

# ***ELSA LANCOM™ Wireless IL-2***

**Manual**

© 1999 ELSA AG, Aachen (Germany)

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

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

#### Trademarks

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

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

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

ELSA AG  
Sonnenweg 11  
52070 Aachen  
Germany

ELSA, Inc.  
2231 Calle De Luna  
Santa Clara, CA 95054  
USA

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

Aachen, October 1999

No. 20943/1099

# Preface

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

Wireless networks from ELSA are economical alternatives or additions to local wired networks (LANs). Notebooks and PCs can use mobile network cards to communicate with one another or access wired networks via base stations and can even be integrated into the ISDN network.

This documentation was written for the user of the *ELSA LANCOM Wireless IL-2* base station. First, we will introduce the device and its possibilities, help you connect it and install the software, and describe a number of common sample applications.

## **Documentation**

The accompanying documentation comprises:

- Manual  
Hardware installation, description of the functions, operating modes and sample configurations
- CD containing electronic documentation  
All product manuals, basic technical information (e.g. wireless networks, general networking technology, TCP/IP etc.), workshop with detailed examples of applications, reference section for general information including a complete description of the menus.



*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>
The basic functions of a wireless network.....	1
What does the <i>ELSA LANCOM Wireless IL-2</i> offer?.....	6
<b>Installation .....</b>	<b>11</b>
Package contents.....	11
Introducing the <i>ELSA LANCOM Wireless</i> .....	11
Connecting the access point.....	13
Software installation .....	14
Basic configuration .....	14
Make basic settings with <i>ELSA LANconfig</i> .....	14
Configuring the basic settings using Telnet .....	16
<b>Configuration modes .....</b>	<b>17</b>
Radio or wired: Configuration approaches.....	17
Preconditions.....	17
Alternatively: Address administration with the DHCP server .....	17
Beginning configuration using <i>ELSA LANconfig</i> .....	18
Start up configuration using Telnet .....	19
Configuration commands .....	19
New firmware with FirmSafe .....	20
This is how FirmSafe works.....	20
How to load new software .....	21
Configuration using SNMP .....	22
<b>Operating modes and functions .....</b>	<b>23</b>
Parameters for the wireless connection.....	23
Security for your configuration .....	25
Password protection .....	25
Login barring .....	25
Access control via TCP/IP .....	26
Security for your LAN.....	26
Security check .....	26
Callback .....	27
The hiding place – IP masquerading (NAT, PAT).....	28
Call charge management.....	28
Time-dependent Connection control.....	28
Settings in the charge module.....	29
ISDN connections .....	29
Name-list.....	29
Interface settings .....	30

Router interface settings .....	31
LANCAPI interface settings .....	31
Layer list .....	32
Round-robin list .....	33
PPP-list .....	33
Script .....	34
Call acceptance .....	34
Number-list .....	34
Point-to-point protocol .....	35
The protocol .....	35
The PPP list .....	36
Everything OK? Checking the line with LCP .....	37
IP-Routing .....	38
The IP routing table .....	38
TCP/IP packet filters .....	39
Proxy-ARP .....	40
Local routing .....	40
Dynamic routing with IP RIP .....	41
IP-masquerading (NAT, PAT) .....	42
DNS forwarding .....	44
Policy based routing .....	44
Automatic address administration with DHCP .....	44
The DHCP server .....	45
DHCP – 'on', 'off' or 'auto'? .....	45
How are the addresses assigned? .....	46
Configuring the DHCP server .....	49
DNS .....	51
What does a DNS server do? .....	51
Setting up the DNS server .....	52
NetBIOS proxy .....	54
To the point: What is NetBIOS? .....	54
Handling of NetBIOS packets .....	55
Which preconditions must be fulfilled? .....	56
Linking two Windows Networks via ISDN .....	58
Dial-up procedure for a remote access station .....	60
Search and Find: the Network Neighborhood .....	60
Office communications and ELSA LANCAPI .....	62
ELSA LANCAPI .....	62
The least-cost router .....	66
<b>Appendix .....</b>	<b>73</b>
Technical data .....	73
Hardware specifications .....	73

Software Specifications.....	73
Radio channels.....	74
Warranty conditions .....	75
Declaration of conformity .....	77

<b>Index .....</b>	<b>79</b>
--------------------	-----------

## **Technical basics (on CD only) ..... R1**

Wireless network according to the IEEE-802.11 standard.....	R1
Ad hoc mode .....	R1
Infrastructure mode.....	R2
Interchangeability with other devices .....	R3
Network technology.....	R4
The network and its components.....	R4
Connection modes.....	R4
Kinds of networks .....	R6
IP addressing.....	R6
IP routing and hierarchical IP addressing .....	R9
Expansion through local networks.....	R11

## **Description of the menu options (on CD only) ..... R17**

Status.....	R19
Status/Connection-state.....	R20
Status/Current-time .....	R20
Status/Operating-time .....	R20
Status/S0-bus .....	R20
Status/WLAN-statistics.....	R21
Status/WAN-statistics.....	R22
Status/LAN-statistics.....	R25
Status/PPP-statistics.....	R26
Status/TCP-IP-statistics .....	R32
Status/IP-router-statistics.....	R38
Status/Config-statistics .....	R40
Status/Queue-statistics .....	R41
Status/Connection-statistics .....	R42
Status/Info-connection .....	R43
Status/Layer-connection.....	R43
Status/Call-info-table .....	R44
Status/Remote-statistics .....	R44
Status/Channel-statistics .....	R45
Status/Time-statistics.....	R46
Status/LCR-statistics .....	R47
Status/PCMCIA-status.....	R47
Status/Delete-values .....	R47



Setup .....	R48
Setup/WAN-module .....	R49
Setup/LAN-module .....	R58
Setup/TCP-IP-module .....	R59
Setup/IP-router-module .....	R62
Setup/SNMP-module .....	R70
Setup/DHCP-server-module .....	R71
Setup/NetBIOS .....	R73
Setup/Config-module .....	R76
Setup/LANCAPI-module .....	R77
Setup/WLAN-module .....	R78
Setup/LCR-module .....	R79
Setup/DNS module .....	R80
Setup/Time-module .....	R82
Firmware .....	R82
Other .....	R84
<hr/>	
<b>Ports and protocols (on CD only) .....</b>	<b>R85</b>
Ports .....	R85
Protocols .....	R87



# Introduction

The advantages of wireless LANs are obvious: Notebooks and PCs can be set up where they are wanted—problems with missing connections or architectural alterations are a thing of the past with wireless networking.

Network links in conferences or presentations, access to resources in adjacent buildings and exchanging data with mobile units are only a few of the options available with a wireless LAN.

The access point plays the central role in enabling these options in an existing wired network. All stations in the wireless network access the LAN via the access point.

Your entire LAN is connected to the outside world via the integrated IP router and the ISDN interface. Access to the Internet for the entire LAN or office functions such as fax and answering machine at all workstations are only some of the advantages offered by the ISDN router.



*The use of radio frequencies in the 2.4 – 2.48 GHz range may be restricted or subject to an application in some European countries. The list of national approvals is enclosed.*

## The basic functions of a wireless network

This chapter introduces the basic functional principles of a wireless network. The terms used will be explained and the structure and possible applications of wireless networks introduced. Detailed information on this and other topics can be found in the electronic documentation on the CD.

*Wireless network adapters  
WLAN*

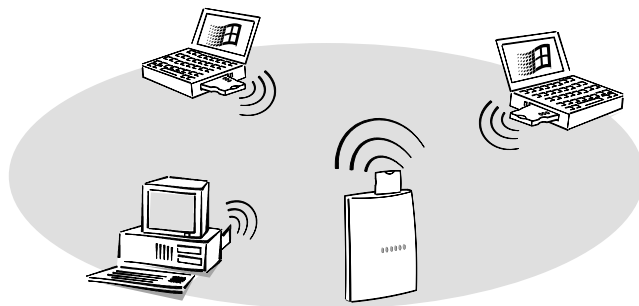
Wireless network adapters connect individual notebooks and PCs to a **Local Area Network (LAN)**. As the usual network cables have been replaced by a radio link in this case, we also refer to this as a **Wireless Local Area Network (WLAN)**.

*Access point*

The access point forms the bridge between the LAN and the WLAN. It has a slot for a wireless network adapter (*ELSA AirLancer MC-2*) as well as a normal Ethernet connection to exchange data between the two networks. In effect, the access point extends a network cable to the mobile stations via a radio link.

*Radio cell*

The maximum area in which wireless network adapters in mobile stations and the access point can reach each other and exchange data is known as a radio cell.

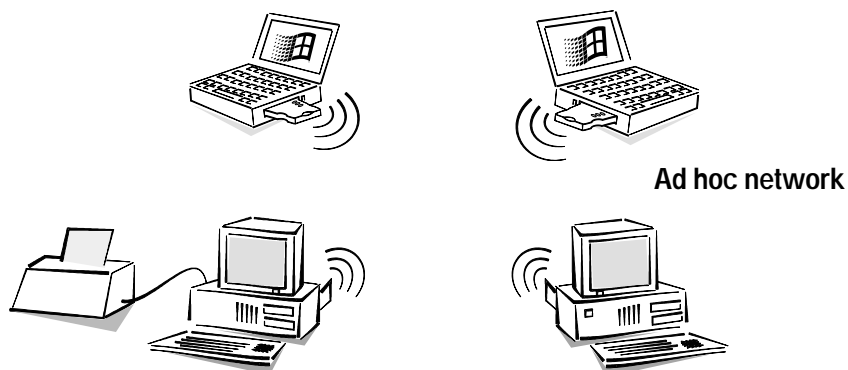


All of the standard functions of a wired network are also available in a wireless network: Access to files, servers, printers etc. is possible as is the integration of the mobile stations into an internal company e-mail system.

The following applications are available using ELSA wireless network adapters and access points:

*Direct PC connection*

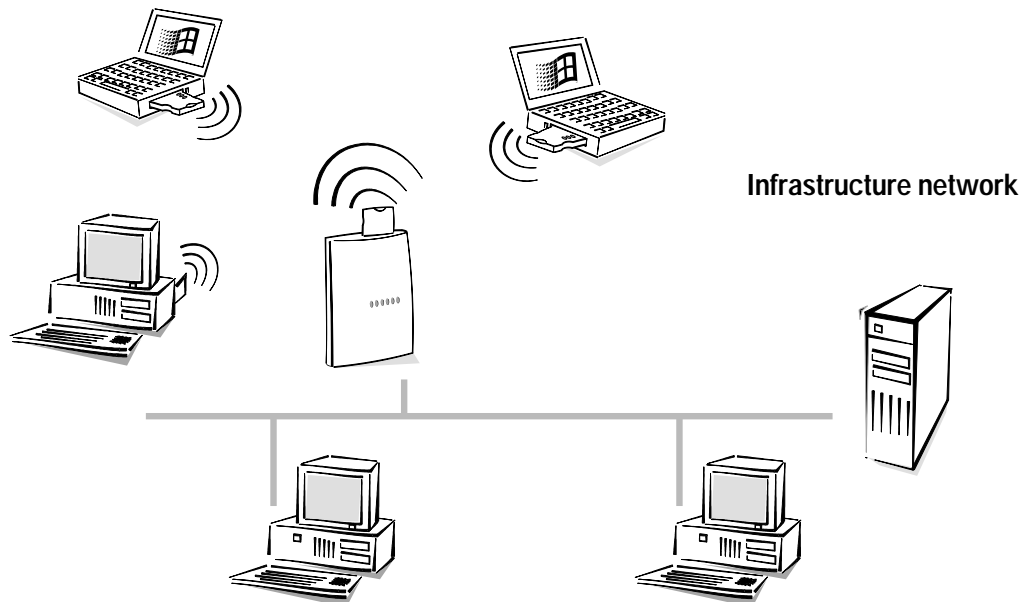
Use the wireless network cards to link two or more computers directly. All computers in a WLAN can then communicate with one another with no additional hardware.

*Peer-to-Peer*

This application is generally called a peer-to-peer network. In the language of wireless networking, it is known as an ad hoc network.

*Connection to wired LAN*

All computers with wireless network cards are able to access a wired network via an access point. The access point acts as the connection between the LAN and the WLAN and it also forms the switching center for data traffic within the WLANs.

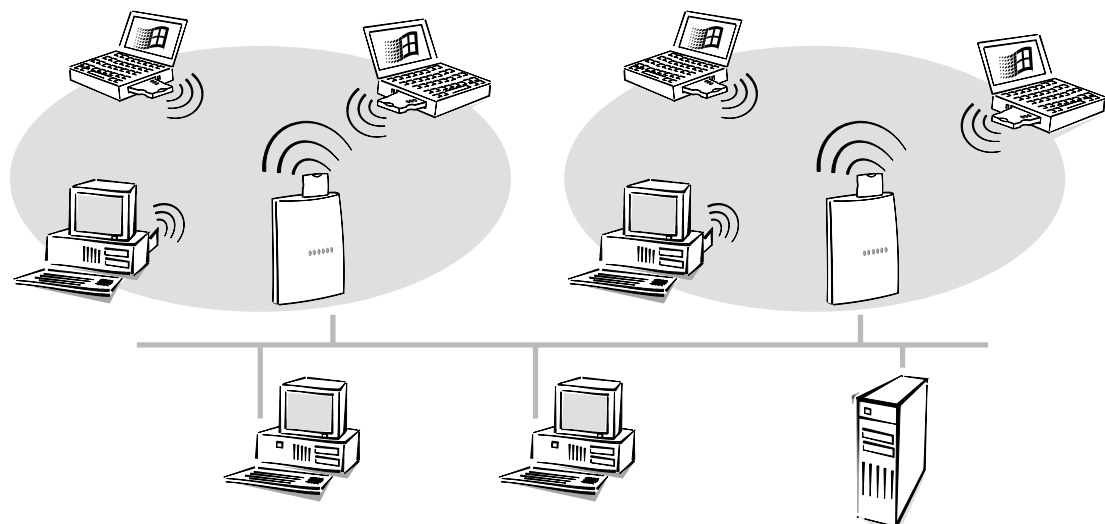
*Peer-to-LAN*

A wireless network with an access point is generally called a peer-to-LAN network. In the language of wireless networking, it is known as an infrastructure network.

This network type is ideally suited as an addition to existing LANs. The infrastructure network is the ideal solution for expansion of a LAN in areas where wiring is not possible or not economical.

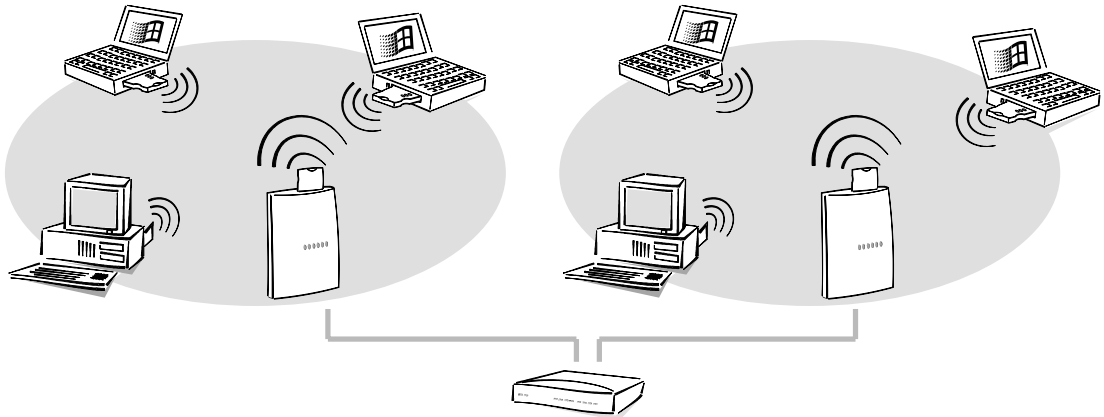
*Scaling*

Multiple access points can be used if the range of a cell is not sufficient to link all mobile stations. In this case, the wired LAN serves extend the range as required.



This principle can also be applied if you are setting up a new wireless network and a wired LAN is not available. If not all mobile stations are within the range of an access

point, add a second access point. The access points can then be connected using simple network cables and a hub, for example.



Radio cells can also overlap to ensure good coverage. Different channels (up to 14 channels are available) can be selected to prevent interference between the cells.

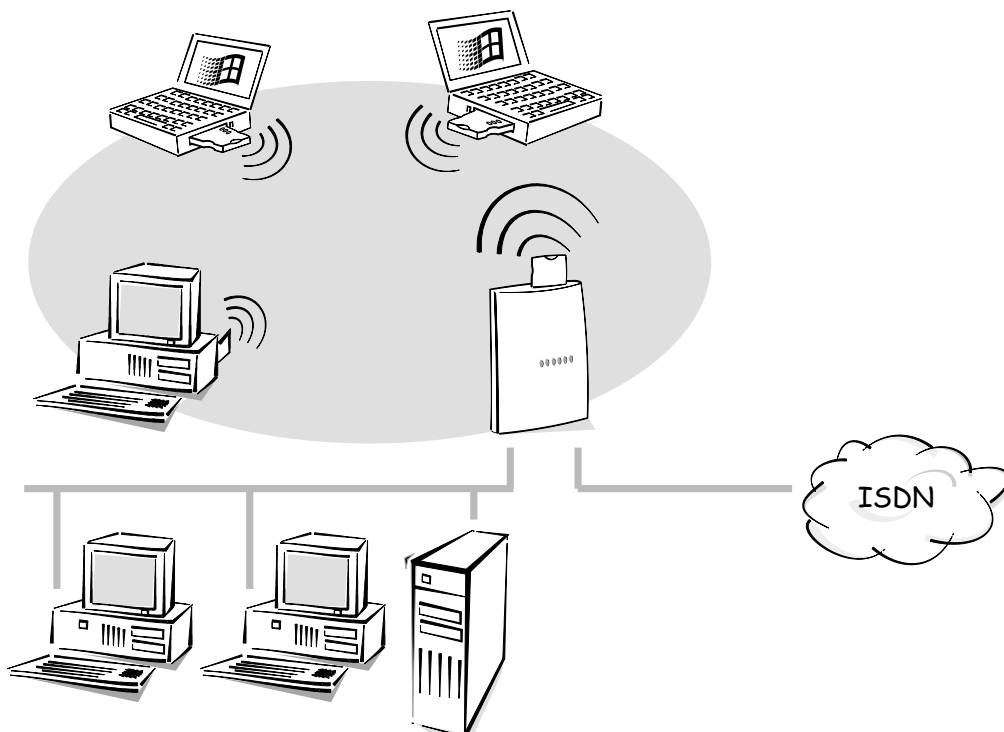
#### Roaming

Roaming is the transparent switching between neighbouring radio cells. The user can move from one cell to the other without losing the network connection. The access points constantly exchange information about the registered radio stations over the wired LAN.

For roaming to function properly, the access points involved must be connected by a common Ethernet network. Bridges, switches and repeaters between the access points are allowed, but routers are not!

#### ISDN connection

The *ELSA LANCOM Wireless IL-2* access point offers a special supplementary function. The access point connects both the wireless network and the ISDN network simultaneously to the wired network via the ISDN interface.



This enables additional applications such as access to the Internet for all computers in the LAN and WLAN together with all the functions of an IP router.

## What does the *ELSA LANCOM Wireless IL-2* offer?

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

### Easy installation

- Connect the *ELSA LANCOM* to the power supply.
- Establish a link to the LAN.
- Plug in the ISDN cable.
- Switch it on.
- Go!

### LAN connection

Access points for wireless networks by ELSA function in Ethernet environments. Use the 10Base-T connection and a hub or switch to connect the *ELSA LANCOM Wireless* to a 10-Mbit LAN.

### Wireless network connection

The wireless network adapters in ELSA access points comply with the IEEE standard 802.11. This standard is a supplement of the existing IEEE standards for LANs, of which IEEE 802.3 for Ethernet is the best known.

In principle, three physical processes can be used for wireless data communications:

- Infrared
- Radio, with frequency hopping
- Radio with the DSSS process (**D**irect **S**equences **S**pread **S**pectrum)

This process, which is also used for military applications to enhance the security of connections, scrambles the data prior to transmission and spreads it over a broad frequency band (spread spectrum). This ensures a reliable, highly secure connection.

ELSA wireless network adapters use the DSSS process. In addition to the advantage of immunity against interference from other transmitters that may be using the same frequency band, this also makes the adapters compatible to systems from other manufacturers.

IEEE 802.11 permits the operation of wireless local networks on private and public property in the ISM (**I**ndustrial, **S**cientific, **M**edical: 2,4 to 2,483 GHz) frequency band.

The maximum available bandwidth for data communications in a wireless network is 2 Mbps. A range of up to 300 meters is available outdoors, or approx. 30 meters in closed buildings (typical range).

## WAN connection

The *ELSA LANCOM Wireless* is connected to the  $S_0$  interface(s) of an ISDN Basic Rate Interface in point-to-multipoint configuration (multi-device terminal) or in point-to-point configuration (system terminal). The router automatically detects your connection type and the D-channel protocol being used. Dial-up connections using DSS1 or 1TR6 can also be used, as can leased-line connections. Leased-line connections are an optional feature that can be requested from ELSA.

## Channel bundling and Compression

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

## Transparent bridging

Data packets from the wired LAN are transmitted to the wireless network and vice versa. Optionally, data traffic can be restricted to certain protocols and stations.

## Status displays

LED indicators on the front of your access point allow you to monitor the ISDN and Ethernet connections and the current line connections, thus simplifying the process of diagnosing any systems failures.

## ELSA LANmonitor

In Windows operating systems this tool always shows the router status information on the monitor. The most important information for every device in the local network is displayed, such as:

- Connection status for each B channel
- Name of the remote site
- The connected unit module (router, *LANCAP*)
- Connection duration and transmission rates
- Excerpts of the device statistics (e.g. PPP negotiation data)

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

## Charge monitoring

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

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

### **Least-cost routing**

Even if there is a large selection of telecommunications service providers you can always use the cheapest lines using the least-cost router. You define once which providers have the most favorable charges for your purposes, and the router automatically selects the most economical provider for you at every connection.

### **Automatic time check**

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

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

Setting up and configuring the devices 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.

The device can be accessed from the WAN (via ISDN), from the WLAN or the LAN. TFTP is supported along with SNMP if configuring from the LAN or WLAN.

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

### **Intruder protection**

Along with password protection and call number recognition (CLIP), the router offers protection against unauthorized access to the company network by means of a callback function which only permits a connection to be established to previously defined telephone connections only. Firewall filters and IP masquerading round out the security concept. Furthermore, login barring prevents any "bruteforce attacks" and denies access to the router after a configurable number of login attempts using an incorrect password.

### **Compatibility through PPP**

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

### **Remote configuration using PPP**

One special configuration feature of the ELSA routers which cannot and should not be setup locally is its ability to be configured remotely via the Windows Dial-Up Network. All you have to do is to plug the new device into the power supply and connect it to the



ISDN Basic Rate Interface. Now you can access the router using a PPP connection and configure it from your location. The first time the device is configured, access to it is secured by a password and thereafter it remains inaccessible to unauthorized callers.

### Software update

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

The current version is always available to you on our online media and can be loaded via the LAN, the WLAN or the WAN (ISDN).

