ELSA LANCOM™ Wireless L-2

Manual

No. 20942/0999

© 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.

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

Aachen, September 1999

Preface

Thank you for placing your trust in this ELSA product.

ELSA wireless networks are a cost-effective way to replace or expand local, wired networks (LANs). With mobile network adapters, PCs and notebooks can communicate with one another and access wired networks or even the ISDN network.

This documentation was written for the user of the *ELSA LANCOM Wireless L-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

  Complete set of manuals for the product family, technical basics (such as information on wireless networks, general network technology, TCP/IP etc.), a workshop with detailed descriptions of sample applications, and a reference section including comprehensive description of the menus.

Our online services (Internet server www.elsa.com) are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. In the Support file section under 'Know-How', you can find answers to frequently asked questions (FAQs). The KnowledgeBase also contains a large pool of information. Current drivers, firmware, tools and manuals can be downloaded at any time.

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

Contents

Introduction

The advantages of wireless networks are obvious. PCs and notebooks can be set up wherever they are most useful—problems related to missing connections or changes to the building are a thing of the past thanks to wireless communications.

Network connections during conferences or presentations, access to resources in neighboring buildings and the exchange of data with mobile terminal devices are only a few of the applications for wireless LANs.

The base station plays a key role in the existing wired LAN. All stations in the wireless network receive access to the LAN via the base station.

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.

How does a wireless LAN work?

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 IWLAN

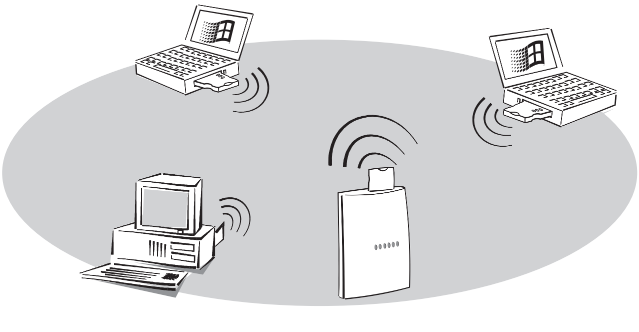
Wireless network adapters connect individual notebooks and PCs to a **L**ocal **A**rea **N**etwork (LAN). As the usual network cables have been replaced by a radio link in this case, we also refer to this as a **W**ireless **L**ocal **A**rea **N**etwork (WLAN).

Base station

The base station 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 on the other side to exchange data between the two networks. In effect, the base station 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 base station can reach each other and exchange data is known as a radio cell.

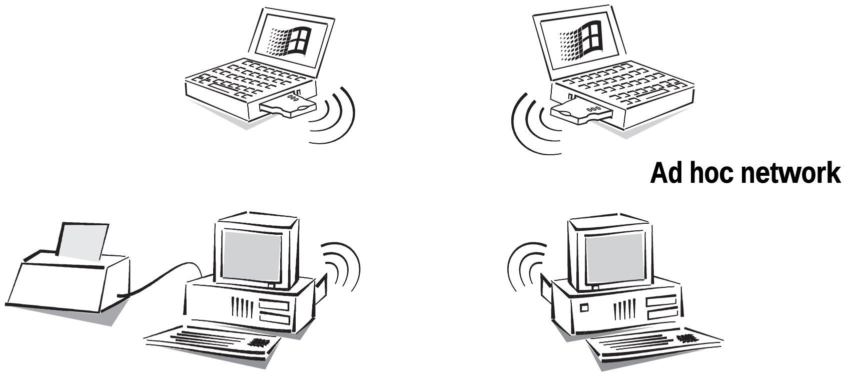


All of the standard functions of a wired network are also available in a wireless network: Access to files, servers, printers, etc. is possible, as is the integration of the mobile stations in a company mail system.

The following applications are available using ELSA wireless network adapters and base stations:

Direct connections between computers

Connect two or more computers directly to one another using wireless network adapters. All computers in a WLAN can communicate with one another without additional hardware.

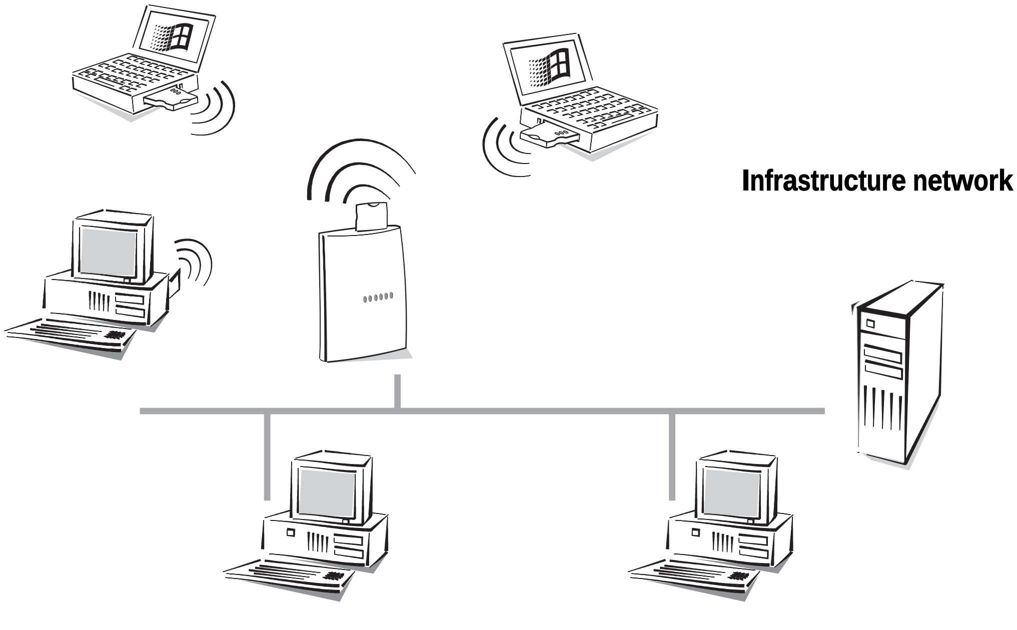


Peer to peer

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 a wired LAN

All workstations with wireless network adapters can be given access to wired networks through a base station. The base station provides a connection between the LAN and WLAN; it also serves as a center for the exchange of data within the WLAN.



