

ELSA LANCOM™ Wireless L-II

© 2000 ELSA AG, Aachen (Germany)

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

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

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

You can find all declarations and approvals for the products, as long as they were available at the time of publication, in the appendix of this documentation.

Trademarks

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

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

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

ELSA AG

Sonnenweg 11

52070 Aachen

Germany

www.elsa.com

Aachen, October 2000

Preface

Thank you for placing your trust in this ELSA product.

Wireless networks from ELSA are economical alternatives or additions to local wired networks (LANs). Notebooks and PCs can use mobile network cards to communicate with one another or access wired networks via access points and can even be integrated into the high-speed Internet via the DSL firmware option.

Documentation

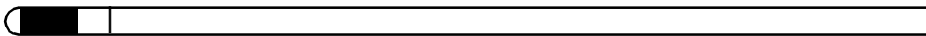
The accompanying documentation comprises:

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

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

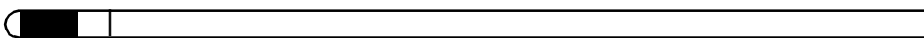


The KnowledgeBase can also be found on the CD. Just open the file `Misc\Support\MISC\ELSA\SIDE\index.htm`.



Contents

1 Introduction	7
1.1 The basic functions of a wireless network	7
1.2 Operating modes	8
1.3 What does the <i>ELSA LANCOM Wireless L-11</i> offer?	10
2 Installation	15
2.1 Package contents	15
2.2 System requirements	15
2.3 Install TCP/IP on your workstation	16
2.3.1 Windows 95 and Windows 98	16
2.3.2 Windows NT 4.0	17
2.3.3 Windows 2000	19
2.4 Introducing the <i>ELSA LANCOM Wireless L-11</i>	21
2.4.1 The front of the unit	21
2.4.2 The bottom of the unit	22
2.5 How to connect the device	23
2.6 Software installation	23
2.7 Quickstart	23
2.7.1 The Wizards	24
2.7.2 Basic settings	25
3 Configuration and management	31
3.1 Radio or wired: Configuration approaches	31
3.2 Configuration using <i>ELSA LANconfig</i>	31
3.3 Configuration with <i>ELSA WEBconfig</i>	32
3.4 Configuration using Telnet	33
3.5 Configuration using SNMP	34
3.6 New firmware with FirmSafe	34
3.6.1 This is how FirmSafe works	34
3.6.2 How to load new software	35
3.7 What's happening on the line?	37
3.8 <i>ELSA LANmonitor</i>	37
3.9 DSL firmware for <i>ELSA LANCOM Wireless</i>	38



4 Operating modes and functions	41
4.1 Establishing wireless connections	41
4.1.1 Considerations for setting up a wireless network	42
4.1.2 Ad hoc network (peer-to-peer)	42
4.1.3 Infrastructure network	43
4.1.4 Point-to-point network	44
4.1.5 Wireless Internet gateway via DSL	44
4.2 Security for your configuration	45
4.2.1 Security for the device	45
4.2.2 Security for your WLAN	47
4.2.3 Security for your LAN	48
4.3 Call charge management	51
4.4 Automatic address administration with DHCP	52
4.4.1 The DHCP server	52
4.4.2 DHCP – 'on', 'off' or 'auto'?	53
4.4.3 How are the addresses assigned?	53
4.4.4 Configuring the DHCP server	57
4.5 Accounting	59
4.5.1 Configuring accounting	60
4.5.2 Reading the accounting data	60
5 Technical data	63
5.1 Power and ratings data	63
5.2 Radio frequency channels	64
6 Appendix	65
6.1 Declaration of conformity	65
6.2 General warranty conditions	66
7 Index	69

LANCOM Wireless reference manual on CD

1

Introduction

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

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

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

The WAN functions mentioned and described in this manual are only available after a firmware upgrade to the DSL version.



Notes on using wireless LAN devices

ELSA Wireless LAN products can use up to 13 radio frequency channels in a frequency band between 2400 MHz and 2483 MHz. The devices are approved for operation in all EU countries and Switzerland. Use of the devices is regulated throughout Europe by the 1999/5/EG guideline of the European Parliament and Council Directive of 9 March 1999 regarding Radio and Telecommunication Terminal Equipment (R&TTE) and the mutual approval of their conformity. Please observe the approved frequencies for individual countries as listed in the appendix.

ELSA is not responsible for disturbances or interference caused by unauthorized modifications made to the devices. ELSA will not be held liable especially for the consequences of connecting external antennas or cables that are not explicitly designed for use with *ELSA LANCOM Wireless* and *Air-Lancer* devices.

See the appendix for more information on CE conformity.

1.1

The basic functions of a wireless network

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

*Wireless network
adapters WLAN*

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

Access point

Furthermore, the access point forms the bridge between LAN and WLAN. The ELSA access point also can function as an Internet router or a wireless bridge between two ethernet LANs. It has a slot for a wireless network adapter (*ELSA AirLancer MC-11*) as well as a normal Ethernet connection on the other side to exchange data between the two networks.