### 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.

### ELSA LANCAPi and ELSA CAPI Faxmodem

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

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

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

The *ELSA CAPI Faxmodem* furthermore provides a Windows fax driver (Fax Class 1) as an interface between the *ELSA LANCAPi* and applications, permitting the use of standard fax programs with an *ELSA LANCOM Wireless*.

### DHCP

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

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

**NetBIOS proxy**

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

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

**DNS server**

The DNS server functionality of the router enables you to set up links between IP addresses and names of computers or networks. The correct route can be directly assigned in the event of queries for known computer names.

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

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

# Installation

This chapter is intended to help you set up your new wireless network as quickly as possible. First we will describe the contents of the package and introduce the device itself. After that we will explain how to connect the unit and put it to use.

## Package contents

Please ensure that the delivery is complete before beginning with the installation. The package should include the following components:

- Access point *ELSA LANCOM Wireless IL-2*
- Power supply unit
- *ELSA AirLancer MC-2* wireless network adapter
- LAN connector cable
- ISDN connector cable
- Documentation
- CD containing *ELSA LANconfig* and other software and electronic documentation

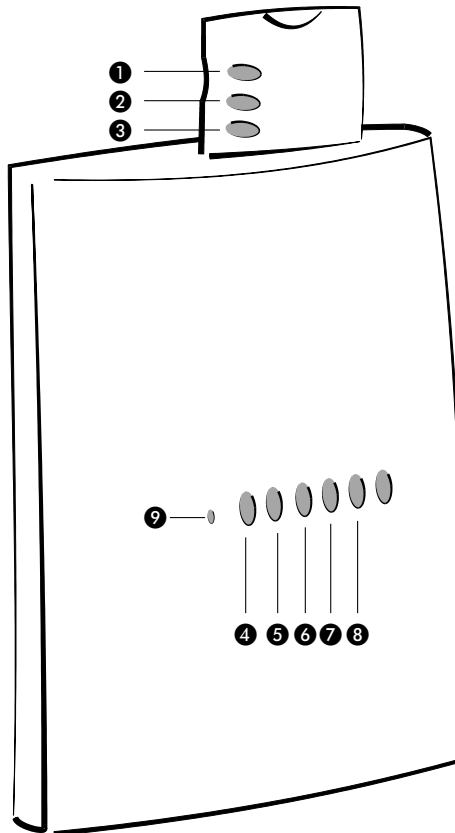
If anything should be missing, please contact your dealer.

## Introducing the *ELSA LANCOM Wireless*

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

*LEDs*

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



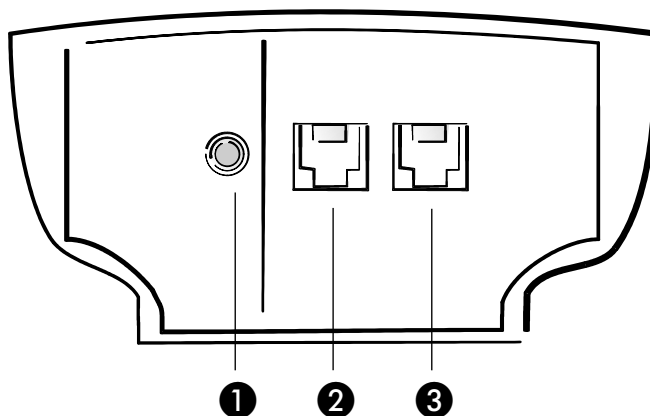
- ❶ The red LED of the wireless network adapter indicates that a connection has been established between the card and access point.
- ❷ The yellow LED of the wireless network adapter indicates the number of mobile stations logged onto the access point. For example, when three stations are logged on, the LED flashes three times in quick succession before pausing briefly.
- ❸ The green LED of the wireless network adapter indicates activity on the wireless network, in other words the sending and receiving that data is being sent and received. If this LED does not light up at all or remains lit permanently, this indicates a fault in the wireless network adapter.
- ❹ The 'Power/Msg' LED on the access point lights up briefly when the power is switched on. After the self-test, either an error is output by a flashing light code or the device starts and the LED remains lit.

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

- ❺ The 'S<sub>0</sub> Status' LED on the access point shows the activity on the D channel.

- ⑥ The 'WAN Channel-1' LED on the access point shows the activity on the first B channel on the ISDN port.
- ⑦ The 'WAN Channel-2' LED on the access point shows the activity on the second B channel on the ISDN port.
- ⑧ The Reset button is recessed in the case and can only be reached with a pointed object such as a paper clip. Press the Reset button until all of the LEDs light up to reset the unit to its factory defaults.

Now turn the whole thing around and take a look at the bottom. There you'll find:



- ① Connection for power supply unit
- ② 10Base-T network connection
- ③ ISDN S<sub>0</sub> port

## Connecting the access point

- ① Connect the *ELSA LANCOM Wireless L-2* access point to the LAN. Insert the included network cable into the 10Base-10 MBitconnection of the access point and into a free network connection socket of your local network such as on the hub of your LAN.
- ② Connect the router to an ISDN-S<sub>0</sub> multifunction port or system port (point-to-multipoint or point-to-point configuration). To take advantage of the charge protection and charge statistics, request the 'charge transfer **during** the connection' ISDN feature (under AOCD) from your telephone company.
- ③ Insert the *ELSA AirLancer MC-2* wireless network adapter in the access point. The LEDs of the PC card must face toward the front of the access point.
- ④ Connect the AC adapter to the access point. The 'Power/Msg' LED on the front panel of the unit lights up after a short self-test. The red LED of the wireless network adapter indicates that a connection has been established between the card

and access point. The flickering of the green LED on the wireless network adapter indicates that it is searching for other stations in the WLAN. The 'LAN Status' LED signals the correct connection between the access point and the LAN.

## Software installation

The access point can be quickly and easily set up for the required application using the *ELSA LANconfig* configuration software for Windows operating systems.

*The default parameters for the wireless network have been set up in such a way that you can generally get started right away. Modifications to the configuration are only required for special applications.*

A PC in either the wired LAN or the WLAN is required to run the configuration software.

- ① Install the TCP/IP network protocol on the computer that you would like to use to set up the access point.
- ② Next, install the *ELSA LANconfig* configuration software. If the setup program does not start up automatically after insertion of the *ELSA LANCOM Wireless* CD, start Windows Explorer, click on 'autorun.exe' on the *ELSA LANCOM Wireless* CD and follow the instructions in the install program.

## Basic configuration

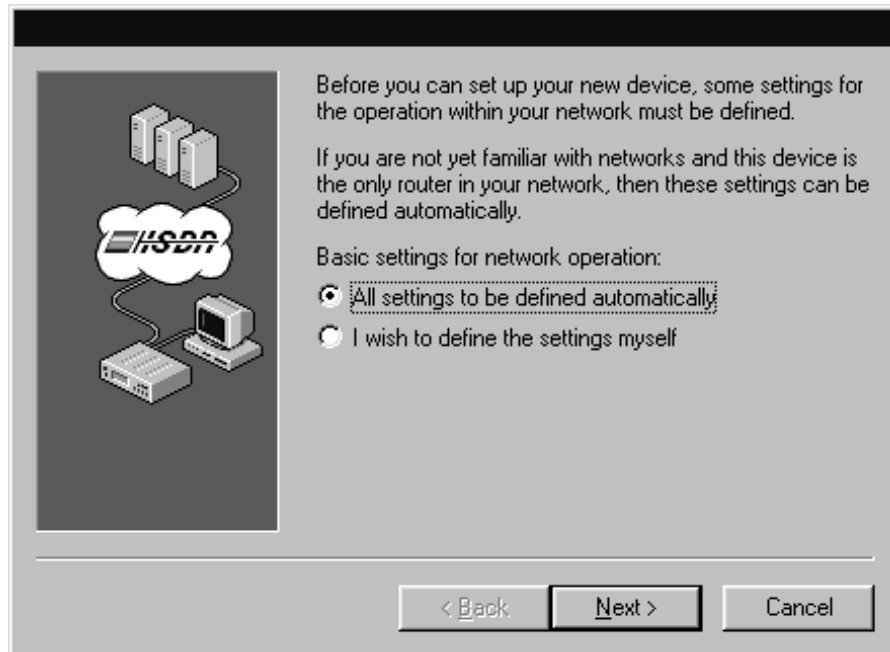
The IP address for the access point is set during the basic configuration. A decision also needs to be made whether or not to use the integrated DHCP server. The basic configuration can be performed using *ELSA LANconfig* or via Telnet.

### Make basic settings with *ELSA LANconfig*

The first time *ELSA LANconfig* is run, the new access point is automatically detected on the TCP/IP network and can immediately be configured. A wizard starts automatically to help you with the basic configuration of the unit; it can also perform the complete basic configuration for you.



- 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 is applicable:
- You have not yet used IP addresses in your network but would like to do so starting now. You are not concerned about the specific IP addresses that will be used. The access point will then act as a DHCP server and automatically assign the IP addresses for all devices in the network (LAN and WLAN).
- or
- You do not want to use IP addresses because you are using a pure Windows network, for example.



*If you are not sure whether your network already uses IP addresses, click on **Start ► Run**, enter `windowsipcfg` on the command line and click **OK**. Select your network adapter in the following window. If the 'IP Address' field contains the value '0.0.0.0', the network adapter does not have an IP address yet.*

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

- ③ Select the option 'I would like to make the settings myself' if you are familiar with networks and IP addresses, and one of the following conditions is applicable:
- You have not yet used IP addresses in your network but would like to do so starting now. You would like to assign the IP address of the access point yourself from the address space reserved for private use, e.g. '10.0.0.1' with the subnet mask '255.255.255.0'. You are thereby also defining the address space that the DHCP server, if active, will use for the other devices on the network.

- You have previously used IP addresses for the computers in your LAN. Assign a free address from the previously used address range to the access point and specify whether the access point should act as a DHCP server.



*Further information on the structure of networks in general and IP addressing can be found in the electronic documentation on the ELSA LANCOM Wireless CD. The functions of the DHCP server are described later in this manual.*

- ④ That was it—your access point is now ready for its basic task, providing mobile stations access to a wired LAN.

## Configuring the basic settings using Telnet

If you do not want to use *ELSA LANconfig*, or cannot use it because you are using a different operating system for example, you can set up the basic configuration using a Telnet connection.

Open a Telnet connection to the address '10.0.0.254' if you have not used IP addresses in your network to date, or the address 'x.x.x.254', in which 'x.x.x' stands for the address range previously used in the network.

Enter the following command:

- ① Start the Telnet connection by clicking **Start ► Run** and entering `Telnet 10.0.0.254` on the command line.

- ② To change the language for the configuration, enter:

```
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.
```



*You may have to reboot the router after changing the Intranet address.*

- ④ To switch off the DHCP function:

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



# Configuration modes

ELSA access points are always delivered with up-to-date software in which a number of the settings have already been prepared for you.

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.

## Radio or wired: Configuration approaches

Using an inband configuration (configuration via the network) allows any computer on the WLAN, LAN or WLAN (ISDN) to access the access point. However, access can be restricted or blocked altogether using the IP access list. This configuration requires the use of either Telnet (supplied with most operating systems) or 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 access point 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 a computer with the address XXX.XXX.XXX.254 is already active on your network, shut down the computer with this IP address before continuing. Give the access point a different, free IP address as soon as you have established a connection to it, using ELSA LANconfig or Telnet.*

### 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

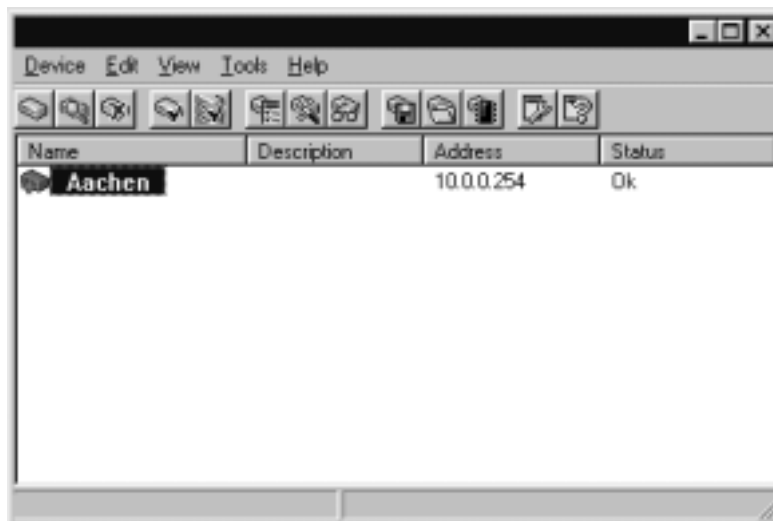
server you can have the IP addresses for all computers on the network assigned automatically (see also chapter 'Automatic Address Administration with DHCP').

## Beginning configuration using *ELSA LANconfig*

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

Just click on the **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 display options are available for the configuration of the devices using *ELSA LANconfig*:

- The 'simple display' mode only shows the settings required under normal circumstances.
- The 'complete display' mode shows all available configuration options. Some of these settings should only be modified by experienced users.

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

Double-clicking the entry for the highlighted device and then clicking the **Configure** button or the **Edit ► Edit Configuration File** option reads the device's current settings and displays the 'General' configuration selection.

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

## Start up configuration using Telnet

Start configuration using Telnet with the command from a DOS box:

```
telnet 10.1.80.125
```

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


After the entry of the password (if you specified one to protect the settings) all commands from the 'Configuration Commands' section are available.

## 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 device.

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 during the configuration 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
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 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  .	

This command...	... means this...	... for instance:
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 <Sprache>	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 device 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 the device.
- '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, it automatically loads the previous firmware version and reboots the device 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)
- 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 router will add the missing values using the default settings.

### *ELSA LANconfig*



When using 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**.

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

The device is booted up following a successful firmware upload and this activates the new firmware switch directly. If an error occurs during the upload (write error in the flash ROM, TFTP transmission error or similar) the device also boots and FirmSafe activates the previous firmware. The configuration remains in operation.

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

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

## Configuration using SNMP

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

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

# Operating modes and functions

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

- Wireless connections
- Security for your configuration
- Security for your LAN
- Charge management
- ISDN connections
- PPP support
- IP routing
- Automatic address administration with DHCP
- DNS server
- NetBIOS proxy
- *ELSA LANCAPI*
- Time check
- Least-cost router

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.

## Parameters for the wireless connection

The same values must be set for a variety of parameters to ensure that the wireless network adapters in the mobile stations and access points can identify each other and exchange data with one another.

All wireless network adapters (in base and mobile stations) that use the same parameters make up a wireless network. The selection of these parameters can be used specifically to set up separate wireless networks that do not interfere with one another.

The parameters for the wireless network adapters in the access points are configured via *ELSA LANconfig* or Telnet.

- ① Start up *ELSA LANconfig* by clicking **Start ► Programs ► ELSAlan ► ELSA LANconfig**. The *ELSA LANconfig* now automatically searches for all access points in the LAN and WLAN.

- ② In the list of found devices, click on the access point that you would like to configure. In the 'Management' configuration group select the 'Interfaces' tab.

The screenshot shows a configuration window titled 'Configure: Management'. It has three tabs: 'General', 'Interfaces', and 'Security'. The 'Interfaces' tab is active. It contains two sections: 'Network adapter' and 'Wireless LAN'. The 'Network adapter' section shows 'Physical address: 0090D1002004'. The 'Wireless LAN' section has three fields: 'WLAN domain' (empty), 'Channel' (set to 11), and 'Packet size' (set to 1.550 byte).

- ③ Set the new value for the WLAN domain. The WLAN domain must be identical for all participants in a wireless network.



*Change this value from its default setting 'ELSA' as quickly as possible, as the WLAN domain name works like a password to protect your wireless network against intruders!*

- ④ Set all participants in the wireless network to the same radio channel. The choice of the radio channel determines the frequency band that will be used by the wireless network adapters to exchange data.

Selecting different channels permits the parallel operation of multiple WLANs. Theoretically, 14 different channels are available, but only 3 completely distinct channels are available in the ISM frequency band due to the frequency overlap in the DSSS process. In the event that several cells are to be operated in close vicinity to one another, please select channels as widely spaced as possible, e.g. Channel 1, 7 and 14 or 3 and 13.



*Please observe the table of permissible channels for specific countries in the Appendix.*

- ⑤ Use the Packet Size setting to determine the length of the data packets to be transmitted across the WLAN. Valid sizes range from 600 to 1,600 bytes. Larger packets must be fragmented by the sender and assembled again by the recipient.

Smaller packets can result in better throughput in areas susceptible to interference, however this worsens the ratio of useful data to administrative information.

- ⑥ Activate the 'roaming' function when you need to combine multiple radio cells with one common Ethernet chain for the "seamless" transition between the radio cells. The settings for the WLAN domain and the radio channels should be identical in all of the access points that are to be involved with roaming.
- ⑦ Switch over to the 'WLAN Bridge' configuration section to





- prevent data transfer between specific mobile stations and the wired LAN or
- block the exchange of data packets with specific protocols.

If the 'WLAN Bridge' configuration section is not visible, switch to the complete display of the configuration options in *ELSA LANconfig* with **View ► Options**.

## 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 Wireless* 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 device's configuration.

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/password-required` menu. In this case, the password itself is set with the command `passwd`.

### Login barring

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

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

These parameters apply globally to all configuration options (Telnet, TFTP/*ELSA LANconfig* and SNMP). If barring is activated on one port all other ports are automatically barred too.

The following entries are provided in the configuration tool *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 computer. The *ELSA LANCOM Wireless* offers you various ways of restricting access from outside:

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

## Security check

Which "Identifier" should be used to detect the caller is set in the 'Communications' configuration area on the 'Call Answer' tab or in the `/Setup/WAN Module/Protection` menu. You have a choice of the following:

- None: Calls are accepted from any remote station.
- Name: Only calls from those remote stations entered in the name list are accepted.

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

### Verification of name

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

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

device name is accepted and verified as the name of the remote station. The PPP list can be found in the *ELSA LANconfig* in the 'Communication' configuration section on the 'Protocols' tab, or in the `/Setup/WAN-module/PPP List` menu.

No password? The PPP does indeed offer this special option: It is possible to request a form of protection available specifically to this protocol, that is to say PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol). This is a form of protection which your device demands from the remote station.



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

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

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

### Checking the number

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

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

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

### Callback

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

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

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

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

the router, if the caller is not identified by means of CLI. On the other hand, the caller incurs no costs if identification of the caller's number is possible and is accepted.

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

## 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.

## 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 to the Internet, for example. 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 210 minutes per week.



*If budget limit is reached, all open router connections that the router itself has established will be automatically terminated. The budgets will not be reset to permit the establishment of connections until the current period has elapsed. Needless to say, the administrator can reset the budgets at any time if required!*

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

## 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.*

## ISDN connections

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

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

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

### 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.

- Dialup-remote

This number should be dialed when the router actively establishes a connection to the remote station.

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

If the remote station is available via a leased line, the number for a dial-up backup connection can be entered here.

- **Timeouts**

These times indicate the length of time the B channels should remain active after

  - the last data has been exchanged across static connections for the holding time B1.
  - the data throughput has dropped below a specified level for the holding time B2 in dynamic connections.
- **WAN-layer**

The layer stands for a collection of protocols to be used for this connection. The layer must be set up identically on both sides of the connection.
- **Callback**

If the router receives a call from this specific remote station, it may be set to refuse the connection. Instead, the remote station is called back using the following options:

  - Normal callback
  - Callback using the fast ELSA process
  - Callback after name verification
  - Await the callback from the remote station using the fast ELSA process

## Interface settings

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

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

- **The D channel protocol used on the  $S_0$  port**

Automatic recognition, DSS1 (Euro-ISDN), DSS1 point-to-point, 1TR6, Group 0 leased-line connections
- **Leased line option**

B channel to be used for the leased line
- **Dialing prefix**

Number to precede outgoing calls, e.g. the prefix for external calls when using a PBX.

## Router interface settings

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

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

- Subscriber numbers (MSN/terminal device selection numbers)  
The router responds to incoming calls for these numbers. Multiple numbers are separated by semicolons. If no number is specified, the router will respond to all incoming calls.  
  
The first number specified will be transmitted to the remote station during the active establishment of a connection. If no number is specified, the main MSN of the connection will be transmitted.
- Option for Y connections  
Enable this option if it should be possible for both B channels of the connection to establish parallel connections to different remote stations.
- Suppression of own subscriber number  
Enable this option in order to suppress the display of your own subscriber number to the remote station during call establishment.

*This function must be supported by the network operator.*

## LANCAPI interface settings

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

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

- Subscriber numbers (MSN/terminal device selection numbers)  
The *LANCAPI* responds to incoming calls for these numbers. Multiple numbers are separated by semicolons. If no number is specified, the router will respond to all incoming calls.
- Access to *LANCAPI*  
Here you can completely disable the *LANCAPI* functions for the interface, or enable it only for incoming or outgoing calls.
- Transfer of own subscriber number



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

## Layer list

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

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

- WAN-layer  
The protocol settings will be saved under this name. In the name list, select the settings with the layer name for the appropriate connection.
- Encapsulation  
Specify here whether an Ethernet header should be added to the data packets. Normally the setting 'Transparent' will be sufficient; this setting may only be required for HDLC connections to third-party devices.
- Layer-3  
Layer-3 protocol for the connection. Recognized automatically in the case of some incoming connections.  
An additional entry is required in the PPP list when using PPP.  
An additional entry is required in the scripts list when using scripts.
- Layer-2  
Layer-2 protocol for the connection.
- Options  
Enables data compression and channel bundling. This option is only effective when supported by the protocols of Layer 2 and Layer 3.
- Layer-1  
Layer-1 protocol for the connection. Recognized automatically in the case of some incoming connections.



## Round-robin list

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

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

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

## 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.

## Script

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

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

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

- Remote site

Name of the remote station as specified before in the name list.

- Script

Enter the script here as described in the reference section of the documentation.

## Call acceptance

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

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

- All

Every call is accepted.

- Name

Every call is accepted at first. During the protocol negotiation the name is determined and checked against the name list. The connection is maintained if the name is present, otherwise it will be rejected.

- Number

The call will only be accepted if the remote station is entered in the number list and the number is transferred to the remote station.

- Name or number

The call will be accepted if one of the two checks was successful.

## Number-list

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

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

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

## Point-to-point protocol

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

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

### The protocol

#### What is PPP?

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

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

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

#### What is PPP used for?

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

- for reasons of compatibility, e.g. when communicating with external routers
- Internet access (when sending addresses)

## The phases of PPP negotiation

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

- Establish phase

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

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

- Authenticate phase

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

- Network-phase

If the negotiation of the parameters is successful, IP packets may be sent over the open (logical) line by the router modules.

- Terminate phase

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

## PPP negotiation in the *ELSA LANCOM*

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

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

```
trace + ppp
```

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

## The PPP list

You can specify a custom definition of the PPP negotiation for each of the remote stations that contact your net. The PPP list can be found in the *ELSA LANconfig* in the 'Communication' configuration section on the 'Protocols' tab, or in the `/Setup/WAN-module/PPP List` menu.

The PPP may have up to 64 entries, containing the following values:

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

## Everything OK? Checking the line with LCP

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

The reliability of the line can be constantly monitored using the LCP once the connection has been established. This is achieved within the protocol by the LCP echo request and the associated LCP echo reply. The LCP echo request is a query in the form of a data packet which is transferred to the remote station along with the data. The connection is

reliable and stable if a valid response to this request for information is returned (LCP echo reply). This request is repeated at defined intervals so that the connection can be continually monitored.

