

# ■ ***ELSA LANCOM™ DSL/10 Office***

© 2000 ELSA AG, Aachen (Germany)

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

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

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

#### Trademarks

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

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

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

ELSA AG

Sonnenweg 11

52070 Aachen

Germany

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

Aachen, February 2000

# Preface

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

By selecting the *ELSA LANCOM DSL/10 Office* you have chosen a router which you can use to connect local area networks or single workstations to the Internet via an xDSL connection. You can now surf the Internet 12 times faster than over a single B channel in the ISDN network.

The highest quality standards in manufacturing and stringent quality control are the basis for high product standards and consistent quality of ELSA products.

## **Documentation**

The accompanying documentation comprises:

- Manual  
Hardware installation, description of functions and operating modes and examples of configurations
- CD containing electronic documentation  
Basic technical information (e.g. on xDSL, general network technology, TCP/IP), workshop with comprehensive usage examples, reference section with complete menu description



*Our online services (Internet server [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 under 'Know-How', you can find answers to frequently asked questions (FAQs). The KnowledgeBase also contains a large pool of information. Current drivers, firmware, tools and manuals can be downloaded at any time.*

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



# Contents

<b>Introduction .....</b>	<b>1</b>
What does a router do? .....	1
What does the <i>ELSA LANCOM DSL/10 Office</i> offer? .....	2
<b>Installation .....</b>	<b>5</b>
Package contents .....	5
Introducing the <i>ELSA LANCOM DSL/10 Office</i> .....	5
How to connect the router .....	7
Software installation .....	8
Basic configuration .....	8
Make basic settings with <i>ELSA LANconfig</i> .....	8
Configuring the basic settings using telnet .....	10
<b>Configuration modes .....</b>	<b>11</b>
Many paths lead to the <i>ELSA LANCOM DSL/10 Office</i> .....	11
The user-friendly method: inband .....	11
Preconditions .....	11
Alternatively: Address administration with the DHCP server .....	12
Beginning configuration using <i>ELSA LANconfig</i> .....	12
Start up inband configuration using telnet .....	13
Configuration commands .....	13
New firmware with FirmSafe .....	14
This is how FirmSafe works .....	14
How to load new software .....	15
Configuration using SNMP .....	17
General .....	17
Accessing tables and parameters using SNMP .....	18
The Management Information Base (MIB) .....	20
<b>Operating modes and functions .....</b>	<b>21</b>
Security for your configuration .....	21
Password protection .....	21
Login barring .....	22
Access control via TCP/IP .....	22
Security for your LAN .....	22
The hiding place—IP masquerading (NAT/PAT) .....	23
TCP/IP packet filters .....	23
Call charge management .....	23
Time-dependent connection control .....	23
Settings in the charge module .....	24
xDSL connections .....	24

Name-list.....	26
PPP-list .....	27
IP routing .....	27
The IP routing table.....	27
Local routing.....	29
Dynamic routing with IP RIP.....	29
IP masquerading (NAT, PAT).....	31
DNS forwarding .....	32
Policy Based Routing.....	32
Automatic address administration with DHCP .....	33
The DHCP server .....	33
DHCP—'on', 'off' or 'auto'?.....	33
How are the addresses assigned? .....	34
DNS.....	36
What does a DNS server do?.....	36
Setting up the DNS server .....	37
<b>Appendix .....</b>	<b>41</b>
Technical data.....	41
Declaration of conformity .....	42
Warranty conditions .....	43
<b>Index .....</b>	<b>45</b>
<b>Description of the menu options (on CD only) .....</b>	<b>R1</b>
Status.....	R3
Status/Connection-state .....	R4
Status/Current-time .....	R4
Status/Operating-time .....	R4
Status/WAN-statistics.....	R4
Status/LAN-statistics.....	R6
Status/PPP-statistics.....	R8
Status/TCP-IP-statistics .....	R13
Status/IP-router-statistics.....	R18
Status/Config-statistics .....	R20
Status/DSL-statistics .....	R20
Status/DSL-statistics/PPPoE-statistics.....	R21
Status/Queue-statistics .....	R22
Status/Connection-statistics .....	R23
Status/Info-connection .....	R23
Status/Remote-statistics .....	R23
Status/Channel-statistics .....	R24
Status/Time-statistics.....	R25
Status/Delete-values .....	R25



Setup .....	R25
Setup/WAN-module .....	R26
Setup/Charges-module .....	R29
Setup/LAN-module .....	R30
Setup/TCP-IP module .....	R31
Setup/IP-router-module .....	R34
Setup/SNMP-module .....	R42
Setup/DHCP-server-module .....	R43
Setup/DNS module .....	R45
Setup/Config-module .....	R46
Setup/Time-module .....	R47
Firmware .....	R47
Other .....	R49





# Introduction

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

New technologies are eliminating the restrictions and are offering the user true broadband communications at significantly higher transfer speeds. An important criterion for the spread of these new access technologies is their availability in as many offices and companies as possible. One new technology is transmission by xDSL, which covers the "last mile" over conventional copper wires.

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

*ELSA LANCOM DSL/10 Office* can connect individual workstations or entire local networks to the Internet. It makes it possible for you to download data from the Internet at previously unknown speeds (768 Kbps).

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

## What does a router do?

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

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

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

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

When precisely should the router be used?

As a matter of fact, wherever computers need to be joined together and a simple modem operation no longer fits the bill. An example is the use of the Internet in the LAN.

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

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

## **What does the *ELSA LANCOM DSL/10 Office* offer?**

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

### **Easy installation**

- Connect the *ELSA LANCOM DSL/10 Office* to the power supply.
- Establish a link to the LAN.
- Connect to the xDSL terminal.
- Switch it on.
- Go!

### **LAN connection**

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

### **WAN connection**

The *ELSA LANCOM DSL/10 Office* can be connected to the Ethernet interface of an xDSL connection.

### **Status displays**

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

### **Configuration with *ELSA LANconfig***

Setting up and configuring the device to your specific needs is made quick and easy in the Windows operating systems by the configuration tool supplied, *ELSA LANconfig*. Users of other operating systems can use any telnet or terminal program.

The integrated installation wizards help you to setup the devices in just a few steps.

### **Software update**

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

### **FirmSafe**

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

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

### **DHCP**

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

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

### **Charge monitoring**

The charges for Internet usage are calculated by the provider depending on the time used. To prevent unpleasant surprises from unexpectedly high telephone bills at the end of the month, you can preset the number of online minutes allowed for a specified period (e.g. 10 hours in 6 days) while using a *ELSA LANCOM DSL/10 Office*.

### **Access protection**

The router offers protection against unauthorized access to the company network not only with simple password protection but also a complete security concept with firewall filters and IP masquerading. Furthermore, login barring prevents any "brute force attacks" and denies access to the router after a configurable number of login attempts using an incorrect password.

**DNS server**

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

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

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.

# Installation

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

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

## Package contents

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

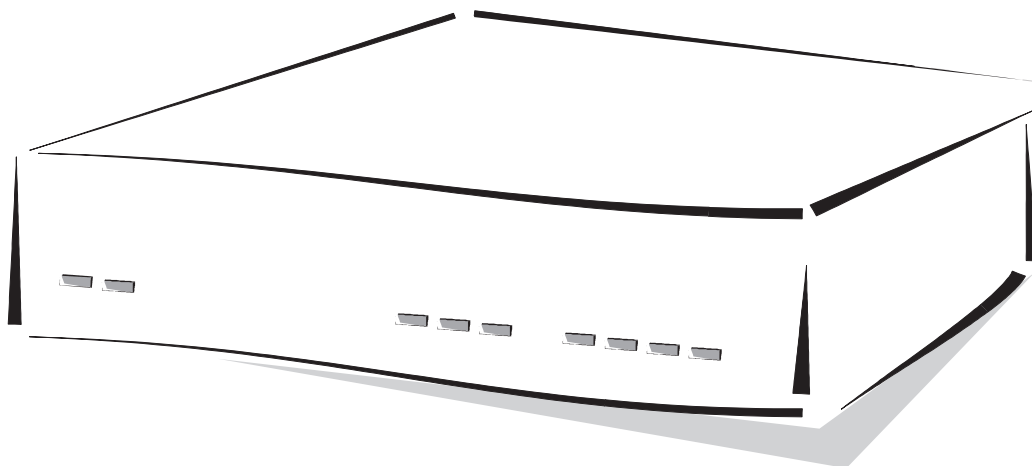
- Power supply unit
- LAN connection cable
- xDSL connection cable
- Configuration interface cable
- Configuration cable adapter
- Documentation
- CD containing *ELSA LANconfig*, other software and electronic documentation

Please contact your dealer directly if anything is missing.

## Introducing the ***ELSA LANCOM DSL/10 Office***

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

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



#### *Power/Msg*

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

Off		Device off
red	1 x short	Boot procedure (test and load) started
red	flashing	Display of a boot error (flashing light code)
red		Device ready for use

#### *DSL-Rx/Tx*

This yellow LED shows that data is moving on the DSL connection.

#### *DSL-Link*

This green LED shows that the Ethernet connection between *ELSA LANCOM DSL/10 Office* and the DSL terminal is operating properly.

#### *DSL-Chan*

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

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



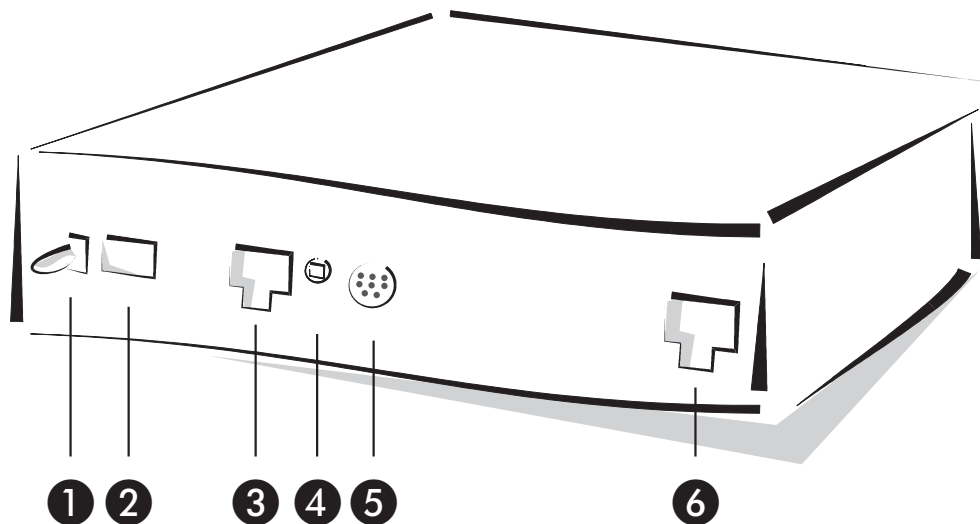
*The connection is active and incurring charges so long as the 'DSL-Chan' LED is green!*

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

These LEDs show the corresponding network controller status:

LAN-rx/tx	yellow	Data packet sent from the device to the LAN or vice versa
LAN coll	red	Sending collision
LAN-Link	green	Connection to LAN is established and ready
LAN-FDpx	green	Router is transmitting and receiving data simultaneously
LAN-Fast	green	<i>ELSA LANCOM DSL/10 Office</i> is operating at 100 Mbit

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



- ❶ On/Off switch
- ❷ Connection for power supply unit
- ❸ 10/100Base-Tx for 10 Mbit or 100 Mbit networks
- ❹ Node/hub selector switch
- ❺ V.24 configuration interface
- ❻ 10Base-T terminal for xDSL or cable modem

## How to connect the router

- ❶ Connect the router *ELSA LANCOM DSL/10 Office* to the LAN. Plug the network cable (supplied) into the 10/100Base-T network terminal of the device and into a free network connector on your local network (or into a free socket on a hub in your LAN).
- ❷ Connect the device to the Ethernet port of the xDSL (e.g. NTBBA from Deutsche Telekom) or cable modem.
- ❸ Give your device the power it needs through the power supply unit! After a short device self-test the 'Power/Msg' LED will be permanently lit. The 'LAN Link' LED indicates that your router is correctly connected to the LAN.



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

## Software installation

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

You will need a PC on the LAN to run the configuration software.

- ① Install the TCP/IP network protocol on the computer that will be used to set up the access point.
- ② Then install *ELSA LANconfig*. If the setup program does not start up automatically after insertion of the *ELSA LANCOM* CD, start Windows Explorer, click on 'autorun.exe' on the CD *ELSA LANCOM* and follow the instructions in the install program.

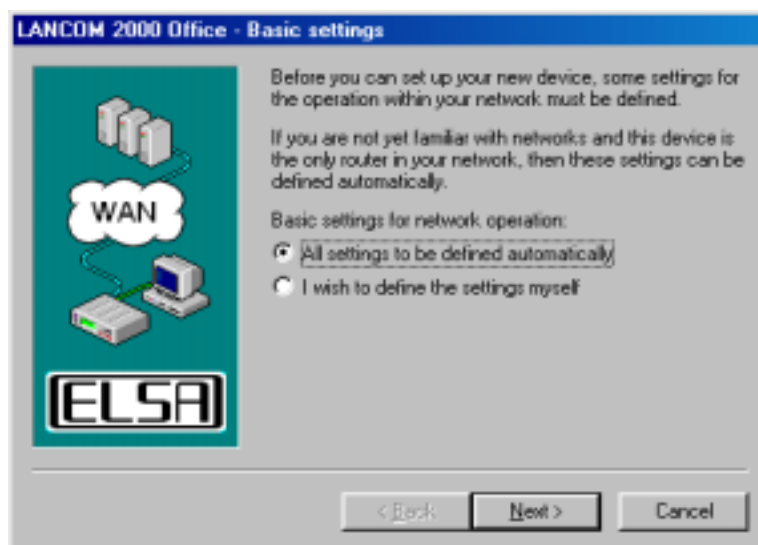
## Basic configuration

The IP address for the access point is set during the basic configuration. In addition, the decision on whether to use the integrated DHCP server is made. You can run the basic configuration with *ELSA LANconfig* or with telnet.

### Make basic settings with *ELSA LANconfig*

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

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





- ② Select the option 'make all settings automatically' if you are **not** familiar with networks and IP addresses and one of the following conditions applies:
- You have not used any IP addresses previously in your network but would now like to do so. You do not care which IP address should be used. The router as a DHCP-server will automatically set and assign the IP addresses for all devices in the network (LAN and WLAN).
- or
- You do not wish to use IP addresses, perhaps because you have a Windows-only network.



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

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

- ③ Select the option 'I want to make the settings myself' if you are familiar with networks and IP addresses and one of the following conditions applies:
- You have not used any IP addresses previously in your network but would now like to do so. However, you wish to set the IP address for the router and assign it an address from an address range reserved for private use, e.g. '10.0.0.1' with the network mask '255.255.255.0'. At the same time you will set the address range that the DHCP server uses for the other devices in the network (so long as the DHCP server is not switched off).
  - You have previously used IP addresses on the computers in the LAN. Assign the router a free address from the previously used address range, and select whether the router should run as a DHCP server or not.



