin	Line
	1	CTS
	2	RTS
	3	RxD
	4	RI
	5	TxD
	6	DSR
	7	DCD
	8	DTR
	U	GND

## 10

## Appendix

## 10.1

## 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 for the defective product. Operating manuals and possibly supplied software are excluded from the warranty.
- b) Material and service charges shall be covered by us, but not shipping and handling costs involved in transport from the buyer to the service station and/or to us.
- c) Replaced parts become property of ELSA.
- d) ELSA are authorized to carry out technical changes (e.g. firmware updates) beyond repair and replacement of defective parts in order to bring the equipment up to the current technical state. This does not result in any additional charge for the customer. A legal claim to this service does not exist.

**2 Warranty period**

The warranty period for this ELSA product is six years. This period begins at the day of delivery from the ELSA dealer. Warranty services do not result in an extension of the warranty period nor do they initiate a new warranty period. The warranty period for installed replacement parts ends with the warranty period of the device as a whole.

**3 Warranty procedure**

- a) If defects appear during the warranty period, the warranty claims must be made immediately, at the latest within a period of 7 days.
- b) In the case of any externally visible damage arising from transport (e.g. damage to the housing), the transport company representative and ELSA should be informed immediately. On discovery of damage which is not externally visible, the transport company and ELSA are to be immediately informed in writing, at the latest within 7 days of delivery.
- c) Transport to and from the location where the warranty claim is accepted and/or the repaired device is exchanged, is at the purchaser's own risk and cost.
- d) Warranty claims are only valid if the original purchase receipt is returned with the device.

**4 Suspension of the warranty**

All warranty claims will be deemed invalid

- a) if the device is damaged or destroyed as a result of acts of nature or by environmental influences (moisture, electric shock, dust, etc.),
- b) if the device was stored or operated under conditions not in compliance with the technical specifications,

- c) if the damage occurred due to incorrect handling, especially to non-observance of the system description and the operating instructions,
- d) if the device was opened, repaired or modified by persons not authorized by ELSA,
- e) if the device shows any kind of mechanical damage,
- f) if in the case of an ELSA Monitor, damage to the cathode ray tube (CRT) has been caused especially by mechanical load (e.g. from shock to the pitch mask assembly or damage to the glass tube), by strong magnetic fields near the CRT (colored dots on the screen), or through the permanent display of an unchanging image (phosphor burnt),
- g) if, and in as far as, the luminance of the TFT panel backlighting gradually decreases with time, or
- h) if the warranty claim has not been reported in accordance with 3a) or 3b).

## 5 Operating mistakes

If it becomes apparent that the reported malfunction of the device has been caused by unsuitable software, hardware, installation or operation, ELSA reserves the right to charge the purchaser for the resulting testing costs.

## 6 Additional regulations

- a) The above conditions define the complete scope of ELSA's legal liability.
- b) The warranty gives no entitlement to additional claims, such as any refund in full or in part. Compensation claims, regardless of the legal basis, are excluded. This does not apply if e.g. injury to persons or damage to private property are specifically covered by the product liability law, or in cases of intentional act or culpable negligence.
- c) Claims for compensation of lost profits, indirect or consequential detriments, are excluded.
- d) ELSA is not liable for lost data or retrieval of lost data in cases of slight and ordinary negligence.
- e) In the case that the intentional or culpable negligence of ELSA employees has caused a loss of data, ELSA will be liable for those costs typical to the recovery of data where periodic security data back-ups have been made.
- f) The warranty is valid only for the first purchaser and is not transferable.
- g) The court of jurisdiction is located in Aachen, Germany in the case that the purchaser is a merchant. If the purchaser does not have a court of jurisdiction in the Federal Republic of Germany or if he moves his domicile out of Germany after conclusion of the contract, ELSA's court of jurisdiction applies. This is also applicable if the purchaser's domicile is not known at the time of institution of proceedings.
- h) The law of the Federal Republic of Germany is applicable. The UN commercial law does not apply to dealings between ELSA and the purchaser.

# 10.2

## Declaration of conformity European Union (CE)

The CE declarations of conformity for the *ELSA LANCOM DSL Office* are available for download on the ELSA web site ([www.elsa.com/download](http://www.elsa.com/download)).