What happens when there is no reply? First a few retries will be initiated to exclude the possibility of any short-term line interference. The line will be dropped and an alternative route sought if all the retries remain unanswered.

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

## IP-Routing

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

### The IP routing table

Use the IP routing table to tell the router which remote station (which other router or computer) it should send the data for particular IP addresses or IP address ranges to. This type of entry is also known as a "route" since it is used to describe the path of the data packet. This procedure is also called "static routing" since you make these entries yourself and they remain unchanged until you either change or delete them yourself. Naturally, there is also "dynamic routing" too. The routers use the routes in this way to exchange data between themselves and continually update it automatically. The static routing table can hold up to 64 entries, the dynamic table can hold 128. The IP router looks at both tables when the IP RIP is activated.

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 address and IP network mask

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

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

#### ■ Router 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	Netmask	Router	Dist.	This is what happens:
192.168.130.0	255.255.255.0	192.168.140.123	0	All data packets with the destination IP addresses 192.168.130.x are sent to the locally available router with the IP address 192.168.140.123.
192.168.0.0	255.255.0.0	0.0.0.0	0	Excludes transmission of all data packets to networks using private address spaces.
172.16.0.0	255.255.0.0	0.0.0.0	0	
10.0.0.0	255.0.0.0	0.0.0.0	0	
224.0.0.0	224.0.0.0	0.0.0.0	0	

## 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'). 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.

## Proxy-ARP

A special feature of the IP router is the proxy ARP. This proxy is used if the transmission of data to IP addresses takes place in the same logical network as the sender, but the destination address is still reached via a router. This is the case when individual workstation computers (teleworkers) are networked via TCP/IP to the company network. The teleworker then has an IP address which is located in the same local network as all the other computers in the LAN. A data packet from LAN to the teleworker would usually only search for a receiver locally, but would not be able to find one.



*To take advantage of this function, enable the 'Proxy ARP active' option (in LANconfig in the 'TCP/IP' configuration section on the 'Routing' tab or in the /Setup/IP-router-module menu for other configuration modes).*

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

IP address	Netmask	Router	Distance	Masquerade
192.168.110.123	255.255.255.255	Teleworker01	0	off

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

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

## 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). In this way you instruct the router itself in your device to send the data packet to other routers. In addition, in this case no more ICMP redirects will be sent.

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

## Dynamic routing with IP RIP

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

### What information is propagated by IP RIP?

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

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

### 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 interaction of static and dynamic tables

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

### IP-masquerading (NAT, PAT)

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

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

## Two addresses for the router

- 'Off': No masquerading.

## 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 new 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').*

## 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 the *ELSA LANconfig* in the 'TCP/IP' configuration area on the 'Masq.' tab or in the menu `Setup/IP Router Module/Masquerading/Service Table`). The packet is forwarded to this computer. All packets that come from the FTP server in the LAN (answers from the server) are hidden behind the IP address of the router.

The only small difference is that:

- 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: "Which IP address belongs to www.domain.com?"

- Initially the router checks whether a DNS server has been entered in its own settings (in the configuration tool *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Addresses' tab or in the `/Setup/TCP-IP-module` menu). If it is successful there, it obtains the desired information from this server.
- If no DNS server is entered in the *ELSA LANCOM Wireless*, the router will attempt to reach a DNS server over a PPP connection (e.g. from the Internet provider) to get the IP address assigned to the name from there. This can only succeed if the address of a DNS server is sent to the *ELSA LANCOM Wireless* during PPP negotiation.

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. Your local network always receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

## 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'.*

## Automatic address administration with DHCP

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

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

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

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

## The DHCP server

As a DHCP server, the *ELSA LANCOM Wireless* can manage 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
- Default gateway
- Period of validity for the parameters assigned

The DHCP server takes the IP addresses either from a freely defined address pool or determines the addresses automatically from its own IP address (or intranet address).

In DHCP mode, a completely unconfigured device can even automatically assign IP addresses to itself and the computers in the network.

In the simplest case, all that is required is to connect the new device to a network without other DHCP servers and switch it on. The router then interacts with the *ELSA LANconfig* using a wizard and handles all of the address assignments in the local network itself.

## DHCP – 'on', 'off' or 'auto'?

The DHCP server can be set to three different states:

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

- 'off': The DHCP server is permanently disabled.
  - 'auto': The server is in automode. In this mode, after switching it on, the device looks for other DHCP server within the local network.
    - 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 booted and requests an IP address via DHCP with its network settings, a device with an activated DHCP module will assign this computer an address. A valid address is taken from the pool as an IP address. If the computer was already assigned an IP address at some point in the past, it requests this same address and the DHCP server attempts to reassign it this address if it has not already been assigned to another computer.

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

### 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.*

### DNS and NBNS assignment

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

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

### Default gateway assignment

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

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

### Period of validity for an assignment

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

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

- Maximum lease time in minutes

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

If a host requests a validity in excess of 6,000 minutes, this will nevertheless be the maximum available validity!

The default setting is 6,000 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 a workstation – Overwriting an assignment

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

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

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

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

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

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

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



## Configuring the DHCP server

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

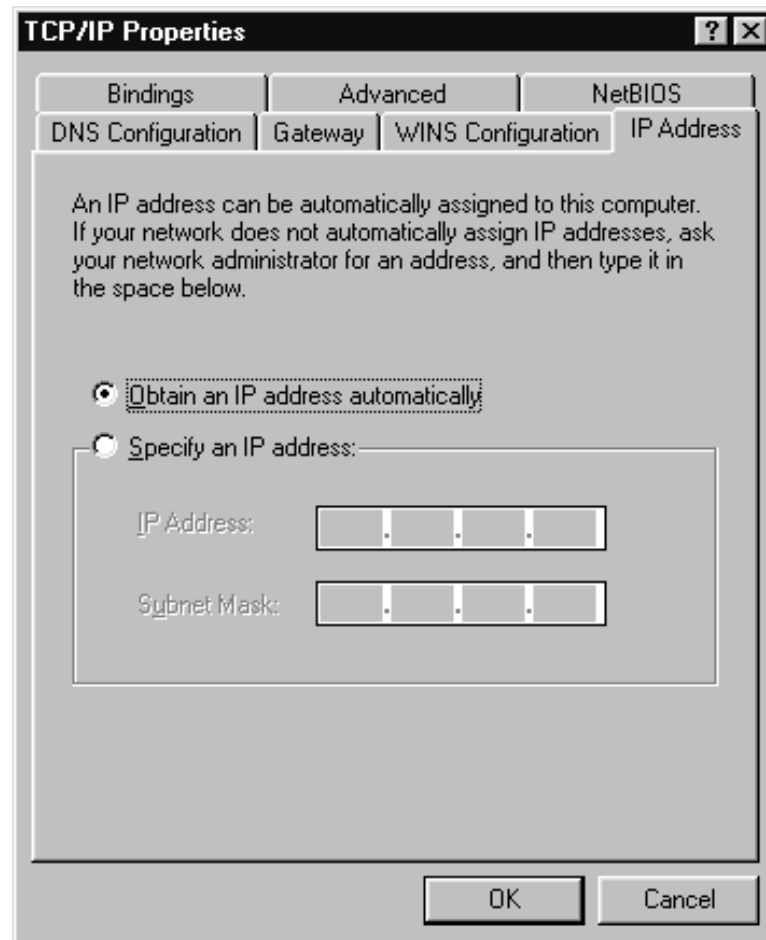
- You have not yet configured a network or your existing local network does not use TCP/IP. The DHCP server in your new ELSA lets you assign IP addresses to all of the computers in the network and to the router in a single operation.
- You are already using TCP/IP but without a DHCP server, and you would now like to convert to DHCP operation.

### Configuration using *ELSA LANconfig* and the wizards

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

- ① Connect the unconfigured device to your local network using a network cable.
- ② Switch the device on. It will not find any other DHCP servers in the network and will thus enable its own DHCP functions.
- ③ If you have not done so already, install the TCP/IP protocol on all computers in the LAN.
  - Usually when the protocol is installed, the default configuration is such that the computers are automatically ready to obtain the IP address from a DHCP server. After rebooting at the end of the protocol installation, the computers automatically request an IP address from the DHCP server.
  - If the protocol is already installed, enable the DHCP function on all of the computers in the local network. Under Windows 95, for example, this is done by selecting **Start ► Settings ► Control Panel ► Network** to open the window for configuring network properties. Double-click the entry for the 'TCP/IP' protocol.  
Enable the 'Obtain an IP address automatically' option. Switch over to the 'DNS Configuration' tab and delete all of the existing DNS addresses. Next, delete any entries under the 'Gateway' tab and click **OK** to close all the windows. This

change will require a reboot, after which the computer will automatically request an IP address from the DHCP server's address pool.



- ④ Install the configuration tool *ELSA LANconfig* on a computer in the network.
- ⑤ Start the program from the 'ELSAIlan' program group. When loading, the *ELSA LANconfig*, will detect an unconfigured router in the network and will launch the wizard for the basic settings.
  - If you have not previously used any IP addresses in your network, select the option 'Make all settings automatically' in this wizard and confirm your selection with **Finish** in the next window.  
The wizard assigns the IP address '10.0.0.1' with the netmask '255.255.255.0' to the router and enables the DHCP server. On the basis of this IP address, the device then determines the valid address pool for the DHCP assignment.
  - In the event that IP addresses were already in use in your network before converting to DHCP operation, select the option 'I would like to adjust the settings manually' in the wizard. In the next window, enter an unused IP address from the previously-used address range and activate the DHCP server.  
The wizard now assigns the selected IP address and associated netmask to the device. On the basis of this IP address, the device then determines the valid address pool for the DHCP assignment.

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

### Manual configuration

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

## DNS

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

### What does a DNS server do?

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

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

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

- The DNS server in the *ELSA LANCOM Wireless* can also be used as an extremely convenient filter mechanism. Requests for domains can be prohibited throughout the LAN, for subnetworks, or even for individual computers – simply by specifying the domain name.

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

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

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

## Setting up the DNS server

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

- ① Switch the DNS server on.

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

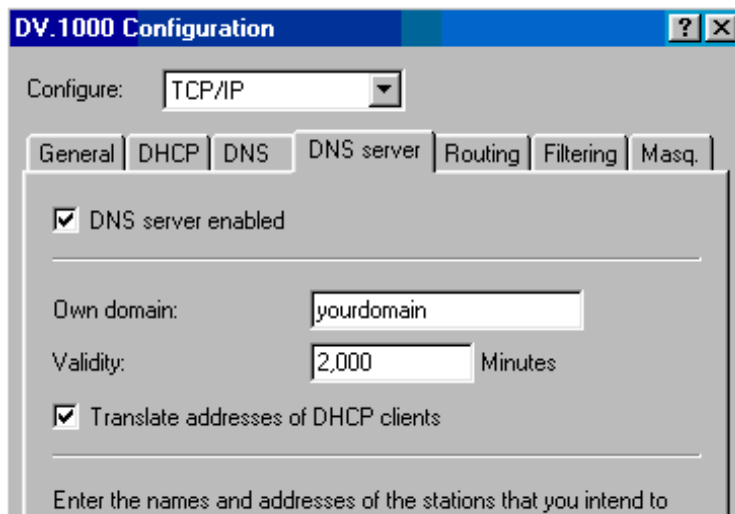
- ② Enter the domain in which the DNS server is located. The DNS server uses this domain to determine whether the requested name is located in the LAN. Entering the domain is optional.

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

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

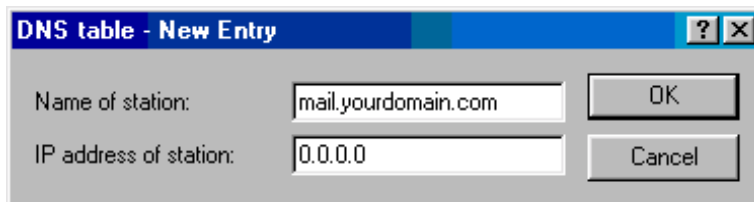
```
set setup/dns-module/dhcp-usage yes
```

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



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

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

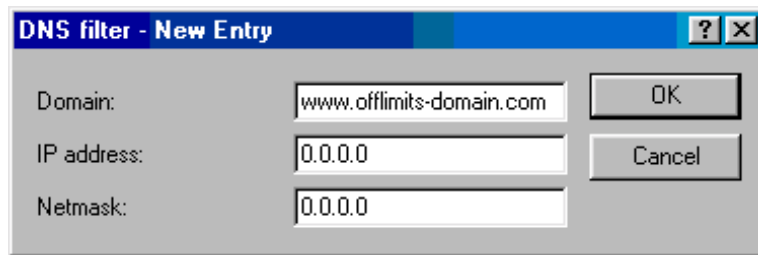


```
cd setup/dns-module/dns-table
set mail.yourdomain.com 10.0.0.99
```

Stating the domain is optional but recommended.

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

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



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

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

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

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



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

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

## NetBIOS proxy

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

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

### To the point: What is NetBIOS?

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

In a Microsoft Network, the computers are only addressed via their names. Multiple computers can be organized into groups, and multiple groups can be grouped further as scopes. The names used must be known throughout the network for all computers to be able to access the resources of the others. NetBIOS computers issue their names into the network at regular intervals to eliminate the necessity of maintaining tables of known names on each computer.

The names publicized in this manner should, of course, be collected and made available at a central location in the Microsoft Network. If two Microsoft Networks are to be connected using a router, then such a name collection point, a so-called NetBIOS nameserver (NBNS), must be present on both sides.

- A WINS server (Windows Internet Name Service server) can be installed in the network for this purpose.
- However, a second option is also available, since many Microsoft Networks can or must make do without a server of their own: Information about the names in use can be placed on a "billboard" of sorts, on which all participating computers only post their names and IP addresses. In this case, the individual computers are responsible for the consistency of their names within the network.

The *ELSA LANCOM Wireless* offers such a billboard. The interconnection of Microsoft Networks is thus possible without a server as a result of this simple realization of the NBNS. The computers in the networks to be interconnected thus publicize their names and add them to the billboards in the respective remote networks.

## Handling of NetBIOS packets

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

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

- In the NetBIOS module, it is possible to specify the remote stations to which the name information should be transferred via NetBIOS to ensure the routing of those packets that are actually required. After the NetBIOS module has been switched on and an unspecified waiting time has elapsed, a connection is established to the NetBIOS remote stations (insofar as these are not individual Remote Access workstations). The duration of the waiting period will be increased if the connection cannot be established. The following exchange of NetBIOS information then fills the billboard for the first time.

- In its proxy function, the unit answers queries to computers already known in the NetBIOS module (on the billboard) by proxy for those computers. After the initial exchange of information, no new connections are established as a result of queries to workstations in the local network, or to known workstations in the remote network.

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

## Which preconditions must be fulfilled?

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

### Installed components

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

- Network protocol

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



*Unlike IPX and IP, NetBEUI is not routable and is thus only available in Microsoft Networks. If multiple Microsoft Networks are to be interconnected using routers, NetBIOS must be based on a routable protocol in the ELSA LANCOM Wireless, such as IP.*

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

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

- Client

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

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



- Service

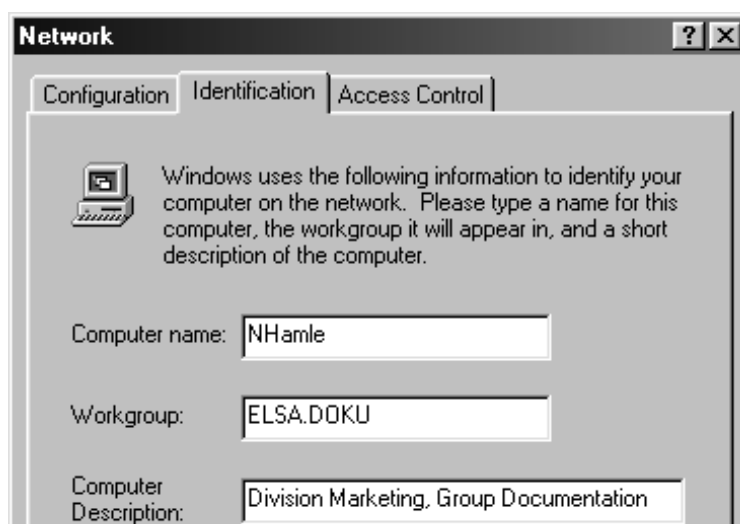
File and printer sharing permits drives and printers to be shared with other users in the Windows Network.

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

### Windows Network settings

- Name and group designation

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



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

- File and printer sharing

Ensure that file and printer sharing is enabled after the installation is complete. Click **Start ► Settings ► Control Panel ► Network ► File and printer sharing**. Specify whether other users in the Windows Network should be allowed access to the printer and/or files of this workstation.



All users intending to access shared resources must log on with their names and passwords when booting Windows.

In the Windows Explorer, right-click the drives, folders or printers that you would like to share with others on the network and select the item **Sharing** from the context menu.



Enter a name for the shared resource and a description if required. The manner in which the resource can be accessed can be selected under Access Type, and by entering passwords as required.



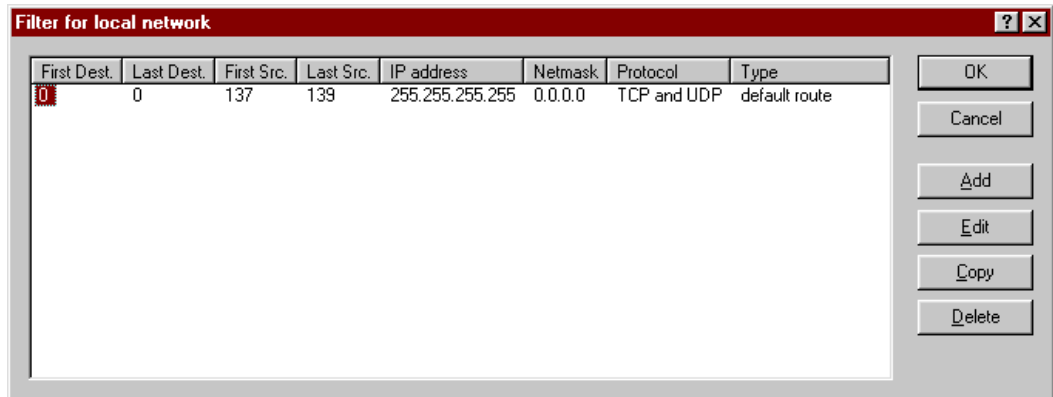
*It's easy to check whether the Windows Network settings have been made correctly: the local computer must appear with its name in the Network Neighborhood.*

## Linking two Windows Networks via ISDN

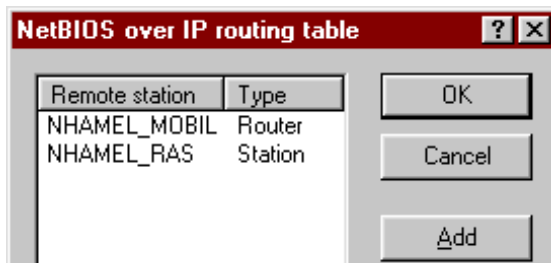
Two Windows Networks can be interconnected once these preparations have been completed. The settings for Workgroup Networks and Domain Networks (Windows NT) are similar. The following steps must be performed for both sides of the connection.

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

connection on the DEFAULT route. This has been preset in the unit's factory defaults.



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



Alternatively, enter the following when configuring via telnet:

```
cd /Setup/NetBIOS-module/Remote-table
set nhamel.mobil router
```

The entry in the 'Type' field specifies whether a connection to the remote station should be dialed up to exchange name information after switching on the NetBIOS module.



*The 'NT-domain' parameter can generally be left blank in the case of Windows 95 or 98 networks. The corresponding domain/workgroup must be entered manually when accessing Windows NT machines.*

- ④ If the NetBIOS link uses a PPP connection, check the PPP list for the activation of NetBIOS for the corresponding entry.
- ⑤ Once all remote stations have been entered, activate the NetBIOS function.

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

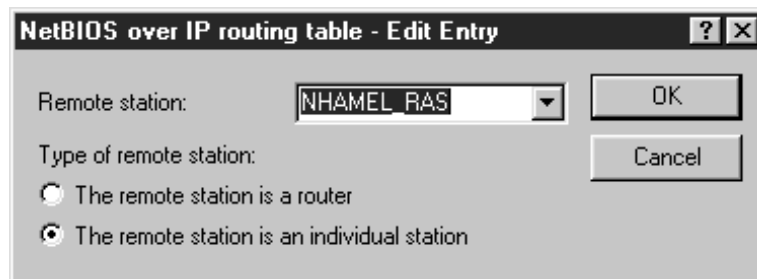
After switching the module on, a connection is established after an unspecified waiting time to all remote stations not identified as dial-up nodes. The required information regarding the other computers in the networks is then exchanged during

this initial connection. Computers on the remote side cannot be accessed until this operation is complete.

## Dial-up procedure for a remote access station

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

- ① The *ELSA LANCOM Wireless* and the remote access computer must be prepared for network access as described in the Workshop. In this case as well, check the IP filters in the *ELSA LANCOM Wireless* (See 'Connecting two Windows networks via ISDN').
- ② A route must also be entered in the IP routing table if the assignment of the IP address for the remote station is realized from the IP pool.
- ③ Also create an entry for the remote stations in the NetBIOS IP routing table.



```
cd /Setup/NetBIOS-module/Remote-table
set nhamel.ras workstation
```



*Be sure to identify this entry as an 'individual station' to ensure that this remote station is not automatically contacted when the NetBIOS module is switched on.*

- ④ If the NetBIOS link uses a PPP connection, check the PPP list for the activation of NetBIOS for the corresponding entry.

## Search and Find: the Network Neighborhood

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

### NetBIOS routing via LAN-LAN interconnections

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

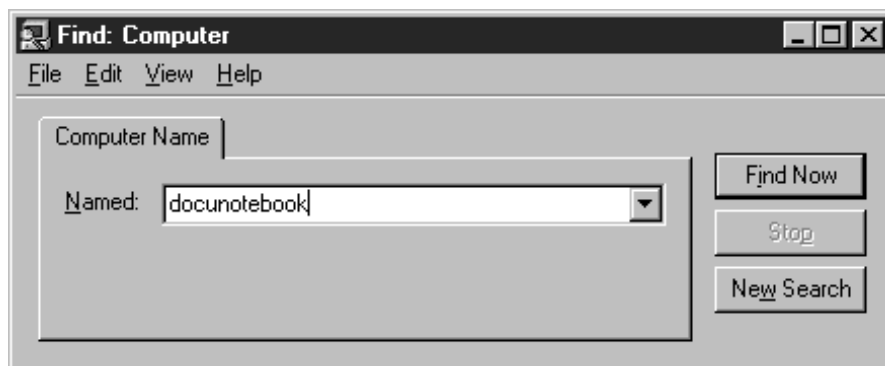
```
dir /Setup/NetBIOS-module/Host-list
```

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

Name	Type	IP address	Remote site	Timeout	Flags
DOKUNOTEBOOK	00	10.10.0.53	NHAMEL.MOBIL	4939	0020
DOKUNOTEBOOK	20	10.10.0.53	NHAMEL.MOBIL	4939	0020
ELSA	1d	10.10.0.53	NHAMEL.MOBIL	4939	0020
ELSA.DOKU	1d	10.1.253.246	4935	0000	
ELSA.DOKU	1d	192.168.100.162	4997	0000	
NHAMEL.MOBIL	00	10.10.0.1	NHAMEL.MOBIL	0	0020

This table shows, for example, that the computer named 'DOKUNOTEBOOK' with the IP address '10.10.0.53' is available via the remote station 'NHAMEL.MOBIL'. The further parameters are covered in the description of the menus.