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

- ④ The Internet access wizard starts automatically on completion of the basic settings wizard. Enter only the user name and the password supplied by your provider.
- ⑤ After these few mouse clicks your router is fully set up for access to the Internet.

## Configuring the basic settings using telnet

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

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

Enter the following command:

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

- ② Change the language for the configuration with the command:

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

- ③ Intranet address and network mask:

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

*After changing the Intranet address, the telnet connection is terminated by the router and you will need to establish a new telnet connection to the set Intranet address.*

- ④ To switch off the DHCP function:

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

- ⑤ Set up provider in the name list:

```
set /Setup/WAN module/name list internet 20
```

- ⑥ Input access data into the PPP list:

```
set /Setup/WAN module/PPP list Internet no 'your password'
0 5 'your user name'
```

- ⑦ Set route into Internet:

```
set /Setup/IP-router-module/IP-routing-tab 255.255.255.255
0.0.0.0 internet 0 ON
```

*Even if the entries at this point are not very clear without further explanation, you can reach the same destination as with the setup with *ELSA LANconfig*: This establishes access to the Internet for the first time!*



# Configuration modes

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

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

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

## Many paths lead to the *ELSA LANCOM DSL/10 Office*

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

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

What is the difference between these?

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

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

## The user-friendly method: inband

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

## Preconditions

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

A device that has not been configured yet will respond to the IP address XXX.XXX.XXX.254, in which the Xs are placeholders for the network address in your LAN. If the computers on your network have addresses such as 192.110.130.1, then you will be able to address the device using 192.110.130.254.



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

## Alternatively: Address administration with the DHCP server

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

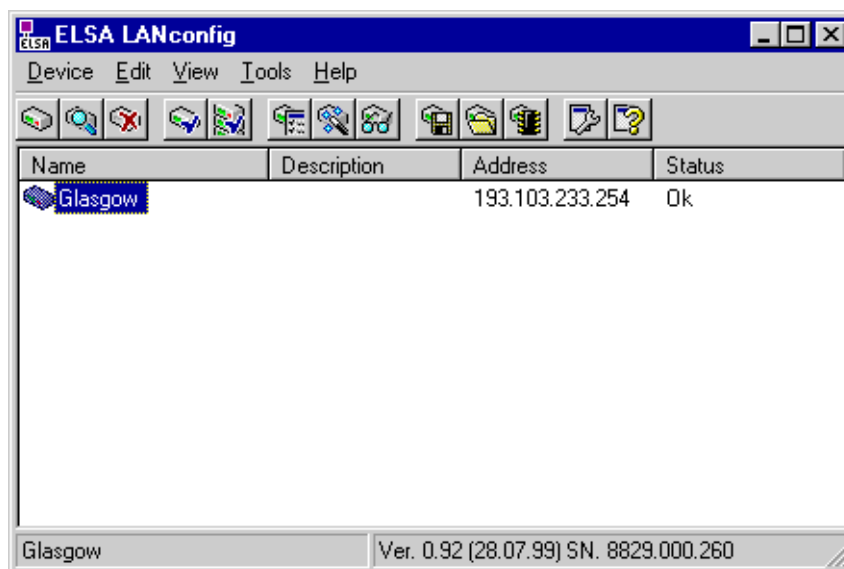
## Beginning configuration using *ELSA LANconfig*

Start up *ELSA LANconfig* from the Windows Start Menu, for instance, by clicking **Start ► Programs ► ELSA LAN ► ELSA LANconfig**. *ELSA LANconfig* searches the local area network for devices. This function can be disabled.



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

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



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

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

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



Start the configuration by double-clicking the entry for the marked device.

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

## Start up inband configuration using telnet

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

```
telnet 10.1.80.125
```

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

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


## Configuration commands

Commands and path specifications are entered using the normal DOS or UNIX conventions if you are using telnet or a terminal program to configure the router.

Enter a forward slash or backslash to separate the path specifications. You do not need to write out commands and table entries in full; an unambiguous abbreviation will do.

The entries for the categories MENU, VALUE, TABLE, TABINFO, ACTION and INFO will be displayed while configurations are made and may be modified. You can use the following commands to do this:

This command...	... means this...	... for instance:
? or help	calls up help text	-
dir, list, ll, ls <MENU>, <VALUE> or <TABLE>	displays the contents of MENU, VALUE or TABLE	dir/status/wan-statistics displays the current WAN statistics
cd <MENU> or <TABLE>	switches to the MENU or TABLE specified	cd setup/tcp-ip-module (or cd se/tc for short) switches to the TCP/IP module

This command...	... means this...	... for instance:
set <VALUE>	this resets the value.	set IP-address 192.110.120.140 sets a new IP address
	insert a space between all entries in table rows. An * leaves the entry unchanged.	set /setup/name AACHEN assigns the name 'AACHEN' to the device.
set <VALUE> ?	shows you which values can be specified here.	
del <VALUE>	deletes a a table row.	del /se/wan/nam/AACHEN deletes the entry for the remote station AACHEN.
do <ACTION> (parameters)	executes the ACTION according to any parameters specified.	do /firmware/firmware-upload starts the upload of new firmware.
passwd	allows a new password to be specified. The old password, if there is one, must be entered first. The new password must then be entered twice in a row and confirmed each time with  .	
repeat <sec> <ACTION>	repeats the action at an interval of the number of seconds specified. Any key can be used to terminate the repetition.	repeat 3 dir/status/wan-statistics displays the current WAN statistics every 3 seconds
time	sets the system time and date	time 24.12.1998 18:00:00
language	sets the language for the current configuration session.	Languages currently supported: English (language English) German (language German)
exit, quit, x	configuration is terminated.	

Text entries with spaces are only accepted if they are placed in quotation marks, i.e.  
`set /se/snmp/admin "The Administrator".`

Text entries (individual and table values) can be deleted as follows:

```
set /se/snmp/admin " "
```

## New firmware with FirmSafe

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

### This is how FirmSafe works

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

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

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

## How to load new software

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

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



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

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

### **ELSA LANconfig**



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

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

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

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

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

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

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

### TFTP

With TFTP you can use the **writelflash** command to install new firmware. To transmit a new firmware version which, for example, is in the 'LC\_1000U.130' file, to a device with the IP address 194.162.200.17, you would enter the following command under Windows NT for example:

```
tftp -i 194.162.200.17 put lc_1000u.130 writelflash
```



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

The device is booted up following a successful firmware upload and this activates the new firmware switch directly. If an error occurs during the upload (write error in the Flash ROM, TFTP transmission error etc.), the device will boot in any case, and FirmSafe will start the available software. The configuration connection remains in operation.



*You should therefore be sure to carry out a firmware upload only when you have a secure (stable) connection.*



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

- `tftp 10.0.0.1 get readconfig file1`: Reads the configuration from the device with the address 10.0.0.1 and saves it as file1 in the current directory.
- `tftp 10.0.0.1 put file1 writeconfig`: Writes the configuration from file1 to the device with the address 10.0.0.1.
- `tftp 10.0.0.1 get dir/status/verb file2`: Saves the current connection information in file2.

## Configuration using SNMP

### General

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. This instance is commonly termed the “manager” while the devices become “agents”. The structure permitted for SNMP information exchange is relatively simple. A manager can access all SNMP-capable devices and services (agents) on the network. The access rights are controlled via “communities”.

SNMP V.1 has only a very limited set of commands at its disposal, as the table below shows:

Command	Target/Source	Function
GetRequest	Manager—Agent	retrieves information from the agent
GetNextRequest	Manager—Agent	retrieves the information contained in the following MIB from the agent
SetRequest	Manager—Agent	modifies a setting in the agent
GetResponse	Agent—Manager	returns the queried value to the manager
Trap	Agent—Manager	reports on an error or special status

These commands can be used for central monitoring and configuration of SNMP-capable devices on a network. The SNMP capabilities of the agents are specified in so-called MIBs = Management Information Bases.

The firmware of ELSA routers includes an implementation for an SNMP V.1 agent (in accordance with RFC 1157). A part of MIB-2 and a private MIB, included in the product as a separate file, are supported. This MIB must be loaded and translated by an SNMP manager (HP OpenView, for example) to allow you to manage a device completely using SNMP. All menus and parameters of the remote configuration will then be available to you on a single branch of the SNMP management tree:

`iso/org/dod/internet/private/enterprises/elsa/lancom` or `1.3.6.1.4.1.2356.1`.

## Accessing tables and parameters using SNMP

Any of the tables and parameters can be read and modified as necessary via the SNMP interface. This also involves specifying in the MIB the variables which should have 'read-only' or 'read-write' status. Commercially available SNMP managers indicate 'read-only' and 'read-write' status using color coding.

### Access protection in SNMP V.1

Access to SNMP objects is controlled using so-called communities. A community is basically a password used to govern access to particular classes of information. The router permits read-only access to all parameters and tables through the 'public' community. Bear in mind that this community cannot execute any write accesses.

You must use the device's password if you wish to write data using SNMP. Write access using SNMP will **not** be granted as a matter of principle if the device's password is not entered.

The settings in 'Setup/Config-module' are evaluated as follows if using SNMP to access the router:

Entry	Value	Meaning
Password-required	On	Access through the 'public' community is barred.
Password-required	Off	Access via the 'public' community is read-only. All actions can be executed if the password is given as the community.
LAN/WAN-config	Off	All access via LAN/WAN is barred.
LAN/WAN-config	On	Access via the 'public' community is read-only. All actions can be executed if the password is given as the community.
LAN/WAN-config	Read	Access via both the 'public' community and the password is read-only.

If the trapping mechanism is enabled and a failed access attempt is detected, an 'Authentication Failed' trap is triggered and sent to the manager(s) in the SNMP trap table.

Bear in mind that the access protection given by the community mechanism in the SNMP V.1 is only very limited since the data, the MIB IDs and the communities are not encrypted in the UDP data blocks of requests and responses as they are transmitted.

### Deleting rows in tables using SNMP

SNMP itself has no mechanisms intended for deleting. You therefore have to use a trick to delete entries from tables.

If you need to delete a row, you have to change the index entry value, i.e. the value in the first column, to its current value.

- For example: You want to delete the 3rd row from following IP routing table.

IP-address	IP netmask	Router-name	Distance
192.168.0.0	255.255.0.0	0.0.0.0	0
172.16.0.0	255.240.0.0	0.0.0.0	0
10.0.0.0	255.0.0.0	ROBERT	0
224.0.0.0	224.0.0.0	0.0.0.0	0

The entry '10.0.0.0' (i.e. the first cell of the third row) is amended in the manager to its current value, i.e. to '10.0.0.0', and the Set command is sent off. The SNMP SetRequest now contains the command to amend the first cell of the third row to '10.0.0.0'. The SNMP software recognizes that this assignment to the index is redundant and interprets it as a delete command.

### Appending rows to tables using SNMP

There are two options for adding rows to a table:

- Use the set command to set a new index entry to create a new row. Use the command in the following syntax:

someTable.1.2.2 = xyz

A row with the index '2' is created in the table 'someTable' into the second column of which the value 'xyz' is input. The '1' after the table name is constant for this command and stands for 'someEntry' in the SNMP syntax.

- With SNMP managers that do not allow index values to be entered, any existing index entry of a row can be changed to the new index value of the new row. The row which has been used as the source for the amendment will itself remain unchanged.

In practice, the first option can be implemented as follows, using the example of Castlerock SNMPc:

- ① Activate the submenu item **Display MIB Table** in the **Manage** menu of the Castlerock SNMPc.
- ② Open the corresponding table. If the table is empty, empty columns are displayed.
- ③ Click **Edit**. Now values for the individual table columns can be input.
- ④ Enter the table index and the value for another column, and click **Set** to the right of the last named column.

There should now be a new column with the new index and the value for another column.

*Values for all columns of the row can also be entered and all columns can be set simultaneously with **Set All**.*



This procedure can also be done with **Edit MIB Vars..** in the **Manage** menu. Here click until you reach the table, click once on the table column that is to be set, enter the new index after the name of this column in the field **Variable Name** and the value in **Variable Value**. There should now be a new table row after clicking Set.

### **Error messages via SNMP trap**

Error or warning messages can be sent to a manager using the SNMP mechanism. The SNMP agent contained in the router permits traps to be sent to up to 20 SNMP managers. The IP addresses of these managers are configured in the Configuration menu under /setup/SNMP-module/IP-Trap-Table. You can enable and disable the transmission of trap messages using the /setup/SNMP-module/Send-Traps switch.

### **SNMP and *ELSA LANmonitor***

The following three entries /setup/SNMP-module/ ...Register-monitor, .../Delete-Monitor and .../Monitor-table are only relevant for the automatic login of the *ELSA LANmonitor* and are of no further importance to the user. They are only displayed in the menu for information purposes.

## **The Management Information Base (MIB)**

A textual representation of the configuration structure (the so-called private MIB) must be supplied with the *ELSA LANCOM DSL/10 Office* so that the SNMP management system can access its configuration. The syntax of this MIB complies with ASN.1 (Abstract Syntax Notation One, ISO 8824). There is usually a so-called MIB compiler included with the SNMP management software. This compiler converts the MIB file into a form that can be used by the manager.

The current ELSA MIB can be found both included with the product on CD and in the ELSA online media.

# Operating modes and functions

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

- Security for your configuration
- Security for your LAN
- Charge management
- xDSL or cable connections
- PPP support
- IP routing
- DHCP server
- DNS server

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

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

## Security for your configuration

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

Needless to say, the parameters that you have set should not be modified by unauthorized persons. The *ELSA LANCOM DSL/10 Office* thus offers a variety of options to protect the configuration.

### Password protection

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

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

## Login barring

The configuration in the *ELSA LANCOM DSL/10 Office* is protected against “brute force attacks” by barring logins. A brute-force attack is the attempt of an unauthorized person to crack a password to gain access to a network, a computer or another device. In order to do so, a computer can, for example, run through all the possible combinations of letters and numbers until the right password is found.

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

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

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

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

## Access control via TCP/IP

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

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

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

## Security for your LAN

You certainly would not like any outsider to have easy access to or to be able to modify the data on your computers. The *ELSA LANCOM DSL/10 Office* offers you various ways of restricting access from outside:

- Data packet filtering
- IP masquerading (also known as NAT or PAT)

## The hiding place—IP masquerading (NAT/PAT)

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

IP masquerading provides a hiding place for every computer while connected with the Internet. Only the router module of the unit and its IP address are visible on the Internet. The computers in the LAN then use the router as a gateway so that they themselves cannot be detected. To do this, the router separates Internet and Intranet, as if by a wall. Therefore, IP masquerading is also called a “firewall function”.

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

## TCP/IP packet filters

You can use your entries in the routing table to determine quite precisely which data should be transferred. Additionally, you can use the '0.0.0.0' entry in the 'Router-name' field to reject whole groups of IP addresses.

Occasionally, you may wish to restrict a transmission even further. You can do this using a characteristic of TCP/IP, which is to send port numbers for destination and source as well as the source and destination IP addresses with a data packet. The destination port in a data packet stands for the service to be addressed in the TCP/IP network. The destination ports are fixed for the various services on the TCP/IP network (see also 'TCP/IP-ports' in the reference section). The source ports, on the other hand, may be selected freely within certain ranges.