Radio cell

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

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

1.2

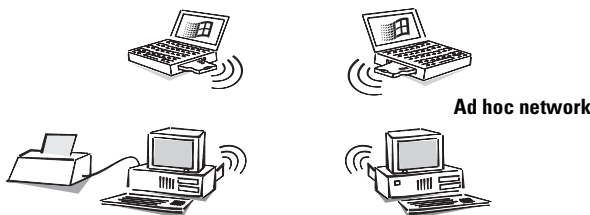
Operating modes

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

- Ad hoc network (peer-to-peer)
- Infrastructure network
- Wireless bridge
- Wireless LAN + DSL gateway

*Direct PC
connection*

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

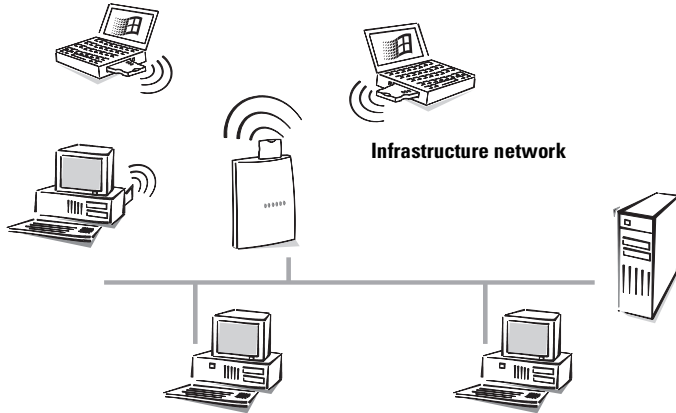


Ad hoc network

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

Infrastructure network

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

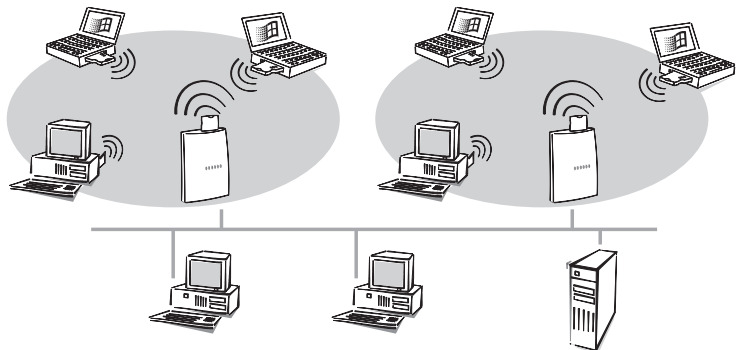


A wireless network with a access point is also referred to as an infrastructure network.

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

Roaming

Multiple access points can be used if the range of a cell is not sufficient to link all mobile stations. This makes it possible to switch from one wireless cell to another without interrupting the connection to the network.



Radio cells can also overlap to ensure good coverage. Different channels (up to 13 channels are available) can be selected to prevent interference between the cells.

1.3

What does the *ELSA LANCOM Wireless L-11* 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 *LANCOM Wireless* to the power supply.
- Establish a link to the LAN.
- Connect to a DSL port.
- Switch it on.
- Go!

LAN connection

Access points for wireless networks by function in ELSA Ethernet environments. Use the 10Base-T connection and a hub or switch to connect the *ELSA LANCOM Wireless L-11* to a 10 Mbit LAN or to a DSL modem.

DSL connection

With special DSL firmware (on CD-ROM), you can connect your *LANCOM* to a DSL modem (such as the T-DSL network offered by Deutsche Telekom). Instead of connecting to the Ethernet, you can have quick access to the Internet. This procedure can be switched in both directions by using the corresponding firmware.

Configuration

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

The management tool *WEBconfig* is just as easy to use. It allows you to access the configuration of the *ELSA LANCOM* access point or even load new firmware using any HTML browser. Furthermore it is possible to access device configuration via SNMP and TFTP.

Access to the device is possible from a WLAN or LAN. SNMP is supported as well as TFTP.

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

FirmSafe

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

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

Wireless and secure with WEP

The WEP (**W**ired **E**quivalent **P**rivacy) encryption method attaches a 40-bit or 128-bit key to the wireless data. The data encryption and authentication of the stations makes it as good as impossible for the data in transit to be intercepted. This ensures a considerably higher level of data security in wireless network operation. Additionally, station filters based on MAC addresses make it possible to allow or deny individual stations access to the access point.

ELSA LANmonitor

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

- Name of the remote site
- Connection duration and transmission rates
- Excerpts of the device statistics (e.g. PPP negotiation data)

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

AirLancer Client Manager

The *ELSA AirLancer Client Manager* is included with the *AirLancer* cards and provides software tools for configuring *AirLancer* adapters and monitoring and diagnosing wireless networks. The wireless connection of WLAN clients to the access point is continuously monitored, and the current status is also displayed. You have a choice of the following:

- Set the wireless parameters and user profiles
- Monitor and analyze the wireless network (site survey)
- Display the available access points
- Carry out tests and diagnostics on the card
- Monitor the signal strength
- Assign the WEP encryption key

Refer to the online help file for detailed information on the *ELSA AirLancer Client Manager*.