To access the shared resources of this computer, simply use the Windows Explorer to search for it with **Start ► Find ► Computer**.



*The workgroups and computers of the remote network cannot be found in the 'Explore Entire Network' function of the Windows Network Neighborhood for technical reasons. Instead, search for remote computers and create associations as described above.*

## NetBIOS routing via RAS

The procedure for access to the Windows Network via RAS is somewhat different. These are the two fundamental differences to LAN-LAN interconnection:

- A host list with the computers in the Windows Network is not available on the dial-up node side. RAS users must know the names of the computers that they intend to access and for which they have access rights.
- The connection is not established automatically. RAS users must first establish a connection to the *ELSA LANCOM Wireless* via Dial-Up Networking.

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

## Office communications and *ELSA LANCAPI*

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

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

### *ELSA LANCAPI*

#### **What are the advantages of *LANCAPI*?**

Above all, the use of *LANCAPI* offers you economic advantages. *LANCAPI* provides all workstations integrated in the LAN (local-area network) with unlimited access to office communications functions such as fax machines, answering machines, online banking and EuroFileTransfer. All functions are supplied via the network without the necessity of additional hardware at each individual workstation, thus eliminating the costs of equipping the workstations with ISDN adapters or modems. All you need do is install the office communications software on the individual workstations.

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

*LANCAPI*'s dynamic design also means that communications paths are easily scaled. If more B-channels are needed to manage the pending tasks, more routers are installed in the network. All devices present in the local network then share the pending tasks.



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

The *LANCAPI* is automatically recognized and used as a Class II hardware fax on installation of most fax programs that support CAPI mode.

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

The *LANCAPI* is made up of two components, a server (in the *ELSA LANCOM Wireless*) and a client (on the PCs). The *LANCAPI* client must be installed on those computers in the LAN that will be using the *LANCAPI* functions.

- ① Place the *ELSA LANCOM Wireless* CD in your CD-ROM drive. If the setup program does not automatically start when you insert the CD, simply click 'autorun.exe' on the *ELSA LANCOM Wireless* CD in the Windows Explorer.

- ② Select the 'Install LANCOM software' entry.
- ③ Highlight the 'ELSA LANCAPI' option. Click **Next** and follow the instructions for the installation routine.

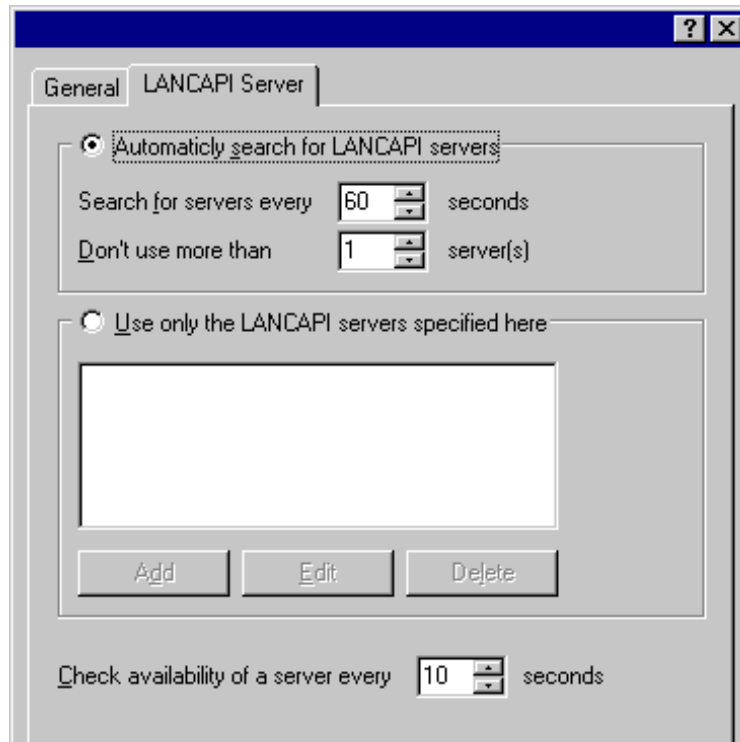
If necessary, the system is restarted and *LANCAPI* is then ready to accept all jobs from the office communications software. After successful installation, an icon for *LANCAPI* will be available in the Start Menu. A double-click on this icon opens a status window that permits current information on the *LANCAPI* to be displayed at any time.

### Configuring the *LANCAPI* client

The configuration of the *LANCAPI* client is used to determine which *LANCAPI* servers will be used and how these will be checked. All parameters can remain at their default settings if you are using only one *ELSA LANCOM Wireless* in your LAN as a *LANCAPI* server.

- ① Start the *LANCAPI* client in the 'ELSAIan' program group. Information regarding the drivers for the available service can be found on the 'General' tab.
- ② Switch to the 'LANCAPI Server' tab. First, select whether the PC should find its own *LANCAPI* server, or specify the use of a particular server.
  - For the former, determine the interval at which the client should search for a server. It will continue searching until it has found the number of servers specified in the next field. Once the required number of servers has been found, it will stop searching.
  - In the event that the client should not automatically search for servers, list the IP addresses of the servers to be used by the client. This can be useful if you are operating several *ELSA LANCOM Wireless* in your LAN as *LANCAPI* servers and you would like to specify a server for a group of PCs, for example.

- It is also possible to set the interval at which the client checks whether the found or listed servers are still active.



### Configuring the *LANCAPi* server

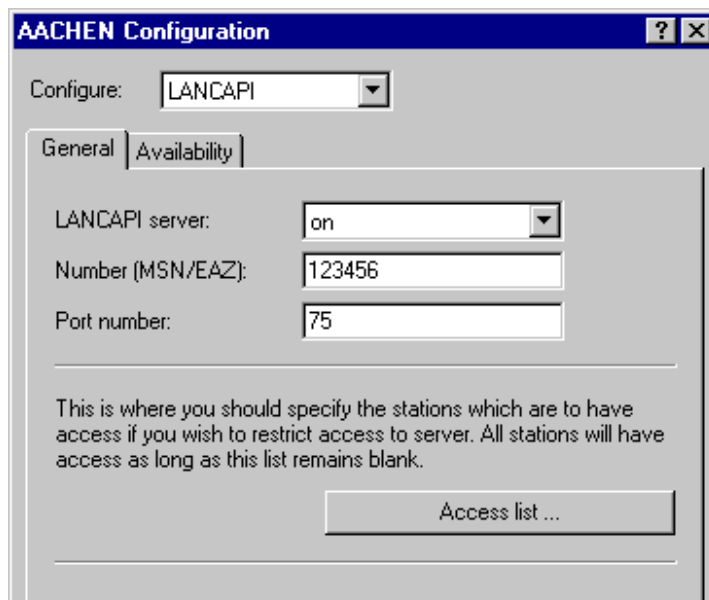
Two basic issues are important when configuring the *LANCAPi* server:

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

Set the relevant parameters as follows:

- ① Start *ELSA LANconfig* which can be found in the 'ELSAIlan' program group. Open the configuration of the router by double-clicking on the device name in the list and select the 'LANCAPi' section.





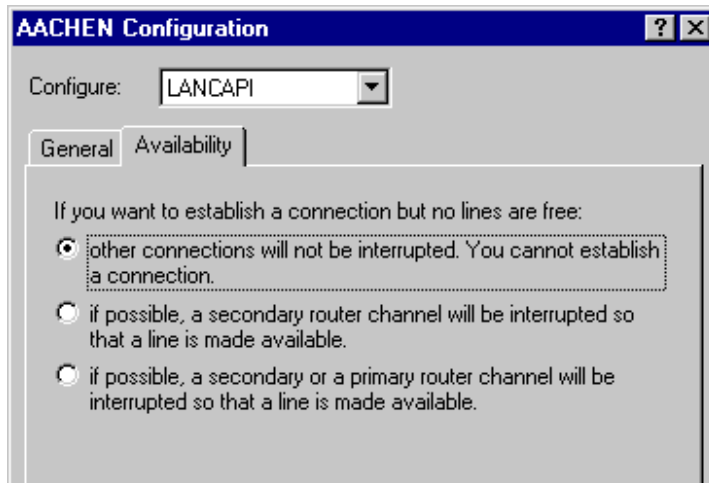
- ② Activate the *LANCAPI* server, or set it to permit outgoing calls only. In the latter case, the *LANCAPI* will not respond to incoming calls – to receive faxes, for example. Permitting outgoing calls only is useful if you do not have a specific call number available for the *LANCAPI*.
- ③ When the *LANCAPI* server is activated, enter the call numbers to which the *LANCAPI* should respond in the 'Number' field. You can enter several call numbers separated by semicolons. If you do not enter a call number here, all incoming calls are reported to *LANCAPI*.
- ④ *LANCAPI* is preset to use port '75' (any private telephony service). Do not change this setting unless this port is already in use by a different service in your LAN.
- ⑤ If you do not wish all the computers in the local network to be able to access the *LANCAPI* functions, you can define all the authorized users (by means of their IP addresses) by entering them in the access list.



*If you enter more than one call number for the LANCAPI, you can, for example, provide each individual workstation with a personal fax machine or personal answering machine. Proceed as follows: When installing communications programs such as ELSA-RVS-COM on the different workstations, specify the various call numbers to which the program should respond.*

Switch to the 'Availability' tab. Here you can determine how the *ELSA LANCOM Wireless* should respond if a connection is to be established via the *LANCAPI* (incoming

or outgoing) when both B channels are already busy (priority control). The available options are:



- The connection cannot be established via the *LANCAPI*. A fax program using the *LANCAPI* will then probably attempt to send again at a later time.
- The connection via the *LANCAPI* can then be established when a main channel is free. A main channel is the first B channel used when a router connection is established. Secondary channels are used for channel bundling.
- A connection can always be established via the *LANCAPI*; an existing router connection will be terminated for the duration of the call if required. This can be used to ensure the permanent availability of the fax function, for example.

### Using the *LANCAPI*

Two options are available for the use of the *LANCAPI*:

- You may use software which interacts directly with a CAPI (in this case, the *LANCAPI*) port, such as *ELSA-RVS-COM*. This type of software searches for the CAPI during its installation and uses it automatically.
- Other programs such as LapLink can establish a variety of connection types, for example, using Windows Dial-Up Networking. You may select the installed communications device that you would like to use when creating a new dial-up connection. For the *LANCAPI*, select the entry 'ISDN WAN Line 1'.

## The least-cost router

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

on a call-by-call basis. The normal telephone number is dialed after the network identification prefix.

Unfortunately, the most inexpensive rates vary from provider to provider depending on the time of day and region. In the morning Provider 1, Provider 2 in the afternoon and possibly Provider 3 for international calls. To always have the most economical connection for telephone calls, surfing the Internet or transferring data to other networks, it would be necessary to decide which provider is the least expensive before each connection. An *ELSA LANCOM Wireless* does this for you. Least-cost routing (LCR) is the function for this task. You define once which providers have the most favorable charges for your purposes, and the device automatically selects the most economical provider for you, regardless of whether you are using the router, the *LANCAPI* etc).

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

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

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

The LCR also requires the following information:

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

### Initial tests

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

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

Dialing prefix	CbC network prefix	Days of week	Time of day
0117	4	Sat + Sun	0:00 AM to 11:59 PM
0117	0800-PIN	Mon + Tue + Wed + Thu + Fri	8:00 AM to 6:00 PM
00	4	Sun	0:00 AM to 11:59 PM

These four entries mean that all connections to Bristol (or other numbers with the prefix '0117') on weekends will be made using the provider with the network prefix '4'. Between 8:00 AM and 6:00 PM on weekdays, these calls will be made using the provider with the network prefix '0800'. International calls on Sundays will be made using the provider with the network prefix '4'.

### **For advanced users: Systematic use of the LCR**

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

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

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

Once you have found the area codes that you would like to reroute, you can start assigning them to call-by-call providers. For this, you need the current rates of as many telephone providers as possible. These can also be found in the Internet. Addresses such as '<http://indigo.ie/~gkernan/>' in the UK, for example, contain complete, up-to-date listings for all types of connections. With this information on hand, you can now begin feeding your least-cost router...

## Setting up the least-cost router

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

- Which operating modes of the *ELSA LANCOM Wireless* should the services of the least-cost router use?
- Which calls should be routed over which provider?

To answer these questions, proceed as follows:

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



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

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

- ④ If you have also made entries in the LCR table for holidays, open the **Public holidays** list. Enter each holiday with its full date (DD.MM.YYYY).
- ⑤ Check the internal clock of the unit (incl. the date), to ensure that the LCR activates the routing at the correct time (see also 'Time for the Selection' further below).

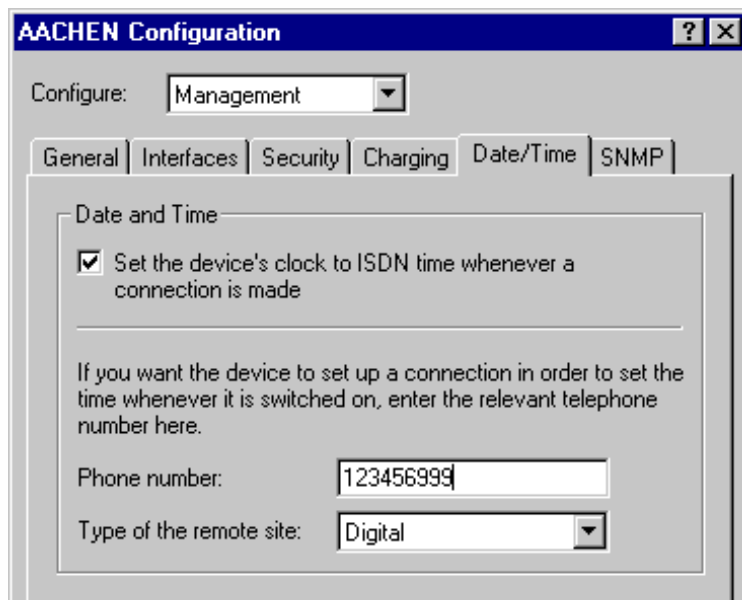


*Build the LCR table one step at a time and check your results. Open the ELSA LANmonitor, for example, and establish connections to the remote stations to be rerouted according to the table using the ELSA LANCAP. Use the dialed number to verify whether the LCR settings suit your requirements. For router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

### Time for the selection

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

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



The screenshot shows the 'AACHEN Configuration' window with the 'Date/Time' tab selected. The 'Configure:' dropdown is set to 'Management'. The 'Date and Time' section contains a checked checkbox 'Set the device's clock to ISDN time whenever a connection is made'. Below this, a text box explains that a telephone number can be entered to set the time when the device is switched on. The 'Phone number:' field contains '123456999' and the 'Type of the remote site:' dropdown is set to 'Digital'.



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





# Appendix

## Technical data

### Hardware specifications

Frequency band:	2400–2483.5 MHz (ISM)
Hardware:	Processor: Hitachi SH3, 60 MHz, 4 MB RAM, 2 MB Flash-ROM
Transfer throughput:	2 Mbps (with an alternative option of 1 Mbps, automatic rate selection)
Range:	up to 300 meters outdoors, approx. 30 meters in closed buildings (typical range)
Bit error rate:	Better than $10^{-5}$
Standard:	IEEE 802.11, DSSS (Direct Sequence Spread Spectrum)
LAN connection:	Ethernet IEEE 802.3, 10Base-T (RJ45)
WAN connection:	ISDN-S <sub>0</sub> bus (RJ45), compatible with I.430
Display/operation:	LEDs for LAN, WAN and device status
Certification:	CE mark (EC), approved for all EU countries and Switzerland
Security:	Password protection, encryption (WEP, in prep.), IP masquerading (NAT), firewall filter
Connects:	10Base-T, ISDN S0, Power
Guarantee service:	6 years
Support:	via hotline, ELSA LocalWeb and Internet

### Software Specifications

Functions:	IP router, DHCP server, DHCP client, DNS server, transparent bridging between WLAN and LAN, <i>LANCAP</i> server, NetBIOS spoofing
Network protocols	ARP, Proxy-ARP, IP, ICMP, UDP, TCP, TFTP, RIP-1, RIP-2, DHCP, NetBIOS via IP
Filter:	Source and target filter for networks, protocols and ports; WAN and LAN separate
Charge monitoring:	maximum charge or connection time in one preset period; security and firewall functions can be set
ISDN D-channel protocols:	DSS1, 1TR6, point-to-multipoint and point-to-point configuration, automatic switching between DSS1 and 1TR6 (can be deactivated), CLIP, MSN, EAZ, DDI

ISDN B channel protocols:	Router: Layer 1: HDLC Kbps HDLC 64 Kbps Layer 2: X.75 LAPB, transparent Layer 3: transparent, PPP, synchronous and asynchronous LZS data compression Stac, Hi/Fn Channel bundling ML-PPP (static and dynamic, incl. BACP) Script processing for CompuServe CAPI mode: Layer 1: HDLC Kbps HDLC 64 Kbps Layer 2: ISO 776 (X.75 SLP), transparent Layer 3: transparent, T.90NL (with T.70NL compatibility)
Masquerade NAT/PAT):	IP address and port conversion via an IP address; static and dynamic assignment of IP address via PPP or DHCP; Masking of TCP, UDP, ICMP and FTP; DNS forwarding; inverse masquerading for IP services from the Intranet (e.g. web server)
Management:	TFTP configuration and firmware upload, SNMP management via SNMP v.1 or v.2, WAN and LAN accesses can be separately activated and configured; Configuration access for WLAN, can be switched separately, diagnosis tools, status display <i>ELSA LANmonitor</i>
Operating security:	Hardware watchdogs, regular self-testing, FirmSafe for remote software upgrades
Security:	Password protection, PAP/CHAP, encryption (WEP in prep.), IP masquerading (NAT/PAT), firewall filter, protection via access lists, WLAN encryption, WLAN filter
Statistics:	LAN and WAN packet counters; error, connection and charge counters, timer

## Radio channels

Every one of the 14 radio channels that can be set for a wireless network has a breadth of 22 MHz with the use of DSSS. This enables a maximum of three mutually independent channels in the ISM frequency band. The table shows the medium frequencies and what channels are permitted in what country.

	Channel no.	Medium frequency [MHz]	EU (ETSI)	Spain	France
1st radio band channel 3	1	2412	X		
	2	2417	X		
	3	2422	X		
	4	2427	X		
	5	2432	X		
2nd radio band channel 8	6	2437	X		
	7	2442	X		
	8	2447	X		
	9	2452	X		
	10	2457	X	X	X
3rd radio band channel 13	11	2462	X	X	X
	12	2467	X		X
	13	2472	X		X
	14	2484			

# 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.

# Declaration of conformity



## KONFORMITÄTSERKLÄRUNG DECLARATION OF CONFORMITY

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

**Geräteart:** Wireless ISDN / LAN Access Point  
**Type of Device:**  
**Typenbezeichnung:** LANCOM Wireless IL-2  
**Product Name:**  
**EG-Baumusterprüfbescheinigungsnummer:** D801136L  
**Registration No.:**  
**Benannte Stelle:** CETECOM ICT Services GmbH  
**Notified Body:** C E 0682 X

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

**Niederspannungs Richtlinie (73/23/EWG)**  
Low Voltage Directive (73/23/EEC)  
**EMV Richtlinie (89/336/EWG)**  
EMC Directive (89/336/EEC)  
**Netzzulassungsrichtlinie (98/515/EG)**  
Commission Decision (98/515/EC)  
**ISDN Richtlinie (97/346/EWG)**  
ISDN Directive (97/346/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: 1998**  
**EN 50082-1: 1992 Teile/ parts: EN 55024: 1999**  
**EN 60950: 1992+ A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997**  
**TBR 3: Nov. 1995**

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, 9. September 1999  
Aachen, 9<sup>th</sup> September 1999

i.V. Stefan Kriebel  
Bereichsleiter Entwicklung  
VP Engineering



# KONFORMITÄTSERKLÄRUNG

## DECLARATION OF CONFORMITY

Diese Erklärung gilt für folgendes Erzeugnis:

This declaration is valid for the following product:

**Geräteart:** **Wireless LAN PC card (PCMCIA)**  
**Type of Device:**  
**Typenbezeichnung:** **AirLancer MC-2**  
**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**

**ETS 300 328: 1996**

**ETS 300 826: 1997**

**EN 50081-1: 1992 Teile/ parts: EN 55022: 1998**

**EN 50082-1: 1992 Teile/ parts: EN55024: 1999**

**EN 60950: 1992+ A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997**

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, 19. August 1999

Aachen, 19<sup>th</sup> August 1999

i.V. Stefan Kriebel  
 Bereichsleiter Entwicklung  
 VP Engineering

# Index

## ■ Numerics

- 1TR6 ..... 7, R50
- 802.11 ..... 6

## ■ A

- Access control ..... 26
- access point ..... 1
- Access protection ..... 8
  - name ..... 26
  - none ..... 26
- Access Type ..... 58
- Access-list ..... R60
- Ad hoc network ..... 2
- Address Administration ..... 18
- Address administration ..... 44
- Address pool ..... 46, 50
- address pool ..... R72
- address ranges ..... R8, R64
- Advice of charge ..... 7
- AOCD ..... 7
- Apple Talk ..... R6
- APPP ..... R54
- ARP cache ..... R62
- ARP-aging-minute(s) ..... R62
- Assembly ..... 24
- asynchronous PPP ..... R54
- Auth. .... R55
- Authentication ..... 37
- auto mode ..... R72
- automatic synchronization ..... 70
- availability ..... 65
- Available workstations ..... 61

## ■ B

- B channel
  - connection status ..... 7
- BACP ..... 7
- Bandwidth ..... 6
- Barring ..... 25
- B-channel protocol ..... 27
- B-channel protocols ..... R53

- Boot system ..... R84
- bridge ..... R55
- Bridging ..... 7
- Broadcast address ..... R8
- Broadcast transfer ..... R11
- Brute force ..... 8, 25
- Buffers ..... R58, R79

## ■ C

- Cable network ..... R7
- cache ..... R62
- Call charge limit ..... 28
- Call charge management ..... 28
- Call establishment ..... 55
- Call number recognition ..... 8
- call numbers ..... R56
- call protection ..... R54
- Callback ..... 27, R51
  - fast call back ..... 28
- callback ..... R56, R58
- Callback function ..... 8
- Callback options ..... R52
- call-by-call ..... 66, 67, R80
- Calling Line Identification Restriction ..... R50
- CAPI interface ..... 62
- Cells ..... R4
- Challenge Handshake Authentication Protocol
  - 27, ..... R55
- Channel bundling ..... 7
- channel bundling ..... 7, R54
  - dynamic ..... 7
  - static ..... 7
- CHAP ..... 27, R55
- charge ..... R52
- Charge monitoring ..... 7
- charges ..... 66
- charging information ..... R51
- charging unit ..... R51
- CLI ..... 27, R56
- CLIP ..... 8