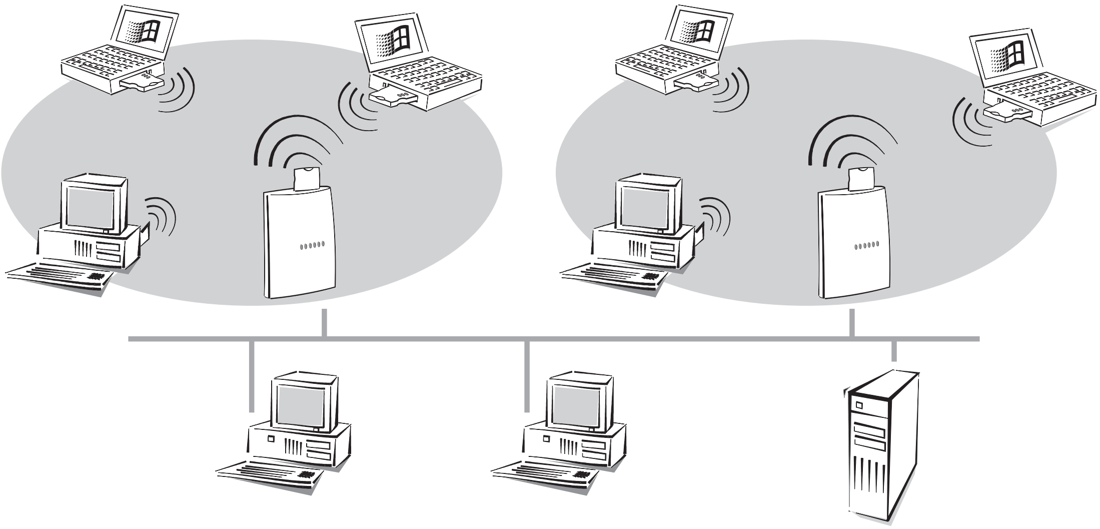
Peer to LAN

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

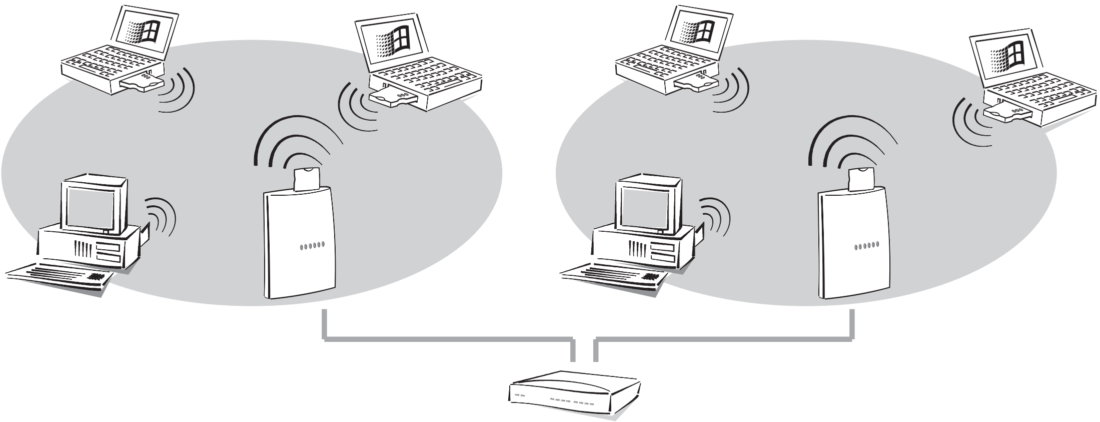
This network type is ideal as a supplement to existing LANs. The infrastructure network is an ideal alternative for expanding LANs into areas in which a wired LAN cannot be realized or is not economically feasible.

Scaling

Multiple base stations 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 a base station, add a second base station. The base stations 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.

What does the *ELSA LANCOM Wireless L-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.
- Switch it on.

- Go!

LAN connection

Base stations 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 base stations 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**equence **s**pread **s**pectrum)

  This process, which is also used for military applications to enhance the security of connections, fragments the data prior to transmission ands 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).

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 base station allow you to monitor the Ethernet connections and the current line connections, thus simplifying the process of diagnosing any systems failures.

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.

This means that you can access the device from the WLAN or from the LAN. TFTP is supported along with SNMP.

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

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 or the WAN.

FirmSafe

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

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

DHCP

ELSA base stations 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.

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:

- *ELSA LANCOM Wireless L-2* base station
- Power supply unit
- *ELSA AirLancer MC-2* wireless network adapter
- LAN 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*

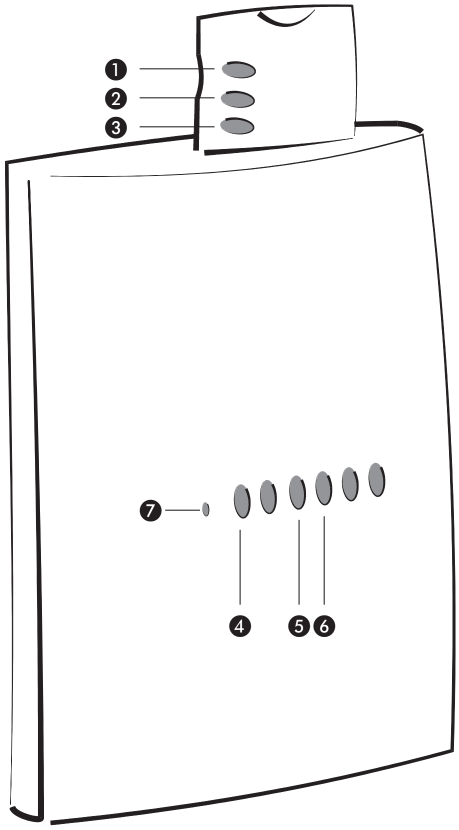
This section introduces the unit's hardware. It covers the unit's display elements and connection options.

Base station The role of a base station is the connection of a wireless cell to a wired Ethernet. In addition to the 10-Base-T connection for the 10-Mbit Ethernet adapter, it also has a slot for the *ELSA AirLancer MC-2* wireless network adapter.

PC card The wireless network adapter *ELSA AirLancer MC-2* has been realized as a PC card and is simply inserted into the slot of the base station. The antenna of the card extends out over the housing of the base station.

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 base station.

❷ The yellow LED of the wireless network adapter indicates the number of mobile stations logged onto the base station. 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 base station 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.

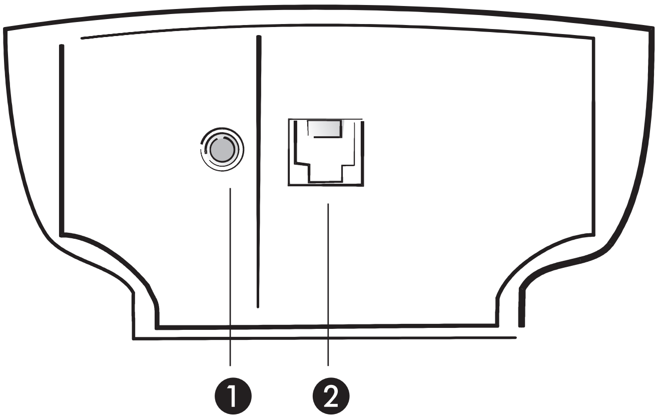
Off		Device off
green	1 x short	Boot procedure (test and load) started
green	flashing	Display of a boot error (flashing light code)
green		Device ready for use

❺ The 'LAN Status' LED on the base station indicates activity on the wireless network and the LAN.

❻ the 'LAN Collision' LED on the base station indicates data collisions on the LAN.

❼ 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:



❶ Connection for power supply unit

❷ 10Base-T network connection

Connecting the base station

① Connect the *ELSA LANCOM Wireless L-2* base station to the LAN. Insert the included network cable into the 10Base-T connection of the base station and into a free network connection socket of your local network such as on the hub of your LAN.

② Insert the *ELSA AirLancer MC-2* wireless network adapter in the base station. The LEDs of the PC card must face toward the front of the base station.

③ Connect the AC adapter to the base station. 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 base station. 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 base station and the LAN.

Software installation

The base station 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 base station.

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

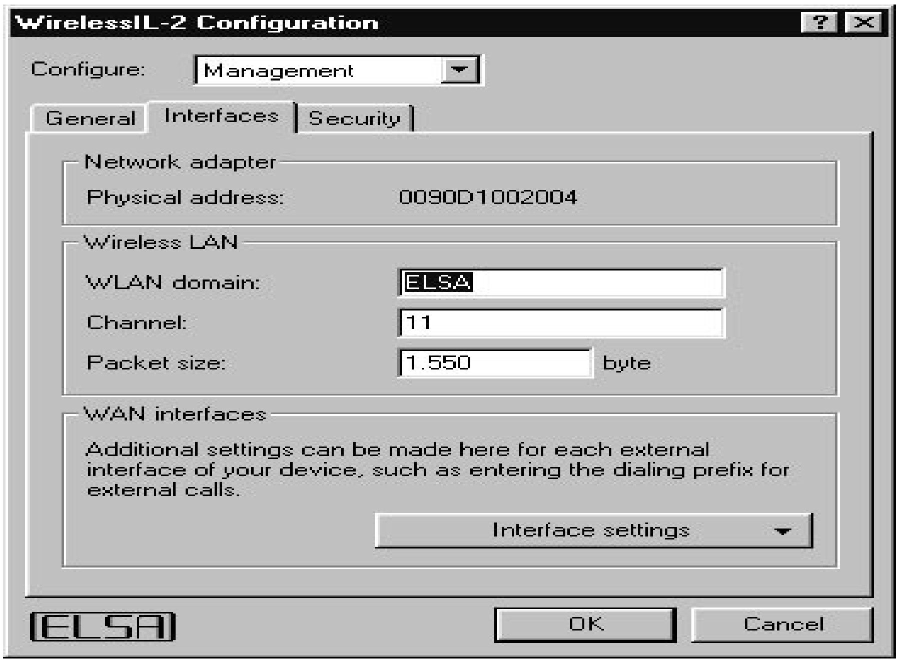
The IP address for the base station is set during the basic configuration. A decision also needs to be made whether or not to use the integrated DHCP server. The basic configuration can be performed using *ELSA LANconfig* or via Telnet.