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

## Call charge management

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

## Time-dependent connection control

The telephone charges can be controlled by limiting the maximum connection time. 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 10 hours within 6 days.



*The device indicates this status with a flashing power/msg LED and in the LANmonitor. 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—in LANmonitor—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.

## Settings in the charge module

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



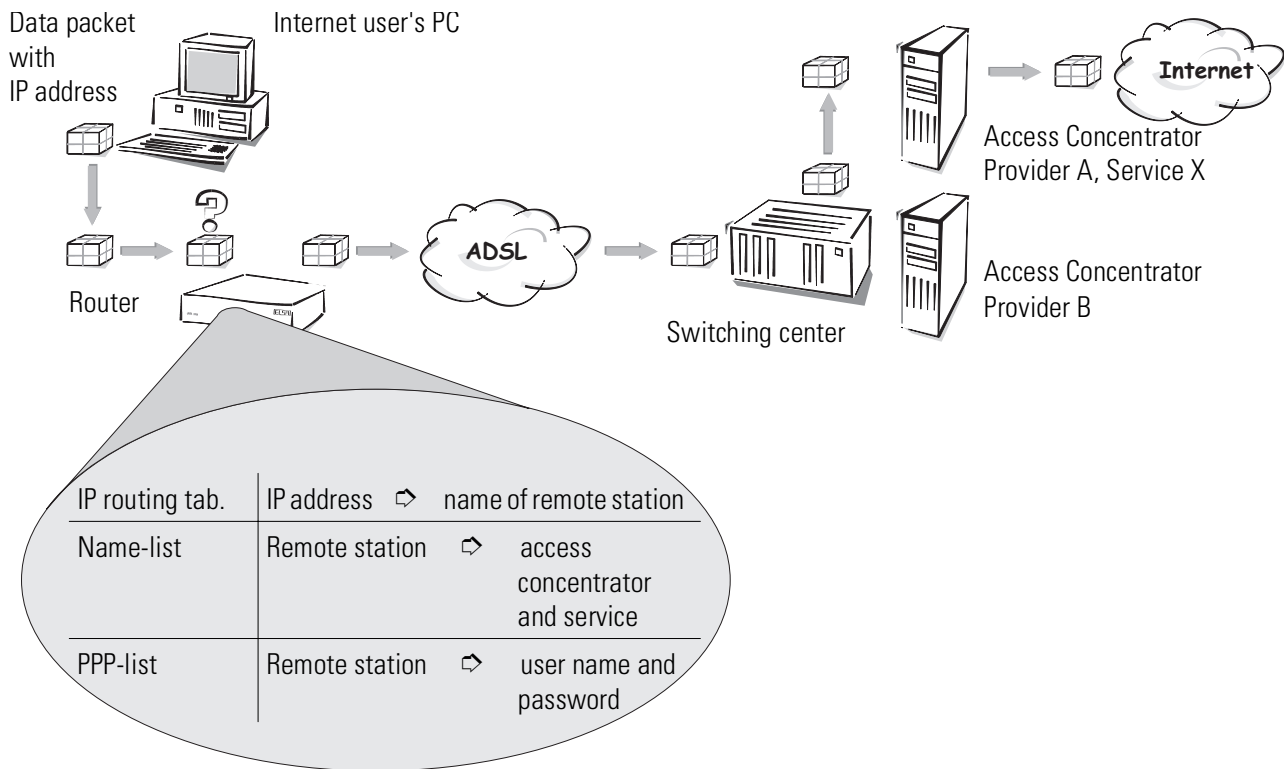
*The current charge and connect-time information is retained when rebooting (e.g. when installing new firmware) is not lost until the unit is switched off. All of the time values indicated here are in minutes.*

## xDSL connections

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



A simplified example will clarify this process.



A data packet from a computer initially finds the path to the Internet through the IP address of the receiver. The computer sends the packet with this address over the LAN to the router. The router uses the IP address first to check the IP routing table and finds the remote station to which this address belongs (e.g. 'Provider\_A'). The router then uses this name to check the name list and finds the name of the associated access concentrators (AC) and the service that should be used with this AC. The router also obtains the user name and password required for login to Provider A from the PPP list.

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

You will find additional information on IP networks etc. in the technical documentation.

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

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

## Name-list

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

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

- Name

This name is used to identify the remote station in the router modules. Once the router module has used the IP address to find which remote station can be used to reach the desired destination, the associated connection parameters can be determined from the name list.

- Time Out

This period indicates how long the connection will remain active after no more data are transferred.

If a zero is given as time out, the connection will not be automatically terminated!

- Access Concentrator

The access concentrator represents the server that can be accessed over this connection. If more than one provider is available over your xDSL terminal, select the one that is responsible for the IP address group of this remote station with the name of the AC.

The value for the AC will be supplied by your provider.

If a value for the AC is not entered, every AC that offers the requested service will be accepted.

- Service

Enter the service that you wish to use with your provider. This can be simple Internet browsing, video downstream or other.

The value for the service will be supplied by your provider.

If a value for the service is not entered, every service that offers the requested AC will be accepted.



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

## PPP-list

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

Use the PPP list to establish additional parameters for connections that use PPP in the communications layer on layer 3.

- Remote site  
Name of the remote station as specified before in the name list.
- Username  
User name to be used when establishing a connection with the remote station.
- Key  
Password to be used when establishing a connection with the remote station.
- Verification  
Authentication process that the router should request from the remote station.
- Time, Rep., Conf., Fail., Term.  
Parameters pertaining to connection characteristics that will not be described in greater detail here.

## IP routing

An IP router works between networks which use TCP/IP as the network protocol. This only allows data transmissions to destination addresses entered in the routing table. This chapter explains the structure of the IP routing table of an ELSA router, as well as the additional functions available to support IP routing.

### The IP routing table

Use the IP routing table to tell the router which remote station (which other router or computer) it should send the data for particular IP addresses or IP address ranges to. This type of entry is also known as a route since it is used to describe the path of the data packet. Because you make these entries yourself and they remain unchanged until you change or delete them, the procedure is also referred to as static routing. In contrast of course, there is also dynamic routing. In this process the routers exchange information on the routes independently and update it continuously. The static and dynamic routing tables can hold up to 128 entries each. When the IP-RIP is active, the IP router uses both tables.

The routing table can be found in the *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Router' tab, or in the `/Setup/IP Router/IP Routing` menu. This, then, is how an IP routing table might look:

What do the various entries on the list mean?

■ IP addresses and IP network masks

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

The route with the IP address '255.255.255.255' with a network mask of '0.0.0.0' is the default route. Any data packets which cannot be routed by other routing entries are transmitted via this route.

■ Router name

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

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

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

■ Distance

Number of routers between your own and the destination router.

Examples with explanatory notes:

IP address	IP netmask	Router name	Dist.	This is what happens:
192.168.130.0	255.255.255.0	192.168.140.123	0	All data packets with destination IP addresses 192.168.130.x are transmitted to the local router with the IP address 192.168.140.123.
192.168.0.0	255.255.0.0	0.0.0.0	0	Prevents transfer of all data packets in reserved IP address ranges.
172.16.0.0	255.255.0.0	0.0.0.0	0	
10.0.0.0	255.0.0.0	0.0.0.0	0	
224.0.0.0	224.0.0.0	0.0.0.0	0	

## Local routing

You know the following behavior of a workstation within a local network: The computer searches for a router to assist with transmitting a data packet to an IP address which is not on its own LAN. This router is usually notified to the operating system by its property of being the default router or gateway. It is often only possible to enter one default router which is supposed to be able to reach all the IP addresses which are unknown to the workstation computer if there are several routers in a network. Occasionally, however, this default router cannot reach the destination network itself but does know another router which can find this destination.

How can you assist the workstation computer now?

By default, the router sends the computer a response with the address of the router which knows the route to the destination network (this response is known as an ICMP redirect). The workstation computer then accepts this address and sends the data packet straight to the other router.

Certain computers, however, do not know how to handle ICMP redirects. To ensure that the data packets reach their destination anyway, use local routing (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Router' tab or in the `/Setup/IP Router-module/Local Routing On` menu). This is how you tell the router in your device to send the data packet to the other, responsible router itself. The router will then no longer send any ICMP redirects.

This may seem to be a good idea in principle, but local routing should still only be used as a last resort, since this function leads to doubling of the number of data packets being sent to the destination network required. The data is first sent to the default router and is then sent on from here to the router which is actually responsible in the local network.

## Dynamic routing with IP RIP

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

### What information is propagated by IP RIP?

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

- Rejected routes with the '0.0.0.0' router setting.
- Routes referring to on other routers in the local network.

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

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

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

### What do the entries mean?

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

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

- The route is incorporated if it is not yet listed in the table (as long as there is enough space in the table).
- The route exists in the table with a time of '5' or '6'. The new route is then used if it indicates the same or a better distance.
- The route exists in the table with a time of '7' to '10' and thus has the distance '16'. The new route will always be used.
- The route exists in the table. The new route comes from the same router which notified this route, but has a worse distance than the previous entry. The route is discarded.

### 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.

## IP masquerading (NAT, PAT)

One continually growing problem for the Internet is the limited number of generally valid IP addresses available. In addition to this, the allocation of fixed IP addresses for the Internet by the Network Information Center (NIC) is an expensive process. What is more obvious than having several computers share one IP address?

This particular solution is called IP masquerading. This is a procedure whereby only one LAN router appears on the Internet with an IP address. This IP address is allocated to the router either permanently by the NIC or temporarily by an Internet provider. All the other computers on the network then “conceal” themselves behind this one IP address. Aside from the welcome savings, IP masquerading has the added benefit of guarding very effectively against attacks on the local network from the Internet.

### 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 also enters this port on the table and forwards the packet with the new information.

The entry in the internal table allows the router to assign this response to the original sender again.

*You can view these tables in detail in the router statistics (see also 'Status' in the reference section of the manual).*



### Simple and inverse masquerading

If, on the other hand, a computer sends a packet from the Internet to, for example, an FTP server on the LAN, from the point of view of this computer the router appears to be the FTP server. The router reads the IP address of the FTP server in the LAN from the entry in the service table (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Masq.' tab or in the *Setup/IP Router-module/Masquerading/Service Table* menu). The packet is forwarded to this computer. All packets that come from the FTP server in the local network (answers from the server) are hidden behind the IP address of the router.

The only small difference is that:

- When accessing the Internet from the LAN, on the other hand, the router itself makes the entry in the port and IP address information table.

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

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

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

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

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

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

### DNS forwarding

Names rather than IP addresses are generally used to access a server over the Internet. Who knows which address is behind 'www.domain.com'? The DNS server, of course.

DNS stands for Domain Name Service and refers to the assignment of domain names (such as domain.com) to the corresponding IP addresses. This information must be constantly updated and be accessible all over the world at any time. DNS servers holding long tables containing IP addresses and domain names exist for this purpose.

If a computer calls up a home page from the Intranet, it first sends out a DNS request: "What IP address belongs to www.domain.com?"

- Initially the router checks whether a DNS server has been entered in its own settings (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Addresses' tab or in the `/Setup/TCP-IP-module` menu). If it finds one it retrieves the required information from this server.

This procedure does not require you to have any knowledge of the DNS server address. This procedure also automatically updates the address of the DNS server. The local network always receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

### Policy-based routing

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



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



## Automatic address administration with DHCP

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

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

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

### The DHCP server

As a DHCP server, the *ELSA LANCOM DSL/10 Office* can administer the IP addresses in its TCP/IP network. In doing so, it passes the following parameters to the workstation computers:

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

### DHCP—'on', 'off' or 'auto'?

The DHCP server can be set to three different states:

- 'on': The DHCP server is permanently active. The configuration of the server (validity of the address pool) is checked when this value is entered.
  - When correctly configured, the device will be available to the network as a DHCP server.
  - In the event of an incorrect configuration (e.g. invalid pool limits), the DHCP server is disabled and switches to the 'off' state.
- 'off': The DHCP server is permanently disabled.
- 'auto': The server is in automode. In this mode, after switching it on, the device looks for other DHCP server within the local network.
  - The device then disables its own DHCP server if any other DHCP servers are found. This prevents the unconfigured device from assigning addresses not in the local network when switched on.

- The device then enables its own DHCP server if no other DHCP servers are found. Whether the DHCP server is active or not can be seen in the DHCP statistics. The default state is 'auto'.

## How are the addresses assigned?

### IP address assignment

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

- The IP address can be taken from the address pool selected (start address pool to end address pool). Any valid addresses in the local network can be entered here.
- It then uses the IP address '10.0.0.254' for itself and the address pool '10.x.x.x' for the assignment of IP addresses in the network. In this state, the DHCP server only assigns IP addresses and their validity to the computers in the network, but not the other information.

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

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

### Network mask assignment

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

### Broadcast address assignment

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



*The default setting for the broadcast address should be changed by experienced network specialists only.*

### Default gateway assignment

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

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

### Period of validity for an assignment

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

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

- **Maximum lease time in minutes**

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

If a host requests a validity in excess of 6000 minutes, 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.

### Priority for computer—overwriting an assignment

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

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

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

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

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

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

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

## 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.

### What does a DNS server do?

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

If there is no DNS server in the local network, all locally unknown names will be searched for using the DEFAULT route. By using a DNS server, it's possible to immediately go to the correct remote station for all of the names with known IP addresses. In principle, the DNS server can be a separate computer in the network. However, the following reasons speak for locating the DNS server directly in the *ELSA LANCOM DSL/10 Office*:

- An *ELSA LANCOM DSL/10 Office* can automatically distribute IP addresses for the computers in the local network when in DHCP server mode. In other words, the DHCP server already knows the names and IP addresses of all of the computers in its own network that were assigned IP addresses via DHCP. With the dynamic address assignments of a DHCP server, an external DNS server might have difficulties in keeping the associations between the names and IP addresses current.
- The DNS server in the *ELSA LANCOM DSL/10 Office* can also be used as an extremely convenient filter mechanism. Requests for domains can be prohibited throughout the LAN, for subnetworks, or even for individual computers—simply by specifying the domain name.

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

- First, the DNS server checks whether access to the name is not prohibited by the filter list. If that is the case, an error message is returned to the requesting computer stating that access to the address has been denied.
- Next, it searches in its own static DNS table for suitable entries.
- If the address cannot be found in the DNS table, it searches the dynamic DHCP table. The use of DHCP information can be disabled if required.

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

## Setting up the DNS server

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

- ① Switch the DNS server on.