CLIR ..... R50  
 Common ISDN Application Programming Inter-  
   face ..... 62  
 compatibility ..... R53  
 Compression ..... 7  
 Computer names ..... 51, 55  
 Config-aging-minute(s) ..... R76  
 Configuration ..... 8  
   Commands ..... 19  
   SNMP ..... 22  
 Configuration options ..... R76  
 Connect ..... R57  
 Connect charges ..... 55  
 connect-charge monitoring ..... 62  
 connect-charge structure ..... 68  
 Connection control ..... 28  
 Connection duration ..... 7  
 connection timeout ..... R54  
 connection timeouts ..... R51

## D

D channel ..... 27  
 data compression ..... R54  
 Data packet ..... R4  
 days of the week ..... 67  
 DDI numbers ..... R53  
 default route ..... R65  
 destination network ..... R63  
 Destination port ..... R65  
 destination ports ..... R65  
 device names ..... R51  
 Device-name ..... R51  
 DHCP ..... 9, 44, R71  
 DHCP mode ..... 45  
 DHCP server ..... 9, 14, 17, 45, 51, R71  
   configuration ..... 49  
 dial prefix ..... R52  
 dialing prefix ..... 67  
 Dial-Up Networking ..... 27  
 Dialup-remote ..... R51  
 Direct sequence spread spectrum ..... 6  
 Disconnect ..... R58  
 Distance of a route ..... 39

DNS ..... 44, 51, R61  
 DNS Forwarding ..... 44  
 DNS forwarding ..... R61  
 DNS forwarding mechanism ..... 52  
 DNS queries ..... R66  
 DNS server ..... 10, 45, 47, 51  
   available information ..... 52  
   filter list ..... 54  
   filter mechanism ..... 52  
 DNS-backup-IP-address ..... R61  
 Domain Name Service ..... 44  
 Domain name service ..... 51  
 Domains ..... 51  
 DSS1 ..... 7, R50  
 DSSS process ..... 6, 24  
 Dst-address ..... R66  
 Dst-netmask ..... R66  
 dynamic assignment of the IP address ..... R63  
 dynamic bundling ..... R51  
 dynamic channel bundling ..... 7, R54  
 Dynamic Host Configuration Protocol ..... 45  
 dynamic IP routing table ..... R68  
 Dynamic routing ..... 38  
 dynamic short-hold ..... R51

## E

ELSA CAPI Faxmodem ..... 9  
 ELSA header ..... R54  
 ELSA protocol ..... R49  
 Encaps ..... R53  
 End address ..... 46  
 End-address-pool ..... R71  
 Ethernet ..... 6, R53  
   10Base-T ..... 6  
 Ethernet connection ..... 1  
 EuroFileTransfer ..... 9  
 Exclusion routes ..... 39

## F

Factory defaults ..... 13  
 Fast Call Back ..... 28  
 fast Callback ..... R52  
 fast callback procedure ..... R52  
 Fax ..... 9



- Fax Class 1 ..... 9
- Fax driver ..... 9
- Faxmodem ..... 9
- File and printer sharing ..... 57
- Filter ..... 26
- firewall ..... 8
- Firewall function ..... 28
- firewall function ..... R66
- firewall functions ..... 62
- FirmSafe ..... 9, 20
- firmsafe ..... R83
- Firmware ..... 9, R82
- Firmware Upload
  - with LANconfig ..... 21
- Firmware upload ..... 21
  - using TFTP ..... 21
- Firmware-upload ..... R82
- Flash ROM ..... 20
- Flash ROM memory ..... 9
- Fragmentation ..... 24
- Frequency band ..... 24
- G**
  - Gateway ..... 28, 45
  - gateway ..... 47
  - Group table ..... R74
  - Groups ..... 55
- H**
  - HDLC packets ..... R54
  - HDLC56K ..... R55
  - HDLC64K ..... R55
  - Heap-Reserve ..... R59
  - Hierarchical IP addresses ..... R9
  - High telephone costs ..... 28
  - holidays ..... 67
  - Host ..... 51, R4
  - Host table ..... R74
- I**
  - IANA ..... R8
  - ICMP ..... R65, R67, R70
  - Identification ..... 57, R48
  - Identifying the caller ..... 26
  - IEEE standard 802.11 ..... 6
  - Inband
    - Preconditions ..... 17
    - using Telnet ..... 19
  - Infrastructure network ..... 3
  - Install software ..... 20
  - Installation ..... 6
  - Interface ..... R4
  - Interface list ..... R49
  - Interference ..... 6
  - Interference immunity ..... 6
  - internal clock ..... 70
  - international calls ..... 67
  - Internet ..... R6
  - Internetwork ..... R6
  - Intranet ..... R60
  - inverse masquerading ..... R69
  - IP ..... R67
  - IP access list ..... 17
  - IP address ..... 14, 17, 28, R59
  - IP addresses ..... 9, R7
  - IP broadcast ..... R68
  - IP filter ..... 56
  - IP header ..... R67
  - IP masquerading ..... 8, 26, 28, R63, R69
    - supported protocols ..... 43
  - IP multicast ..... R68
  - IP network ..... R6
  - IP network mask ..... R60
  - IP routing
    - Filter ..... 39
    - FTP ..... 40
    - Telnet ..... 40
  - IP routing table ..... 38
  - IP-Masquerading ..... 42
  - IP-routing-table ..... R63
  - IPX ..... R6
  - ISDN cable ..... 6
  - ISDN layers ..... R53
  - ISDN network ..... R7
  - ISDN time ..... 8, R20
  - ISDN-S0 port ..... 13
  - ISM frequency band ..... 6

■ **K**

Key ..... 37, R55

■ **L**

LAN ..... 1, R6, R11

LAN connection ..... 6

LAN connector cable ..... 11

LANCAPi ..... 9, 62, R77

LANCAPi client ..... 62

LANCAPi server ..... 64

LANCOM

LED indicators ..... 7

LANconfig ..... 8, 14, 17, 18, 21, 23

LAN-configuration ..... R76

LAN-filter-table ..... R65

Language ..... R77

LANmonitor ..... 7, 70

layer name ..... R51

Layer-name ..... R53

LCP echo reply ..... 37

LCP echo request ..... 37

LCR ..... 8, 67, R79

LCR table ..... 67

leased-line connection ..... R53

Least-cost router ..... 66

least-cost router ..... 69

automatic fallback ..... 69

connect-charge monitoring ..... 69

operating modes ..... 69

Least-cost routing ..... 8

LED ..... 12

Power/Msg ..... 12

Local Area Network ..... 1, R6

local calls ..... 68

Local network ..... R6

Local-routing ..... R67

location ..... R49

Lock-minutes ..... R77

Login ..... 20, 25

Login barring ..... 25

log-in block ..... R77

Login-errors ..... R77

long distance calls ..... 67

Looser ..... R52

■ **M**

MAC address ..... R58, R79

MAC addresses ..... R12

MAC protocol ..... R12

Mail server ..... 53

manual connection ..... R57

Masquerading ..... R63, R69

masquerading ..... R60

Masquerading table ..... R69

Medium ..... R4

Medium Access Control ..... R11

Microsoft Network ..... 54

Microsoft Network client ..... 56

MLPPP ..... 7

modem operation ..... R54

Multi-device terminal ..... 7

Multipoint cabling ..... R11

Multiprotocol capability ..... R12

■ **N**

Name ..... R48

Name and group designation ..... 57

Name information ..... 55

name server ..... R61

name verification ..... R56

Name-list ..... R51

Names ..... 55

NAT ..... 26, 28, 42

NBNS ..... 55, R62

NBNS server ..... 45, 47

NBNS-backup ..... R62

neighboring local exchanges ..... 68

NetBIOS ..... 10, 51

IP filter ..... 58

LAN-LAN interconnection ..... 58

network protocol ..... 56

remote access ..... 60

remote station ..... 59

TCP/IP ..... 56

NetBIOS name server ..... R62

NetBIOS nameserver ..... 55

NetBIOS networks ..... 51

NetBIOS ports ..... 56  
 NetBIOS proxy ..... 54  
 NetBIOS remote stations ..... 55  
 Network ..... R4  
 Network adapter ..... R4  
 Network address ..... R7  
 Network cable ..... R4  
 network connection ..... R58  
 network identification prefix ..... 67  
 Network Information Center ..... 42  
 Network mask ..... R7  
 Network names ..... 51  
 Network Neighborhood ..... 60  
 network operators ..... 66  
 Network protocol ..... R6  
 NIC ..... 42  
 Node-ID ..... R58  
 NT domain ..... R74  
 number ..... R51  
 Number list ..... R56

## O

office communications ..... 62  
 Online media ..... 17  
 Operating ..... R63  
 Operating modes ..... 23  
 options for saving telephone charges ..... 68  
 Other ..... R84

## P

Package contents ..... 11  
 Packet ..... R4  
 Packet Size ..... 24  
 PAP ..... 27, R55  
 Password ..... 24, 27  
 password ..... 27, R60  
 Password Authentication Protocol ..... 27, R55  
 Password protection ..... 8, 25  
 Password-required ..... R76  
 Passwords ..... 58  
 PAT ..... 26, 28, 42  
 Peer-to-LAN network ..... 3  
 Peer-to-peer network ..... 2  
 Peer-to-peer networks ..... 10

Period of validity ..... 45, 47  
 Physical medium ..... R4  
 Point-to-multipoint configuration ..... 7  
 Point-to-multipoint connection ..... R5  
 Point-to-point configuration ..... 7  
 Point-to-point connection ..... R4  
 point-to-point protocol ..... R54  
 port ..... 65  
 Power supply unit ..... 11  
 PPP ..... 8, 27, R54, R55, R56  
   checking the line with LCP ..... 37  
 PPP list ..... 26  
 PPP negotiation ..... R60  
 prefix ..... 66  
 preselection ..... 66  
 priority control ..... 66  
 Private address spaces ..... R8  
 Prohibited address ranges ..... R64  
 Prohibiting domains ..... 54  
 protect ..... R56  
 Protocol ..... R6  
 providers ..... 66  
 Proxy ..... 10  
 proxy ARP ..... R63, R64  
 Proxy-ARP ..... R67

## R

R1-mask ..... R68  
 Radio cell ..... 2  
 Radio channel ..... 24  
 Range ..... 3, 6  
 rate zones ..... 68  
 Registered IP address ..... R8  
 registered IP address ..... R60  
 Remote Access ..... 55, R67  
 Remote configuration ..... 8  
 remote station verifications ..... R56  
 Remote-table ..... R74  
 Reset button ..... 13  
 Reset system ..... R84  
 RIP ..... R68  
 RIP-type ..... R68  
 Roaming ..... 4, 24

Round robin list ..... R52  
 round robin list ..... R52  
 Round-Robin ..... R53  
 Router ..... R4  
 Router name ..... 39  
 Routing ..... 55, R9  
 Routing Microsoft Networks ..... 54  
 Routing table ..... R9

## S

S0 interface ..... 7  
 Scaling ..... 3  
 Scope ID ..... R74  
 Scopes ..... 55  
 Script list ..... R57  
 script processing ..... R54, R57  
 Security ..... 25, 26, 28  
 security procedure ..... R55  
 Security procedures ..... 27  
 semipermanent leased-line connection ..... R52  
 Server list ..... R75  
 Service ..... 51  
 Service table ..... R69  
 Setup  
   DHCP-module ..... R71  
   IP-router-module ..... R62  
   LAN-module ..... R58  
   TCP-IP-module ..... R59  
   WAN-module ..... R49  
 Shared Medium ..... R11  
 Shared medium ..... R6  
 Shared resources ..... 58  
 Sharing ..... 58  
 Short-hold ..... R51  
 Single user access ..... 28  
 SNMP ..... 22, R70  
 Software update ..... 9  
 Source port ..... R65  
 special dialing characters ..... R51, R52  
 special prefixes ..... 68  
 speed ..... R55  
 Stac ..... R54  
 Stac data compression ..... 7

Start address ..... 46  
 Start-address-pool ..... R71  
 State ..... R59  
 static bundling ..... R51  
 static channel bundling ..... 7, R54  
 static IP address ..... R63  
 Static routing ..... 38  
 Status ..... R19  
   Call-info-table ..... R44, R46, R47  
   Config-statistics ..... R40  
   Connection-state ..... R20  
   Connection-statistics ..... R42  
   Delete values ..... R47  
   Info-connection ..... R43  
   IP-router-statistics ..... R38  
   LAN-statistics ..... R25  
   Layer-connection ..... R43  
   operating time ..... R20  
   PPP-statistics ..... R26  
   Queue-statistics ..... R41  
   S0-bus ..... R20  
   TCP-IP-statistics ..... R32  
   WAN-statistics ..... R21, R22  
 Status Displays ..... 7  
 Subnet ..... R9  
 Suppresses the outgoing MSN ..... R50  
 System terminal ..... 7  
 System-administrator ..... R70  
 System-location ..... R70

## T

Table-ARP ..... R62  
 Table-RIP ..... R68  
 TCP ..... R65, R70  
 TCP max. connections ..... R62  
 TCP/IP ..... 14, 17, 38, R6  
 TCP/IP networks ..... 51  
 TCP/IP stack ..... R6  
 TCP-aging-minute(s) ..... R62  
 Technical data ..... 73  
 telephone company ..... R80  
 telephone provider ..... 68  
 teleworkers ..... R67

Telnet ..... 8, 16  
Telnet server ..... R61  
TFTP ..... 17  
TFTP server ..... R61  
Time ..... R20, R56  
time ..... 67, 70, R82  
Time budget ..... 28  
Time check ..... 8  
time in the ISDN ..... 70  
time of day ..... 67  
Time-dependent connection control ..... 28  
Timeout ..... R73  
TOS ..... R67  
Transmission rates ..... 7  
Trap-IP ..... R70  
Traps-active ..... R70  
trunk seizure ..... R52  
Type of Service ..... 44  
Type-of-service ..... R67

**U**

UDP ..... R65, R70, R77  
Upload ..... 9, 20  
Upload-system ..... R84  
User name ..... 27, 37  
Username ..... R56

**V**

V.42bis ..... R54  
verification attempt ..... R56

Version-table ..... R83

**W**

WAN connection ..... 7  
WAN-configuration ..... R76  
WAN-filter-table ..... R66  
Wildcards ..... 54  
Windows Internet Name Service Server ..... 55  
Windows Networking ..... 60  
Windows networks ..... 10  
Winipcfg ..... 15  
winipcfg ..... 15  
WINS server ..... 55  
wire ..... R4  
Wireless LAN ..... 1  
Wireless links ..... R4  
Wireless network ..... 23  
wireless network ..... 1  
Wireless network adapter ..... 6  
wireless network adapter ..... 1  
WLAN ..... 1, 23  
WLAN domain ..... 24  
WWW ..... 28

**X**

X.75 data protection ..... R54  
X.75 secured format ..... R54

**Y**

Y connections ..... R50



# Technical basics

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

## Wireless network according to the IEEE-802.11 standard

The *ELSA LANCOM Wireless* series devices conform to the IEEE-802.11 standard. This standard is a supplement to the current IEEE standards for LANs, with IEEE 802.3 for Ethernet being the most well-known. In fact, wireless networks that comply with 802.11 can easily be connected to existing Ethernet networks. This is the most important function of the *ELSA LANCOM Wireless* units. With the exception of a couple of additional parameters, wireless adapters that comply with 802.11 are seen by the computer as a normal Ethernet card. This means that you can also use any protocol that you would otherwise use in a wired Ethernet (IP, IPX, NetBIOS,...) on an 802.11 wireless network; the only difference is that there's no need for wires between the computers!

The range of wireless LAN systems is limited as the IEEE standard only covers the definition of LANs; a typical line-of-sight range would be under 300 meters, with considerable reductions in range due to building walls. The group of wireless LAN stations directly within one another's range is generally referred to as a cell.

### Ad hoc mode

The IEEE standard makes provision for two operating forms that differ with regard to the security and range of such wireless LANs.

A wireless LAN in ad hoc mode consists of a single cell which is 'closed' from the Ethernet vantage point, i.e. an external connection is only possible by routing superordinate protocols. An example for such an element would be a *ELSA LANCOM Wireless IL-2* that serves as an Internet access router for all other stations via its ISDN port. Ad hoc networks tend to be spontaneous, for example when a workgroup would like to network its workstations for data exchange purposes. Workstations can enter and leave the network as required; there is no expressly designated node that must be present at all times. A special authentication process is not required, or for that matter possible, because of the lack of a central station to monitor the participants.

But what happens when a workgroup in a neighboring office has the same idea and also sets up a network? While normal Ethernets would consist of two wired physical structures without connections between them, it's not quite so simple to lock up radio waves to prevent interference. This problem is avoided in that every IEEE wireless LAN

has a specific parameter – the name of a WLAN domain. From the viewpoint of the user, the WLAN domain is a freely chosen string of up to characters; at the radio level, this name is converted to an additional addressing component that permits data packets to be associated with a specific cell. To enter an existing wireless LAN, the name of the WLAN domain must be entered in the advanced settings for the network adapter driver. When initialized, the driver will then look for an existing wireless network with this identification. If it finds one, it will then establish a connection, permitting you to communicate with the computers in that wireless network. If it does not find an existing network, it will establish a new cell of its own.

Even if the cells are logically separated in this manner, they can still interfere with one another physically, as only one station can transmit at a time. In other words, none of the cells would be able to take advantage of the full bandwidth in the event of an overlap. This can be prevented by not only assigning different domain names, but also different radio channels to the individual networks. Just as two radio transmitters can transmit simultaneously on different frequencies, two wireless LANs can work simultaneously on different channels without interference. If two cells are very close to one another, there should be a difference of 4–5 channels between the channels used, as the cells also partially use the neighboring channels.



*Not all of the channels included in the IEEE standard are permitted in all countries!*

## Infrastructure mode

The actual strength of wireless networks based on the IEEE 802.11 standard is the ease of interoperability with existing Ethernet networks. A wireless network can be used to connect mobile stations to an existing wired network. Existing networks can also be used to link multiple cells, thus increasing the range of the wireless network. This requires all participants to operate in a different mode, the infrastructure mode.

In addition to the mobile stations, infrastructure mode uses an access point, also known as an access point or distribution system. The *ELSA LANCOM Wireless* units were designed to serve as access points. The access point handles monitoring functions in the infrastructure mode. Domain names and radio channels are still required, and stations entering a network still search for an existing cell. However, unlike ad hoc mode, the cell is always established by the access point, and each station entering the network must log onto to the access point before being permitted to exchange data in the cell. The access point generally also fulfills the function of a “relay station” for data. While this reduces the achievable data rate, careful positioning of the access point can increase the size of a cell. The actual role of an access point, however, is the connection of a wireless cell to a wired Ethernet. If the access point receives a data packet for a computer that is not logged in to it, it forwards the packet to the Ethernet; in the other direction it continuously monitors the Ethernet for data directed to stations logged on to it and forwards the packets to the radio cell. As all mobile stations must log onto the access point, the access point always knows which stations are available on the wireless side,



and thus knows exactly how any given data packet is to be handled. This process is also known as bridging.



*Important: Because it is not necessary to log on in ad-hoc mode, this bridging (which fully automatic from the user's point of view) is only possible in infrastructure mode. Therefore, no provision is made for operating a ELSA LANCOM Wireless in ad-hoc mode.*

As mentioned earlier, an Ethernet backbone can also be used to extend the range of a wireless LAN. In this case, multiple access points can be incorporated in the same LAN and configured to the same WLAN domain. When a mobile station wants to establish a connection with the network, it seeks out and logs onto the access point with the strongest signal. Two mobile stations logged onto different access points can thus communicate with one another even though they are not within direct radio range. The Ethernet linking the access points closes the gap.

If a station continues to monitor the radio situation after logging on, it can determine the relative signal strengths of the access points and automatically switch over to the strongest access point at any given time without user intervention. This process is known as roaming.

## Interchangeability with other devices

*ELSA LANCOM Wireless* devices based on the IEEE-802.11 standard are in principle interoperable with devices based on 802.11 from other manufacturers; but because the 802.11 standard is still quite new and many manufacturers are only now converting from proprietary wireless LAN solutions to 802.11, interoperability cannot in principle be guaranteed. At the very latest, interoperability can fail due to the modulation process used: *ELSA LANCOM Wireless* devices use the so-called direct sequenced spread spectrum (DSSS) process, while some other manufacturers use the frequency hopping spread spectrum (FHSS) process. The exchange of data between devices based on FHSS with those using DSS is not possible as a rule.

## Network technology



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

### The network and its components

*network,  
transmission  
medium,  
interfaces*

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



*Packets  
Cells*

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

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



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

*Host*

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

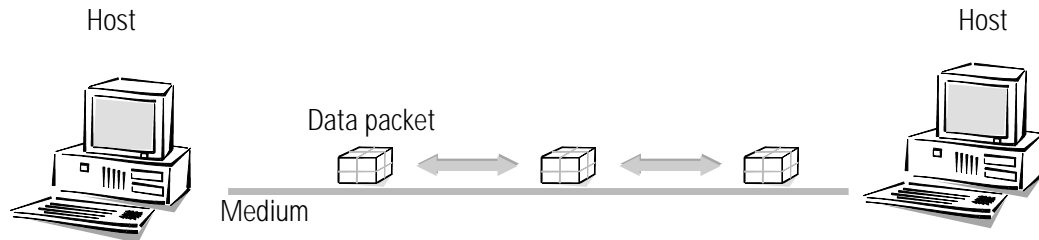
*Router*

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

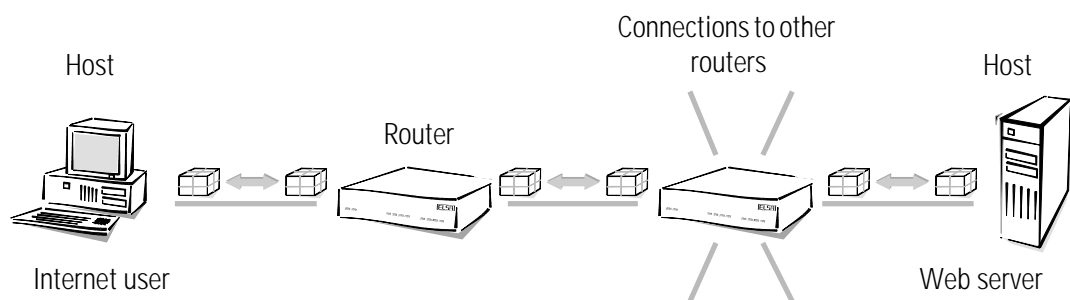
### Connection modes

*Point-to-point  
connection*

When exactly two hosts are connected via a medium, this is referred to as a point-to-point connection. One host transmits packets that can only be received by exactly **one** recipient (unambiguous connection).