Basic settings using *ELSA LANconfig*

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

To activate an *ELSA LANCOM Wireless*, the IP address XXX.XXX.XXX.254 must not be in use in your network. If you already have a device with this address, shut it down while setting up the *ELSA LANCOM Wireless*.

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



WirelessIL-2 Configuration

Configure: Management

Network adapter

Physical address: 0090D1002004

Wireless LAN

WLAN domain: ELSA

Channel: 11

Packet size: 1.550 byte

WAN interfaces

Additional settings can be made here for each external interface of your device, such as entering the dialing prefix for external calls.

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 base station 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* `winipcfg` *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.*

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 base station 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 base station and specify whether the base station 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 base station 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 base stations 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 a configuration via the network allows any computer on the WLAN or LAN to access the base station. 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 base station 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 base station 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

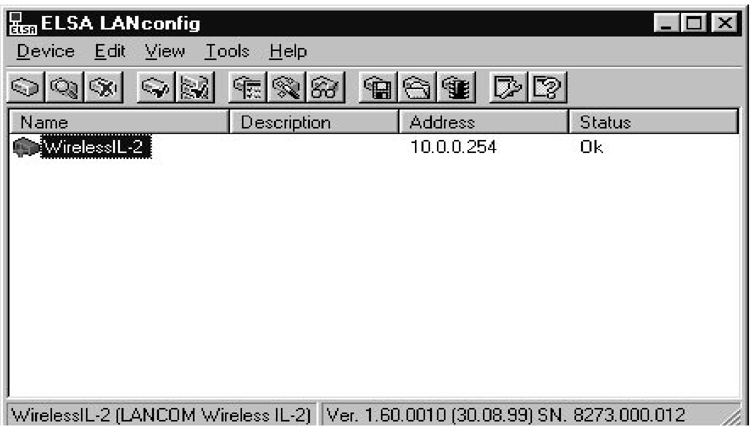
If it is not absolutely essential that you configure the correct IP addresses “manually”, the DHCP server will gladly do this task for you automatically. When using the DHCP server you can have the IP addresses for all computers on the network assigned automatically (see also chapter 'Automatic Address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