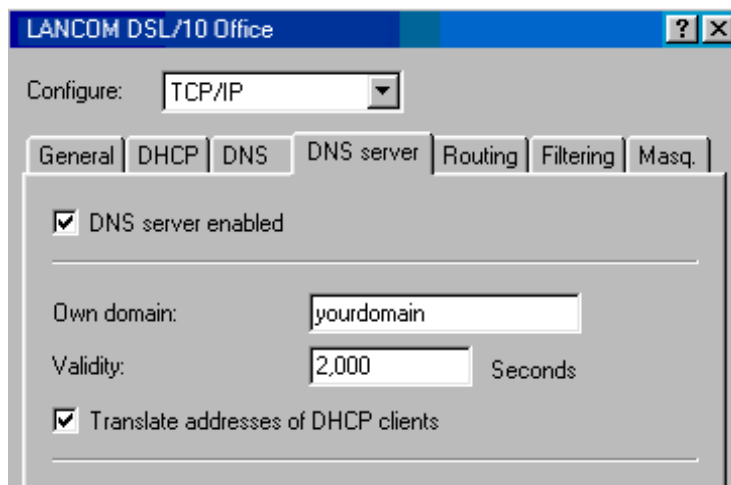
```
set setup/dns-module/operating on
```

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

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

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

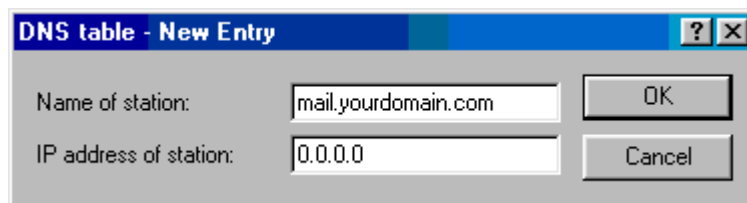
```
set setup/dns-module/dhcp-usage yes
```



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

- for which you know the name and IP address,
- that are not located in your own LAN,
- that are not on the Internet and
- that are accessible via the router.

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

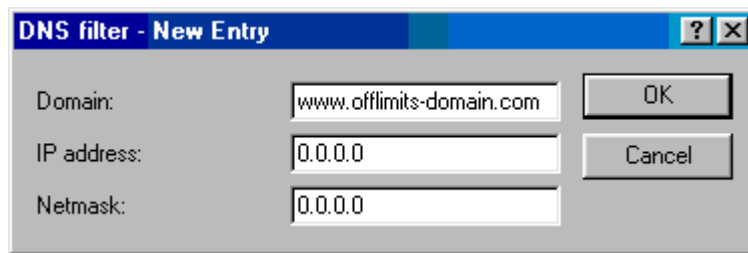


```
cd setup/dns-module/dns-table
set mail.yourdomain.com 10.0.0.99
```

Stating the domain is optional but recommended.

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

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



```
cd setup/dns-module/filter-list
```

```
set 001 www.offlimits-domain.com 0.0.0.0 0.0.0.0
```

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

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



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

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





# Appendix

## Technical data

Functions	IP router, DHCP server, DHCP client
LAN connection	Ethernet IEEE 802.3, 10/100Base-T (RJ45, node/hub switch), auto-sensing, full duplex operation
Network protocols	PPP via Ethernet, ARP, PROXY ARP, IP, ICMP, UDP, TCP, TFTP, RIP-1, RIP-2, DHCP, DNS
Filter possibilities	Source and target filters for networks, protocols and ports; separate WAN and LAN
WAN interface	Ethernet IEEE 802.3, 10Base-T (RJ45)
Charge monitoring	Maximum charges or connection time for a preset period can be set
Security and firewall functions	PAP and CHAP, authentication mechanisms in PPP; filter options in IP mode; configuration protection with access lists and password; IP masquerading
IP masquerading (NAT/PAT)	IP address and port implementation using a single IP address, static/dynamic IP address assignment via PPP or DHCP, masking of TCP, UDP, ICMP, FTP; DNS forwarding; inverse masquerading Intranet IP services such as web server
Management	V.24/V.28 outband interface (8-pin mini-DIN), TFTP configuration and firmware upload, SNMP management via SNMP v.1 or v.2, WAN or LAN accesses can be activated separately, diagnosis outputs for protocols and interfaces, diagnosis tools, status display <i>ELSA LANmonitor</i>
Operating security	Hardware watchdogs, regular self-testing, FirmSafe concept for remote software upgrades
Statistics	LAN and WAN packet counters; error, connection and charge counters, timer
Display/operation	LEDs for LAN, WAN and device status
Power supply	12 VA with AC adapter for 230 V, 12 VA
Environmental conditions	Temperature: 5-40°C, humidity: 0-80%, non-condensing
Dimensions and design	Rugged metal case, connections on rear panel; dimensions 158 x 40 x 125 mm (W x H x D)
Package contents	Power adapter, cable for outband interface, two LAN twisted-pair cables, detained documentation and <i>ELSA LANCOM</i> CD  <i>ELSA LANconfig</i> , <i>ELSA LANmonitor</i> for status display, terminal program <i>ELSA-ZOC</i>
Approvals:	in preparation: Germany, Switzerland and all other EU countries
Service	Warranty: 6 years Support: by Infoline and Internet; test inputs

## Declaration of conformity



# KONFORMITÄTSERKLÄRUNG

## DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

**Geräteart:** Ethernet to Ethernet Router  
**Type of Device:**  
**Typenbezeichnung:** LANCOM DSL/10 Office  
**Product Name:**

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:

This is to confirm that this product meets all essential protection requirements relating to the

### Niederspannungs Richtlinie (73/23/EWG)

Low Voltage Directive (73/23/EEC)

### EMV Richtlinie (89/336/EWG)

EMC Directive (89/336/EEC)

Zur Beurteilung der Konformität wurden folgende **Normen** herangezogen:

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

**EN 50081-1: 1992 Teile/** parts: **EN 55022: 1994**

**EN 50082-1: 1997 Teile/** parts: **EN 55024: 1999**

**EN 60950: 1992+ A1: 1993 +A2: 1993 +A3: 1995 +A4: 1996**

Diese Erklärung wird verantwortlich für den Hersteller / Importeur:

On behalf of the manufacturer / importer:

**ELSA AG**  
**Sonnenweg 11**  
**D-52070 Aachen**

abgegeben durch: / this declaration is submitted by:

Aachen, 23. August 1999

Aachen, 23<sup>rd</sup> August 1999

i.V. Stefan Kriebel  
Bereichsleiter Entwicklung  
VP Engineering

## Warranty conditions

The ELSA AG warranty, valid as of June 01, 1998, is given to purchasers of ELSA products in addition to the warranty conditions provided by law and in accordance with the following conditions:

### 1 Warranty coverage

- a) The warranty covers the equipment delivered and all its parts. Parts will, at our sole discretion, be replaced or repaired free of charge if, despite proven proper handling and adherence to the operating instructions, these parts became defective due to fabrication and/or material defects. Also we reserve the right to replace the defective product by a successor product or repay the original purchase price to the buyer in exchange to the defective product. Operating manuals and possibly supplied software are excluded from the warranty.
- b) Material and service charges shall be covered by us, but not shipping and handling costs involved in transport from the buyer to the service station and/or to us.
- c) Replaced parts become property of ELSA.
- d) ELSA are authorized to carry out technical changes (e.g. firmware updates) beyond repair and replacement of defective parts in order to bring the equipment up to the current technical state. This does not result in any additional charge for the customer. A legal claim to this service does not exist.

### 2 Warranty period

The warranty period for ELSA products is six years. Excepted from this warranty period are ELSA color monitors and ELSA videoconferencing systems with a warranty period of 3 years. This period begins at the day of delivery from the ELSA dealer. Warranty services do not result in an extension of the warranty period nor do they initiate a new warranty period. The warranty period for installed replacement parts ends with the warranty period of the device as a whole.

### 3 Warranty procedure

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

### 4 Suspension of the warranty

All warranty claims will be deemed invalid

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

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

## **5 Operating mistakes**

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

## **6 Additional regulations**

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

# Index

## ■ Numerics

10/100Base-TX .....	7
100 Mbit network .....	7
100BASE-T .....	R30

## ■ A

Access control .....	22
Access protection .....	3
Access-list .....	R32
Address Administration .....	12, 33
Address pool .....	34, R43
Address ranges .....	R35
ARP cache .....	R34
ARP-aging-minute(s) .....	R34
Auth. ....	R27
Auto mode .....	R43

## ■ B

Barring .....	22
Boot system .....	R49
Brute force .....	3, 22
Budget .....	R29
Budget charges .....	R29
Buffers .....	R30

## ■ C

Cache .....	R34
Call charge limit .....	23
Call charge management .....	23
Challenge Handshake Authentication Protocol .....	R27
CHAP .....	R27
Charge lock .....	R29
Charge monitoring .....	3
Charge protection .....	R29
Communities .....	17
Computer names .....	36
Config-aging-minute(s) .....	R47
Configuration .....	3
Commands .....	13

methods .....	11
SNMP .....	17
Configuration interface .....	11
Configuration options .....	R46
Connect .....	R28
Connection control .....	23
Connection time-outs .....	R27
Connections .....	7
Connector .....	R30

## ■ D

Day(s)-per-period .....	R29
Default route .....	R36
Destination network .....	R35
Destination port .....	R, 36, R37
Device names .....	R26, R27
DHCP .....	3, 33, R43
DHCP server .....	8, 12, 33, 37, R43
Disconnect .....	R28
Distance of a route .....	28
DNS .....	32, 36, R33
DNS forwarding .....	32, R33
DNS forwarding mechanism .....	37
DNS queries .....	R37
DNS server .....	4, 36
available information .....	37
filter list .....	39
filter mechanism .....	37
DNS-backup-IP-address .....	R33
Domain Name Service .....	32, 36
Domains .....	36
DSL terminal .....	7
Dst-address .....	R38
Dst-netmask .....	R38
Dynamic assignment of the IP address .....	R35
Dynamic Host Configuration Protocol .....	33
Dynamic IP routing table .....	R40
Dynamic routing .....	27

- **E**
  - E-mail ..... 2
  - End address ..... 34
  - End-address-pool ..... R43
  - Ethernet ..... 2
    - 10/100Base-T ..... 2
    - Fast Ethernet ..... 2
  - Exclusion routes ..... 28
- **F**
  - Fast-Ethernet
    - 10/100Base-T ..... 2
  - File transfer ..... 2
  - Filter ..... 22
  - Firewall ..... 3
  - Firewall function ..... 23, R37
  - FirmSafe ..... 3, 14, R48
  - Firmware ..... 3, R47
  - Firmware upload
    - with *LANconfig* ..... 15
  - Firmware upload ..... 15
    - using TFTP ..... 16
    - with terminal program ..... 16
  - Flash ROM ..... 14
  - Flash ROM memory ..... 3
- **G**
  - Gateway ..... 23, 35
- **H**
  - High telephone costs ..... 23
  - Host ..... 36
- **I**
  - ICMP ..... R37, R39, R41
  - Identification ..... R26
  - Inband ..... 11
    - preconditions ..... 11
    - using telnet ..... 13
  - Inband ..... 11
  - Inband configuration ..... 11
  - Install software ..... 14
  - Installation ..... 2
  - Interfaces ..... 7
  - Internet ..... 2
    - Internet service provider ..... 1
    - Intranet ..... R32
    - Intranet-mask ..... R32
    - Inverse masquerading ..... R40
    - IP ..... R39
      - IP access list ..... 11
      - IP address ..... 8, 11, 23, R31
      - IP broadcast ..... R39
      - IP header ..... R38
      - IP masquerading ..... 2, 3, 22, 23, 31, R35, R41
        - supported protocols ..... 32
      - IP multicast ..... R39
      - IP routing
        - filter ..... 23
        - FTP ..... 23
        - telnet ..... 23
      - IP routing table ..... 27
      - IP-netmask ..... R31
      - IP-routing-table ..... R35
  - **K**
    - Key ..... R27
  - **L**
    - LAN connection ..... 2
    - LAN connection cable ..... 5
    - LAN-Coll ..... 6
    - LANconfig* ..... 3, 8, 11, 12, 15
    - LAN-configuration ..... R46
    - LAN-filter-table ..... R36
    - Language ..... R47
    - LAN-Link ..... 6
    - LAN-Rx ..... 6
    - LAN-Tx ..... 6
    - LED ..... 6
    - LED indicators ..... 2
    - Local-routing ..... R38
    - Location ..... R26
    - Lock-minutes ..... R47
    - Login ..... 15, 22
    - Login barring ..... 22
    - Login block ..... R47
    - Login-errors ..... R47

■ **M**

MAC address .....	R30
Mail server .....	38
Management Information Base .....	20
Manager .....	20
Manual connection .....	R28
Masquerading .....	R35, R40
masquerading .....	R32
Masquerading table .....	R41
Maximum number of simultaneous connections .....	R47
MIB .....	18
Monitoring .....	R29

■ **N**

Name .....	R26
Name server .....	R33
Name-list .....	R26
NAT .....	22, 23, 31
NBNS .....	R33
NBNS-backup .....	R33
NetBIOS name server .....	R33
Network connection .....	1, R30
Network Information Center .....	31
Network names .....	36
NIC .....	31
Node/hub selector switch .....	7
Node-ID .....	R30
Number list .....	R28

■ **O**

Objects .....	18
Online media .....	11
Online research .....	2
Operating .....	R31, R35
Operating modes .....	21
Other .....	R49
Outband .....	11
Outband configuration .....	11

■ **P**

Package contents .....	5
PAP .....	R27
password .....	R32

Password Authentication Protocol .....	R27
Password protection .....	3, 21
Password-required .....	R46
PAT .....	22, 23, 31
Period of validity .....	33, 35
Power .....	6
Power supply unit .....	5, 7
PPP negotiation .....	R32
Prohibited address ranges .....	R35
Prohibiting domains .....	39
Proxy-ARP .....	R35, R38

■ **R**

R1-mask .....	R40
Registered IP address .....	R32
Remote Access .....	R38
Remote station verifications .....	R27
Reset system .....	R49
RIP .....	R39
Router name .....	28

■ **S**

Security .....	21, 22, 23
Security features .....	2
Security procedure .....	R27
Serial port .....	11
Service .....	36
Service table .....	R40
Setup	
Charges-module .....	R29
DHCP-module .....	R43
IP-router-module .....	R34
LAN-module .....	R30
TCP-IP module .....	R31
WAN-module .....	R26
Single user access .....	23
SNMP .....	17, R42
Agents .....	17
Manager .....	17
MIB .....	17
Software update .....	3
Source port .....	R37
Spare-heap-blocks .....	R30
Start address .....	34

Start-address-pool ..... R43  
 static IP address ..... R35  
 Static routing ..... 27  
 Status ..... R3, R31  
   Call-info-table ..... R23, R25  
   Config-statistics ..... R20  
   Connection-state ..... R4  
   Connection-statistics ..... R23  
   Delete values ..... R25  
   Info-connection ..... R23  
   IP-router-statistics ..... R18  
   LAN-statistics ..... R6  
   operating time ..... R4  
   PPP-statistics ..... R8  
   Queue-statistics ..... R22  
   TCP-IP-statistics ..... R13  
   WAN-statistics ..... R4  
 Status Displays ..... 2  
 System-administrator ..... R42  
 System-location ..... R42

## T

Table-ARP ..... R34  
 Table-RIP ..... R40  
 TCP ..... R37, R41  
 TCP max. connections ..... R34  
 TCP/IP ..... 8, 11, 27  
 TCP/IP networks ..... 36  
 TCP-aging-minute(s) ..... R34  
 Technical data ..... 41  
 Teleworkers ..... R38  
 Telnet ..... 3, 10  
 Telnet server ..... R32  
 Terminal program ..... 3