Status displays

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

Statistics

The comprehensive statistics function lets you keep track of your *ELSA LANCOM Wireless L-11*. These statistics give you all the information you need on the data packets transferred, for example, so that you can optimize the configuration of your device.

DHCP

Your *LANCOM* provides the following DHCP modes:

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

With its factory-preset configuration, the device operates using a sophisticated automatic mode, which makes it extremely easy to get the *LANCOM* running either on an existing network or a new network.



DNS server

This function is only supported by the DSL firmware.

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

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

Routing: Line connection and management

The router checks all data on the network to determine whether they have to be sent to another network or computer. If data transfer is necessary, the router establishes the connection itself and closes the connection once the transfer is complete. Any partly used call charge units are used up fully if call charge information is transmitted during the connection.

To reduce transfer costs, the router offers various filter options depending on the mode of operation. These filters can be used to exclude data from being transmitted to all or part of the network. Data that belongs to specific services (e.g. printing services) can also be excluded from transfer.

NetBIOS proxy

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

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

Accounting

Most data transfers through the ELSA router take place via dial-up connections, where the charges are calculated based on the online time, or via static connections, where the charges are calculated based on the transferred data volume. Only a small portion of users use true leased-line connections with flat-rate charging.

For many users it is important to determine which of the immediate LAN computers use the connection to the router and what charges they incur.

With its accounting feature, *ELSA LANCOM Wireless L-11* offers the ability to breakdown online times and data transfer volumes for ISDN and DSL connections based on the individual computers that use the connections. This allows you to determine the incorrect configuration of the computer or router quickly and allocate the resulting expenses to their appropriate causes.

Roaming

The roaming feature lets you construct bigger wireless networks using any number of access points. When stations switch from one wireless cell to another while connected, they are automatically logged off of the previous access point and logged onto the next.

2 Installation

This section will help you to connect 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 quickly.

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

2.1 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-11*
- *ELSA AirLancer* wireless network adapter with integrated antenna (already in the access point)
- Power adapter
- LAN connector cable
(also suitable when connecting to a DSL modem)
- Documentation
- CD containing *ELSA LANconfig*, other software and electronic documentation

If anything should be missing, please contact your dealer.

2.2 System requirements

PCs that are to communicate with a *LANCOM Wireless* access point have to meet the following minimum requirements:

- The TCP/IP protocol must be installed.
- A web browser must be installed (for HTML configuration).
- An *ELSA AirLancer* or other ethernet card has to be installed.

Several programs and drivers, such as ELSA LANconfig require a Windows operating system.



2.3

Install TCP/IP on your workstation

To establish a connection to a *ELSA LANCOM* access point for the first time, the TCP/IP protocol has to be set up. The following describes how to install this protocol on various operating systems.

2.3.1

Windows 95 and Windows 98

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

- Installing TCP/IP

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

- Allocate IP addresses (using DHCP)

If you are going to use the router as a DHCP server, set the workstations to obtain IP addresses automatically: **Start ► Settings ► Control panel ► Network ► TCP/IP ► Properties ► IP address ► Automatically receive IP address**. Also, delete any existing entries for DNS servers and gateways (found under the 'Gateway' and 'DNS Configuration' tabs). When the computer is restarted, it then searches for a DHCP server on the network and lets it assign an IP address to it.

- Setting fixed IP addresses (not using DHCP)

If you are not going to use a DHCP server on your network, assign the workstations fixed IP addresses: **Start ► Settings ► Control panel ► Network ► TCP/IP ► Properties ► IP address ► Determine IP address**.

Assign unique IP addresses, for example taken from a reserved range of addresses. For example, the workstations can be assigned addresses from '10.1.1.2' to '10.1.1.253', the router can be given '10.1.1.1' and all can have the subnet mask of '255.255.255.0'. To test whether or not a specific IP address, such as '10.1.1.1', is free, enter `ping 10.1.1.1` in a DOS session. If you do not receive a response, the address is most likely free.

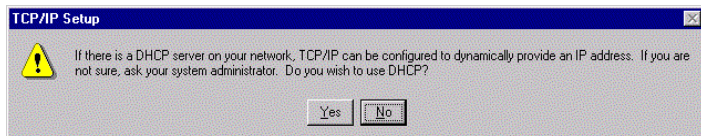
- Entering the gateway and DNS server (not necessary when using DHCP)
On the workstation computers, specify the address of the local network router as the gateway and as the Domain Name Server (DNS server):
Start ► Settings ► Control panel ► Network ► TCP/IP ► Properties ► Gateway and DNS configuration. Also enter a host name on the DNS configuration page. In doing so, use the name of the PC, which ideally matches the user's name, to maintain a certain amount of consistency.
- Checking the IP configuration
Under Windows 95 and Windows 98, you can view the current IP configuration of your computer with by using **Start ► Run ► winipcfg.** Among other information, this shows you which IP address was assigned to the computer by the DHCP server and which addresses have been specified for DNS servers and the gateway.