Name	Description	Address	Status
WirelessIL-2		10.0.0.254	Ok

WirelessIL-2 (LANCOM Wireless IL-2) Ver. 1.60.0010 (30.08.99) SN. 8273.000.012

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 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 **writeflash** 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 writeflash
```

*This command sends the corresponding file to the given IP address using the **writeflash** 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 via a standardized management protocol.

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 networks
- Security for your configuration
- Automatic address administration with DHCP

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

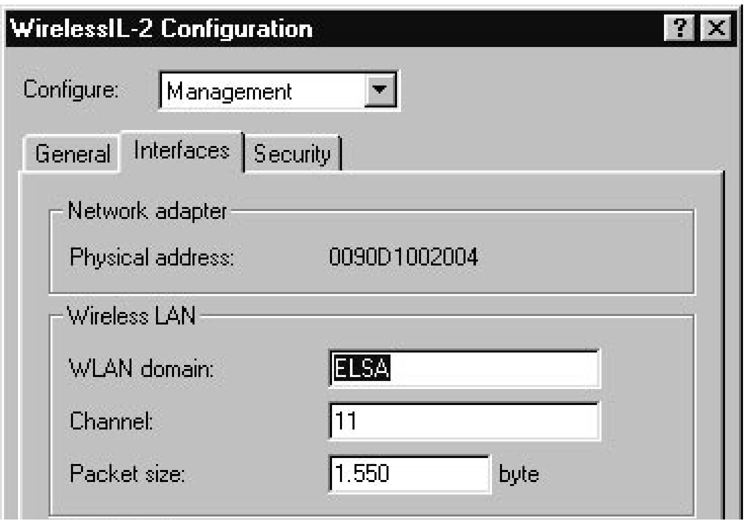
The same values must be set for a variety of parameters to ensure that the wireless network adapters in the mobile stations and base stations can identify each other and exchange data with one another.

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 base stations 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 base stations in the LAN and WLAN.

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



Configure: Management

Network adapter

Physical address: 0090D1002004

Wireless LAN

WLAN domain: ELSA

Channel: 11

Packet size: 1.550 byte

③ Set the new value for the WLAN domain. The Die 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 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 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 die configuration.

Password protection

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

The password input field can be found in the *ELSA LANconfig* in the 'Management' configuration section on the 'Security' tab. The password prompt can be activated in a terminal or telnet session in the `/Setup/Config-module/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 *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.

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.
- If '0.0.0.0' is entered instead, the DHCP server automatically determines the addresses (start or end) from the IP address settings in the 'TCP/IP module'.
- If the cable modem has no IP address of its own, the device will go into a special operating mode. It then uses the IP address '10.0.0.254' for itself and the address

pool '10.x.x.x' for the assignment of IP addresses in the network. In this state, the DHCP server only assigns IP addresses and their validity to the computers in the network, but not the other information.

If only one computer in the network is 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 the DNS or NBNS servers of the wired LAN should also be available to the WLAN, their addresses must be specified. Otherwise, the base station will give its own IP address to the stations in the WLAN as that of the DNS or NBNS server, in which case the relevant queries cannot be answered.

Default gateway assignment

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

If a gateway in a wired LAN should also be available in the wireless network, enter the IP address of the gateway in the DHCP module as the 'Gateway Address'. Otherwise, the base station will give its own IP address to the stations in the WLAN as that of the gateway, in which case the relevant queries cannot be answered.

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

Period of validity for an assignment

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

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

- Maximum lease time in minutes

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

  If a host requests a validity in excess of 6000 minutes, this will nevertheless be the maximum available validity!

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

- Default lease time in minutes

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

Priority for the DHCP server—Request assignment

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

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

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

① Connect the unconfigured router to your local network using a network cable. If you are connecting the device to a hub, the node/hub switch must be set to 'Node'. If you are connecting the router directly to the network adapter of a computer in your network, set the switch to the 'Hub' position.

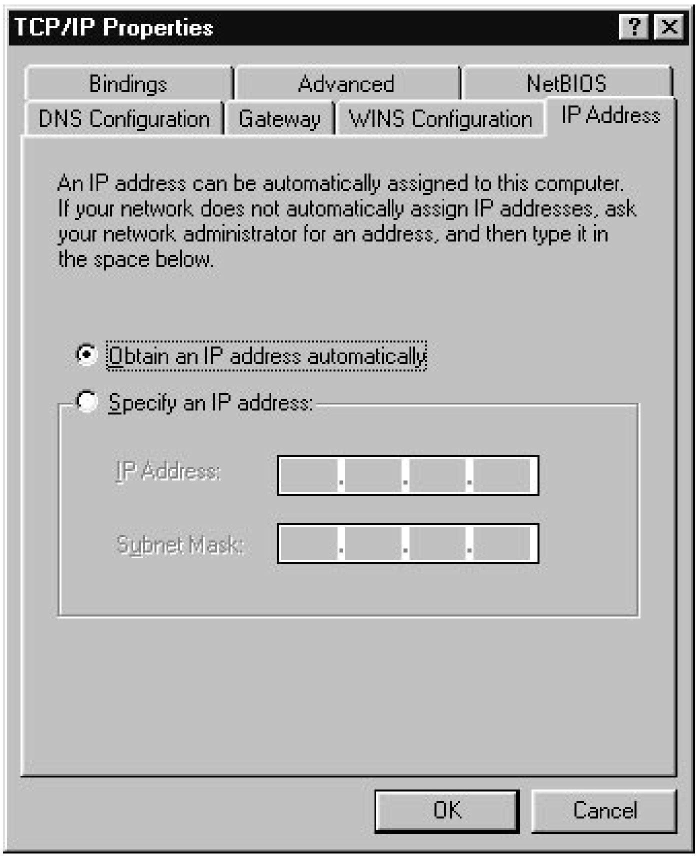
② Switch the device on. The router will not find any other DHCP servers in the network and will thus enable its own DHCP functions.

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.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

④ Install the *ELSA LANconfig* on a computer in the network.

⑤ Start the program from the 'ELSAlan' program group. When loading, the *ELSA LANconfig*, will detect an unconfigured router in the network and will launch the wizard for the basic settings.

– If you have not previously used any IP addresses in your network, select the option 'Make all settings automatically' in this wizard and confirm your selection with **Finish** in the next window.

  The wizard assigns the IP address '10.0.0.1' with the netmask '255.255.255.0' to the router and enables the DHCP server. On the basis of this IP address, the device then determines the valid address pool for the DHCP assignment.

– In the event that IP addresses were already in use in your network before converting to DHCP operation, select the option 'I would like to adjust the settings manually' in the wizard. In the next window, enter an unused IP address from the previously-used address range and activate the DHCP server.
  The wizard now assigns the selected IP address and associated netmask to the device. On the basis of this IP address, the device then determines the valid address pool for the DHCP assignment.
– After a few seconds, all of the computers in the network will be checked and are assigned a new IP address by the DHCP server as required. The computers also receive additional parameters such as the broadcast address, DNS server, default gateway, etc.