# 11 Index

## ● Numerics

10/100Base-TX .....	22
100-Mbit network .....	22
10Base-T connection .....	22

## ● A

Access control .....	58
Access protection .....	66
name .....	66
name or number .....	67
number .....	67
Additional limit .....	86
Address administration .....	73
Address pool .....	75
Answer-phone .....	11
AOCD .....	87
Authentication .....	16, 123
Autosensing .....	22
Availability .....	95

## ● B

Backup .....	118
BACP .....	17
Barring .....	57
B-channel	
connection status .....	14
protocol .....	68
Block domain .....	84
Brute force .....	13, 57

## ● C

Cable modem .....	10, 12
Cable modem connection .....	22
Call charge information .....	87, 126
Call charge limit .....	85
Call charge management .....	85
Call charge units .....	126

Callback .....	11, 66, 68
fast callback .....	69
Callback function .....	16
Caller ID .....	66
Caller identification .....	16
Calling Line Identifier Protocol .....	69
CAPI Faxmodem .....	97
CAPI interface .....	91
CBCP .....	122
Challenge Handshake	
Authentication Protocol .....	67
Channel bundling .....	17, 125
dynamic .....	17, 126
Static .....	126
static .....	17
CHAP .....	67
Charge monitoring .....	15
Charge units .....	87
CLIP .....	16, 68, 69
Common ISDN Application Programming	
Interface .....	91
Compression .....	17
Computer names .....	78
Conf .....	119
Configuration .....	14
procedures .....	37
SNMP .....	42
Configuration interface .....	23, 37
Connect-charge monitoring .....	92
Connection control .....	87
Connection duration .....	14
Connection limits .....	87
Connections .....	21
Contact assignment .....	131
configuration interface .....	132
Ethernet port .....	131
ISDN S <sub>0</sub> interface .....	131

LAN port .....	131
Outband .....	132
WAN port .....	131
Cost reduction .....	85

## D

Data compression procedures	
LZS .....	127
Data transmission .....	126
D-channel .....	50, 68
Device name .....	118
DHCP .....	50, 73
DHCP for WINS Resolution .....	77
DHCP mode .....	74
DHCP server .....	73, 79
Dial-up connection .....	11
Dial-Up Network .....	42, 67
Distance of a route .....	103
DNS .....	50, 78
DNS forwarding .....	80
DNS forwarding mechanism .....	80
DNS server .....	13, 73, 76, 79
available information .....	80
filter list .....	84
filter mechanism .....	79
DNS table .....	83, 84
Domain .....	84
Domain name service .....	78
Domains .....	78
Drivers .....	3
DSL connection .....	22
DSL modem .....	10, 12
Dynamic channel bundling .....	17, 126
Dynamic Host Configuration Protocol .....	73
Dynamic routing .....	101

## E

ELSA CAPI fax modem .....	16
ELSA FirmSafe .....	15, 52
ELSA LANCAPI .....	14

ELSA LANCAPI .....	43
ELSA LANconfig .....	38, 43, 53
ELSA LANmonitor .....	46
Display options .....	47
Monitor Internet connection .....	47
System information .....	47
ELSA protocol .....	68
ELSA WEBconfig .....	53
ELSA-RVS-COM .....	11
ELSA-ZOC .....	11
E-mail .....	10
End address .....	75
Ethernet .....	12
10/100Base-T .....	12
Fast Ethernet .....	12
Eurofile transfer .....	16
Exclusion routes .....	103

## F

Fail .....	119
FAQs .....	3
Fast callback .....	69
Fast Ethernet .....	12
Fast-Ethernet	
10/100Base-T .....	12
Fax .....	11, 17, 97
Fax Class 1 .....	97
Fax driver .....	97
Fax modem .....	16
Fax transmission .....	97
File transfer .....	10
Filter .....	58
Filter list .....	65
Filter mechanisms .....	11
Firewall .....	13, 58, 59
Firewall filter .....	10
Firewall functions .....	92
Firmware .....	3, 15
Firmware update .....	15
Firmware upload .....	53