TFTP ..... 11  
 TFTP server ..... R32  
 Time ..... R4, R27, R47  
 Time budget ..... 23  
 Time-dependent connection control ..... 23  
 Timeout ..... R44  
 TOS ..... R39  
 Trap ..... 20  
 Trap-IP ..... R42  
 Traps-active ..... R42  
 Type ..... R39  
 Type of service ..... 32, R38

## U

UDP ..... R37, R41  
 Upload ..... 3, 15  
 Upload-system ..... R49  
 Username ..... R28

## V

V.24 configuration interface ..... 7  
 Verification attempt ..... R28  
 Version-table ..... R48

## W

WAN connection ..... 2  
 WAN-configuration ..... R46  
 WAN-filter-table ..... R37  
 Wildcards ..... 39  
 winipcfg ..... 9  
 WWW ..... 23

## X

XModem ..... 16



# Description of the menu options

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







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

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











































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

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

## Symbols

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

## Overview of the menus


















	<b>Setup</b>		<b>Status</b>
	Name		Connection
	WAN-module		Current-time
	Charges-module		Operating-time
	LAN-module		WAN-statistics
	TCP-IP-module		LAN-statistics
	IP-router-module		PPP-statistics
	SNMP-module		TCP-IP-statistics
	DHCP-module		IP-router-statistics
	DNS module		Config-statistics
	Config-module		DNS-statistics
	Time-module		Queue-statistics
	<b>Firmware</b>		Connections-statistics
	Version-table		Info-connection
	Table-firmsafe		Remote-statistics
	Mode-firmsafe		Channel-statistics
	Timeout-firmsafe		Time-statistics
	Test-firmware		Delete-values
	Firmware-upload		<b>Other</b>
			Manual-dialing
			Boot-system
			Reset-system
			System-upload

## Status

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


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

The menu has the following layout:

Status		Running status displays
Connection		Status of the WAN route
Current-time		Current time in device
Operating-time		Period of time the device has operated since it was last switched on
WAN-statistics		Displays WAN statistics
LAN-statistics		Displays LAN statistics
PPP-statistics		Point-to-point-protocol statistics
TCP-IP-statistics		Statistics from the TCP/IP area
IP-router-statistics		Statistics from the IP router
Config-statistics		Remote configuration statistics
DNS-statistics		DSL connection statistics
Queue-statistics		Statistics relating to the packets in the queues of the individual modules
Connections-statistics		Connection information for each interface
Info-connection		Information on the last connection for each interface
Remote-statistics		Statistics on the last 100 connections
Channel-statistics		Information of the status of the individual channels.
Time-statistics		Time module information
Delete-values		Deletes all values in the substatistics except tables

## Status/Connection-state

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

/Connection-state	Running status displays	
Connection		Ch01: Ready

## Status/Current-time

This displays the current device time, used, e.g., for certain statistics. This time can be set manually (with the command 'time').










## Status/Operating-time

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

## Status/WAN-statistics

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

The **Status/WAN-statistics** menu has the following layout:

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

*Byte-transport-statistics*

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

lfc	CRx-bytes	Rx-bytes	Tx-bytes	CTx-bytes
Ch01	0	0	0	0

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

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

*Packet-transport-statistics*

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

lfc	Rx	Tx-total	Tx-normal	Tx-reliable	Tx-urgent
Ch01	0	0	0	0	0

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

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

*Error-statistics*

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

lfc	Rx-l1-error	Rx-l2-error	Rx-l3-error	Stack-error	Tx-error
Ch01	0	0	0	0	0

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

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

#### Throughput-statistics

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








Ifc	Rx/s current	Tx/s current	Rx/s average	Tx/s average
Ch01	0	0	0	0
















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

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

### Status/LAN-statistics










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

/LAN-statistics	Running status displays	
LAN-rx-packets		Number of data packets received
LAN-tx-packets		Number of data packets sent
LAN-rx-errors		Number of data packets incorrectly received
LAN-tx-errors		Number of data packets incorrectly sent
LAN-stack-errors		Number of packets without a suitable receive module (IP router)
LAN-NIC-errors		Number of data packets discarded by the NIC
LAN-heap-packets		Number of buffers available

/LAN-statistics		Running status displays
LAN-queue-packets		Number of buffers in use
LAN-queue-errors		Number of packets discarded due to a lack of buffers
LAN-collisions		Number of collisions during a send procedure
Connection -established		Display of correct Ethernet connection (data transfer possible). Corresponds to the 'Link' LED on the device.
Negotiation -complete		The negotiation of the transfer mode between the router and the remote station is complete. This is only relevant if Setup/LAN/Connection is set to 'Auto'.
Connect		This item shows the connection type currently being used on the Ethernet connection: 10B-TX: 10 Mbit, half-duplex FD10B-TX: 10 Mbit, full-duplex 100B-TX: 100 Mbit, half-duplex FD100B-TX: 100 Mbit, full-duplex If 'Auto' is set under Setup/LAN, then this is the connection type the two units have negotiated. This corresponds to the 'Fast' and 'FDpx' LEDs on the unit. If, on the other hand, a fixed transfer mode has been set, this value will be the same as the one in Setup/LAN/Connection.
LAN-rx-bytes		Number of bytes received from the LAN
LAN-tx-bytes		Number of bytes sent to the LAN
LAN-rx-broadcasts		Number of broadcast packets received from the LAN
LAN-rx-multicasts		Number of multicast packets received from the LAN
LAN-rx-unicasts		Number of directly addressed packets received from the LAN
WAN-rx-broadcasts		Number of broadcasts received from the WAN
WAN-rx-multicasts		Number of multicasts received from the WAN
WAN-rx-unicasts		Number of unicasts received from the WAN
Delete-values		Deletes LAN statistics

## Status/PPP-statistics

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

/PPP-statistics		Running status displays
PPP-phases		Statistics relating to the status of PPP protocol negotiation for each interface
LCP-statistics		Displays PPP/LCP statistics
PAP-statistics		Displays PPP/PAP statistics
CHAP-statistics		Displays PPP/CHAP statistics
IPCP-statistics		Displays PPP/IPCP statistics
CCP-statistics		Displays PPP/CCP statistics
Rx-options		Displays the LCP and IPCP information received
Tx-options		Displays the LCP and IPCP information sent
Delete-values		Deletes PPP statistics.

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

### PPP-phases

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

lfc	Phase to	LCP	IPCP	CCP
Ch01	DEAD	Initial	Initial	Initial

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

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



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

### Status/PPP-statistics/LCP-statistics

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

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

**Status/PPP-statistics/PAP-statistics**

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

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

**Status/PPP-statistics/CHAP-statistics**

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

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

### Status/PPP-statistics/IPCP-statistics

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

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

### Status/PPP-statistics/CCP-statistics

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

Rx-discarded	Number of all CCP packets discarded
Rx-config-request	Number of CCP queries received
Rx-config-ack.	Number of CCP queries accepted
Rx-config-nak.	Number of CCP queries rejected because query parameters were not accepted.
Rx-config-reject	Number of CCP rejected for other reasons.
Rx-terminate-request	Number of CCP queries after releasing the compression.
Rx-terminate-ack.	Number of confirmed CCP queries after releasing the compression.
Rx-code-reject	Number of CCP queries rejected because the remote station will not or cannot apply compression.
Rx-reset-request	Number of CCP queries after synchronizing the compression (e.g. after transfer errors)
Rx-reset-ack.	Number of confirmed CCP queries after synchronizing the compression

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



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

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

*Rx-options* This shows information on what the remote station requested (LCP) or what was assigned to the router (IPCP).

*Tx-options* This shows information on what the router requested from the remote station (LCP) or what it assigned to it (IPCP).

The two submenus have the same layout:

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

The LCP table has separate listings for every channel:









MRU	<b>M</b> aximum <b>R</b> ecieve <b>U</b> nit designates the maximum packet size that the remote station can receive
Auth.	Authentication procedure used (PAP/CHAP)
Magic-Num	Magic Number used to detect loops

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

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

## Status/TCP-IP-statistics

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

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

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

### Status/TCP-IP-statistics/ARP-statistics

These statistics include the following values:

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

*Table-ARP*

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

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

### Status/TCP-IP-statistics/IP-statistics

These statistics include the following values:

IP-LAN-rx	Number of IP packets received from the LAN
IP-LAN-tx	Number of IP packets sent to the LAN
IP-LAN-checksum-errors	Number of IP packets incorrectly received from the LAN
IP-LAN-service-errors	Number of IP packets received from the LAN for an incorrect service
IP-LAN fragmentation error	Number of unfragmentable IP packets to be sent to the LAN
IP-LAN fragmentation	Number of fragmented IP packets sent to the LAN
IP-LAN forced fragmentation	Number of IP packets with minimum size sent to the LAN
IP-WAN-fragmentation-errors	Number of unfragmentable IP packets to be sent to the WAN
IP-WAN-fragmentations	Number of fragmented IP packets sent to the WAN
IP-WAN forced fragmentations	Number of IP packets with minimum size sent to the WAN
IP-WAN-rx	Number of IP packets received from the WAN
IP-WAN-tx	Number of IP packets sent to the WAN
IP-WAN-checksum-errors	Number of IP packets incorrectly received from the WAN
IP-WAN-service-errors	Number of IP packets received from the WAN for an incorrect service
IP-WAN-rx-disconnect	Number of packets from the WAN discarded by timeout
Delete-values	Deletes IP statistics

### Status/TCP-IP-statistics/ICMP-statistics

These statistics include the following values:

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

**Status/TCP-IP-statistics/TCP-statistics**

These statistics include the following values:

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

**Status/TCP-IP-statistics/TFTP-statistics**

These statistics include the following values:

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

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

### Status/TCP-IP-statistics/DHCP-statistics

These statistics include the following values:

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












Table-DHCP

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

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

### Status/TCP-IP-statistics/DNS-statistics

The DNS statistics provide supplementary information about the DNS module. This menu has the following structure:

LAN-rx		Number of DNS packets received by the LAN
LAN-tx		Number of DNS packets sent on the LAN
WAN-rx		Number of DNS packets received by the WAN
WAN-tx		Number of DNS packets sent on the WAN
Forwarded		Number of requests that could not be fulfilled and were thus forwarded
Errors		Number of invalid requests
DNS-access		Indicates the number of names that were looked up from the DNS table
DHCP-access		Indicates the number of names that were looked up from the DHCP table
Hit-list		This table contains the 64 most popular requests. These may then be prohibited via the filter list if desired.

The hit list has the following structure:

Domain	Requests	Time	IP-address
www.elsa.com	1	00.00.0000 00:00:29	10.0.0.123





















The individual fields of this list have the following significance:

Domain	Name of the requested computer
Requests	Total number of requests for this name since its appearance in the table
Time	Time of the last request
IP-address	Address of the computer that last requested this name

This list is sorted according to the frequency of requests. When the table is full, the names that have not been requested for the longest period will be deleted to make room for new entries.

## Status/IP-router-statistics

This menu groups together the statistics from the IP router module.

/IP-router-statistics	Statistics from the IP router area	
IPr-LAN-rx		Number of data packets to be routed from the LAN
IPr-LAN-tx		Number of data packets routed to the LAN
IPr-LAN-local-routings		Number of packets received from the LAN and routed to the LAN
IPr-LAN-network-errors		Number of LAN packets that were not routed
IPr-LAN-routing-errors		Number of LAN packets that must be sent to another router
IPr-LAN-ttl-errors		Number of LAN packets with an expired time-to-live value
IPr-LAN-filters		Number of LAN packets filtered by the filter table
IPr-LAN-discards		Number of LAN packets discarded
IPr-WAN-rx		Number of data packets to be routed from the WAN
IPr-WAN-tx		Number of data packets routed to the WAN
IPr-WAN-network-errors		Number of WAN packets that were not routed
IPr-WAN-ttl-errors		Number of WAN packets with an expired time-to-live value
IPr-WAN-filters		Number of WAN packets filtered by the filter table
IPr-WAN-discards		Number of WAN packets discarded
IPr-WAN-type-errors		Number of packets from the WAN without an IP router ID
IPr-ARP-errors		Number of unsuccessful accesses to the ARP cache
Delete-values		Deletes IP router statistics
Establish-table		Table of the last 100 packets that required a connection
Protocol-table		Table of routed packets arranged by protocol
RIP-statistics		Statistics from the IP/RIP area

*Establish-table* The **establish table** contains the last 100 entries, which provide information on the system time, destination and source addresses, IP protocol, destination port and source port of the data packets that should have caused a connection to be established.

An IP router establish table might have the following appearance:

Time	Dest	Source	Protocol	D-port	S-port
1T; 16:45:01	192.120.131.40	192.120.130.10	tcp	23	4711
1T; 10:45:10	192.120.131.50	192.120.130.10	udp	53	8123

Either the device operating time or, if existing, the real time is displayed as the 'System Time'. The destination and source addresses are IP addresses. The protocol might refer, for example, to tcp, udp, or the like; the destination and source ports provide a more detailed description of the relevant services (e.g. telnet via TCP and D-port 23, name server via UDP and D-port 53).

*Protocol-table*

The protocol table also supplies valuable information on the volume of packets transferred to the LAN or WAN. These values are encrypted as per the various IP protocols, such as ICMP, TCP, UDP.

A protocol table might have the following appearance:

Protocol	LAN-tx	WAN-tx
tcp	14	30
udp	15	50
icmp	60	40

### Status/IP-router-statistics/RIP-statistics

This option allows you to display the IP-RIP packets received by the device. These substatistics provide you with the following entries:

RIP-rx	Number of IP-RIP packets received
RIP-request	Number of IP-RIP request packets received
RIP-response	Number of IP-RIP response packets received
RIP-discards	Number of IP-RIP packets discarded
RIP-errors	Number of defective IP-RIP packets
RIP-entry-errors	Number of defective entries in IP-RIP packets
RIP-tx	Number of IP-RIP packets sent
Table-RIP	Routing table of routes learned through RIP broadcast

*Table-RIP*












The associated RIP table contains all of the routes learned from the network. The router itself maintains this table; you cannot modify it manually.

An IP-RIP table might have the following appearance:

IP-address	IP-netmask	Time	Distance	Router
223.245.254.0	255.255.255.0	1	1	192.38.9.100
223.245.257.0	255.255.255.0	1	1	192.38.9.200




## Status/Config-statistics














This menu allows you to display the statistics from the remote configuration area. It allows you to retrieve information on the number of past and present configuration sessions at any time. Encryption is performed by LAN, WAN and outband port.

/Config-statistics	Remote configuration statistics	
LAN-active-connections		Current number of active configuration connections from the LAN
LAN-total-connections		Total number of configuration connections from the LAN up until the present
WAN-active-connections		Current number of active configuration connections from the WAN
WAN-total-connections		Total number of configuration connections from the WAN up until the present
Outband-active-connections		Current number of active outband configuration connections
Outband-total-connections		Total number of previous outband configuration connections up until the present
Outband-bitrate		Bit rate of the last outband configuration session
Login-errors		Total number of defective logins
Login-locks		Number of login locks
Login-rejects		Number of login attempts while the login lock was active
Delete-values		Deletes the config statistics

## Status/DSL-statistics











The DSL statistics show information on data transfer on the DSL terminal. The displayed values on sent and received packets, packet types etc. aid in the search for errors between the *LANCOM DSL/10 Office* and the connected xDSL or cable modem.