Manual configuration

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

Appendix

Technical data

Frequency band	2400–2483,5 MHz (ISM)
Transfer throughput	2 Mbps (fallback to 1 Mbps, automatic rate selection)
Range	up to 300 meters outdoors, approx. 30 meters in closed buildings (typical range)
Bit error ratio	better than 10-5
Standard	IEEE 802.11, DSSS (Direct Sequence Spread Spectrum)
Operating systems	Windows 95, Windows 98, Windows NT 4.0, Windows 2000, Windows CE (in Prep.)
Network protocols	any network protocols can be transferred between the WLAN and LAN via bridge
Connects	10Base-T, Power
Package contents	Extended documentation in German, English, French and Italian Network cable, configuration software
Service	Warranty: 6 years
Support	Via Hotline and Internet

Wireless channels

Each of the 14 wireless channels that can be selected for a wireless network has a width of 22 MHz. As a result, a maximum of three completely independent channels are available in the ISM frequency band. The table states the middle frequencies and indicates which channels are approved in which countries.

	Channel no.	Middle frequency [MHz]	EU (ETSI)	Spain	France
Radio band 1 Channel 3	1	2412	X		
	2	2417	X		
	3	2422	X		
	4	2427	X		
	5	2432	X		
Radio band 2 Channel 8	6	2437	X		
	7	2442	X		
	8	2447	X		
	9	2452	X		
	10	2457	X	X	X
Radio band 3 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.

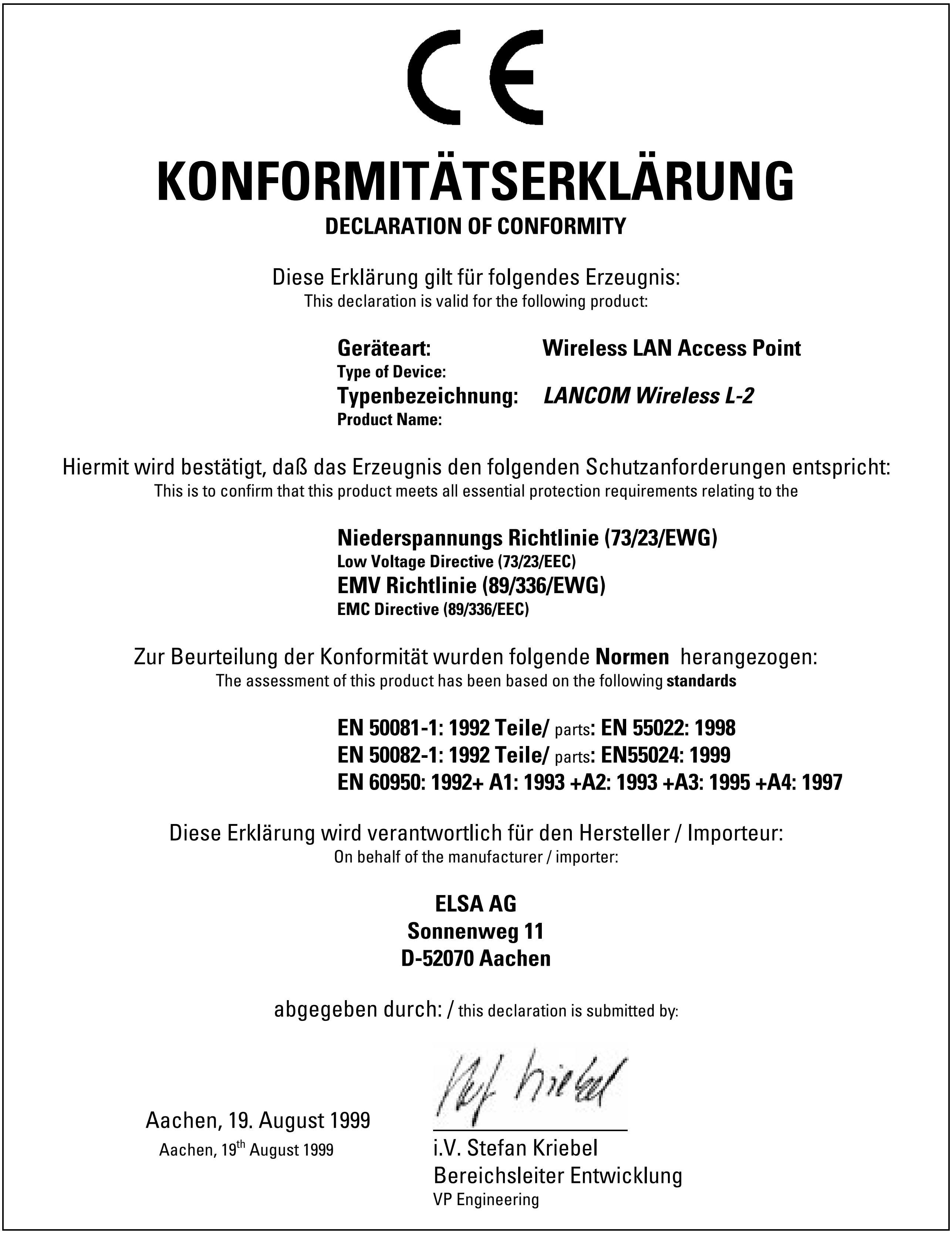
e) In the case that the intentional or culpable negligence of ELSA employees has caused a loss of data, ELSA will be liable for those costs typical to the recovery of data where periodic security data back-ups have been made.

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 LAN Access Point**
Type of Device:
Typenbezeichnung: ***LANCOM Wireless L-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**

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

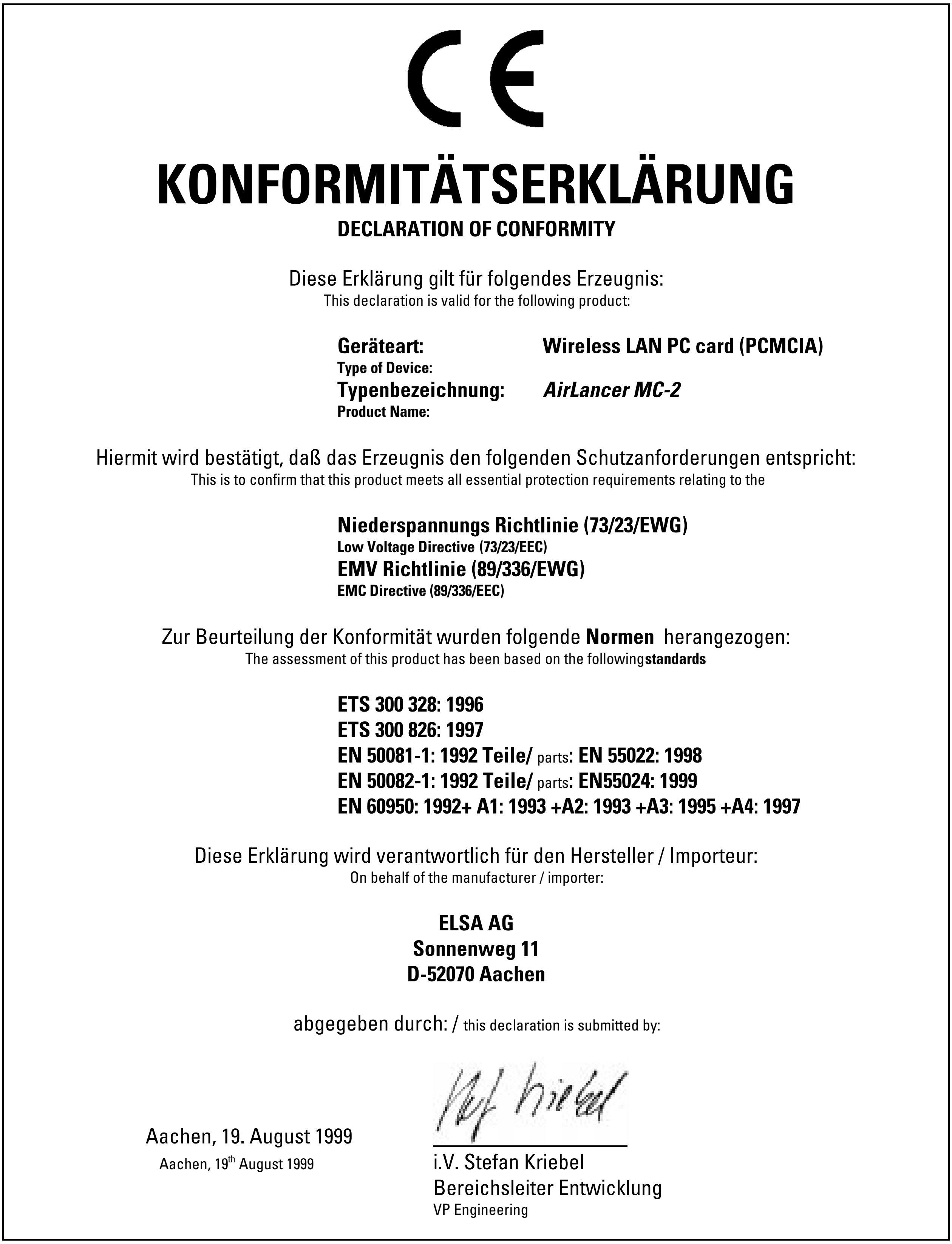
Diese Erklärung wird verantwortlich für den Hersteller / Importeur:
On behalf of the manufacturer / importer:

ELSA AG
Sonnenweg 11
D-52070 Aachen

abgegeben durch: / this declaration is submitted by:

Aachen, 19. August 1999
Aachen, 19th August 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, 19th August 1999

i.V. Stefan Kriebel
Bereichsleiter Entwicklung
VP Engineering

Index

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 networks in accordance with the IEEE 802.11 standard

The units of the *ELSA LANCOM Wireless* series comply with the IEEE 802.11 standard. This standard is a supplement of the existing IEEE standards for LANs, of which IEEE 802.3 for Ethernet is the best 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 32 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 a a base station, also known as an access point or distribution system. The *ELSA LANCOM Wireless* units were designed to serve as base stations. The base station 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 base station, and each station entering the network must log onto to the base station before being permitted to exchange data in the cell. The base station generally also fulfills the function of a “relay station” for data. While this reduces the achievable data rate, careful positioning of the base station can increase the size of a cell. The actual role of a base station, however, is the connection of a wireless cell to a wired Ethernet. If the base station receives a data packet for a workstation that is not logged onto it, it forwards the packet to the Ethernet. In the other direction, the base station “listens” to the Ethernet for data intended for wireless stations and forwards it accordingly. As all mobile stations must log onto the base station, the base station 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.

As mentioned earlier, an Ethernet backbone can also be used to extend the range of a wireless LAN. In this case, multiple base stations 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 base station with the strongest signal. Two mobile stations logged onto different base stations can thus communicate with one another even though they are not within direct radio range. The Ethernet linking the base stations closes the gap.

If a station continues to monitor the radio situation after logging on, it can determine the relative signal strengths of the base stations and automatically switch over to the strongest base station 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 802.11 devices from other manufacturers. However, as the 802.11 standard is relatively new and many manufacturers are only just making the transition from proprietary wireless LAN solutions to 802.11, interoperability cannot be guaranteed at all times. 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).

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.

Packets Cells

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

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

Host

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

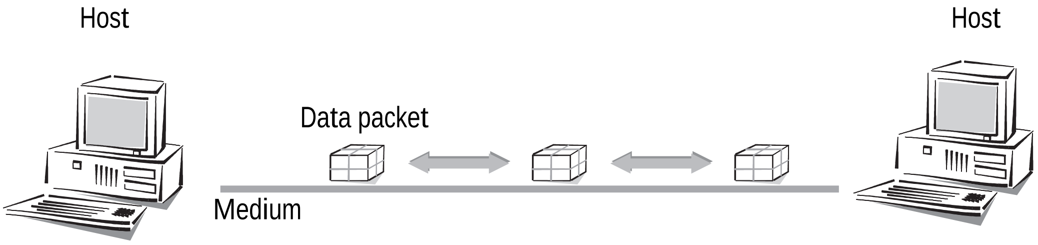
Router

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.

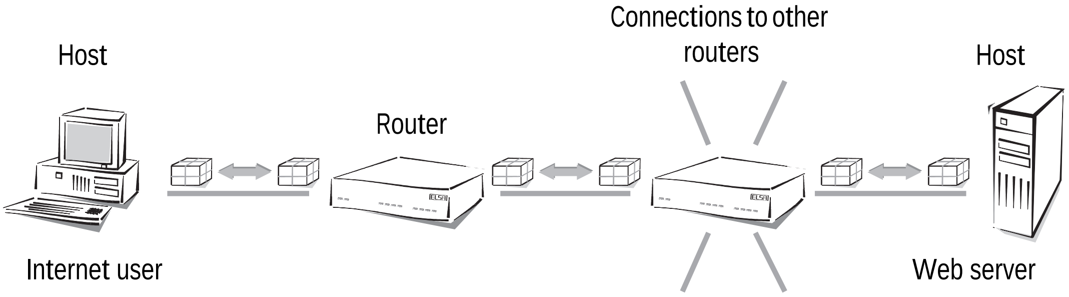
Connection modes

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).



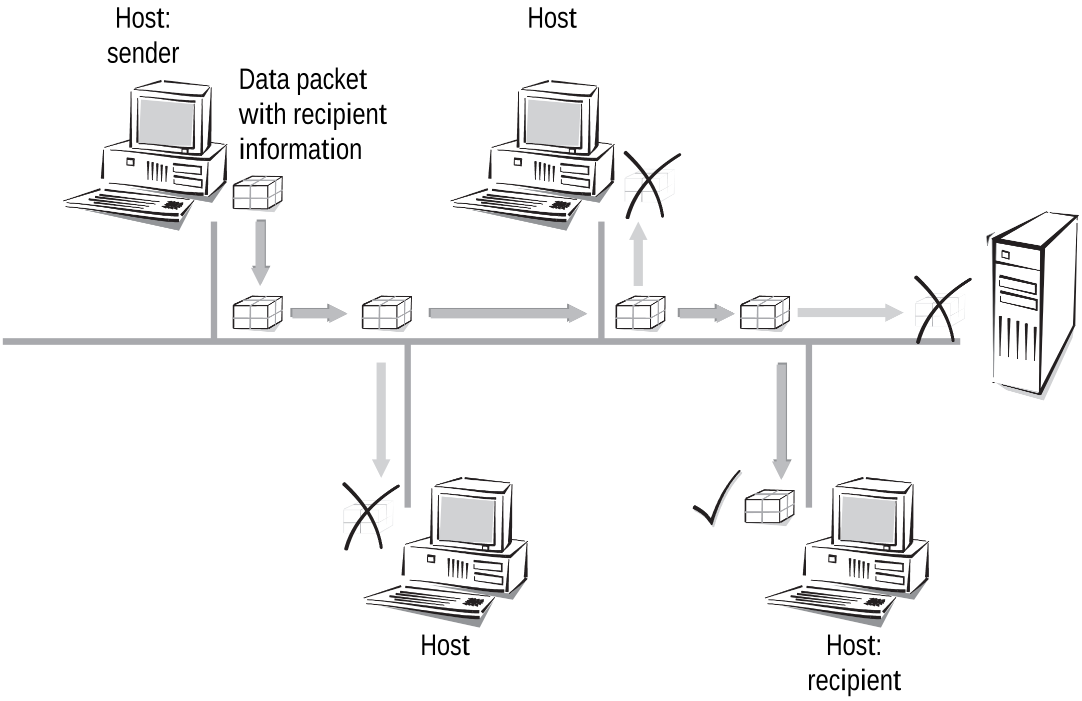
Access to the Internet is also established through point-to-point connections. Even though the data packets are sent from the host at the Internet user to the host at the Internet provider (server) via several routers, every data packet still has its own specific destination. Furthermore, the routers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



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

Point-to-multipoint connection

Generally speaking, it would be uneconomical to directly connect all computers in a network via point-to-point 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