2.3.2

Windows NT 4.0

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

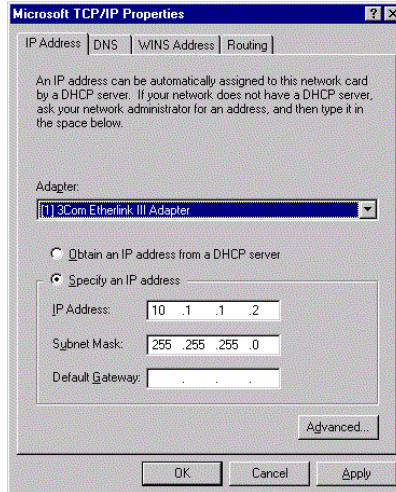
- Installing TCP/IP
To install TCP/IP, click **Start ► Settings ► Control Panel ► Network ► Protocols ► Add.** Select the 'TCP/IP protocol' network protocol.
- Allocate IP addresses (using DHCP)
If you are going to use the router as a DHCP server, set the workstations to obtain IP addresses automatically. To do so, select **Yes** when completing the network protocol installation.



Windows then copies the required files and, when finished, requests you to reboot.

- Setting fixed IP addresses (not using DHCP)

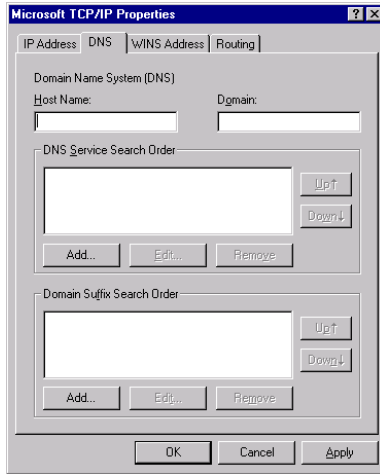
If you are not going to use a DHCP server on your network, assign the workstations fixed IP addresses: **Start ► Settings ► Control Panel ► Network ► Protocols ► Properties**. This tab also lets you set the standard gateway.



Assign unique IP addresses, for example taken from a reserved range of addresses. For example, the workstations can be assigned addresses from '10.1.1.2' to '10.1.1.253', the router can be given '10.1.1.1' and all can have the subnet mask of '255.255.255.0'. To test whether or not a specific IP address, such as '10.1.1.1', is free, enter `ping 10.1.1.1` in a DOS session. If you do not receive a response, the address is most likely free.

- Entering the DNS server (not necessary when using DHCP)

On the workstation computers, specify the address of the local network router as the Domain Name Server (DNS server) on the 'DNS' tab. Also enter a host name on the DNS configuration page. In doing so, use the name of the PC, which ideally matches the user's name, to maintain a certain amount of consistency.



● Checking the IP configuration

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

2.3.3

Windows 2000

With Windows 2000, helpful hardware setup wizards provide support when you install the new hardware. If your network card is not detected during system startup, launch the hardware wizard by selecting

Start ► Settings ► Control Panel ► Add/Remove Hardware.

- ① Select to search for new hardware and then select the 'Add a new device' from the list that follows and click **Next >**.
- ② The search should detect the network card. Click again **Next >**. The system then configures the new hardware and a LAN connection.
- ③ To verify the new LAN connection, open its window by selecting

Start ► Settings ► Network and Dialup Connections

From there, click the connection with the right mouse button and open its properties.

- ④ The dialog that appears contains a list box containing the installed network components. TCP/IP should be listed in any case.
- ⑤ Select its entry and click the **Properties...** button.

This opens a dialog where you can define all of the properties for this network protocol. The procedures for setting address, DHCP, gateway and DNS are the same here as in Windows 98.

2.4

Introducing the *ELSA LANCOM Wireless L-11*

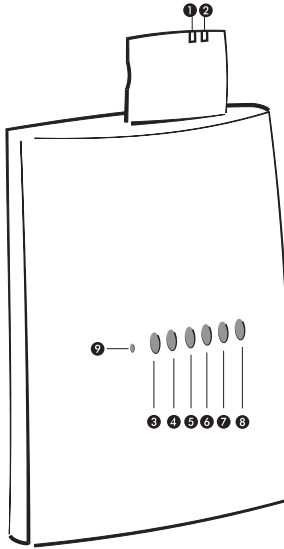
This section introduces the unit's hardware. It covers the unit's display elements and connection options.

2.4.1

The front of the unit

LEDs

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



- 1** This LED shows the send and receive status of the card:
 - ☐ Off – no wireless activity
 - ☐ Blinking – wireless data being sent or received
- 2** The second LED indicates the card's operating mode:
 - ☐ Lit green – standard mode
 - ☐ Blinking green – the card is in energy-saving mode

- 3 The 'Power/Msg' LED on the access point lights up briefly when the power is switched on. After the self-test, either an error is output by a flashing light code or the device starts and the LED remains lit.