/DSL-statistics	DSL terminal statistics	
DSL-rx-packets		Number of packets received from the DSL interface
DSL-tx-packets		Number of packets sent to the DSL interface
DSL-rx-errors		Number of packets with defective content received from the DSL interface

/DSL-statistics		DSL terminal statistics
DSL-tx-errors		Number of packets with defective content sent to the DSL interface
DSL-Rx-no-conn.		Number of packets without logical connections received at the DSL interface
DSL-NIC-errors		Number of internal errors at the DSL interface
DSL-queue-packets		Number of packets still to be sent
DSL-queue-errors		Number of packets discarded due to a lack of buffers
DSL-rx-bytes		Number of characters received via the DSL interface
DSL-tx-bytes		Number of characters sent via the DSL interface
DSL-rx-unicast		Number of packets directed directly to the LANCOM
DSL-tx-broadcast		Number of broadcasts sent to the DSL interface
DSL-tx-unicast		Number of packets sent directly to the AC
Connection established		Display of link status of the DSL connection
PPPoE-statistics		Statistics on special PPP over Ethernet packets
Delete-values		Deletes DSL statistics

## Status/DSL-statistics/PPPoE-statistics





















Statistics on establishing the connection with PPP via Ethernet are displayed here. If a connection to the Internet provider cannot be established, this information will assist the error search.

/PPPoE-statistics		Statistics on special PPP over Ethernet packets
Tx-PADI		Number of PPP Active Discovery Indications sent (start of negotiation)
Rx-PADO		Number of PPP Active Discovery Offers received (AC offers)
Tx-PADR		Number of PPP Active Discovery Requests sent (AC requests)
Rx-PADS		Number of PPP Active Discovery Session Confirmations received (AC session confirmation)
Tx-PADT		Number of PPP Active Discovery Terminates sent (end of session)
Rx-PADT		Number of PPP Active Discovery Terminates received (end of session)
Tx-protocol		Number of protocol packets sent
Rx-protocol		Number of protocol packets received
Tx-data		Number of user data packets sent
Rx-data		Number of user data packets received

/PPPoE-statistics	Statistics on special PPP over Ethernet packets	
Rx-bad		Number of faulty packets received
AC-name		Name of selected access concentrator
Service		Name of negotiating service

## Status/Queue-statistics

These statistics allow you to observe the flow of the individual packets through the various modules of the *ELSA LANCOM*.

/Queue-statistics	Statistics on the queue	
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
WAN-heap-packets		Number of buffers available
WAN-queue-packets		Number of buffers in use
ARP-query-queue-packets		Number of ARP packets in the query queue
ARP-queue-packets		Number of ARP packets in the normal queue
IP-queue-packets		Number of IP packets in the normal queue
IP-urgent-queue-packets		Number of IP packets in the secured queue
ICMP-queue-packets		Number of ICMP packets
TCP-queue-packets		Number of TCP packets
TFTP-queue-packets		Number of TFTP packets
SNMP-queue-packets		Number of SNMP packets
Prot-heap-packets		Number of prot heap packets
IPr-queue-packets		Number of packets remaining to be processed by the IP router.
DHCP-server-queue-packets		Number of packets in the receive queue of the DHCP server.
IPr-RIP-queue-packets		Number of packets in the receive queue of the IP-RIP module (for RIP queries, RIP propagations...).
DNS-tx-queue-packets		Number of packets to be forwarded to DNS or NBNS servers.
DNS-rx-queue-packets		Number of packets that come from DNS or NBNS servers and are to be forwarded to the host.
IP-Masq.-tx-queue-packets		Number of packets to be sent masked (to the Internet).
IP-Masq.- Rx-queue-packets		Number of packets received from the Internet and have to be demasked.

## Status/Connection-statistics

This menu allows you to display connection times and other useful information related to DSL port utilization.

For each available interface, the **Status/Conn.-statistics** menu option provides statistics on the connections established via this interface. The table maintained here has the following layout:

Ifc	Connection	Errors	Con.-Time
Ch01	0	0	No connection

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

Ifc	Designates the associated channel.
Connection	Indicates the number of connections to the particular channel.
Errors	Indicates the number of connection errors.
Con.-Time	Indicates the period of time the current connection has existed. If no connection exists, "No-connection" is output.

## Status/Info-connection

The menu item **Status/Info-connection** has additional information on the current connection status (logical remote station etc.) for every available interface. The table maintained here has the following layout:

Ifc	Status	Device-name	SH-time
Ch01	Ready		0

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

Ifc	Designates the associated channel.
Status	Indicates the status of the particular connection. The possible values are: <b>initialization, setup WAN, ready, establish PPPoE, protocol, connection, release</b>
Device-name	Indicates the logical name of the remote station (if it can be detected).
SH-time	Indicates the short timeout for the connection.

## Status/Remote-statistics

This table shows the last hundred connections of the *ELSA LANCOMs* with information on the remote station.

The table has the following layout:

Conn.-start	Remote-ID	Conn.-time
0T; 00:20:57	BERLIN	50
0T; 00:20:46	CHEMNITZ	230

The different entries have the following meaning:

Conn.-start	Time at which the connection was established. Either the device operating time or the current time is displayed (if the user has input them).
Remote-ID	Logical remote station name
Conn.-time	Duration of connection in years, months, days (optional) and hours, minutes and seconds

A connection remains in the table for at least as long as it is established. Every new connection fills the table from top to bottom. If an existing connection is the lowest entry in the table, an already released connection will be deleted from the table instead if necessary.

## Status/Channel-statistics

This table shows information on the current status of the DSL channel. The information from this table is primarily used for output via *ELSA LANmonitor*. Therefore, some values are shown simply as bits with no further explanation.

The table has the following layout:

Channel	State	App	Mode	Cause	Sub-address	Conn.-time	Extra
Ifc-ERR	00000000	Router	active	0000	00000000	0	
Line	00000000	Router	active	0000	00000000	20	

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

Channel	Channel for the entry is valid. Only the latest status of a channel is ever displayed. A dedicated "channel" is maintained for error messages on channels.
State	The status of a channel is shown here as, e.g., 'ready'.
App	Application that occupies the channel: Router
Mode	Types of last connection establishment: Active
Cause	Last error






Subaddress	Addition to application that, e.g., indicates the logical channel for the router
Conn.-time	Duration of the last connection on this channel
Extra	Additional information on the connection, e.g. the name of the remote station for router connections

## Status/Time-statistics

This menu has information on the current time in the device and on the path over which the *LANCOM Office* router has obtained the time.

The menu has the following layout:

/Time statistics	Time module statistics	
Current-time		Current device time
Source		Time output source. The possible values are: 'Manual' for the manual setting of the time with the 'time' command, 'RAM' for time imported from the device RAM after booting.
Setup		Number of time imports from one of the above sources.









## Status/Delete-values




With the exception of the tables, this option allows you to delete all the values in the substatistics. To do so, enter the following command:

```
do delete-values
```

## Setup

This menu allows you to query and modify all the system parameters that are necessary to the functioning of the devices.

/Setup	System configuration	
Name		Entering the device name
WAN-module		WAN settings
Charges-module		Charge management settings
LAN-module		LAN settings
TCP-IP-module		TCP/IP module settings
IP-router-module		IP router module settings
SNMP-module		Settings for configuration via SNMP
DHCP-module		DHCP server settings

/Setup		System configuration
DNS-module		DNS server settings
Config-module		Configuration module settings
Time-module		Time module settings

*Name*

Here you can enter the device name (maximum 16 characters). The set of characters available includes uppercase and lowercase letters as well as some special characters. You can display the full range of available characters during a configuration session by entering the following command:

```
set \setup\name ?
```

In the default configuration, no name is entered.




The device name is required for identification purposes; it is a prerequisite for any connection via the IP router module, since the routers can exchange data only with known remote stations.

In the case of PPP connections, either the user name with the password from the PPP list or the device name is transferred to the remote station as a device ID during a verification by PAP or CHAP.

In addition, the device names you assign must be unique. For example, you might match the device names to the location (e.g. Aachen, Berlin, Provider, etc.).

## Setup/WAN-module

This menu groups together all the settings necessary for starting up the WAN interface and controlling connections to logical remote stations.

/WAN-module		WAN settings
Name-list		Remote station settings
PPP-list		Parameter settings for PPP connections
Manual-dialing		Settings for manual connection control

*Name-list*

The names entered in the name list are needed by the router to determine the correct remote station and corresponding layer name. The name list is also used for the callback function.

The name list can contain 16 different device names and might, for example, have the following appearance:

Device-name	SH-time	AC-name	Service name
AACHEN	180		
BERLIN	20		

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

Device-name	In the <b>Device Name</b> column, you can enter an original remote station name, which you must then assign to the relevant remote station via the <b>Name</b> option in the <b>Setup</b> menu.
SH-time	In this column, you can define appropriate connection time-outs (in seconds) for the DSL connection. If no data is being transmitted when this time expires, the connection on this channel is released (default: 20).
AC-name	Name of desired access concentrator. If nothing is input here the <i>LANCOM</i> will accept every AC with an appropriate service.
Service name	Name of desired service. If nothing is input the <i>LANCOM</i> will accept every service offered.

#### PPP-list

The router needs the device names contained in the PPP list in order to determine the security procedure settings suitable for the connection and to determine the PPP parameters. It contains a maximum of 16 entries and is structured as follows:

Device-name	Auth.	Key	Time	Try	Conf	Fail	Term	Username
AACHEN	CHAP	*****	0	5	10	5	2	ELSA

Not all parameters can be reached via the telnet configuration. Use *ELSA LANconfig* so far as possible.




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

Device-name	In the Device-name column, you can enter the name with which the remote station logs onto the router. Entries are not case-sensitive!	
Auth.	In this column, you can enter the security procedure to be used for verification of the remote station. Default: PAP	
	none	The router does not negotiate authentication with the remote station when establishing a connection. However, the remote station can itself require authentication from the router. This is the case when dialing up a connection to an ISP, for example.
	PAP	The remote station is checked as per the Password Authentication Protocol.
	CHAP	The remote station is checked as per the Challenge Handshake Authentication Protocol.
Key	A password may be entered in this column. Its presence is indicated by the symbol * and it is used to check the remote station. It may consist of 95 characters (7-bit ASCII, including spaces). Default: None The <code>set ?</code> command shows a list of the allowable characters.	
Time	In this column, you can enter the period of time between two remote station verifications specified in minutes. The CHAP protocol must be set here. Default: 0	

Try	In this column, you can specify the number of times the verification attempt is to be repeated. If verification fails, the connection is immediately terminated. Default: 5
Conf, Fail and Term	These parameters may be used to influence the operation of the PPP. They are defined and described in RFC 1661. The default values are sufficient for most remote stations. If nothing is entered here, the values 0,0,0 appear in the display but the default values 10, 5, 2 are still used. These parameters can only be changed via SNMP or TFTP (using the <i>ELSA LANconfig</i> configuration program)!
Username	The user name (max. 64 characters) transmitted to the remote station during PPP negotiation. The router identifies itself to the remote station with it. If no user name is entered, the device name serves as the user name. Entries are case-sensitive here.

### Setup/WAN Module/Manual Dial

This option can be used for manual connection control for testing purposes.

/Manual-dialing	Settings for manual connection control	
Connect		Establishes a connection
Disconnect		Termination of connections
Status		Displays the current connection status.

#### Connect

Parameter: Remote station's device name (via remote configuration only).

You can use the command

Do `/Setup/WAN-module/Manual-dialing/Connect` to remote station to initiate the manual establishment of a connection via remote configuration. The remote station's device name specified as a parameter must also be entered in the name list with a call number.

If you attempt to establish a connection to a logical remote station for which no call number is specified in the name list, the 'No number' error message is displayed.






#### Disconnect

This command allows you to release an existing connection. If a connection is released manually, the name of a remote station may also be entered in the remote configuration. In this case, only the connection to the remote station specified is released. If a connection to the remote station specified does not exist, there is no further response. However, if a remote station name is not entered, all existing connections will be released.

## Setup/Charges-module

This menu item is used to make the required settings for charge protection.

The default setting for charge protection is 10 hours per six days. The menu has the following layout:

/Charges-module	Charge management settings	
Day(s)/Period		Length of one period in days
Minutes budget		Minutes available for each period
Spare-minutes		Remaining number of available minutes
Router-minutes		Number of minutes used by the router modules
Time-table		Local budget settings for the individual interfaces

Every charge unit incurred by a connection is immediately deducted from the minute budget, enabling monitoring of the minutes still available.

*Day(s)/Period* This menu option allows you to define a period of time in days (0 to 255) during which the online minutes are to be added up and compared to the budget. The default setting is six days. When this period has expired, the adding up of online minutes starts over again.

If the value 0 is entered, a connection can no longer be established after the minutes budget has been used.

*Minutes budget* This option allows you to define the number of charge monitoring online minutes that are to be available. These minutes can only be entered in increments of ten, with a maximum total of 2550. The default setting is 600.




*You can cancel a charge lock either by switching the device off and on again, by activating the **Boot-system** option in the **Other** menu or by entering a new charges budget.*

This table can be used only for setting the budget units; all other entries are automatically managed by the system.

Entering zero budget minutes deactivates charge monitoring.

## Setup/LAN-module

This menu allows you to select the settings needed for the local network. The menu has the following layout:

/LAN-module	LAN settings	
Connect		Selection of the network connection
Node ID		MAC layer address of the device
Spare-heap		Buffers that receive data packets from the local network

### Connector

This option allows you to select from among the following network connections:

Connect	Meaning
Auto	Default setting; enables the Autosense function of the network chip. This automatically sets the router to the port in use without requiring manual configuration of this item.
10BTX	10BASE-T in half-duplex mode
FD10BTX	10BASE-T in full-duplex mode
100BTX	100BASE-T in half-duplex mode
FD100BTX	100BASE-T in full-duplex mode



*When making settings for the fast-Ethernet operation, please note that the selected transfer mode must also support the additional terminals.*

*When the system is switched off and on again, the last port to be selected remains activated.*

### Node-ID















This option allows you to display the router's own Ethernet address. The value displayed here was set at the factory and cannot be changed. The Ethernet address is displayed as a 12-digit hexadecimal value, with the first six digits '00a057' standing for an ELSA device.

### Spare-heap

The spare heap blocks for the local network affect the number of buffers that are always available for receiving frames from the local network. The default value is 10, which ensures that, e.g., four telnet sessions can be activated via the local network at any time.