Protocol 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”.

TCP/IP The most broadly distributed network protocol is the TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol). It is used mainly in the Internet, but nowadays more and more company networks use it. Examples of other network protocols are IPX or Apple Talk. Because of its wide use, this chapter deals mainly with the TCP/IP.

IP network 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.

Internetwork Internet 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.

Local network (LAN) A network covering a limited area with hosts on the same hierarchical level and using the same medium (shared medium) is called a local network (**L**ocal **A**rea **N**etwork, LAN).

IP addressing

Packet-oriented transfer 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 254x254 = 64.516 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

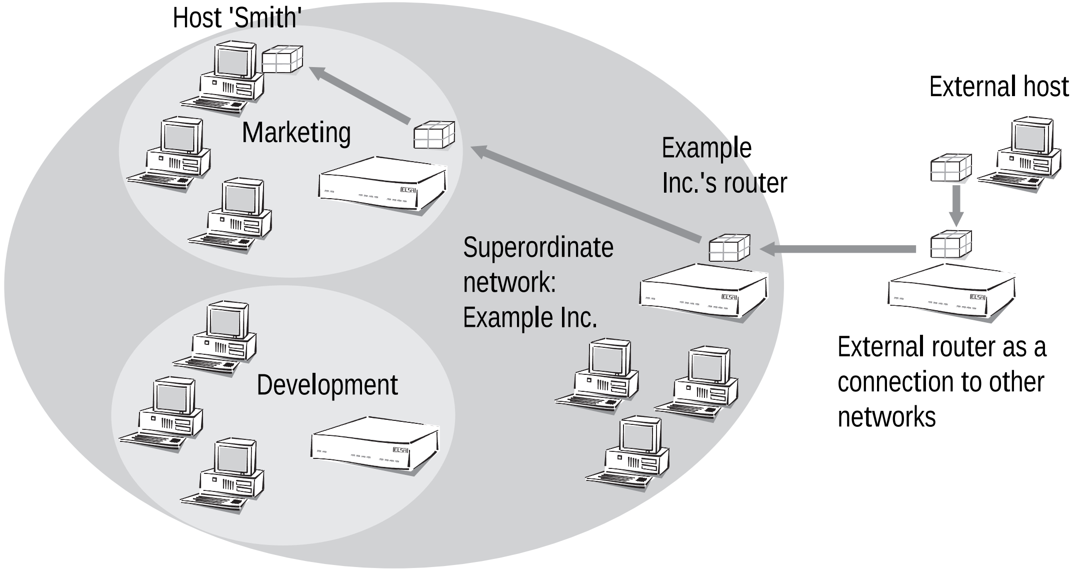
Every router manages a table (routing table). This table indicates the quickest interface connection to the host for every host in the network. You can imagine that, as they grow, these tables may exceed the capacity of the router—the Internet, as a worldwide linking up of publicly accessible IP computers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


Host 'Smith'
Marketing
Development
Example Inc.'s router
Superordinate network: Example Inc.
External host
External router as a connection to other networks

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, MAC) for the avoidance and resolution of such collisions.

LAN and IP network

The connection of all computers communicating through a shared medium using a MAC protocol is called a LAN (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. LAN refers to a limitation of the area covered by the network, not a restriction of the number of workstations connected to it.

MAC-address

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

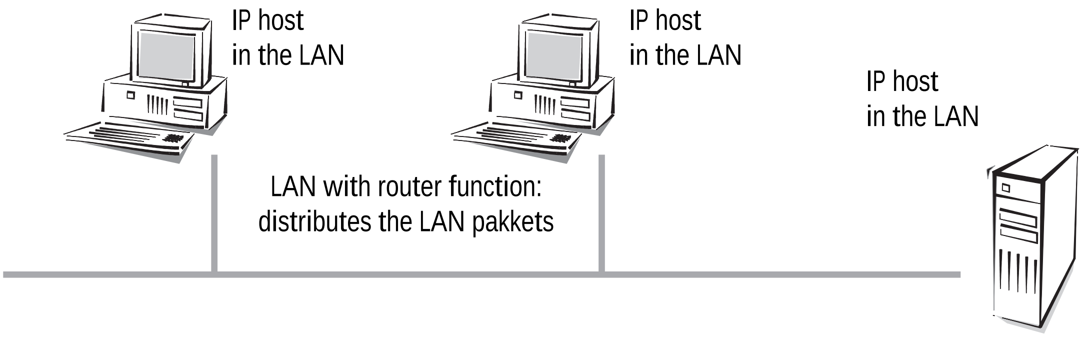
MAC addresses are independent of IP addresses. An IP host whose interface works through a LAN has an IP and a MAC address. Whereas the structure of IP addresses with its similarity to postal addresses is supposed to simplify routing in enormous IP networks, the fingerprint-like MAC addresses are designed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

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

IP in the LAN

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

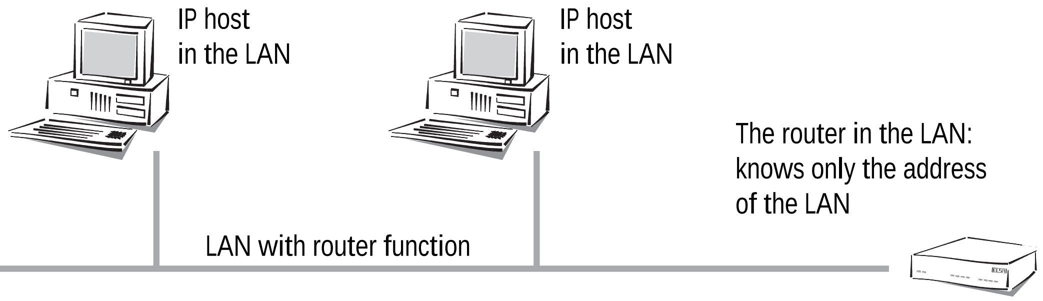
To an IP host, a LAN behaves as if it were an independent network with a router. The hosts gives the packets to the LAN which handles the further distribution of the data packet. This is why only IP addresses from the numerical space of the specific network should be used for the internal communication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

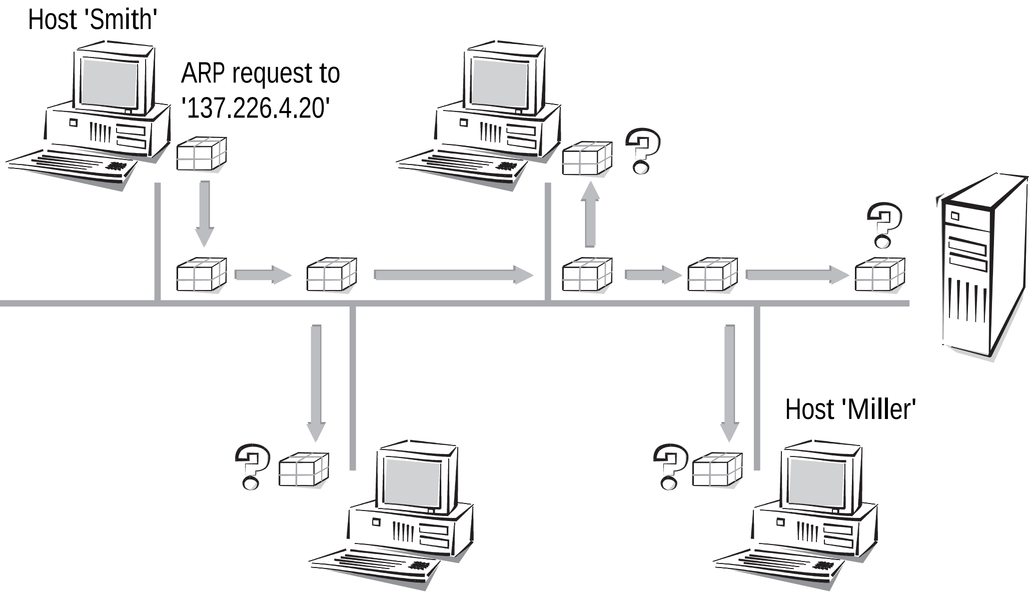
Let's use an example to explain this. Imagine the hosts of the subnet in the marketing division are linked via a LAN. The hosts have IP addresses from the numerical space '137.226.4.1' to '137.226.4.254' (the addresses '137.226.4.0' and '137.226.4.255' are reserved), the network address is '137.226.4.0' 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.

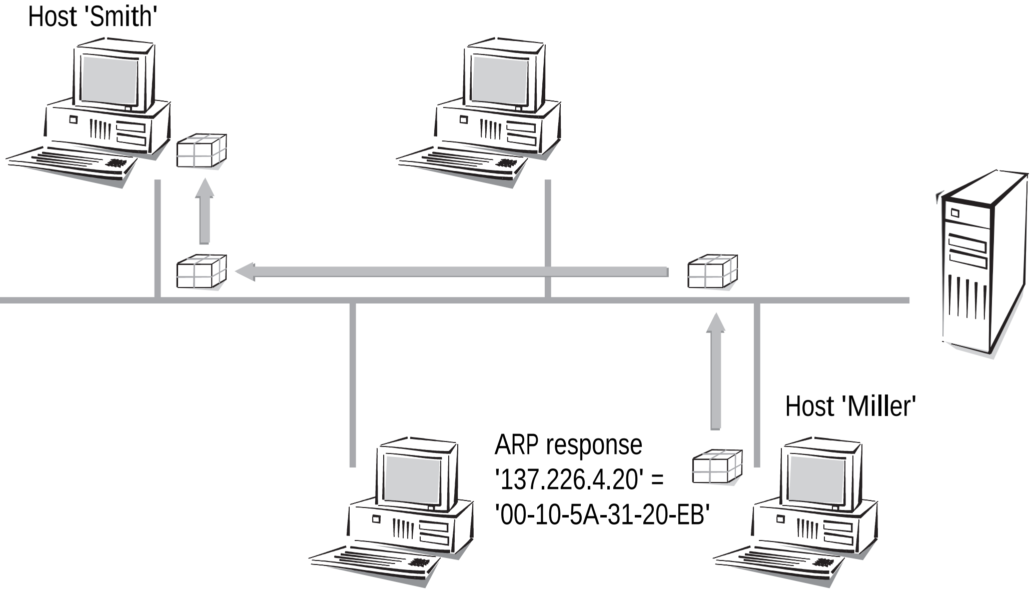
This is why every host has to manage a table that translates IP addresses to MAC addresses. But how do the entries end up in the table? They could be entered manually, but that would not satisfy the objective of making the connecting of a new computer to the LAN as easy as possible.

ARP

Therefore the LAN has a special mechanism that automates this process: the **A**ddress **R**esolution **P**rotocol, ARP. The table itself is called the ARP table. Whenever a host does not find an entry in the table for a particular IP address (in our example '137.226.4.20'), it sends an ARP request packet to all hosts in the LAN (with the LAN broadcast address as a target address).



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

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

Symbols

📁	Menu	Indicates a further submenu.
ℹ	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.
▦ℹ	Info table	Indicates a table whose entries cannot be modified.
Action	Action	Performs an action.

Overview of the menus

- **Setup**
  - Name
  - LAN-module
  - TCP-IP-module
  - SNMP-module
  - DHCP-module
  - Config-module
  - WLAN-module
- **Firmware**
  - Version-table
  - Table-firmsafe
  - Mode-firmsafe
  - Timeout-firmesafe
  - Firmware-upload
  - Test-firmware
- **Status**
  - Current-time
  - Operating-time
  - WLAN-statistics
  - LAN-statistics
  - TCP-IP-statistics
  - Config-statistics
  - Queue-statistics
  - PCMCIA-status
  - Delete-values
- **Other**
  - 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
Current-time	ℹ	Current time in device
Operating-time	ℹ	Period of time the device has operated since it was last switched on
LAN-statistics	📁	Displays LAN statistics
TCP-IP-statistics	📁	Statistics from the TCP/IP area
Config-statistics	📁	Remote configuration statistics
Queue-statistics	📁	Statistics relating to the packets in the queues of the individual modules
Delete-values	Action	Deletes all values except tables with substatistics.

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/WLAN-statistics

The current status of the WLAN interface is described here.

LAN-rx-packets	ℹ	Number of data packets received
LAN-tx-packets	ℹ	Number of data packets sent
LAN-rx-errors	ℹ	Number of data packets incorrectly received
LAN-tx-errors	ℹ	Number of data packets incorrectly sent
LAN-stack-errors	ℹ	Number of packets without a suitable receive module (bridge/ router)
LAN-queue-packets	ℹ	Number of buffers in use
LAN-queue-errors	ℹ	Number of packets discarded due to a lack of buffers
LAN-rx-bytes	ℹ	Number of bytes received from the LAN
LAN-tx-bytes	ℹ	Number of bytes sent to the LAN
LAN-rx-broadcasts	ℹ	Number of broadcast packets received from the LAN