- using TFTP ..... 54
  - with *ELSA LANconfig* ..... 53
  - with *ELSA WEBconfig* ..... 54
  - with terminal program ..... 54
- Flash ROM ..... 15, 52
- Flatrate ..... 120
- Frequently Asked Questions ..... 3
- **G**
  - Gateway ..... 59, 73, 76
- **H**
  - High telephone costs ..... 85
  - Hold time ..... 127
  - Home office ..... 11
  - Host ..... 79
- **I**
  - Identification control ..... 66
  - Identifying the caller ..... 67
  - Inband ..... 37
    - using Telnet ..... 41
  - Inband configuration ..... 37
  - Install software ..... 52
  - Installation ..... 12
  - Interfaces ..... 21
  - Internet ..... 10, 58
  - Internet access ..... 35, 117
  - Internet address ..... 60
  - Internet service provider ..... 10
  - Intranet address ..... 60
  - Inverse masquerading ..... 61
  - IP address ..... 48, 59, 116
  - IP address administration ..... 73
  - IP address range ..... 62
  - IP broadcast ..... 107
  - IP masquerading ..... 10, 13, 50, 58
    - simple masquerading ..... 61
    - supported protocols ..... 62
  - IP multicast ..... 107
  - IP port ..... 95
  - IP routing ..... 12
  - IP routing table ..... 101
  - IP-Routing
    - Standard router ..... 103
  - ISDN
    - B-channel ..... 68
    - D-channel ..... 12, 69
  - ISDN cable ..... 12
  - ISDN connection charges ..... 85
  - ISDN time ..... 17
  - ISDN/S<sub>0</sub> connection ..... 22
- **K**
  - Keep-Alive ..... 120
  - KnowledgeBase ..... 3
- **L**
  - LAN connection ..... 12
  - LAN connector cable ..... 23
  - LAN to LAN coupling ..... 11
  - LANCAP1 ..... 16
  - LCP echo reply ..... 116
  - LCP echo request ..... 116
  - LCR ..... 17, 87
  - Leased lines ..... 11
  - Leased-line option ..... 17
  - Least-cost routing ..... 17, 87
  - LED ..... 19
  - LED indicators ..... 14
  - Line connection ..... 12
  - Line management ..... 11, 12
  - Login ..... 52, 57
  - Login barring ..... 57
  - LZS data compression ..... 127
- **M**
  - MAC address ..... 62
  - MAC address filters ..... 13
  - Mail server ..... 83

Media Access Control .....	62
MLPPP .....	17, 125, 126
Mode .....	74
Monitoring .....	46
MS CHAP .....	115
MS-CHAP .....	114
Multi-device connection .....	12
Multilink PPP .....	114, 126

## N

NAT .....	58
NBNS server .....	73, 76, 77
NetBIOS .....	50, 79
NetBIOS networks .....	79
NetBIOS-Proxy .....	16
Network names .....	78
No charge information .....	87
Node/hub switch .....	22

## O

Object table .....	64
Office communications .....	91
online minutes .....	85
Online research .....	10
Outband .....	37
Outband configuration .....	37

## P

Package contents .....	23
Packet dump .....	50
PAP .....	67
passwd .....	56
Password .....	45, 47, 66, 67, 118
Password Authentication Protocol .....	67
Password protection .....	16, 55
PAT .....	58
Peer-to-peer networks .....	16
Period .....	85
Period of validity .....	74, 76
Point-to-multipoint configuration .....	12

Point-to-point configuration .....	12
Point-to-Point Tunneling Protocol .....	119
Policy Based Routing .....	108, 130
Port .....	95
Port number .....	61
Power .....	19
Power supply unit .....	21, 23
PPP .....	16, 48, 67, 126
Assigning IP addresses .....	116
Callback functions .....	122
checking the line with LCP .....	116
LCP Extensions .....	124
PPP client .....	37, 43
PPP connection .....	44
PPP list .....	67
PPP negotiation phase .....	45
PPTP .....	119
Priority control .....	95
Protection for the configuration .....	55
Protection for the LAN .....	58
protection of the configuration .....	55

## R

Remote access .....	11, 42, 117
Remote configuration .....	16, 37
Remote connection .....	43
Remote site .....	118
Rep .....	119
Repetitions .....	119
RIP .....	49
Router .....	102
Router interface list .....	127
Rules table .....	65

## S

S <sub>0</sub> port .....	12
Security .....	55, 58
Security checklist .....	69
Security functions .....	10
Security procedures .....	68

Security settings .....	56
Serial port .....	37
Service .....	79
Set up access to the Internet .....	35
Single User Access .....	58
SNMP .....	42
Specify IP parameters yourself .....	33
Stac .....	127
Stac data compression .....	17
Standard fax programs .....	97
Start address .....	75
Static channel bundling .....	17, 126
Static routing .....	101
Station Name Table .....	82
Statistics .....	15
Status displays .....	14
Support .....	3
SYN/ACK speedup .....	109, 130
System connection .....	12

## T

TCP/IP .....	101
TCP/IP networks .....	78
Technical data .....	129
Telnet .....	14, 43
Term .....	119
Terminal program .....	14, 53
TFTP .....	42
Throughput .....	126
Time .....	119
Time budget .....	87

Time check .....	17
Time limit .....	85
Time-dependent connection control .....	87
Time-out .....	126
Trace	
code and parameters .....	49
Examples .....	50
outputs .....	48
starting .....	49
Transmission rates .....	14, 48
Troubleshooting .....	46
Type of Service .....	108

## U

Upload .....	15, 52
User name .....	45, 67, 118

## V

V.24 configuration interface .....	22
------------------------------------	----

## W

WAN connection .....	12
WAN connector cable .....	23
Warranty conditions .....	133
Wildcards .....	84
Windows network .....	77
Windows networks .....	16
WINS Address .....	77

## Y

Y connection .....	127
--------------------	-----