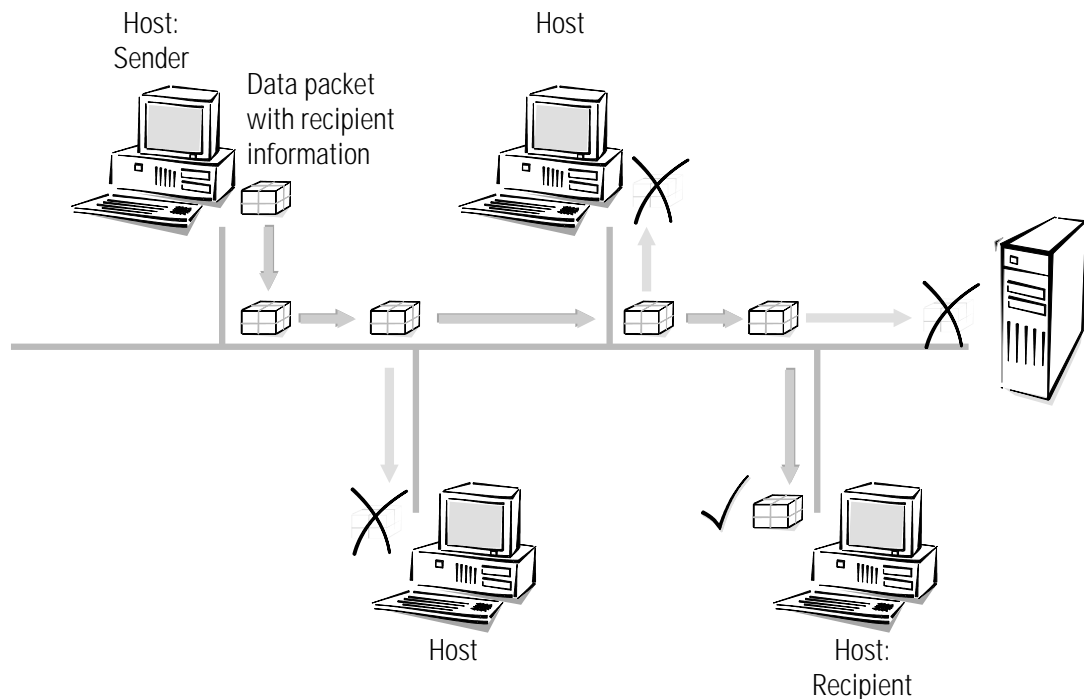
Access to the Internet is also established through point-to-point connections. Even though the data packets are sent from the host at the Internet user to the host at the Internet provider (server) via several routers, every data packet still has its own specific destination. Furthermore, the routers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



*Point-to-multipoint connection*

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

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



## Kinds of networks

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

## IP addressing

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

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

#### IP address

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



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

#### Network address

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

#### Netmask

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

Examples:

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

The same IP address, this time with another netmask:

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

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

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

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

#### *IP address management*

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

#### *Private address spaces*

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

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

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

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

There are two considerations when using these IP addresses:

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

## IP routing and hierarchical IP addressing

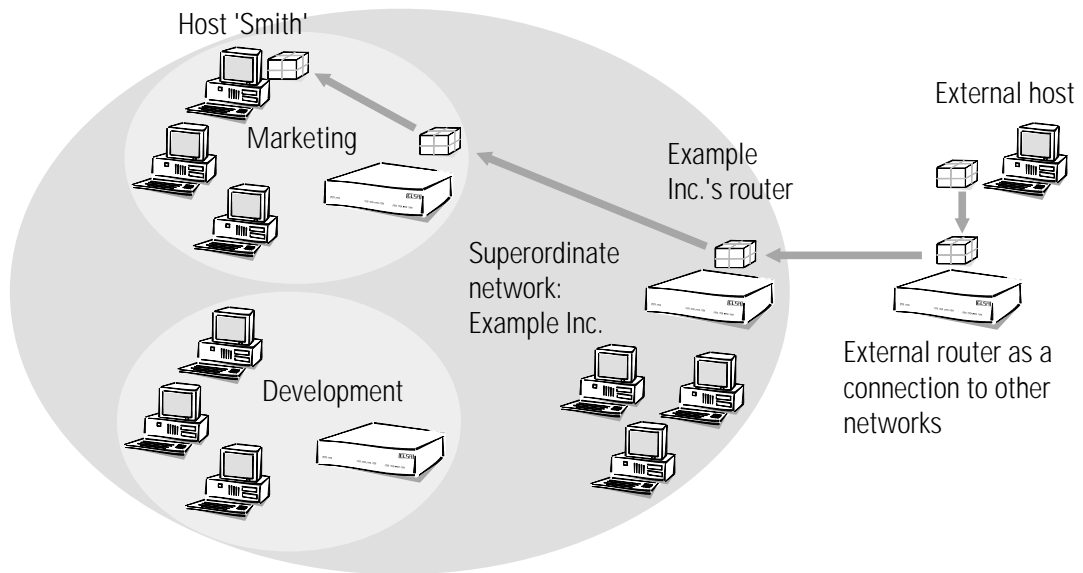
*Routing-method* Every IP packet contains the IP addresses of the source and of the recipient. A router receives IP packets at its interface, interprets the destination address and passes the packets on to those interfaces that are nearest to the recipient. Finding the appropriate path is called routing.

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

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

The consequences of this hierarchical IP addressing:

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



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

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

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

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



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

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

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

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

## Expansion through local networks

*Media access control*

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

*LAN and IP network*

The connection of all computers communicating through a shared medium using a MAC protocol is called a LAN (local area network). A LAN forms an independent network and is subordinate to the IP network, i.e. IP networks can use the physical connections of the LAN to establish connections between the hosts and the routers. A LAN – Local Area Network – is, as the name indicates, spatially limited.

*MAC-address*

Specific LAN addresses hardwired into the interfaces by their manufacturers are used to manage the transfer in the LAN. Since the LAN addresses are used for communication

via the MAC protocol, they are called MAC addresses. They can be thought of as the fingerprint of the interface hardware. MAC addresses can look like this, for example: 00-80-C7-6D-A4-6E.

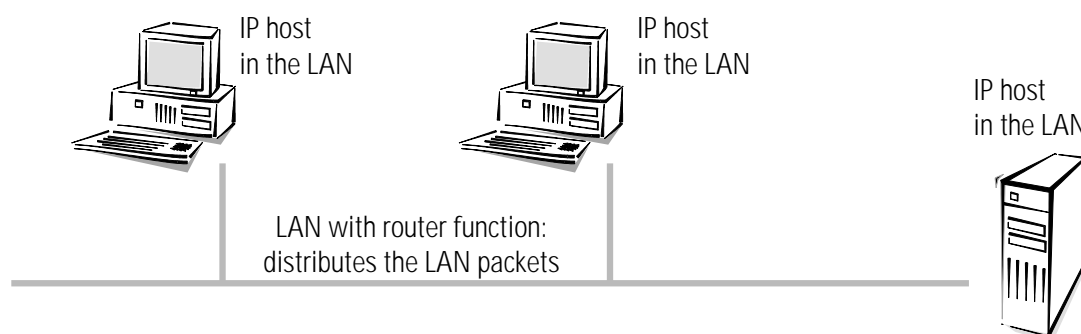
MAC addresses are independent of IP addresses. An IP host whose interface works through a LAN has an IP and a MAC address. Whereas the structure of IP addresses with its similarity to postal addresses is supposed to simplify routing in enormous IP networks, the fingerprint-like MAC addresses are designed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

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

#### *IP in the LAN*

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

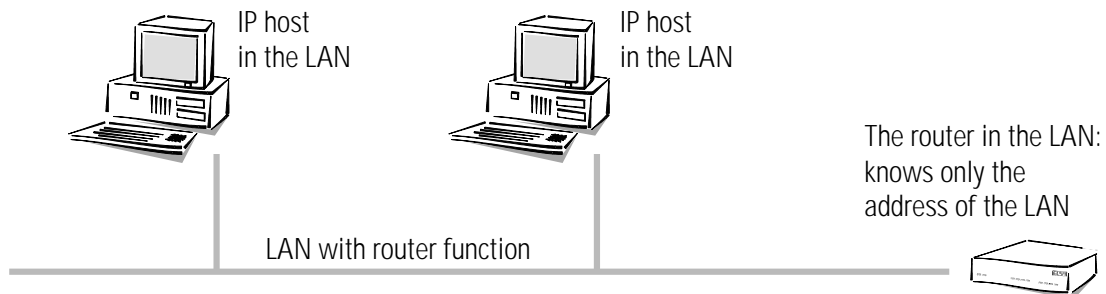
To an IP host, a LAN behaves as if it were an independent network with a router. The hosts gives the packets to the LAN which handles the further distribution of the data packet. This is why only IP addresses from the numerical space of the specific network should be used for the internal communication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



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

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

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



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

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

### Data transfer within the LAN

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

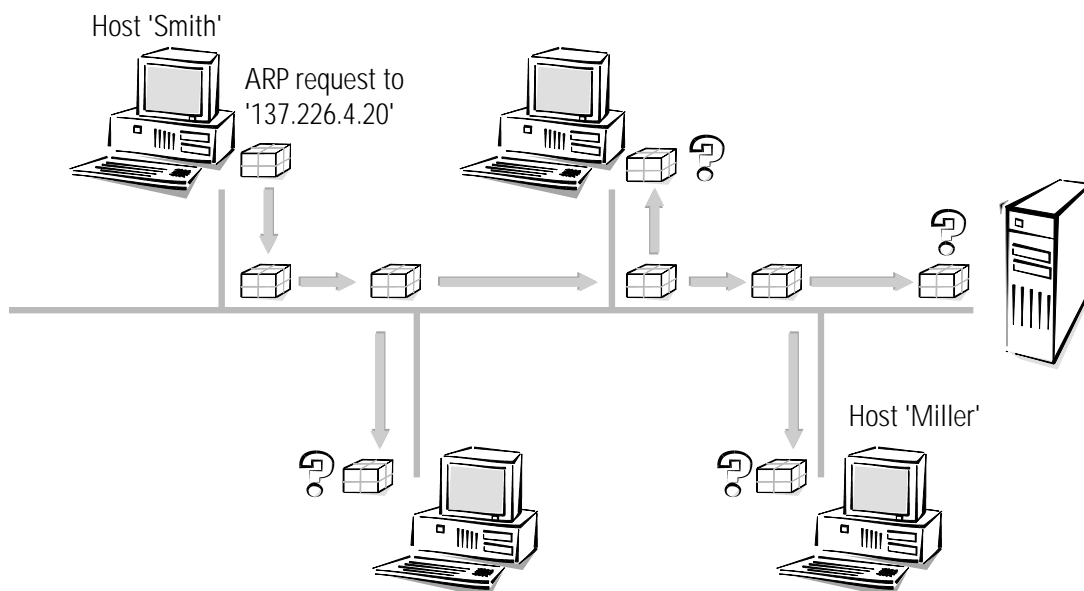
Imagine wanting to send an IP packet from host 'Smith' (with IP address '137.226.4.10' and MAC address '00-10-5A-31-20-DF') to host 'Miller' (with IP address '137.226.4.20' and MAC address '00-10-5A-31-20-EB'). Using the network address and the netmask, host 'Smith' recognizes that host 'Miller' is located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

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

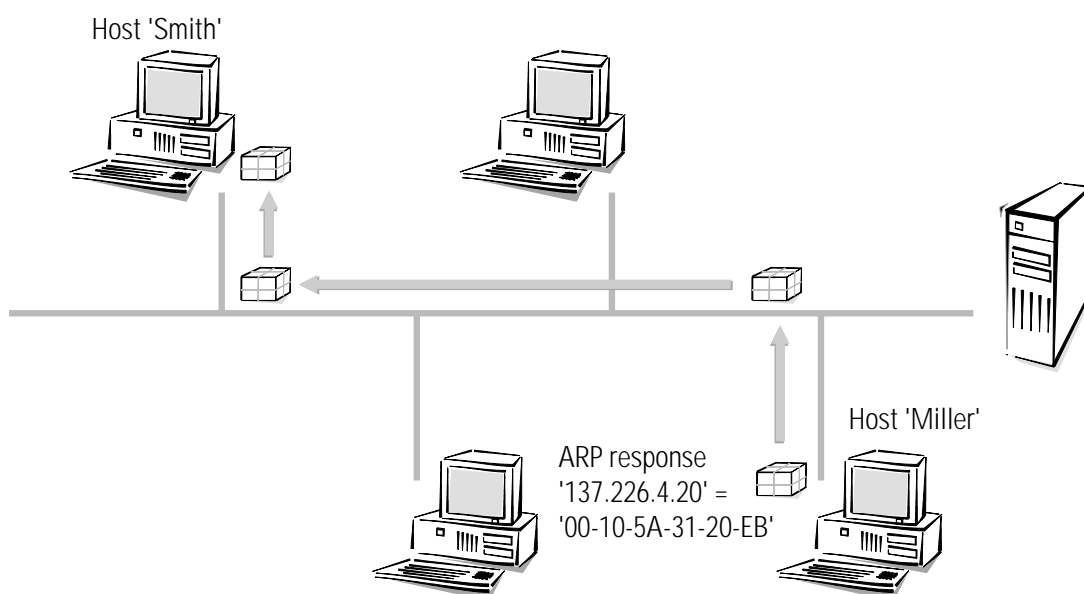
ARP

Therefore the LAN has a special mechanism that automates this process: the **Address Resolution Protocol**, ARP. The table itself is called the ARP table. Whenever a host does not find an entry in the table for a particular IP address (in our example '137.226.4.20'), it

sends an ARP request packet to all hosts in the LAN (with the LAN broadcast address as a target address).



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



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

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

### Data transfer from the LAN onto the Internet

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

### LAN coupling on MAC basis

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

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

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



# Description of the menu options

The menu tree for the 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		WLAN-statistics
	TCP-IP-module		WAN-statistics
	IP-router-module		LAN-statistics
	SNMP-module		PPP-statistics
	DHCP-module		TCP-IP-statistics
	DNS module		IP-router-statistics
	NetBIOS-module		Config-statistics
	Config-module		Queue-statistics
	WLAN-module		Connections-statistics
	LANCAPI-module		Info-connection
	LCR-module		Layer-connection
	Time-module		Call-info-table
	<b>Firmware</b>		Remote-statistics
	Version-table		S <sub>0</sub> -bus
	Table-firmsafe		Channel-statistics
	Mode-firmsafe		Time-statistics
	Timeout-firmsafe		LCR-statistics
	Firmware-upload		PCMCIA-status
	Test-firmware		Delete-values
			<b>Other</b>
			Manual-dialing
			Reset-system
			Boot-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
S <sub>0</sub> -bus		Status of the S <sub>0</sub> interface
WAN-statistics		Displays WAN statistics
LAN-statistics		Displays LAN statistics
WLAN-statistics		Wireless network area statistics
PPP statistics		Point-to-point-protocol statistics
Bridge-statistics		Bridge area statistics
TCP-IP-statistics		Statistics from the TCP/IP area
IP-router-statistics		Statistics from the IP router
Config-statistics		Remote configuration statistics
Queue-statistics		Statistics relating to the packets in the queues of the individual modules
Connections-statistics		Connection information for each interface
Info-connection		Information on the last connection for each interface
Layer-connection		Information on the B-channel protocol used for each interface
Call-info-table		Information on the last 10 calls received
Remote-statistics		Statistics on the last 10 connections
Channel-statistics		Information of the status of the individual channels. Also information on the a/b ports with <i>ELSA LANCOM Wireless L-2</i> .
Time-statistics		Time module information

Status		Running status displays
LCR-statistics		Least-cost router information
PCMCIA-status		Information on PCMCIA status
Delete-values		Deletes all values except tables with substatistics. Delete statistics

## 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; CH02: Ready

## Status/Current-time



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

## Status/Operating-time

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

## Status/S<sub>0</sub>-bus

This option allows you to display the current status of the S<sub>0</sub> interface. The statistics have the following layout:

/S <sub>0</sub> -bus		Running status displays
D-info		Overview of the D channel status
D2-statistics		Breakdown of the Layer-2 information of the D channel for the B channels.

### D-info

This table shows general information related to the D channel:

Channel	B channel identification.
Protocol	D channel protocol. Either the protocol fixed in the interface table or the protocol detected in the 'Auto' settings at the ISDN terminal.

Layer-2	Activation of layer 2 of the D channel ('Yes' or 'No')
TEI	TEI assigned ('Yes' or 'No')
S <sub>0</sub> -activation	Displays activation status ('Yes' or 'No')

*D2-statistics*






This table shows layer 2 information for the individual B channels:

Channel	B channel identification.
TEI	<b>T</b> erminal <b>E</b> quipment <b>I</b> dentifier assigned by the switching center.
L2-activation	Activation of layer 2 of the D channel ('Yes' or 'No').
Connections	Number of connections made over the displayed TEI.

## Status/WLAN-statistics

The current status of the WLAN interface is described here.

LAN-rx-packets		Number of data packets received
LAN-tx-packets		Number of data packets sent
LAN-rx-errors		Number of data packets incorrectly received
LAN-tx-errors		Number of data packets incorrectly sent
LAN-stack-errors		Number of packets without a suitable receive module (bridge/router)
LAN-queue-packets		Number of buffers in use
LAN-queue-errors		Number of packets discarded due to a lack of buffers
LAN-rx-bytes		Number of bytes received from the LAN
LAN-tx-bytes		Number of bytes sent to the LAN
LAN-rx-broadcasts		Number of broadcast packets received from the LAN
LAN-rx-multicasts		Number of multicast packets received from the LAN
LAN-rx-unicasts		Number of directly addressed packets received from the LAN
LAN-Tx-broadcasts		Number of broadcasts received from the WAN
LAN-Tx-multicasts		Number of multicasts received from the WAN
LAN-Tx-unicasts		Number of unicasts received from the WAN
LAN-tx-discarded		Number of packets discarded by the LAN
LAN-repeats		Number of packets that were repeated before being received successfully
LAN-multiple-repeats		Number of packets that were repeated several times before being received successfully

BSSID		Numerical cell identifier; numerical translation of the WLAN domain name. In infrastructure mode this is always identical with the MAC address of the access point
Phy-channel		The radio channel currently being used by the base port.
LAN-Ready		Successful initialization of the wireless network adapter.
Station table		Display of the mobile stations currently logged on.
WLAN parameters		Wireless network parameters

*Station table* This table displays information on the individual mobile stations:

Channel	B channel identification.
Index	displays the sequence of entries in the table.
Age	Age of the station: Time since the last data packet was transferred.
Phy-signal	Average signal strength of the data packets received from this station.
Node ID	Address of the station. Depending on availability, a MAC address, IP address or a symbolic name if this station uses DHCP.
LAN-tx-bytes and LAN-rx-bytes	Data volume transmitted from or to this station.
Status	Can be either 'None', 'Auth' or 'Assoc'. When logging on, a station first authenticates itself, then it 'associates' itself, i.e. makes itself available for data communications. The base port will to transfer data without the 'Assoc' status! 'Auth' indicates whether the station replies to an authentication on the part of the base port.
Encaps.	Ethernet frames can be encapsulated in a variety of ways in a WLAN frame. In the 'IEEE' method, a new header is prepended to the complete Ethernet packet. A different method uses a more intelligent process in which the headers are converted in one another and 'LLC-SNAP' coding is applied to identify the protocol. The base port automatically recognizes both coding forms. If the choice is available, select SNAP coding, as the overhead per frame is 6 bytes lower.

*WLAN parameters*










This table displays the current wireless-network parameters:

Regulatory domain		The frequency band made available by the WLAN-card firmware
PHY type		Radio transmission technique used, set to DSSS.

## Status/WAN-statistics

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

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

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

#### Byte-transport-statistics

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

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

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

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
Ch02	0	0	0	0	0

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

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

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

Ifc	Rx-I1-error	Rx-I2-error	Rx-I3-error	Stack-error	Tx-error
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0

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

Ifc	Designates the associated channel.
Rx-I3-error	Number of layer-3 errors in data received (i.e., the protocol header of layer-3 is incorrect)
Rx-I2-error	Number of layer-2 errors in data received (i.e., similar to the layer-3 errors, e.g. defective PPP header)
Rx-I1-error	Number of layer-1 errors in data received (similar to layer-3 errors)
Tx-error	Number of transmission errors that occurred while sending
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).

*Throughput-statistics*

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





















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

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

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 (bridge/router)
LAN-NIC-errors		Number of data packets discarded by the NIC
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
LAN-queue-errors		Number of packets discarded due to a lack of buffers
LAN-collisions		Number of collisions during a send procedure
Connection -established		Display of correct Ethernet connection (data transfer possible). Corresponds to the 'Link' LED on the device.
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
CBCP-statistics		Displays PPP/CBCP statistics
CCP-statistics		Displays PPP/CCP statistics
ML-statistics		Displays PPP/ML statistics
BACP-statistics		Displays PPP/BACP statistics
Rx-options		Displays the LCP, IPCP and IPXCP information received
Tx-options		Displays the LCP, IPCP and IPXCP information sent
Delete-values		Deletes PPP statistics.

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

### PPP-phases

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

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



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

Ifc	Designates the associated channel.
Phase to	Indicates the current phase of the PPP. The possible values are <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/CBCP-statistics

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

Rx-request	Number of CBCP request packets received
Rx-response	Number of CBCP response packets received
Rx-discarded	Number of CBCP packets discarded
Rx-acknowledge	Number of CBCP acknowledge packets received

Tx-request	Number of CBCP request packets sent
Tx-response	Number of CBCP response packets sent
TX-acknowledge	Number of CBCP acknowledge packets sent
Delete-values	Deletes IPCP statistics.

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

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

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

### Status/PPP-statistics/ML-statistics

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

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



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

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

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

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

The two submenus have the same layout:

/Rx- and Tx-options	Display	
LCP		Information on packet sizes, control characters, security procedures and callback
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
ACCM	<b>A</b> synchronous <b>C</b> ontrol <b>C</b> haracter <b>M</b> ap designates the character in the asynchronous data flow that is interpreted as the control character
Auth.	Authentication procedure used (PAP/CHAP)
Callback	Callback negotiation type

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
TCP-statistics		Statistics for TCP packets from TCP sessions to the router
TFTP-statistics		Statistics for TFTP operations
DHCP-statistics		Statistics from the DHCP server
NetBIOS-statistics		NetBIOS module statistics
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
Delete-values	Deletes ARP statistics
Table-ARP	Displays ARP table

### 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 fragmentation errors	Number of fragmentations incorrectly received from the LAN
IP-LAN fragmentations	Number of fragmentations received from the LAN
IP-LAN forced fragmentation	Number of fragmentations forced by the LAN
IP-LAN-service-errors	Number of IP packets received from the LAN for an incorrect service
IP-WAN-rx	Number of IP packets received from the WAN
IP-WAN-tx	Number of IP packets sent to the WAN
IP-WAN-checksum-errors	Number of IP packets incorrectly received from the WAN
IP-WAN fragmentation errors	Number of fragmentations incorrectly received from the WAN
IP-WAN fragmentations	Number of fragmentations received from the WAN
IP-WAN forced fragmentation	Number of fragmentations forced by 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	Activate/deactivate server flags
Delete-values	Deletes DHCP statistics.









*Table-DHCP*




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

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

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

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












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

P-Nodes		Number of currently active P nodes (peer-to-peer) in the network
M-Nodes		Number of currently active M nodes (mixed-mode) in the network
W-Nodes		Number of currently active W nodes (hybrid) in the network

<i>B-Nodes</i>	Broadcast nodes. A B node performs name negotiations exclusively via broadcasts. Such a computer is not visible over a router connection, since broadcasts may not be routed.
<i>P-Nodes</i>	Point-to-point nodes. For name negotiations, a P node requires a NetBIOS nameserver (NBNS) as well as a NetBIOS datagram distribution server (NBDD) to transfer datagrams over a router.
<i>M-Nodes</i>	Mixed nodes. This type is a mixture of B and P nodes. It acts as a B node in the local network; if the required partner can't be found in the local network, it attempts to locate it using an NBNS query (P node behavior).
<i>W-Nodes</i>	This type of node is not permissible according to RFC, but was introduced nevertheless by Microsoft as a hybrid node.