LAN-rx-multicasts	ℹ	Number of multicast packets received from the LAN
LAN-rx-unicasts	ℹ	Number of directly addressed packets received from the LAN
LAN-Tx-broadcasts	ℹ	Number of broadcasts received from the WAN
LAN-Tx-multicasts	ℹ	Number of multicasts received from the WAN
LAN-Tx-unicasts	ℹ	Number of unicasts received from the WAN
LAN-repeats	ℹ	Number of packets that were repeated before being received successfully
LAN-multiple-repeats	ℹ	Number of packets that were repeated several times before being received successfully
BSSID	ℹ	Numerical cell identifier; numerical translation of the WLAN domain name. In infrastructure mode this is always identical with the MAC address of the base station
Phy-channel	ℹ	The radio channel currently being used by the base port.
LAN-Ready	ℹ	Successful initialization of the wireless network adapter.
Station table	▦ℹ	Display of the mobile stations currently logged on.

Station table

This table displays information on the individual mobile stations:

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.
State	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.

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	ℹ	Number of data packets received
LAN-tx-packets	ℹ	Number of data packets sent
LAN-rx-errors	ℹ	Number of data packets incorrectly received
LAN-tx-errors	ℹ	Number of data packets incorrectly sent
LAN-stack-errors	ℹ	Number of packets without a suitable receive module (bridge/ router)
LAN-NIC-errors	ℹ	Number of data packets discarded by the NIC
LAN-heap-packets	ℹ	Number of buffers available
LAN-queue-packets	ℹ	Number of buffers in use
LAN-queue-errors	ℹ	Number of packets discarded due to a lack of buffers
LAN-collisions	ℹ	Number of collisions during a send procedure
Connection -established	ℹ	Display of correct Ethernet connection (data transfer possible). Corresponds to the 'Link' LED on the device.
Negotiation -complete	ℹ	The negotiation of the transfer mode between the router and the remote station is complete. This is only relevant if Setup/LAN/Connection is set to 'Auto'.
Connect	ℹ	The preselected LAN connection is fixed at 10Base-T. See Setup/LAN-/connection.
LAN-rx-bytes	ℹ	Number of bytes received from the LAN
LAN-tx-bytes	ℹ	Number of bytes sent to the LAN
LAN-rx-broadcasts	ℹ	Number of broadcast packets received from the LAN

/LAN-statistics		Running status displays
LAN-rx-multicasts	ℹ	Number of multicast packets received from the LAN
LAN-rx-unicasts	ℹ	Number of directly addressed packets received from the LAN
WAN-rx-broadcasts	ℹ	Number of broadcasts received from the WAN
WAN-rx-multicasts	ℹ	Number of multicasts received from the WAN
WAN-rx-unicasts	ℹ	Number of unicasts received from the WAN
Delete-values	Action	Deletes LAN statistics

Status/TCP-IP-statistics

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

TCP-IP statistics		Statistics from the TCP/IP area
ARP-statistics	📁	Statistics from the ARP area
IP-statistics	📁	Statistics from the IP area
ICMP-statistics	📁	Statistics for ICMP packets
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
Delete-values	Action	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-service-errors	Number of IP packets received from the LAN for an incorrect service
IP-WAN-rx	Number of IP packets received from the WAN
IP-WAN-tx	Number of IP packets sent to the WAN
IP-WAN-checksum-errors	Number of IP packets incorrectly received from the WAN
IP-WAN-service-errors	Number of IP packets received from the WAN for an incorrect service
IP-WAN-rx-disconnect	Number of packets from the WAN discarded by timeout
Delete-values	Deletes IP statistics

Status/TCP-IP-statistics/ICMP-statistics

These statistics include the following values:

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

Status/TCP-IP-statistics/TCP-statistics

These statistics include the following values:

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

Status/TCP-IP-statistics/TFTP-statistics

These statistics include the following values:

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

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

Status/TCP-IP-statistics/DHCP-statistics

These statistics include the following values:

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

Table-DHCP

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

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

Status/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	ℹ	Current number of active configuration connections from the LAN
LAN-total-connections	ℹ	Total number of configuration connections from the LAN up until the present
WAN-active-connections	ℹ	Current number of active configuration connections from the WAN
WAN-total-connections	ℹ	Total number of configuration connections from the WAN up until the present
Outband-active-connections	ℹ	Current number of active outband configuration connections
Outband-total-connections	ℹ	Total number of previous outband configuration connections up until the present
Outband-bitrate	ℹ	Bit rate of the last outband configuration session
Login-errors	ℹ	Total number of defective logins
Login-locks	ℹ	Number of login locks
Login-rejects	ℹ	Number of login attempts while the login lock was active
Delete-values	Action	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	ℹ	Number of buffers available
LAN-queue-packets	ℹ	Number of buffers in use
WAN-heap-packets	ℹ	Number of buffers available

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

Status/PCMCIA-status

General information on the inserted card can be found here:

LAN adapter present	ℹ	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	ℹ	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	ℹ	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
LAN-module	📁	LAN settings
TCP-IP-module	📁	TCP/IP module settings
SNMP-module	📁	Settings for configuration via SNMP
DHCP-module	📁	DHCP server settings
WLAN-module	📁	Wireless network settings
Config-module	📁	Configuration 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\nname ?
```