## Setup/TCP-IP module

This menu allows you to enter settings for the TCP/IP module. The menu has the following layout:

/TCP-IP-module		TCP/IP module settings
State		Activates or deactivates the TCP/IP module.
IP-address		Local IP address
IP-netmask		Local network's matching IP network mask
Intranet addr.		Local Intranet address
Intranetmask		Local network's matching Intranet network mask
Access-list		Restricts access to internal functions via TCP/IP.
DNS-default		Domain name server
DNS-backup		Backup domain name server
NBNS-default		NetBIOS name server
NBNS-backup		Backup NetBIOS name server
Table-ARP		ARP table for mapping an IP address onto a MAC address
ARP-aging-min.		Dwell time for entries in the ARP table
TCP-aging-min.		Time limit for configuration connections that are inactive
TCP-max.-conn.		Max. number of simultaneous configuration connections to the <i>ELSA LANCOM</i>

### Operating

The TCP/IP module of the router may be activated or deactivated here. In the default configuration, the TCP/IP module is activated.

*Configuration via TCP/IP using telnet and the IP router is possible only if the TCP/IP module is activated.*

### IP address

The IP address for the router may be entered here. The default address on delivery is '0.0.0.0'.

If IP masquerading is used, this address takes on a special meaning in connection with the Intranet address:

If the IP address is assigned to the router by the Internet provider by PPP, all computers in the network linked by IP address and IP network mask are normally routed. These computers can then also be accessed directly from the Internet.

### IP-netmask

The network mask belonging to the IP address must be entered here. The default setting is 255.255.255.0 (class C network). A network mask of 255.255.255.255 means that there is only one computer in this network (the router itself). This setting (an IP address registered in the Internet with a fully assigned network mask) can be used for

masquerading via a raw IP access, such as that offered by the provider of the individual network. With such an access an IP address is not assigned to the router by a PPP negotiation, but it must have a fixed IP address registered in the Internet.

*Intranet-address*

A second IP address for the router may be entered here. This enables the router to be used as a router for two logical IP networks and also this address has a specific meaning with the use of IP masquerading:

In this case, all computers that are in the network linked by Intranet address and Intranet mask are hidden behind the address assigned by the provider (or the Internet address (IP address)).

The default address on delivery is '0.0.0.0'.

*Intranet-mask*

The network mask belonging to the IP address must be entered here. The default setting is 255.255.255.0 (class C network).



*If neither an IP nor an Intranet address has been specified, the device responds to a default IP address, the first three digits of which are identical to the first three digits of the sending device XXX.XXX.XXX.YYY. The device can then be reached by dialing the IP address XXX.XXX.XXX.254.*

*In the event that such an address already exists in the network, a different address must be entered via outband configuration (terminal program).*



*If both an IP address and an Intranet address have been entered, the network defined by an IP address and IP network mask must contain only workstations (i.e. no routers).*

*Access-list*

The access to "internal functions" of the router may be controlled by an access list in TCP/IP applications.



*The configuration data of the device are protected by a password, however this is always transferred in plain text, making it possible in principle to detect it and for any computer to read the configuration or to delete it. In order to prevent this from happening, the access list can be used to determine which computers or which networks can access the configuration.*

For reasons of consistency, the access control is based on all "internal functions" of the router. The term "internal functions" refers to the following:

- Telnet server: the configuration interface based on the telnet protocol
- TFTP server: the configuration interface based on the TFTP protocol
- SNMP: the configuration interface based on the SNMP



Each of the maximum of 16 entries in the access list has the following structure:

IP-address	IP netmask
IP address of the authorized user (or user circle)	IP network mask of the user circle

Once an IP workstation with its IP address and the network mask 255.255.255.255 is entered into the list, the internal functions of the router can only be accessed from this computer. Any requests from devices with different IP addresses are ignored.

If a complete network has access enabled to an *ELSA LANCOM*, this can be done as follows for a class C network:

IP-address	IP netmask
192.234.222.0	255.255.255.0

With this entry all IP addresses in the class C network 192.234.222.0 are authorized to use internal functions of the router.

#### *DNS-default*

The entry **DNS** (Domain Name Server) is required to announce the name server responsible for their own network for computers that have direct access via PPP to the router.

If the router is configured for access to the Internet via an Internet Service Provider, the DNS server is usually given by the provider. There are then two possible settings in the router:

- '0.0.0.0' is entered as the address of the DNS server. All computers in the local network can then use the provider's DNS server.
- The router's own IP address is entered as the DNS server. Then he uses the DNS information from the provider not only for its own local network but also forwards this information (DNS forwarding). Remote stations such as computers that dial in via remote access can then also access the provider's DNS server. This procedure is also referred to as DNS forwarding.

#### *DNS-backup*

With the entry **DNS-Backup** a second name server can be named, which is used if the DNS fails.

#### *NBNS-default*

The entry **NBNS-default** (NetBIOS Name Server) is required to announce the NBNS responsible for their own network for computers that have direct access via PPP to the router.

#### *NBNS-backup*

With the entry **NBNS-Backup** a second name server can be named, which is used if the NBNS fails.

*Table-ARP* This option allows you to display the ARP table (ARP cache), which is managed automatically for the purpose of mapping IP addresses onto physical terminal addresses. Individual entries can be removed from this table but no new entries can be entered manually.

The entries in the ARP table might, for example, have the following appearance if different devices with different IP addresses (192.168.139.20, 192.168.130.30) communicated with the router:

IP-address	Node-ID	Last-access	Connect
192.168.130.20	0000c0717860	6780443 tics	local
192.168.130.30	0800091eebf4	6214514 tics	local










*ARP-aging-min.* This option allows you to enter a time (from 1 to 99 minutes) at the end of which the ARP table is automatically updated, i.e. all IP addresses that have not been accessed since the last automatic update are removed. The default setting is 15 minutes.

*TCP-aging-min.* If data transfer stops during a TCP connection to the router, e.g. if the user does not enter any more data during the remote configuration, it will automatically release the TCP connection on expiry of the time entered here. Possible settings are from 1 to 99 minutes; The default setting is 15 minutes.

*TCP-max.-conn.* The maximum number of allowable connections possible at the same time can be set here. DEFAULT setting is '0', meaning the same as "any number".

## Setup/IP-router-module

This menu allows you to enter settings for the IP router module. The menu has the following layout:

/IP-router-module	IP router module settings	
State		Activates or deactivates the IP router module.
IP-routing-table		Router table for IP network and remote station assignment
LAN-filter-table		Negative/connect filter table for the TCP/UDP destination ports of LAN packets
WAN-filter-table		Negative filter table for the TCP/UDP destination ports of WAN packets
Proxy-ARP		Activates/deactivates the proxy ARP function
Loc.-routing		Activates/deactivates local routing
Routing-method		Routing method for IP packets
RIP-config		Settings for IP-RIP operation
Masquerading		Settings for IP masquerading

## Operating



This option allows you to activate or deactivate the IP router module. In the default configuration, the IP router module is activated.

*Activating the IP router module also activates the TCP/IP module.*

## IP-routing-table

The routing table can contain a maximum of 128 entries of destination network addresses or direct IP addresses with netmasks, and the names or IP addresses of other local routers. Alternatively, you can enter a setting by means of which packets to specific destination IP addresses are discarded and are not answered by proxy ARP. This is done by entering 0.0.0.0 for the name of the responsible router.

The 'Masquerade' field indicates whether the route should be masked or not. The following options are offered here:

- **On:** IP masquerading is switched on and functions with dynamic assignment of the IP address by the remote station. In this procedure the router queries the IP address '0.0.0.0' at the remote station and is assigned a random IP address by the remote station, which is then used for further processing.
- **Off:** Masquerading is switched off.
- **Static:** IP masquerading is switched on and functions with assignment of a static IP address previously assigned by the remote station. In this procedure the router queries the IP address entered under 'Setup/TCP-IP-module' at the remote station and is assigned this address by the remote station. Use this setting when the remote station (e.g. your Internet provider) has assigned you a fixed IP address in the access data. Of course, this procedure will only function when this address has also been entered in the router as the IP address.

The IP routing table is generally sorted as shown below:

- The longest network mask is placed on top.
- For network masks of equal length, the one with the smallest IP address is placed on top.

In order to identify the correct remote station, the router searches the routing table from top to bottom using the destination IP address received. If a matching entry is found, the router name found is used for establishing the connection.

Address ranges that are prohibited in the Internet are excluded from transmission by preset entries in the IP routing table (the router name 0.0.0.0 means that packets to these addresses are not transmitted). The IP routing table below is provided by way of example and also shows the default settings:

IP-address	IP netmask	Router-name	Distance	Masquerade
192.168.0.0	255.255.0.0	0.0.0.0	0	Off
172.16.0.0	255.240.0.0	0.0.0.0	0	Off
10.0.0.0	255.0.0.0	0.0.0.0	0	Off
224.0.0.0	224.0.0.0	0.0.0.0	0	Off

However, if these addresses are required for Intranet use, for example, it is possible to delete the predefined entries at any time. If the routing table contains no entries with the router name 0.0.0.0, the router processes all IP addresses with valid routes.

■ Example

- The local network address is 192.120.130.0.
- Data packets for the destination network 193.140.300.0 are to be sent to another local router with the IP address 192.120.130.200.
- Absolutely nothing is to be transmitted to the destination network 193.140.200.0.
- All other non-local data packets must be sent to the router 'PROVIDER' at the Internet service provider.

In this example, the router table would contain the following entries:

IP-address	IP netmask	Router-name	Distance	Masquerade
193.140.200.0	255.255.255.0	0.0.0.0	0	Off
193.140.300.0	255.255.255.0	192.120.130.200	0	Off
255.255.255.255	0.0.0.0	PROVIDER	0	On

The last line is an entry for the "default route". The IP address 255.255.255.255 means the same as 0.0.0.0 (for technical reasons, 0.0.0.0 cannot be entered in the first column). Because it contains the IP network mask 0.0.0.0, this line is always appropriate after the rest of the table has been searched. Therefore, the router sends everything that it cannot transfer over other routes and should not discard or that comes from a WAN terminal and is not local to the router at the provider.

*LAN-filter-table* This table allows you to filter specific ranges of destination ports. In addition, you can determine how the packets are to be filtered. If packets with the entered ports are received from the LAN side, they will not be forwarded (always filter) unless a connection is currently in place (connect filter) or unless they can be routed over other than the DEFAULT route (I-Net filter).

The LAN port filters are defined in a table with the following layout::

Idx.	D-st.	D-end	S-st.	S-end	Source	Src-netmask	Prot	Type
WIN	0	0	137	139	255.255.255.255	0.0.0.0	TCP and UDP	Always-filt.

The table fields have the following meaning:

- **Idx.**  
Unique index. This entry is required to enable the filters to be distinguished. The index may be four characters long and selected as desired.
- **D-st., D-end**  
Destination port range that is to be filtered. A range of 0 to 0 means that no destination port is affected by this filter.
- **S-st., S-end**  
Source port range that is to be filtered. A range of 0 to 0 means that no source port is affected by this filter.
- **Src-address, Src-netmask**  
A subnetwork of the local network for which the filter is valid can be entered here. A source address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).
- **Prot**  
Protocol that is to be filtered. Possible entries are **TCP**, **UDP**, **ICMP** and **all**.  
The setting **all** filters out every packet from the specified source network or to the destination network.
- **Type**  
Filter type. The possible values are Always-filt., Connect-filt. and Internet-filt.
  - **Always** filter: The packet is discarded.
  - **Connect** filter: The packet is discarded if there is no connection to the remote station.
  - **Internet** filter: The packet is discarded if its destination can be accessed only via the default route.

The default filter is entered in the above table. It suppresses the unwanted and cost-intensive connections in Windows networks on IP. These networks regularly send items such as DNS queries to the local network, which are routed to the Internet without this filter.

WAN-filter-table

This table allows you to enter specific ranges of destination ports. If packets with the entered ports are received from the WAN side, they will not be forwarded (firewall function).

The WAN port filters are defined in a table similar to the LAN filter table:

Idx.	D-st.	D-end	S-st.	S-end	Dest	Dst-netmask	Prot
WIN	53	53	137	139	0.0.0.0	0.0.0.0	TCP and UDP

The fields in the table have the same meaning as in the LAN filter table, with the following exception:

- Dst-address, Dst-netmask

A subnetwork of the local network for which the filter is valid can be entered here. A destination address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).

The table entries are sorted in a similar fashion to the IP router table:

- Longest network mask is placed on top.
- For two network masks of equal length, the one with the smaller IP address is placed on top.

Network masks and IP addresses of 0.0.0.0 can be used as "wildcards". Specified computers and networks may be simultaneously subjected to targeted filtering while others pass the router unfiltered.

The tables are processed from top to bottom. As soon as a matching filter is found, the packet is handled accordingly.

Proxy-ARP

This option allows you to activate or deactivate the proxy ARP mechanism (default: 'Off'). This function permits data to be transmitted to IP addresses within the same logical network as the sender, e.g. when linking individual workstation computers (teleworkers) to the corporate network via TCP-IP.



Loc.-routing

Local routing enables the router to forward data packets via the local network. The local routing is necessary if the router, as the default gateway for the workstations receives packets for destination networks to which it cannot establish a connection itself. If the router cannot return the address of the appropriate router to the workstation via ICMP, it will forward the data to the corresponding router itself (see also 'Local Routing'). Since this setting increases network utilization in the LAN, the default setting is 'Off'.

### Setup/IP-router-module/Routing-method

The router offers two methods for IP routing, which can be separately set for IP and ICMP packets. Both methods are based on the evaluation of the field 'Type-of-service' in the IP header.

The menu has the following layout:

/Routing-method	Routing method settings	
Routing-method		Routing method for IP packets
ICMP-routing-method		Routing method for ICMP packets

*Routing-method* This option allows you to define the routing method used for IP packets:

- If you select 'Normal', all IP packets are handled in the same way as per the routing specifications of the Internet protocol.
- If you select 'Type-of-service', IP packets are placed in the urgent queue or reliable queue, depending on the contents of the 'Type-of-service' field. All other packets are placed in the normal send queue. In this way, transmission is guaranteed, provided that it is possible.




*ICMP-routing-method*

This option allows you to define the routing method used for ICMP packets:

- If you select 'Normal', the ICMP packets are handled like any other IP packets as per the routing specifications of the Internet protocol.
- If you select 'Reliable', all ICMP packets received are placed in the reliable queue.

### Setup/IP-router-module/RIP-configuration

This option allows you to enter settings for the management of IP-RIP packets. The menu has the following layout:

/RIP-configuration	Settings for IP-RIP operation	
Type		RIP compatibility switch
R1-mask		Management of network masks
Table-RIP		Dynamic IP routing table

*Type*

This option allows you to select the method to be used for handling the IP-RIP packets. The different settings have the following meaning:

- **Off:** IP-RIP is not supported (default).
- **RIP-1:** RIP-1 and RIP-2 packets are received but only RIP-1 packets are sent.
- **R1-comp:** RIP-1 and RIP-2 packets are received. RIP-2 packets are sent as an IP broadcast.
- **RIP-2:** Same as **R1-comp** except that all RIP packets are sent to the IP multicast address 224.0.0.9.