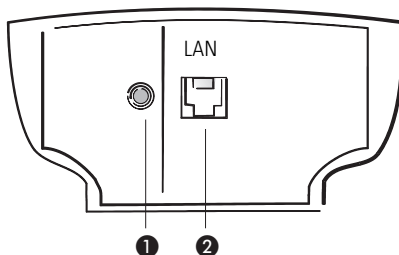
off		Device off
green	1 x short	Boot procedure (test and load) started
green	flashing	Display of a boot error (flashing light code)
green		Device ready for use

- 4 The 'WLAN link' LED on the access point indicates activity on the wireless network.
- 5 The 'LAN-Rx' on the access point indicates data activity received on the LAN.
- 6 The 'LAN-Tx' on the access point indicates data activity sent on the LAN.
- 7 The 'LAN Collision' LED on the access point indicates data collisions on the LAN.
- 8 The LED 'LAN link' on the access point indicates data activity in the Ethernet network.
- 9 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.

2.4.2

The bottom of the unit

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



- 1 Connection for power supply unit

② 10Base-T network connection

2.5

How to connect the device

- ① Connect your *ELSA LANCOM Wireless L-11* to the LAN. Plug the network cable (supplied) into the 10Base-T terminal of the device and into a free network connector on your local network (or into a free socket on a hub in your LAN). Connect your *ELSA LANCOM Wireless L-11* to the LAN. Plug the network cable (supplied) into the 10Base-T terminal of the device and into a free network connector on your local network (or into a free socket on a hub in your LAN). The cable for the LAN connector is labeled with a colored bend-proof protector.
- ② Connect the AC adapter to the device and switch it on. After a short device self-test the 'Power/Msg' LED will be permanently lit. The 'LAN Link' LED indicates that your router is correctly connected to the LAN.

2.6

Software installation

The *ELSA LANconfig* configuration software for Windows operating systems enables you to set up your router easily and conveniently for the desired application. To use it, first install *ELSA LANtools* from the CD onto your system. With other operating systems, you can use *ELSA WEBconfig* in an HTML browser to carry out the configuration.

You will need a Windows PC on the LAN to run *ELSA LANconfig*. ELSA also provides a Linux version of *ELSA LANconfig* which can be downloaded from their website.

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

2.7

Quickstart

The following steps should help you get your device running quickly and easily. Choose from three different installation scenarios:

The TCP/IP protocol is installed on the system and there is no DHCP server on the LAN

In this case, the *LANCOM* activates the DHCP server in automatic mode. It assigns IP addresses in the range of 10.x.x.x. You can assign a fixed IP address to the *LANCOM* or let it be assigned automatically. In the later case, the *LANCOM* is assigned the address 10.0.0.1.

The TCP/IP protocol is installed on the system and there is already a DHCP server on the LAN

The *LANCOM* acquires its IP address from the DHCP server on the LAN. *LANconfig* finds the *LANCOM* at its address. The setup wizard asks for a static IP address. Because the address is previously unknown, you cannot access the *LANCOM* using *WEBconfig*.

The TCP/IP protocol is installed on the system with a fixed IP address

In this case, *LANconfig* finds *LANCOM* at the client computer's address, which ends in 254 (x.x.x.254). The setup wizard asks for a static IP address.

2.7.1

The Wizards

The following wizards, which make it very easy to set up and configure the *ELSA LANCOM Wireless L-11*, are available in *ELSA LANconfig* and *ELSA WEBconfig*: Various wizards are offered, depending on whether your *ELSA LANCOM Wireless L-11* has only the standard network connection or whether the DSL option is installed:

- *ELSA LANCOM Wireless L-11* with network connection (standard)
 - Basic settings
 - Changing security settings
- *ELSA LANCOM Wireless L-11* with DSL option (optional)
 - Basic settings
 - Changing security settings
 - Setting up Internet access
 - Selecting the Internet provider

Wizards in *ELSA LANconfig*

- ① Start the software *ELSA LANconfig* with **Start ► Programs ► ELSA lan ► ELSA LANconfig**.
- ② Select your *ELSA LANCOM Wireless L-11* in the list of devices and call up the wizards.

Wizards in *ELSA WEBconfig*

- ① Launch your browser and enter the device's IP address, which you configured in the basic settings, into the address field. If you did not specify an IP address while carrying out the basic settings, the address is '10.0.0.1'.
- ② The start page provides links to the wizards.

The wizards guide you through the individual configuration steps. Each step is accompanied by an explanation of its values. The following provides a detailed description of the basic settings for the *ELSA LANCOM Wireless L-11*.

2.7.2

Basic settings

With the basic settings, you assign a name to the unit and define the IP addresses for operation in the local network.

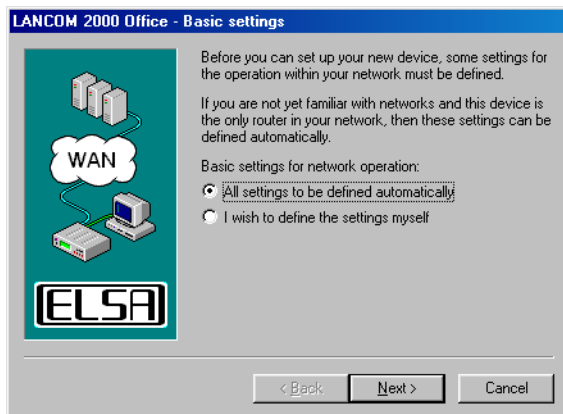
ELSA LANconfig

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

The start page for automatic configuration does not appear in all described cases. In some cases you are asked to enter an IP address in the next step (③).