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/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	ℹ	MAC layer address of the device
Spare-heap	📂	Buffers that receive data packets from the local network

Connect

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

Connect	Meaning
Auto	Default setting, as the LAN connection is fixed at 10Base-T. This item does not require manual configuration.

ℹ

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

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

Node-ID

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

Spare-heap

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

Setup/TCP-IP-module

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

TCP-IP-module		TCP/IP module settings
State	📂	Activates or deactivates the TCP/IP module.
IP-address	📂	Local IP address
IP-netmask	📂	Local network’s matching IP network mask

TCP-IP-module		TCP/IP module settings
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.	ℹ	Max. number of simultaneous configuration connections to the *ELSA LANCOM*

Operating

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

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

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 TFT 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.

DNSDNS-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/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	Action	Command to set a destination address to which the traps are to be sent
Delete-monitor	Action	Command to delete an address that was set with 'Register-monitor'
Monitor-table	▦ℹ	Table with all currently active destination addresses that were set with 'Register-monitor'

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

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

Administrator
Administrator's name

Location
Device location

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

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

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

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

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

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

Monitor-table
The monitor table has the following structure:

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

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

Setup/DHCP-server-module

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

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

State

On: The device operates as a DHCP server

Off: The device does not operate as a DHCP server

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

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

Start-address-pool End-address-pool

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

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

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

A valid address is then taken from the pool for the IP address. If the computer was already assigned an IP address at some point in the past, it requests this same address and the DHCP server attempts to reassign it this address if it has not already been assigned to another computer.

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

Netmask

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

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

Broadcast

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

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

Max.-lease-time-minute(s)

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

The DEFAULT value of 6000 minutes equals approximately 4 days.

Default-lease-time-minute(s)

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

The DEFAULT value of 500 minutes equals approximately 8 hours.

Table-DHCP

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

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

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

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

  – **new**: The computer has made its initial request. The DHCP server verifies the uniqueness of the address that is to be assigned to the computer.

- **unkn.**: While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the DHCP server has no means of obtaining additional information on this computer.
- **stat.**: A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.
- **dyn.**: The DHCP server assigned an address to the computer.

Setup/Config-module

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

/Config-module		Configuration module settings
LAN-config	📂	Switch for configuring from the LAN side
WAN-config	📂	Switch for configuring from the WAN side
Password-required	📂	Password required on/off if there is no password
Farconfig-(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/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. *Not all channels are permitted in all countries (please see the table of radio channels in the Appendix).*
Packet size	📁	A value between 600 and 1600 that states the maximum size of WLAN packets in bytes. The default setting is 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. *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.*
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 *In this case as well, traffic is blocked between WLAN stations and the LAN or WAN, but not between the WLAN stations themselves. See protocol table in the Appendix*
Protocol mode	📂	Positive/negative switch for the protocol list
Node ID	ℹ	MAC layer address of the device
Spare-heap	📂	Buffers that receive data packets from the local network

Firmware

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

/Firmware		Display and keyboard settings
Version-table	▦ℹ	Displays hardware releases and serial numbers for the router
Table-firmsafe	▦ℹ	Information on the two firmware versions stored in the device and on the bootloader.
Mode-firmsafe	📂	Firmware activation mode
Timeout-firmesafe	📂	Time in minutes required to test new firmware
Test-firmware	Action	Tests the inactive firmware
Firmware-upload	Action	Initiates a firmware upload

Version table

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

Ifc	Module	Version	Serial number
Ifc	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.
```

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
Boot-system	Action	Boots the device.
Reset-system	Action	Resets to factory settings.
System-upload	Action	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.

TCP/IP Protocols

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
www	80	tcp

Capab.	Port no.	Protocol
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
nbsession	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

Capab.	Port no.	Protocol
sytek	500	udp
biff	512	udp
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
rvd-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

Capab.	Port no.	Protocol
acctdisk	707	udp
kerberos	750	tcp
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

Capab.	Port no.	Protocol
rscsb	10011	udp
qmaster	10012	tcp
qmaster	10012	udp