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

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

LAN-rx		Number of DNS packets received by the LAN
LAN-tx		Number of DNS packets sent on the LAN
WAN-rx		Number of DNS packets received by the WAN
WAN-tx		Number of DNS packets sent on the WAN
Forwarded		Number of requests that could not be fulfilled and were thus forwarded
Errors		Number of invalid requests
DNS-access		Indicates the number of names that were looked up from the DNS table
DHCP-access		Indicates the number of names that were looked up from the DHCP table
NetBIOS-access		Indicates the number of names that were looked up from the NetBIOS tables
Filter		Number of DNS packets filtered by the filter table
Hit-list		This table contains the 16 most popular requests. These may then be prohibited via the filter list if desired.

The hit list has the following structure:

Name	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:






Name	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

/IP-router-statistics	Statistics from the IP router area	
IPr-ARP-errors		Number of unsuccessful accesses to the ARP cache
Delete-values		Deletes IP router statistics
Establish-table		Table of the last 20 packets that required a connection
Protocol-table		Table of routed packets arranged by protocol
RIP-statistics		Statistics from the IP/RIP area

*Establish-table* The **establish table** contains the last 20 entries, which provide information on the system time, destination and source addresses, IP protocol, destination port and source port of the data packets that should have caused a connection to be established.

An IP router establish table might have the following appearance:

Time	Dest	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

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

*Protocol-table*

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

A protocol table might have the following appearance:

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

**Status/IP-router-statistics/RIP-statistics**

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

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

*Table-RIP*








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





An IP-RIP table might have the following appearance:

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

**Status/Config-statistics**



















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




/Config-statistics	Remote configuration statistics	
LAN-active-connections		Current number of active configuration connections from the LAN
LAN-total-connections		Total number of configuration connections from the LAN up until the present
WAN-active-connections		Current number of active configuration connections from the WAN
WAN-total-connections		Total number of configuration connections from the WAN up until the present
Outband-active-connections		Current number of active outband configuration connections
Outband-total-connections		Total number of previous outband configuration connections up until the present
Outband-bitrate		Bit rate of the last outband configuration session

/Config-statistics	Remote configuration statistics	
Login-errors		Total number of defective logins
Login-locks		Number of login locks
Login-rejects		Number of login attempts while the login lock was active
Delete-values		Deletes the config statistics

## Status/Queue-statistics

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

/Queue-statistics	Statistics on the queue	
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
WAN-heap-packets		Number of buffers available
WAN-queue-packets		Number of buffers in use
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.

/Queue-statistics	Statistics on the queue	
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.
WLAN management heap packets		Number of packets available in the buffer.

## Status/Connection-statistics

This menu allows you to display connection times, all charges incurred and other useful information related to ISDN port utilization.

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

lfc	Connection	Active	Passive	Errors	Con.-Time	Charge
Ch01	0	0	0	0	No connection	0
Ch02	0	0	0	0	No connection	0

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

lfc	Designates the associated channel.
Connection	Indicates the number of connections to the particular channel.
Active	Indicates the number of connections actively established for the channel.
Passive	Indicates the number of connections established for the channel by incoming calls.
Errors	Indicates the number of connection errors.
Con.-Time	Indicates the period of time the current connection has existed. If no connection exists, "No-connection" is output.
Charge	Indicates the amount of charges for the current connection. This value is reset to zero when a new connection is established.

The total charges incurred are not displayed directly. However, the charges are totaled internally in order to permit the management of the charges budget (also see **Setup/Charges-module**).



## Status/Info-connection

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

lfc	Status	Mode	Dialup-remote	Device-name	B1-HZ	B2-HZ
Ch01	Ready				0	0
Ch02	Ready				0	0

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

lfc	Designates the associated channel.
Status	Indicates the status of the particular connection. The possible values are: <b>Init</b> , <b>Setup WAN</b> , <b>Ready</b> , <b>Dial</b> , <b>Incoming call</b> , <b>Protocol</b> , <b>Connection</b> , <b>Callback</b> , <b>Bundle</b> and <b>Reserved</b> . The <b>Bundle</b> status is indicated in the display <i>ELSA LANCOM Wireless IL-2</i> by the addition of a <b>"/2"</b> in columns 15 and 16 of the associated display line. <b>Bundle</b> is displayed for the second interface either when a bundle connection has been activated via the first interface or when a leased-line connection with two B channels has been set. <b>Reserved</b> is displayed for the second interface when a connection exists to the first B channel and the Y connection has been deactivated.
Mode	Reflects the type of establishment. The following are possible: <b>Active</b> (active call establishment = dialing) <b>Passive</b> (passive call establishment = call acceptance) <b>CB</b> (call establishment via callback)
Dialup-remote	Indicates the call number of the remote station from the name list.
Device-name	Indicates the logical name of the remote station (if it can be detected). The device name is also displayed on the appropriate display line as soon as a logical connection is established.
B1-HZ	Indicates the short timeout for the connection.
B2-HZ	Indicates the short timeout for bundled channels for this connection.

## Status/Layer-connection

The menu item **Status/Layer-connection** has information on the B channel protocol used on the interface for every available interface. The entries in this table correspond to those in the layer list **Setup/WAN-module/Layer-list** in the WAN module. An additional entry exists for the interface itself. The menu has the following layout:

lfc	WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
Ch01	DEFAULT	ETHER	ELSA	X.75ELSA	compr.	HDLC64K
Ch02	PPPHDL	TRANS	TRANS	PPP	none	HDLC64K

## Status/Call-info-table

This table displays the last ten incoming calls, regardless of whether the router answered these calls.

This allows you, for example, to determine the internal MSN used when the system is operated in connection with a PBX. The table has the following layout:

Time	Ifc	CLIP-Caller	Dial-Caller	Capab.	B chan.
OT; 00:20:57	S <sub>0</sub>	5678	1234	HDLC64K	2
OT; 00:20:46	S <sub>0</sub>	4321	1234	HDLC64K	1
OT; 00:19:47	S <sub>0</sub>	4321	1234	HDLC64K	1
OT; 00:11:33	S <sub>0</sub>	5678	1234	HDLC64K	1
OT; 00:01:13	S <sub>0</sub>	4321	1234	HDLC64K	2
OT; 00:01:02	S <sub>0</sub>	4321	1234	HDLC64K	1
OT; 00:00:06	S <sub>0</sub>	5678	1234	HDLC64K	1

The different entries have the following meaning:

Time	Time when the call came. Either the device operating time or the system time of the ISDN is displayed (if made available from the ISDN terminal).
Ifc	Designates the associated interface.
CLIP-Caller	Call number (CLIP) of the caller
Dial-Caller	The MSN/EAZ dialed by the caller
Capab.	The service requested by the caller. Possible values are HDLC64K, HDLC56K and unknown. An analog call is displayed as unknown here. <i>LANCOM Office-Router</i> can also display the values A-3 kHz (analog 3 kHz), language (for normal speech transmission) and fax G2/3 (for analog fax transmission as per group 2 or 3).
B-chan.	The B channel used. A value of 0 means that all channels have already been seized, i.e. call waiting is activated.



*A tip for those using a router in a PBX: Following a call to any ISDN device under the number of the ISDN bus, the MSN/EAZ displayed under 'Dial-Caller' is exactly the entry that must be entered in the router at /SETUP/WAN-MODULE/ROUTER-INTERFACE-LIST/MSN-EAZ in order for a call to be correctly answered from an external station.*

## Status/Remote-statistics

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

The table has the following layout:

Conn.-start	Remote-ID	Mode	Ifc	Conn.-time	Charge
OT; 00:20:57	BERLIN	Active	Ch01	50	5
OT; 00:20:46	CHEMNITZ	Passive	Ch02	230	10

The different entries have the following meaning:

Conn.-start	Time at which the connection was established. Either the device operating time or the system time of the ISDN is displayed (if made available from the ISDN terminal).
Remote-ID	Logical remote station name.
Mode	Type of connection establishment: Active – the connection was actively established by the device Pas. – The device received a call RR – The device called the remote station back
Ifc	Interface, over which the connection is made (Ch01, Ch02).
Conn.-time	Duration of the connection in seconds
Charge	Charges for this connection in units.

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

## Status/Channel-statistics

This table shows information on the current status of the two B channels. With the *ELSA LANCOM Wireless IL-2* information on the a/b ports is also shown. The information from this table is primarily used for output via *ELSA LANmonitor*. Therefore, some values are shown simply as bits with no further explanation.

The table has the following layout:

Channel	State	App	Mode	Cause	Dialup-remote	Sub-address	Charge	Conn.-time	Extra	ISDN-display
S <sub>0</sub> -ERR	0000000 0	Router	active	0000	0241123456	00000000	3	0		
S <sub>0</sub> -B1	0000000 0	a/b	active	0000	0241123457	00000000	2	20		
S <sub>0</sub> -B2	0000000 0	LANCAP I	passive	0000	0241123458	00000000	4	180		





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

Channel	Channel (or a/b port) for the entry is valid. Only the latest status of a channel is ever displayed. A dedicated "channel" is maintained for error messages on channels.
State	The status of a channel is shown here as, e.g., 'ready'.
App	Application that occupies the channel: Router, <i>LANCAPI</i> or a/b port
Mode	Types of last connection establishment: active or passive
Cause	Last error
Dialup-remote	Remote station call number: with active establishment the number dialed, with incoming calls the number sent.
Subaddress	Addition to application that, e.g., indicates the logical channel for the router for the <i>LANCAPI</i> , e.g., the IP address of the client that is using the CAPI.
Charge	Number of charging units incurred for this connection.
Conn.-time	Duration of the last connection on this channel
Extra	Additional information on the connection, e.g. the name of the remote station for router connections.
ISDN-display	Information from the switching center, e.g. error messages, if connected to the PBX possibly also the caller's name, etc.

## Status/Time-statistics

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

The menu has the following layout:

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

## Status/Time-statistics/ISDN






These statistics include the following values:

Connection	Number of attempts to read time information from the ISDN
Information	Number of time updates received from the ISDN
Info-error	Number of erroneous time updates received from the ISDN

## Status/LCR-statistics




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

The menu has the following layout:

/LCR-statistics		Least-cost router statistics
Total calls		Total number of LCR calls
Successes		Number of calls in which the router found a suitable rule in its tables and successfully rerouted the connection.
Not-found-errors		Number of calls in which the router did not find a suitable rule in its tables and thus could not reroute the connection.
No-time-errors		Number of calls in which the LCR could not become active due to lack of time
Provider-statistics		A table with all providers used (or their prefixes), the number of successful and unsuccessful calls
Delete-values		Deletes LCR statistics

## Status/PCMCIA-status

General information on the inserted card can be found here:

DHCP adapter present		Indicates whether card is inserted – this does not necessarily mean that the card is working, but only that something has been inserted in the PCMCIA slot!)
Card ID		The card name read out of the PCMCIA-Config-Space, i.e. the device name for which Windows requests a driver when the card is inserted for the first time.
Firmware version		Information about the firmware of the WLAN card, provided that the card initialized correctly.
