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





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

- You have not yet used IP addresses in your network but would like to do so starting now. You are not concerned about the specific IP addresses that will be used. The router as a DHCP server will automatically set and assign the IP addresses for all devices in the network (LAN and WLAN).

or

- You do not 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 `winiipcfg` on the command line and click **OK**. If the next window shows the value '0.0.0.0' in the field 'IP address', the computer has never had an IP address.*



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

- ③ Select the option 'I wish to define the settings myself' if you are familiar with networks and IP addresses and one of the following conditions applies:

- You have not yet used IP addresses in your network but would like to do so starting now. However, you wish to set the IP address for the router and assign it an address from an address range reserved for

private use, e.g. '10.0.0.254' with the netmask '255.255.255.0'. At the same time you will set the address range that the DHCP server uses for the other devices in the network (so long as the DHCP server is not switched off).

- You have previously used IP addresses for the computers in your LAN. Assign the router a free address from the previously used address range, and select whether the router should run as a DHCP server or not.



You can find more information on the general structure of networks and setting IP addresses in the electronic documentation on the ELSA LANCOM CD.

- ④ Enter a password for access to the unit and choose whether to use it as a DHCP server on your LAN.



Disable 'Automatically configure workstations via DHCP' only if you want to use IP addresses on your network or already use another DHCP server. The functions of the DHCP server are described in this manual on CD.

ELSA WEBconfig

If you do not wish to or cannot use *ELSA LANconfig* (e.g. because you have installed a different operating system), you can configure the basic settings using a normal HTML browser.

- ① Start your browser.
 - If you do not yet have a DHCP or DNS server on your LAN, the router reacts to any name (like 'LANCOM' or 'Router') that you specify in the address field. The startup page will appear automatically.
 - If you already use a DHCP server or work with fixed IP addresses on your LAN, enter the address as 'x.x.x.254' in the browser's address field, where 'x.x.x' stands for the currently configured range of addresses.

From this point on, the procedure is the same as for the *ELSA LANconfig*.



Telnet

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.

Procedure example:

- ① Start the Telnet connection by clicking **Start ► Run** and entering
Telnet 10.0.0.254 on the command line.
- ② Set the IP address on the LAN/WLAN:

```
cd /setup/TCP-IP
set intranet-addr. 10.0.0.1
set intranet-mask 255.255.255.0
```

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

- ③ Set up DHCP

```
cd /setup/DHCP/
dir
set Condition on
```

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

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

3

Configuration and management

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

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

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

3.1

Radio or wired: Configuration approaches

Using a configuration via the network allows any computer on the WLAN or LAN to access the access point. However, you can restrict or block the access altogether by using the IP access list.

The configuration of *ELSA LANCOM Wireless L-11* requires the use of either *ELSA LANconfig* for Windows, *ELSA WEBconfig* or Telnet (supplied with most operating systems). *ELSA LANconfig* is supplied with your device. You can always obtain up-to-date releases from our online media.

3.2

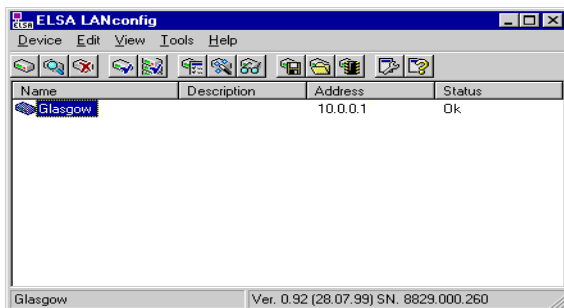
Configuration using *ELSA LANconfig*

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



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

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



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

- The 'simple 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 in the **View ► Options** menu.



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

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

3.3 Configuration with *ELSA WEBconfig*

You can configure the basic settings of the device from any web browser, even a simple text-based browser. *ELSA WEBconfig* provides setup wizards similar to *LANconfig*, making the configuration procedure for the *LANCOM Wireless* as comfortable as possible from any operating system.

To establish a connection to the *LANCOM Wireless*, there has to be a LAN connection present using the TCP/IP protocol. Access generally is established using the device's IP address:


```
http://<LANCOM IP address>
```

A *LANCOM Wireless* that has not been reconfigured or has been reset will even respond to all IP addresses. A prerequisite is that the last set of numbers in the IP address is '254' (e.g. <http://10.0.0.254> and <http://192.168.0.254>).

Extensive, context-sensitive documentation for each *WEBconfig* page and field is available at all times in *WEBconfig* by selecting the 'Help (Reference Manual)' link.

HTTP module

Use the HTTP module to define the document root for the HTML help files under *ELSA WEBconfig*. The preset defaults refer the help link to the ELSA's website. If you want to store the help files locally, you can enter here the directory where the files are kept.