*R1-mask*

If **RIP-1** is set, this option allows you to influence the management of network masks. Therefore, these settings are required only for subnetting under **RIP-1**. The different settings have the following meaning:

- **Class** (default): The network mask used in the RIP packet is derived directly from the IP address class, i.e. the following network masks are used for the network classes:
  - Class A: 255.0.0.0
  - Class B: 255.255.0.0
  - Class C: 255.255.255.0
- **Address**: The network mask is derived from the first bit that is set in the IP address entered. This and all high-order bits within the network mask are set. Thus, for example, the address 127.128.128.64 yields the IP network mask 255.255.255.192.
- **Cl+Addr**: The network mask is formed from the IP address class and a part attached after the address procedure. Thus, the above-mentioned address and the network mask 255.255.0.0 yield the IP network mask 255.128.0.0.

*Table-RIP*






This option allows you to display the entries in the current dynamic IP routing table.

An IP-RIP routing table might, for example, have the following appearance:

IP-address	IP netmask	Time	Distance	Router
223.245.254.0	255.255.255.0	1	1	192.38.9.100
223.245.257.0	255.255.255.0	1	1	192.38.9.200

**Setup/IP-router-module/Masquerading**

This menu allows you to enter settings for the masking function. The menu has the following layout:

/Masquerading	Settings for IP masquerading	
TCP-aging-second(s)		Time in seconds after which a TCP masking becomes invalid
UDP-aging-second(s)		Time in seconds after which a UDP masking becomes invalid
ICMP-aging-second(s)		Time in seconds after which an ICMP masking becomes invalid
Service-table		Static masquerading table
Table-masquerading		Dynamic masquerading table

*Service-table*

The use of inverse masquerading makes 'services' (e.g. a file server) selectively visible in the Internet by entering specified ports in the service table in the IP network, while all other services and computers remain invisible from the local network (see also



'IP Masquerading (NAT, PAT)'). The service table (also called the static masquerading table) can contain up to 16 entries and has the following layout:

D-port	Intranet addr.
20	10.1.1.10
21	10.1.1.10

The different columns have the following meaning:

- D-port: Destination port for the particular entry
- Intranet-addr.: Destination IP address for the computer in the local network

Through this assignment, it is possible, for example, to address the relevant service directly via telnet. Enter the IP address of the router and attach the port number, separated by a double point, to the address.

You can use the command

```
telnet 192.38.50.100:27
```

to connect directly to a news server that can be reached via a router with the IP address 192.38.50.100.

*Table-  
masquerading*

With IP masquerading, the IP addresses of computers in the local network are rendered invisible to external devices by means of a conversion of addresses and ports in the router. The dynamic masquerading table displays the IP addresses from the local network that the router is currently masking. The dynamic masquerading table can contain up to 2048 entries and has the following layout:








Intranet addr.	S-port	Protocol	Time
10.1.1.10	1234	TCP	10

The different columns have the following meaning:

- Intranet-addr.: IP address of the computer in the local network
- S-port: Source port for this entry
- Protocol: Protocol used (TCP/UDP/ICMP)
- Timeout: Time in seconds until the entry is removed from the table

## Setup/SNMP-module

This menu allows you to enter settings for configuration of the router via SNMP. The menu has the following layout:

/SNMP-module		SNMP module settings
Send-Traps		Switch for issuing SNMP traps
IP-Trap-Table		Table with 20 destination addresses for trap messages
Administrator		Device administrator
Location		Device location
Register-monitor		Command to set a destination address to which the traps are to be sent
Delete-monitor		Command to delete an address that was set with 'Register-monitor'
Monitor-table		Table with all currently active destination addresses that were set with 'Register-monitor'

*Send-Traps* This entry controls trap output (No/Yes).

*IP -Trap-Table* Enters the IP addresses to which the trap messages will be sent.

*Administrator* Administrator's name

*Location* Device location

You can also query the last two parameters via SNMP (MIB-2).

*Register-monitor* This command logs on applications with the router to retain targeted trap information. The *ELSA LANmonitor*, for example, queries the channel statistics in this way and converts them to a graphic display (under Windows).

In principle, any SNMP manager can use this command to obtain information from the router. The syntax

```
register-monitor IP-address:port mac address timeout
```

is used to direct the router to enter the given address in the monitor table and to send traps to it. If the traps are not received within the set hold time, the address will be automatically deleted from the table. A hold time of '0' permanently retains the entry in the table.

*Delete-monitor* This command removes the entries from the monitor table.









*Monitor-table* The monitor table has the following structure:

IP-address	Port	MAC-address	Timeout
10.0.0.53	1057	0080c76da46e	1

This entry indicates, for example, that an *ELSA LANmonitor* has logged on to the router.

## Setup/DHCP-server-module

This menu allows you to enter settings for the DHCP server. The menu has the following layout:

/DHCP-server-module	DHCP server settings	
State		Switch for activating the DHCP module
Start-address-pool		Start address for the address pool
End-address-pool		End address for the address pool
Netmask		Network mask for the address pool
Broadcast-address		Broadcast address for the LAN
Max.-lease-time-minute(s)		Maximum period of validity for the address assignment via DHCP
Default-lease-time-minute(s)		Default period of validity for the address assignment via DHCP
Table-DHCP		Table of current assignments via DHCP

State

On: The device operates as a DHCP server

Off: The device does not operate as a DHCP server

Auto: The device regularly checks whether there is another DHCP server in the LAN. If not, it operates as a DHCP server and issues IP addresses to local clients.



*If there is no IP or Intranet address entered in the TCP/IP module (e.g. delivery status), the router will issue IP addresses from the address range 10.0.0.2–10.0.0.253 to all DHCP clients in auto mode.*

Start-address-pool  
End-address-pool

The IP address assigned is taken from the address pool selected ('Start-address-pool' to 'End-address-pool'). Any valid addresses in the local network can be entered here.

If 0.0.0.0 is entered instead, the device will determine the appropriate addresses (start or end) from the settings under 'Setup/TCP module'. The procedure is as follows:

- If only the IP address or only the Intranet address is entered, the start or end of the pool is determined by means of the associated network mask.
- If both addresses have been specified, the Intranet address has priority for determining the pool.
- The start address of the pool is either the address given in the DHCP module or the first valid address in the local network.
- The end address of the pool is either the address given in the DHCP module or the last valid address in the local network.

A valid address is then taken from the pool for the IP address. If the computer was already assigned an IP address at some point in the past, it requests this same address

and the DHCP server attempts to reassign it this address if it has not already been assigned to another computer.

The DHCP server also checks whether the address that is to be assigned to the computer is unique in the local network. It does this by issuing an ARP request to the address. If the ARP request is answered, the DHCP server begins the procedure again with a new address. As soon as the uniqueness of an address has been established, the requesting computer is assigned the address found.

#### *Netmask*

The network mask is assigned in the same way as the address:

The system either assigns the network mask entered in the DHCP module or uses the network mask that belongs to the local network (determined during address assignment).

#### *Broadcast*

The broadcast mask is assigned in the same way as the address:

The system either assigns the broadcast address entered in the DHCP module or uses the broadcast address that belongs to the local network (determined during address assignment).

#### *Max.-lease-time-minute(s)*

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

The DEFAULT value of 6000 minutes equals approximately 4 days.

#### *Default-lease-time-minute(s)*

Here you can enter the period of validity that is assigned if the host makes no request.

The DEFAULT value of 500 minutes equals approximately 8 hours.

#### *Table-DHCP*

In the DHCP module, the 'Table-DHCP' option allows you to verify (or look up) the assignment of IP addresses to the relevant computers. This table has the following layout:

IP-address	MAC-address	Timeout	Hostname	Type
10.1.1.10	00a0570308e1	500	ELSA	new

- IP-address: IP address assigned
- MAC-address: Computer's Ethernet address
- Timeout: Time remaining until the assignment becomes invalid
- Hostname: Computer's name in plain text if it was transmitted in the request
- Type: This field contains additional information on the assignment.







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

- **new**: The computer has made its initial request. The DHCP server verifies the uniqueness of the address that is to be assigned to the computer.
- **unkn.**: While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the DHCP server has no means of obtaining additional information on this computer.

- **stat.:** A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.
- **dyn.:** The DHCP server assigned an address to the computer.

## Setup/DNS module

The settings for the DNS server can be modified here as required. The menu contains the following items (incl. their default settings):

State		On (default) or off
Domain		Own domain, optional, 32 characters max.
DHCP-usage		Yes (default) or no
DNS-table		Static DNS table for the manual association of IP addresses to names, 64 entries
Filter-list		Filter list for the exclusion of prohibited domains, 64 entries
Leasetime		Specifies the name validity information to be given to a requesting computer. Default: 2000

### DNS-table

The DNS table contains a simple association of local names to IP addresses. The table is sorted alphabetically by names.

The table is restricted to 64 entries, as large networks are configured more effectively using the DHCP server, which can also be used to handle name requests. The table has the following layout:

Hostname	IP-address
Host10	10.0.0.10

The name is restricted to a maximum of 32 characters. Longer names are not necessarily practical in a local network.

### Filter-list

The filter list contains the entries for prohibited domains. In addition, it is possible to specify for whom a given domain will be prohibited. This is set using an IP address/netmask pair. An IP address of 0.0.0.0 prohibits this domain for all computers. A subnet mask of 0.0.0.0 prohibits the domain for all networks. The table has the following layout:

Name	Domain	IP-address	Netmask
F001	*xxx*	0.0.0.0	0.0.0.0

Clear IDs can be freely selected and assigned to the filters in the 'Idx.' field.

Enter the name of the domain to be prohibited in the 'Domain' field. Wildcards such as '?' and '\*' may be used. The wildcard '?' replaces exactly one character, while '\*' can stand for a random number of characters. Multiple instances of the wildcard '\*' can be used. For example, \*xxx\* filters all names containing the letters xxx in any position within the name.









The IP address and subnet mask fields can be used to specify the subnet for which the domain will be prohibited.

The filter table is sorted according to the subnet masks in descending order (the longest at the top); entries with identical subnet masks are sorted according to the IP addresses in ascending order. In the event of identical IP addresses, the entries are sorted in ascending order according to the domain to be prohibited.

The table is searched from top to bottom and an error message is returned to the requesting computer in the event of a match.

## Setup/Config-module

This menu allows you to enter settings for router configuration options. The menu has the following layout:

/Config-module		Configuration module settings
LAN-config		Switch for configuring from the LAN side
WAN-config		Switch for configuring from the WAN side
Password-required		Password required on/off if there is no password
Maximum-connections		Maximum number of simultaneous connections
Config-aging-minute(s)		Time limit for remote configuration connections
Login-errors		Number for failed login attempts before the login block is activated
Lock-minutes		Duration of block and period until old login errors are forgotten.
Language		Configuration language

*LAN-config*    This option allows you to define whether remote configuration from the LAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting for this option is **On**.

*WAN-config*    This option allows you to define whether remote configuration from the WAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting for this option is **Off**.

*Password-required*    This specifies whether a new password should be requested every time a remote configuration is begun (**On**), or the password request should be suppressed (**Off**). The default setting for this option is **On**.

Maximum  
connections

This option allows you to display the maximum number of remote configuration sessions that can occur simultaneously for the device.

Config-aging-  
minute(s)

If data transmission halts during a remote configuration session, e.g. because the user is no longer entering data, the device automatically releases the connection at the end of the time period specified here. Possible settings are from 1 to 99 minutes; the default setting is 5 minutes.

Login-errors

This entry specifies the number of failed attempts allowed before the login block is activated. An empty password (simply pressing <ENTER> at the password prompt) is not considered an attempt and therefore does not activate the block.



*The default value is 5. A lower value may cause the login block to be activated with only one access on an older ELSA LANconfig! In this case obtain an updated ELSA LANconfig version over our online media.*

Lock-minutes

This entry has two meanings. It indicates how long the access is blocked if the login block has been activated. It also sets the period after which the device forgets all prior login errors.



Language

This option allows you to select whether you will use the German or English version of the software for performing the configuration.

## Setup/Time-module




The time can be set manually (with the command 'time').




The time module has the following layout:

/Time-module	Time module settings	
State		Activating the module: <b>On, Off</b>
Current-time		Displays the current time in the device.

## Firmware

This menu allows you to display various firmware parameters and to initiate a firmware upload:

/Firmware	Display and keyboard settings	
Version-table		Displays hardware releases and serial numbers for the router
Table-firmsafe		Information on the two firmware versions stored in the device and on the bootloader.
Mode-firmsafe		Firmware activation mode

/Firmware		Display and keyboard settings
Timeout-firmesafe		Time in minutes required to test new firmware
Test-firmware		Tests the inactive firmware
Firmware-upload		Initiates a firmware upload

*Version table* The version table displays the firmware version and serial number of the device.

lfc	Module	Version	Serial number
lfc	LANCOM DSL/10 Office	1.70.0006 / 01.09.1999	8427.000.020

*Table firmsafe* This table provides the following details for the two firmware versions stored in the device: the position in memory (1 or 2), status information (active or inactive), the version number, the date, the size and the index (sequential number).

Position	Status	Version	Date	Size	Index
1	Inactive	1.70	30081999	535	6
2	Active	1.70	01091999	366	7
3	<Lader>	1.60	01091999	64	0

Enter the following command to activate an inactive firmware version:

```
set <position number> active
on.
```

*Mode-firmsafe* Only one of the firmware versions stored in the device can be active at any one time. When new firmware is loaded the inactive firmware is overwritten. You can decide which firmware will be activated after the upload:

- 'immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
  - The new firmware is successfully loaded and then operates as desired. Everything is then in order.
  - However, if the new firmware does not operate correctly, it may not be possible to communicate with the device after the restart. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots the device.
- 'login': To prevent problems caused by defective firmware, the second option will load the firmware and start it immediately.
  - In contrast to the first option, the firmsafe will wait until it has successfully logged on over outband or inband (by telnet). In contrast to the first option, the firmsafe will wait until it has successfully logged on (by telnet). The new







firmware will only be permanently activated when the login occurs successfully within the time set under 'Timeout firmsafe'.

- If the device no longer responds and it is therefore impossible to log in, the firmware automatically loads the previous firmware version and reboots the device with it.
- 'manual': The third option allows you to set a period (Timeout firmsafe) beforehand for testing the new firmware. The device will start with the new firmware and wait for the preset period until the loaded firmware is manually activated and therefore becomes permanently effective.

## Other

The **Other** menu allows you to manage the following functions:

/Other		Various functions
Manual-dialing		Connection testing
Boot-system		Boots the device.
Reset-system		Resets to factory settings.
System-upload		Loads new firmware.

### Other/Manual Dialing

Select this option when you wish to establish a connection manually for testing purposes.

*Boot-system*

This option allows you to reboot the device.



*Before executing the command all open connections (DSL or TCP) will be released or closed.*

*Reset-system*

This option resets all the settings that have been entered. The device is reset to the delivery version.

For safety's sake, the system asks you to enter the configuration protection password in order to ensure that you have not mistakenly selected this command instead of the `Boot-system` command. If no password has been assigned, you must press Enter a second time.

*Upload-system*

This option starts a firmware upload (refer to chapter 'How to set up new software').

The flash ROM technology permits flexible and service-friendly handling of the system software by allowing different firmware versions to be read in. It also allows devices can be retrofitted for all future options.