## 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
WLAN-module		WLAN 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
Config-module		Configuration module settings
DNS module		DNS server settings
NetBIOS-module		NetBIOS module settings
LANCAPi-module		<i>ELSA LANCAPI</i> settings
LCR-module		Least-cost router 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 ?
```

display. In the default configuration, no name is entered.

The device name is required for identification purposes; it is a prerequisite for any connection via the IPX or IP router module, since the routers can exchange data only with known remote stations, and is also required for the unambiguous identification of a remote bridge station.












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

Since the router permits only upper case letters in the device name list, the name is transferred in uppercase letters in the case of a verification by the ELSA protocol. Special characters should not be used in device names unless the remote station can process them.

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
Interface-list		S <sub>0</sub> interface settings
Router-interface-list		Router module settings
Name-list		Remote station settings
RoundRobin-list		Settings for different remote station numbers
Layer-list		Settings for the layer combinations used
PPP-list		Parameter settings for PPP connections
Number-list		Settings for call numbers with access authorization
Script-list		Dial script settings
Manual-dialing		Settings for manual connection control
Protect		Protection for answering incoming calls
CB-attempts		Number of callback attempts when the remote station is busy

### Interface-list

This table contains the interface settings, which apply to all operating modes (modules) of the devices.

lfc	Protocol	FV-B-chan.	Dial-prefix
S0	Auto	1	0

Additional, special interface settings are also available for the various modules, e.g. the call numbers to which a module should react, see also

Setup/WAN-module/Router-interface-list

setup/lancapi-module

setup/ab-module/port-list

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

Ifc	Designates the associated interface.
Protocol	D channel protocol setting. The possible values are: <b>Auto</b> : automatic detection of the D-channel protocol <b>DSS1</b> : Euro-ISDN <b>1TR6</b> : National ISDN <b>GRP0</b> : Leased-line connection group 0 <b>GRP2</b> : Leased-line connection group 2 <b>P2P-DSS1</b> : Point-to-point connection
FV-B-chan.	B channel settings for a leased-line connection. The possible values are: <b>none</b> : Leased-line connection not assigned to a specific channel. <b>1</b> or <b>2</b> : Leased-line connection operates over the assigned B channel. Please refer to the information on setting these parameters in the fixed connection description. The fixed connection function is not a standard component of the <i>ELSA LANCOM Wireless</i> .
Dial-prefix	Global dialing prefix for all modules of the devices. The digits entered here (maximum 8) are automatically prefixed to the selected call number in every call. Use this prefix when, for example, the router is connected to a PBX.

Router-  
interface-list

This table contains the interface settings that apply to the router modules of the *ELSA LANCOM*.

Ifc	MSN/EAZ	YV.	CLIP
S0	123456	Off	On

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

Ifc	Designates the associated interface.
MSN-EAZ	If your device is connected to an ISDN port with 1TR6, enter the EAZ to which the interface is to respond. If your device is connected to an ISDN port with DSS1, enter the MSN to which the interface is to respond. If you wish the interface to respond to several different MSNs, enter them here separated by semicolons. A '#' in the list enables any number of incoming MSNs. For outgoing calls, the first MSN in this list will be reported to the remote station. If no MSN is entered, the switching center sends the main MSN of the terminal.
YV.	This entry can be used to control the interface's ability to establish Y connections. Possible settings are: <b>On</b> : Y connection is supported; a number of connections can be established simultaneously (default). A channel bundling connection is broken off when a second connection to another remote station has to be established. Refer also to the settings for the availability of the <i>LANCAP</i> and the telephone system with the <i>ELSA LANCOM Wireless IL-2</i> . <b>Off</b> : Y connection not supported; only one connection can be established. The second connection is blocked. If a connection to an additional remote station is to be established, this establishment is rejected. A channel bundling connection is not affected.
CLIP	Calling Line Identification Protocol: Suppresses the outgoing MSNs. Possible values: <b>Yes</b> : Activate CLIR, do not send MSN. <b>No</b> : Deactivate CLIR, send MSN to remote station. Please note: The "selective suppression of call number transmission" may be a service feature that will have to be obtained from the telephone company.



*Name-list*

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

The name list can contain 64 different device names and might, for example, have the following appearance:

Device-name	Dialup-remote	B1-HZ	B2-HZ	WAN-layer	Callback
AACHEN	875463	180	0	PPPHDLC	On
BERLIN	040785647	20	20	DEFAULT	Off

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.
Dialup-remote	In this column, you can store the number to be called and, if applicable, supplement it with special dialing characters (see above, default: None).
B1-HZ	In this column, you can define appropriate connection timeouts (in seconds) for the first B channel. If no data is being transmitted when this time expires, the connection on this channel is released (default: 20). If charging information is transmitted over the ISDN network during the connection, the <i>ELSA LANCOM</i> will make full use of every charging unit and will only terminate the connection just before the beginning of the next unit. This function is also referred to as dynamic short-hold.
B2-HZ	In this column, you can define appropriate connection timeouts for the second B channel (same as B1-DT, default: 20). The B2 hold time controls the bundling behavior during a channel bundling. Values of 0 or 9999 identify static bundling, values between them dynamic bundling.
WAN-layer	In this column, a name is stored that must also be entered in the layer list. This establishes the transfer protocol required for this connection.
Callback	In this column, you can define whether a callback is to be made for the relevant remote station (Off/Name/Auto/Looser/ELSA; default: Off).

## ■ Callback options

Off	No callback is made.
Looser	The router stops attempting to establish a connection when there is a call from this remote station (reciprocal call establishment). This setting must be used when a callback from the remote station is expected.
Auto (not applicable to Windows 9x or Windows NT)	The connection will be rejected and a direct callback will be initiated if the remote station is specified in the number list. This means that the caller is not charged. If the remote station is not specified in the number list, a callback will be negotiated in a protocol negotiation (ELSA or PPP). A charge of one unit is incurred for this.
Name	This setting forces a protocol negotiation. This enables call number protection to be set in the number list and also a callback to be started using the protocol negotiation. A charge of one unit is incurred for this.
ELSA	This setting enables a particularly fast callback procedure. The called-back remote station must use the 'looser' setting.

- The special dialing characters in the table below can be entered along with the call number in the name list, round robin list, or logical dial prefix. They control the line access, the use of a semipermanent leased-line connection or determine the interface to be used for the connection:

#	Trunk seizure (only with some PBXs).
F	The remote station can be reached via the leased-line connection only. Syntax: F[channel:][subscriber number] The channel and subscriber number are both optional. In the case of several leased lines, the channel specifies the B channel to be used. Depending on the setting in the channel list, the subscriber number indicates whether a dynamic channel bundling or backup line is to be realized over the dial-up connection.

When **S** or **S2** is appended to the call number, the semipermanent connection (SPV) is activated for the D-channel protocol 1TR6.

*You must subscribe to an SPV through your telephone company for a fixed payment.*

*If you forget to append an **S** or **S2**, the SPV will behave like a standard dial-up line and your charges will be unnecessarily high. The telecommunications provider then charges you the fixed charges and the dial-up line charges incurred during the time the line was used.*

*RoundRobin-list* The round-robin list enables a remote station to be reached with several call numbers. It has the following layout:

Device-name	RoundRobin	Head
AACHEN	4321-5555-6666	Last

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

Device-name	In the device name column, you can enter a remote device name from the name list. If one line in the Round Robin list is insufficient for all desired call numbers, the line can be extended as shown below: The # character and a unique index are added to the device name (e.g. AACHEN#1) and it is entered on the next line.
Round-Robin	The DDI numbers of all possible remote stations are entered here under their corresponding device names. The individual DDI numbers must be separated by hyphens.
Head	In the <b>Head</b> column, the following entries are possible: <b>Last:</b> The next connection to be established will begin with the DDI that was successfully used for establishing the last connection (default). <b>First:</b> The next connection to be established will always begin with the first DDI. For a logical remote station, this field can be modified only by means of its <b>first</b> entry in the table. The field is automatically updated when other entries are made for this remote station.

#### Layer-list

In the layer list, you can freely define the different B-channel protocols by combining various ISDN layers. This enables compatibility to devices from other manufacturers that use different B-channel protocols to be set.

The following standard settings are valid for *LANCOM Office-Router*:

WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	TRANS	PPP	TRANS	compr.	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	none	HDLC64K
RAWHDLC	TRANS	TRANS	TRANS	none	HDLC64K
BRIDGE	ETHER	TRANS	X.75LAPB	none	HDLC64K

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

Layer-name	In this column, you can enter an original name designating the layer combination that you use. These names can then be used in the name list 'layer name' column depending on their spelling to set the protocol. If an entry with the name <b>DEFAULT</b> is defined in this column, the settings stored there are always used when no layer name can be assigned (e.g. a caller does not transmit his or her call number). This entry is also used when a group 0 leased-line connection is established. If the <b>DEFAULT</b> entry is not present, a B channel protocol developed by ELSA is used as the default. The user may delete or change any of the layers predefined here.	
Encaps.	Additional information regarding the data to be transmitted may be specified in the <b>Encaps</b> column. The following entries are possible:	
	ETHER	The data is provided with an Ethernet header. This setting is required for communication with older <i>ELSA LANCOM</i> devices or in bridge operation.
	TRANS	No Ethernet header is sent in this setting. Only "pure" IP data packets are transferred, for example. This setting provides the greatest possible effective data throughput.

Lay-3	In the lay-3 column, you can define additional headers for data transmission in ISDN. You can select from among the following settings:	
	TRANS	No additional header is inserted (higher data throughput). Always select this setting if the remote station sends the data transparently via ISDN layer 3 (e.g. transparent HDLC, transparent X.75LAPB).
	ELSA	The data is provided with an ELSA header. In addition, when a connection is established, a protocol negotiation is performed in which the remote stations exchange names. Incoming-call protection by name is possible only if this setting is selected. Without an ELSA setting, incoming-call protection is possible by call number only. This setting is required for communication with older <i>ELSA LANCOM</i> devices or the workstation drivers.
	PPP	A negotiation is performed according to the point-to-point protocol.
	APPP	A negotiation is performed as per the asynchronous PPP. APPP is then used when synchronous PPP is not possible because the connection does not permit a synchronous transmission (e.g. for analog modem operation).
	SCPPP	Following completion of script processing, a synchronous PPP negotiation is initiated.
	SCAPPP	Following completion of script processing, an asynchronous APPP negotiation is initiated.
	SCTrans	Following completion of script processing, a connection exists to the remote station. No further protocol negotiation is performed.
Lay-2	In this column, you can select the protocol for ISDN layer 2:	
	TRANS	The data is packed directly in HDLC packets. Always select this setting if communication is to take place via transparent HDLC.
	X.75LAPB	The data is exchanged in X.75 secured format. Always select this setting if the remote station is to work with X.75 data protection.
L2-Opt.	The L2-opt. enables the setting of an option for the data transfer setting under Lay-2 with an additional <i>ELSA LANCOM</i> .	
	none	No data compression or channel bundling is performed.
	compr.	V.42bis ( <i>ELSA LANCOM Wireless IL-2</i> ) or Stac data compression will be used. Data compression as per V.42bis is possible only in connection with X.75ELSA or X.75LAPB. Compression as per Stac (Hi/fn) must be used in connection with PPP or multilink PPP. Stac compression may also be used in connection with Windows remote stations.
	bundle	Channel bundling is performed via several B channels. Channel bundling is only possible for the Lay-2 settings of 'PPP' Static or dynamic channel bundling depends on the B2 connection timeout. A B2 hold time of '0' or '9999' will set a static channel bundling in which both channels are always used. In the event of dynamic channel bundling with other B2 hold times, the second channel is only activated when the data throughput exceeds a specified threshold.
	bnd+cmpr	Channel bundling and data compression takes place over two B channels.

Lay-1	The lay-1 column allows you to define the speed at which the data is sent in ISDN.	
	HDLC64K	The data is transmitted at 64,000 bps.
	HDLC56K	The data is transmitted at 56,000 bps. This setting is especially important for connections in the USA.

In order for the device to function correctly as a bridge, **ETHER** must always be entered in the **Encaps** field. If the ELSA LANCOM is used as a router, any entry may be made and it should be adapted to the remote station.

To link to devices from other manufacturers, please check with that manufacturer for the data format used (PPP is almost universally supported).

For Internet and remote access, PPP is generally specified.

#### PPP-list

The router needs the device names contained in the PPP list in order to determine the security procedure settings suitable for the connection and to determine the PPP parameters. It contains a maximum of 64 entries and is structured as follows:

Device-name	Auth.	Key	Time	Try	Conf	Fail	Term	Username
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. In the case of connections via the data transmission network, this is the name entered as "Username". For remote access via the data transmission network, the 'Username' field (see below) is not evaluated! Entries are not case-sensitive!	
Auth.	In this column, you can enter the security procedure to be used for verification of the remote station. Default: PAP	
	none	The router does not negotiate authentication with the remote station when establishing a connection. However, the remote station can itself require authentication from the router. This is the case when dialing up a connection to an ISP, for example.
	PAP	The remote station is checked as per the Password Authentication Protocol.
	CHAP	The remote station is checked as per the Challenge Handshake Authentication Protocol.
Key	A password may be entered in this column. Its presence is indicated by the symbol * and it is used to check the remote station. It may consist of 95 characters (7-bit ASCII, including spaces). Default: None The <code>set ?</code> command shows a list of the allowable characters.	

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

*Number-list*

Under this option, a number list is managed in which you can enter 64 different call numbers with their associated device names. This list can be used to assign the call numbers (CLI) transferred by remote stations to the remote station names.

The entries in the number list for the two calling devices AACHEN and BERLIN might appear as in the table below, thus permitting the name to be derived from the call number supplied and, if applicable, permitting a callback to be initiated via the name list:

Dialup-remote	Device-name
875463	AACHEN
040785647	BERLIN

This number list is required for passive connection establishment. The remote station call numbers must be entered without leading zeros.

The D-channel protocol that is currently activated is then used for a call number test.

If the 'Protect number' setting is selected and a call is received from a remote station, the remote station call number sent is compared to the entries in the number list. If the station number sent is identical to an entry in the list, the caller is authorized and the connection is established.

If the 'Protect no./name' setting is selected and a call is received from a remote station, the remote station call number sent is compared to the entries in the number list. If the call number sent is identical to an entry in the list, the caller is authorized to establish the connection. In addition, it is possible to derive the name of the remote station from the number list and, therefore, the layer that is to be used for this connection. The connection is then established using this layer and name verification is initiated using the layer detected (or using the default layer if no layer is detected).

If the name of the remote station (and thus the layer to be used) cannot be determined using the number list, the call will be accepted using the default layer and the name list will be checked for a suitable entry after the protocol (PPP) negotiation.

*Script-list*

Some Internet providers (e.g. CompuServe) conduct a script-controlled log-on procedure before a PPP negotiation. In order to be able to establish this type of connection as well, a simple script processing procedure is also implemented in the *ELSA LANCOM* (see 'Script processing').

In this table, the scripts are defined and assigned to the remote stations. The table has the following layout:




Device-name	Script
CSEVERE	<>[Host]<CIS>[User]\$U[Password]\$P[PPP]\$C

The entries in the script list have the following meaning:

- Device name: Name of the logical remote station
- Script: All commands to be executed – a maximum of 58 characters per line is available. If the required command sequence is longer, an additional entry for the logical remote station may be added as in the round-robin list. The syntax for this is: Device name followed by '#' and a number. The entries are processed from top to bottom.

### Setup/WAN-module/Manual-dialing

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

/Manual-dialing	Settings for manual connection control	
Connect		Establishes a connection.
Disconnect		Termination of connections
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.

When the function is activated by the keyboard of the *ELSA LANCOM*, the error message 'No remote station' is displayed, because a name cannot be entered here. Therefore, this function must not be used from the keyboard of the *ELSA LANCOM*. If you attempt to establish a connection to a logical remote station for which no call number is specified in the name list, the 'No number' error message is displayed.

*Disconnect*

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

**Setup/WAN-module/protection**

This option allows you to select the conditions under which incoming calls are to be answered at the transmission module.




- If 'Protect' is set to 'none', all pending calls are answered provided that the remote end supports the connection protocol.
- If this option is set to 'name', calls are accepted only from remote stations for which an entry is found in the name list. This verification provides additional protection. This verification is only available when using PPP.
- If this option is set to 'number', calls are accepted only from remote stations that are entered in the number list as authorized remote stations.
- The 'no./name' setting allows you to select combined protection using a name list and number list. First a verification that there is an entry in the number list is made. If this is not possible, the router will attempt to determine the name using the protocol negotiation.

**Setup/WAN -module/CB-attempts**

This option allows you to set the number of times (from 1 to 9) a callback is to be attempted when the remote station is busy. For international connections, you should enter a value from 3 to 5 in order to optimize the callback functions. The default setting is 3.

**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

*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 ELSA LANCOM

#### State

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 network mask* 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. The second IP address enables the device 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 IP address).

*Intranetmask* The network mask belonging to the IP address of the local network 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 the keyboard (ELSA LANCOM Wireless IL-2 only) or via outband configuration (terminal program).*



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

*Access-list*

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



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

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

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

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

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

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

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

IP-address	IP netmask
192.234.222.0	255.255.255.0

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

#### DNS-default

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

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

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

#### DNS-backup

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

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

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

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

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

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






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





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

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

## Setup/IP-router-module

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

/IP-router-module	IP router module settings	
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

/IP-router-module	IP router module settings	
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.
- Three terminal units must be available via proxy ARP with the IP addresses 192.120.130.10, 192.120.130.11 and 192.120.130.12 via an *ELSA LANCOM* 'Dresden'.
- Two destination networks 192.120.131.0 and 192.120.132.0 can be accessed by the remote stations 'AACHEN' and 'BERLIN'.
- Data packets for the destination network 193.140.300.0 are to be sent to another local router with the IP address 192.120.130.200.
- Absolutely nothing is to be transmitted to the destination network 193.140.200.0.
- All other non-local data packets must be sent to the router 'PROVIDER' at the Internet service provider.

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

IP-address	IP netmask	Router-name	Distance	Masquerade
192.120.130.10	255.255.255.255	DRESDEN	0	Off
192.120.130.11	255.255.255.255	DRESDEN	0	Off
192.120.130.12	255.255.255.255	DRESDEN	0	Off
192.120.131.0	255.255.255.0	AACHEN	0	Off
192.120.132.0	255.255.255.0	BERLIN	0	Off
193.140.200.0	255.255.255.0	0.0.0.0	0	Off
193.140.300.0	255.255.255.0	192.120.130.200	0	Off
255.255.255.255	0.0.0.0	PROVIDER	0	On



If the connection to the selected remote station is to be realized via a PPP connection, the IP rights must be enabled for the corresponding entry in the PPP table.

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

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

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

Idx.	D-st.	D-end	S-st.	S-end	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-

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 IMCP, it will forward the data to the corresponding router itself (see also 'Local Routing'). Since this setting increases network utilization in the LAN, the default setting is 'Off'.

### 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

### *RIP-type*

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

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

### *R1-mask*

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

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

### *Table-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

Here specify whether RIP packets will be sent to the LAN or the cable network.

### 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 device 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
Gateway-address		Gateway-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/NetBIOS

The Setup/NetBIOS menu contains the settings for the NetBIOS module. The menu has the following layout:

State		On or off
Scope-ID		NetBIOS scope in which the router is located.
NT-Domain		Workgroup/domain in which the router is located.
Remote-table		All remote stations with which NetBIOS information is to be exchanged must be entered in the remote-station table.
Group-list		All workgroups known to NetBIOS are recorded in the group list.
Host-list		All computer names known to NetBIOS are recorded in the host list.
Server-list		All servers that have logged onto the network are recorded in the server list.

Watchdogs		Sets handling of watchdog packets.
Compensation		Compensation type of routing information.
WAN-update-min.		Compensation interval in minutes.

*Scope-ID* The Scope-ID menu item can be used to specify the NetBIOS scope in which the device is located. It then sees only those NetBIOS packets originating in the same NetBIOS scope; all other packets are automatically rejected. The scope ID is only used in conjunction with Windows name servers (WINS). This entry can generally be left blank.

*NT-Domain* A workgroup/domain can be specified in the NT domain item to trigger the search procedure when starting the NetBIOS module. This is required if the network does not contain any computers running Windows 95 or Windows 98.

*Remote-table* All remote stations that are to provide or receive NetBIOS information must be entered in the remote table. When the NetBIOS module is switched on, NetBIOS packets from remote stations other than those specified will be rejected automatically. The remote-table has the following structure:

Name	Type
AACHEN	Router or workstation



*If the connection to the selected remote station is to be realized via a PPP connection, the NetBIOS rights must be enabled for the corresponding entry in the PPP table.*

*Type*

The 'Type' field specifies whether the remote station is a router or a workstation. In the case of a workstation, all of the known names and servers in the local network and all other connected routers are logged off and deleted from their respective tables as soon as the connection to the remote station is closed.

*Host table* The host table has the following structure:

Name	Type	IP-address	Remote-ID	Timeout	Flags
REMOTE	00	10.0.1.100	AACHEN	5000	xx20
WORKSTATION	00	10.0.0.10		5000	xx00

*Group table* The group table thus looks like this:

Group/Domain	Type	IP-address	Remote-ID	Timeout	Flags
WORKGROUP	1e	10.0.0.10		5000	xx00
WORKGROUP	1e	10.0.1.100	AACHEN	5000	xx20



The fields of the table have the following significance:

Name	Name of the host in the host table.
Group/Domain	Name of the group or domain in the group list. Groups and NT domains are handled in the same manner from the NetBIOS point of view.
Type	WINS type of the host. The type is not relevant for NetBIOS, but Microsoft Networks assign certain properties to the name on the basis of the type.
IP-address	IP address of the owner of the name. The same name can be assigned to multiple IP addresses in the group list.
Remote-ID	Name of the remote station for which the name became known.
Timeout	Time until the name is no longer valid. The timeout is also associated with an aging counter in the flags.
Flags	The flags contain additional information pertaining to the name.

### Flags

The flags have the following significance:

0X0003	This counter increments up each time the validity expires. The entry will be deleted if the name is not refreshed after the second expiration at the latest.
0X0004	This identifies an entry that still needs to be transferred.
0X0008	This identifies an entry that is queued for deletion, i.e. the name has not yet been refreshed after the establishment of a connection.
0X0010	Reserved
0X0020	This identifies a remote station.
0X0040	Reserved
0X0080	Reserved

The server list has the following structure:

Host	Group/ Domain	UPD	IP- address	OS- Ver	SMB- Ver	Server- type	Remote- ID	Timeout	Flags
REMOTE	WORKGROUP	00	10.0.1.100	0400	010F	0004140B	AACHEN	13	0020
WORKSTATION	WORKGROUP	07	10.0.0.10	0400	0415	00452003		31	0000

Unlike the host and group lists, this table fills gradually, as the NetBIOS module depends on messages from the servers themselves.










The individual fields have the following significance:

Host	Name of the server
Group/Domain	Workgroup or domain in which the server is located.
UPD	Update counter: indicates the number of times that the server has already propagated itself
IP-address	Address of the server

OS-Ver	Operating system version number
SMB-Ver	Version number of the SMB protocol used
Server-type	Bit mask in which the services of the server are coded
Remote-ID	Name of the remote station from which the server was announced
Timeout	Time until the entry loses its validity (for entries from the LAN) or time until the router propagates a remote entry.
Flags	Corresponds to the flags in the host or group tables.

## Setup/Config-module

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

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

*Farconfig-(EAZ-MSN)* This subscriber number permits remote configuration via PPP. If no number is specified here, remote-configuration calls will be accepted on all numbers.

*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 15 minutes.

#### Login-errors

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



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

#### Lock-minutes

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

#### Language

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

## Setup/LANCAPI-module

Configuring *LANCAPI* basically involves answering two questions:

- What call numbers from the telephone network should *LANCAPI* respond to?
- Which of the computers in the local network should be able to access the telephone network via *LANCAPI*?
- Via which UDP port do the *LANCAPI* server and *LANCAPI* clients communicate?

The *LANCAPI* module has the following layout:

/LANCAPI-module		<i>LANCAPI settings</i>
Access-list		List of computers allowed to use the <i>LANCAPI</i>
LANCAPI-UDP-port		UDP port for communication between the <i>LANCAPI</i> server and clients
EAZ-MSN(s)		EAZ or MSN to which the <i>LANCAPI</i> should respond
Prio-out		Priority for the <i>LANCAPI</i> versus router connections







- **Operating:** 'on', 'off' or 'outgoing'. Under the last setting the *LANCAPI* will not accept incoming calls.
- **Access-list:** This option allows you to limit the circle of computers permitted to use the *LANCAPI*. This table can have a maximum of 16 entries. If the table is empty, all computers can access the *LANCAPI*.
- **LANCAPI-UDP-port:** In the default configuration, this option is set to '75'. Change this setting only if other devices in your network are already using this port.







*When you change the port, all active connections via the LANCAPI are lost!*

- **EAZ/MSN(s)**: This option allows you to enter the call numbers to which the *LANCAPi* is to respond. If you wish to enter more than one number, place a semicolon between the individual numbers.
- **Prio-out**: The priority for a port controls the option for breaking outgoing connections via the *LANCAPi* router connections. Option '1' does not break router connections, the setting '2' breaks only auxiliary connections of a router connection with channel bundling, the selection '3' also breaks main channels of a router connection.

## Setup/WLAN-module

the WLAN module is configured using this menu:

WLAN-Domain		The WLAN domain is entered here, i.e. the symbolic name that the mobile stations use to find the base port. An ASCII string with a maximum of 32 characters. The default setting is 'ELSA'.
Phy-channel		The radio channel to be used by the base port. The possible values are 1 to 14. However, the channels overlap due to the spread-spectrum process, so that the entire radio band offers a maximum of 3 completely independent channels. <i>Not all channels are permitted in all countries (please see the table of radio channels in the Appendix).</i>
Packet size		A value between 600 and 1600 that states the maximum size of WLAN packets in bytes. Default: 1550.
Access-list		This list can be used to explicitly exclude WLAN stations from data communications with the LAN/base port. Alternatively, authorized stations can be specified. Enter the MAC addresses of stations in this list – in other words, the 12-character hexadecimal numbers printed on the cards – but without separators, i.e. 00-60-B3-1F-02-11 would become 0060B31F0211. <i>This only denies the stations access to the LAN or WAN. Data communications between stations in the WLAN via the base port – which typically serves as a relay – is not affected.</i>
Access-mode		This positive/negative switch determines whether the list is to serve as an authorization or exclusion. By default, the mode is set to negative and the access list is empty, i.e. no stations are excluded from data communications.
Protocol-list		This list permits data packets to be blocked or permitted (depending on the positive/negative setting of the switch) on the basis of their protocol. Every Ethernet frame contains a 16-bit identifier stating the Layer-3 protocol of its data. These can be entered in the list as hexadecimal numbers. Common protocols include: 0800 = IP 0806 = IP/ARP 8137 = IPX F0F0, E0E0 = IPX 809B and 80F3 = Appletalk 6001 to 6007 = Decnet 80D5 and 0808 to 0D0D = IBM SNA <i>In this case as well, traffic is blocked between WLAN stations and the LAN or WAN, but not between the WLAN stations themselves.</i>





Protocol mode		Positive/negative switch for the protocol list
Node ID		MAC layer address of the device
Spare-heap		Buffers that receive data packets from the local network
IAPP protocol		On/Off switch for roaming. Roaming requires that all access points involved must be set with the same WLAN domain and must use the same radio channels.
IAPP announce interval		Time interval for the communication of an access point to all other access points within the wired LAN when roaming is activated.
IAPP handover timeout		Maximum wait period for the access point to communicate with the mobile station.

## Setup/LCR-module

Enter the following information when setting the least-cost router:

- For which modules in the device should the LCR functions be active?
- Which area codes should be diverted when via which call-by-call provider?

The LCR module has the following layout:

/LCR module	Least-cost router settings	
Router-usage		Activate LCR for the router modules, <b>On</b> or <b>Off</b>
Lancapi-usage		Activate LCR for the <i>LANCAPi</i> , <b>On</b> or <b>Off</b>
Timetable		Call forwarding table
Celebration-day-table		List of holidays affecting the timetable.

### Timetable

The table has 256 entries and the following structure:

Index	Prefix	Days	Start	Stop	Number-list	Fallback
1	0171	192	0:00	23:59	01013;01070	On

The individual entries have the following meaning:

Index	Continuing index of entries in the table.
Prefix	Area code to be diverted.
Days	Validity of the entry for week days and holidays shown in an 8-bit mask: Bit 0 represents Monday, bit 7 holidays. The entry '31' therefore designates all business days, '192' Sundays and holidays.
Start	Beginning time for the validity of the entry on the defined days.

Stop	Termination time for the validity of the entry on the defined days.
Number-list	Network identification number of the call-by-call providers.
Fallback	Automatic fallback to your own telephone company if all call-by-call numbers are busy.

For example:

`set 1 02 31 1:00 11:59 01030;01090;01070` On diverts all long-distance calls to region '02' between one and twelve o'clock to the provider with the network identification number '01030'. If this number is busy, the network identification numbers '01090' and '01070' will be attempted. If they are also not available, the connection will be made via the normal telephone company.

*Celebration-day-table*

The celebration-day-table has 256 entries and the following structure:





Index	Date
1	01010000
2	01050000
3	03100000
4	25120000
5	26120000
6	02041999
7	13051999




The individual entries have the following meaning:

Index	Continuing index of entries in the table.
Date	Dates of holidays. Enter the index and the date in full without separators, e.g. 'set 8 13041999' for April 13, 1999 as the eighth entry in the list. Enter '0000' as the year for annually occurring holidays.

## Setup/DNS module

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

State		On (default) or off
Domain		Own domain, optional, 32 characters max.
DHCP-usage		Yes (default) or no
NetBIOS-usage		Yes (default) or no

DNS-table		Static DNS table for the manual association of IP addresses to names, 64 entries
Filter-list		Filter list for the exclusion of prohibited domains, 64 entries
Leasetime		Specifies the name validity information to be given to a requesting computer. Default: 2000

*DNS-table*

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

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

Hostname	IP-address
Host10	10.0.0.10

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

*Filter-list*

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

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/Time-module

The least-cost router in the device requires correct time information to calculate the call number diversions via call-by-call provider. Precise time information is also desirable for some statistics.

The time may be set manually (with the 'time' command) or automatically read from the ISDN network.







For automatic time comparison when the module is switched on, a previously specified remote station is called directly and the time information is taken from the ISDN network. So long as the time module is switched on, the time will be taken from the ISDN every time the router establishes a connection.

The time module has the following layout:

/Time-module	Time module settings	
State		Activating the module: <b>On, Off</b>
Current-time		Displays the current time in the device.
Time-EAZ-MSN		Call number to which a connection must be established to receive time information from the ISDN.
Dialing-attempts		Number of possible attempts to receive time information

## 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
Timeout-firmsafe		Time in minutes required to test new firmware
Test-firmware		Tests the inactive firmware
Firmware-upload		Initiates a firmware upload



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

lfc	Module	Version	Serial number
lfc	LANCOM Business 4100	1.60.0012 / 30.06.1999	8427.000.020

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

Position	Status	Version	Date	Size	Index
1	Inactive	1.60	23061999	690	6
2	Active	1.60	30061999	692	7
3	<Lader>	1.60	07061999	64	0

Enter the following command to activate an inactive firmware version:

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





*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). 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 (ISDN or TCP) will be released or closed.*

*Reset-system*

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

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

*Upload-system*

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

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

# Ports and protocols

## Ports

Capab.	Port no.	Protocol
echo	7	tcp
echo	7	udp
discard	9	tcp
discard	9	udp
systat	11	tcp
systat	11	tcp
daytime	13	tcp
daytime	13	udp
netstat	15	tcp
qotd	17	tcp
qotd	17	udp
chargen	19	tcp
chargen	19	udp
ftp-data	20	tcp
ftp	21	tcp
Telnet	23	tcp
smtp	25	tcp
time	37	tcp
time	37	udp
rlp	39	udp
name	42	tcp
name	42	udp
whois	43	tcp
domain	53	tcp
domain	53	udp
nameserver	53	tcp
nameserver	53	udp
mtp	57	tcp
bootp	67	udp
tftp	69	udp
rje	77	tcp
finger	79	tcp

Capab.	Port no.	Protocol
www	80	tcp
www	80	udp
link	87	tcp
supdup	95	tcp
hostnames	101	tcp
iso-tsap	102	tcp
dictionary	103	tcp
X400	103	tcp
x400-snd	104	tcp
csnet-ns	105	tcp
pop	109	tcp
pop2	109	tcp
pop3	110	tcp
portmap	111	tcp
portmap	111	udp
sunrpc	111	tcp
sunrpc	111	udp
auth	113	tcp
sftp	115	tcp
path	117	tcp
uucp-path	117	tcp
nntp	119	tcp
ntp	123	udp
nbname	137	udp
nbdatagram	138	udp
nbssession	139	tcp
NeWS	144	tcp
sgmp	153	udp
tcprepo	158	tcp
snmp	161	udp
snmp-trap	162	udp
print-srv	170	tcp
vmnet	175	tcp
load	315	udp
vmnet0	400	tcp
sytek	500	udp
biff	512	udp

Capab.	Port no.	Protocol
exec	512	tcp
login	513	tcp
who	513	udp
shell	514	tcp
syslog	514	udp
printer	515	tcp
talk	517	udp
ntalk	518	udp
efs	520	tcp
route	520	udp
timed	525	udp
tempo	526	tcp
courier	530	tcp
conference	531	tcp
rxd-control	531	udp
netnews	532	tcp
netwall	533	udp
uucp	540	tcp
klogin	543	tcp
kshell	544	tcp
new-rwho	550	udp
remotefs	556	tcp
rmonitor	560	udp
monitor	561	udp
garcon	600	tcp
maitrd	601	tcp
busboy	602	tcp
acctmaster	700	udp
acctslave	701	udp
acct	702	udp
acctlogin	703	udp
acctprinter	704	udp
elcsd	704	udp
acctinfo	705	udp
acctslave2	706	udp
acctdisk	707	udp
kerberos	750	tcp

Capab.	Port no.	Protocol
kerberos	750	udp
kerberos_master	751	tcp
kerberos_master	751	udp
passwd_server	752	udp
userreg_server	753	udp
krb_prop	754	tcp
erlogin	888	tcp
kpop	1109	tcp
phone	1167	udp
ingreslock	1524	tcp
maze	1666	udp
nfs	2049	udp
knetd	2053	tcp
eklogin	2105	tcp
rmt	5555	tcp
mtb	5556	tcp
man	9535	tcp
w	9536	tcp
mantst	9537	tcp
bnews	10000	tcp
rscs0	10000	udp
queue	10001	tcp
rscs1	10001	udp
poker	10002	tcp
rscs2	10002	udp
gateway	10003	tcp
rscs3	10003	udp
remp	10004	tcp
rscs4	10004	udp
rscs5	10005	udp
rscs6	10006	udp
rscs7	10007	udp
rscs8	10008	udp
rscs9	10009	udp
rscsa	10010	udp
rscsb	10011	udp
qmaster	10012	tcp

## Protocols

Protocol	Protocol no.
apollo domain	8019
apple talk 1 & 2	809B
apple talk arp 1 & 2	80F3
banyan vines	0BAD
banyan vines echo	0BAF
decnet phase IV	6003
hp probe control	8005
ibm sna services	80D5
IP	0800
ip-arp	0806
novell (econfig e)	8137
rarp reverse arp	8035
snmp over ethernet	814c
xyplex	0888