Ideally, keep the help files on a server that is always accessible. Use the following syntax when specifying the directory.

- On a local computer (for example):

```
file:///C:\Program Files\ELSA\lan/HTMLRef/500/4/1
```

- On a server (for example):

```
http://<IP address of the server>/HTMLRef/500/4/1
```

Note that the path for the *ELSA LANCOM Wireless L-11* is always completed as 500/4/1 and has to be configured as such locally.

The latest versions of the HTML help files are always available for download at ELSA's website.



3.4

Configuration using Telnet

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

```
C:\>Telnet 10.0.0.1
```

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

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

3.5 Configuration using SNMP

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

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

3.6 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.

3.6.1 This is how FirmSafe works

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

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

- 'Immediate': The first option loads the new firmware and activates it immediately. This can result in the following situations:
 - The new firmware is loaded successfully and works as desired. Then all is well.
 - The device no longer responds after loading the new firmware. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots 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.

3.6.2

How to load new software

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

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

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

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

ELSA WEBconfig

Launch your browser and enter the device's IP address, which you configured in the basic settings, into the address field. If you did not specify an IP address while configuring the basic settings, the address is 'http://10.0.0.254'.

There is a link on the start page called 'Upload New Firmware'. In the next window, you can search for the firmware file in the directory index and then click the **Upload** button.

TFTP

With TFTP you can use the **writeflash** command to install new firmware. To transmit a new firmware version to a device with the IP address 194.162.200.17, you would enter the following command under Windows NT for example:

```
tftp -i 194.162.200.17 put lc_wl1iu.200 writeflash
```

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

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

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

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



3.7

What's happening on the line?

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

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

3.8

ELSA LANmonitor

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

Installing *ELSA LANmonitor*

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

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

During the installation you should activate the 'LANmonitor'.

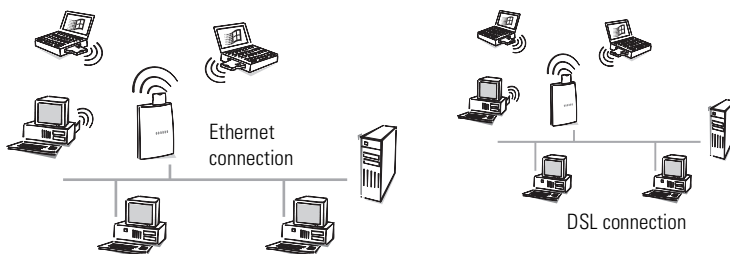
With ELSA LANmonitor you can only monitor those devices that you can access inband, i.e. via the local network. Your computer must also have the TCP/IP network protocol installed on it. With this program you cannot access any router connected to the serial interface.

3.9 DSL firmware for *ELSA LANCOM Wireless*

With the accompanying DSL firmware, the *ELSA Wireless* router can be configured for communication via DSL (e.g. the T-DSL connector of Deutsche Telekom).



Make sure that no ethernet network connections are active after uploading the firmware. It is advised that you should setup connection to the access point via WLAN. Wireless connection to the access point is also possible after the firmware upgrade.



Before upgrading the firmware, network access is possible via the Ethernet interface.



After the firmware upgrade, connection to an Ethernet network is no longer possible! The Ethernet interface on the Wireless router is now available for a DSL connection.

Procedures

- ① Disconnect the access point from the network, and establish a connection via the wireless network card (WLAN connection).
- ② Insert the accompanying CD in the computer, which is connected with the access point via WLAN.
- ③ Initialize *ELSA LANconfig* and select

Processing ► Firmware Management ► Upload New Firmware

Open the firmware directory on the CD and highlight the file.

`LC_Wireless_L-11_DSL_200`

After copying the firmware, the system should be reset. Then the DSL connection can be set up.



If you would like to delete this setup and install your access point for LAN operation within an Ethernet network, proceed likewise.

4

Operating modes and functions

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

- Wireless connections
- Security for your configuration
- Security for your LAN
- Security for your WLAN
- Call charge management
- DSL connections
- Automatic address administration with DHCP
- DHCP server
- Time check

*Only when
connecting to xDSL*

*Only when
connecting to xDSL*

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

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

4.1

Establishing wireless connections

This section explains how to get a wireless network going. There are several different basic operating systems:

- Ad hoc network
- Infrastructure network
- Point-to-point network (wireless bridge)
- Wireless Internet gateway DSL

The network structures are described in the introduction of this manual. For information on the topic of security and device configuration, refer to the chapter entitled 'Security for your configuration' on page 45.

Before configuring a network connection manually, check whether one of the available wizards might be applied to this purpose ('Die Assistenten' on page 31).



4.1.1

Considerations for setting up a wireless network

When designing networks for several access points, first determine where the access points will be positioned and how far apart they will be from each another. To ensure that the infrastructure of your wireless cells is free of gaps, use a mobile computer and the *AirLancer Client Manager* to test the wireless connections within the planned range. Use this method to measure the maximum distance between the individual access points. Wireless gaps between access points are irrelevant where no workstations are planned or network access does not have to be guaranteed.

Each access point spans its own wireless cell using a specific channel. In most countries there are 13 available radiofrequencies, some of which however overlap. The actual number of channels on the ISM frequency band that do not overlap are a maximum of three (e.g. channels 1, 6 and 13). This means that no more than three access points within reach of a wireless LAN can be operated completely free of interference; i.e. only three access points per room or floor. A frequency or neighboring channel, naturally, can be used again by other stations outside of the range.

When analyzing the network environment, the Site Monitor and Link Test tools of the AirLancer Client Manager are very useful.

Refer to the appendix in this manual for a detailed list of frequency bands for the individual channels.

4.1.2

Ad hoc network (peer-to-peer)

Define the direct connection between several computers in the configuration profile using the *AirLancer Client Manager*.

- ① Select the **Add/Edit Configuration Profile** command in the 'Action' menu.
- ② Select and label one of the four profiles and specify 'Peer-to-peer group' in the drop-down menu.
- ③ Click **Edit Profile** and enter the name of the network. This name has to be the same for all computers on the network.

You have now established the wireless bridge. You now have to set up a network in order to access other computers.

In Windows, set up Client for Microsoft Networks and file printer sharing under the Network Neighbourhood properties. If you want to use TCP/IP as your network protocol, be sure it is installed.

4.1.3

Infrastructure network

Define the wireless connection between the computers with *AirLancer MC-11* and the access point in the configuration profile using the *AirLancer Client Managers*.

- ① Select the **Add/Edit Configuration Profile** command in the 'Action' menu.
- ② Select and label one of the four profiles and specify 'Access Point' in the drop-down menu.
- ③ Click **Edit Profile** and enter the name of the network. The name has to be the same for each computer on the network and has to match the name that has been assigned to the access point.

If you are creating an infrastructure network with more than one access point, the roaming function is always available. Roaming guarantees the ability of a mobile computer to switch from one wireless cell to another. The IAPP protocol has to be enabled for the access points so that the roaming computer can be logged on and off of the various access points. You also have to set the channel numbers at the access points (refer to page 'Considerations for setting up a wireless network')42. As the network name, you can enter 'ANY'. This allows the roaming stations to log onto any nearby access point. In this case, access at the access point has to be permitted for the network name, 'ANY'.

The corresponding menu commands are as follows:

WEBconfig:

Advanced configuration ► Setup ► WLAN module ► IAPP protocol
and

Advanced configuration ► Setup ► WLAN module ► Closed network

LANconfig:

► **WLAN access ► General ► Roaming** and
► **Management ► Interfaces**

4.1.4

Point-to-point network

On a point-to-point network (also called „Bridge mode“) two or more access points communicate with each other. When configuring mobile stations, proceed exactly as you would for setting up an infrastructure network. It is also possible to connect point-to-point networks and infrastructure networks.

For the access points in this case, however, both the network name and the radio frequency have to be the same and interpoint communication has to be enabled. Furthermore, in the list of protocols you can only define the protocols that are copied in the network. You can increase data throughput by excluding any unneeded protocols.

The corresponding menu commands are as follows:

WEBconfig:

Advanced configuration ► Setup ► WLAN module

LANconfig:

► **Management ► Interfaces**

► **WLAN access ► General ► Point-to-point**

4.1.5

Wireless Internet gateway via DSL



The use of the LANCOM Wireless as a DSL router or DSL gateway is only possible if your provider uses the PPPoE protocol.

For a wireless Internet gateway via DSL, proceed on the client side exactly as you would for setting up an infrastructure network.

Configure the following settings for the access point:

First you have to load the DSL firmware into the access point. **Note that, after doing so, the LAN interface will no longer be available!** It then functions as a DSL interface.

● **Name list**

Data for remote stations and the phone numbers. Here, for example, enter the Internet provider you call for a DSL connection. The recommended idle time is about 300 seconds. PPPoE is always used as the protocol and you will not find a layer list for the DSL settings.

● **PPP list**

Here enter the device name of the remote station and the password. If

the user name is different from the device name, enter the user name here as well. Be sure that no check is executed.

- **IP router module**

Here define the default route in the routing table. This should match the device name defined in the name list. The IP address of the default route is always 255.255.255.255 and the subnet mask is 0.0.0.0. The router sends the data packets that are not intended for stations within the LAN directly to the default route (such as an Internet provider).

Advanced configuration ► Setup ► WAN module and

Advanced configuration ► Setup ► IP router module

LANconfig:

► **Communication ► Remote stations and Protocols**

► **IP router ► Routing ► Routing table**

4.2

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 L-11* thus offers a variety of options to protect the configuration.

4.2.1

Security for the device

Password protection

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

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

In this case, the password itself is set with the command `passwd`.

Login barring

The configuration in the *ELSA LANCOM Wireless L-11* 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 (outband, Telnet, TFTP/*ELSA LANconfig* and SNMP). 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 refer to configuration sessions via *ELSA LANconfig*, *ELSA WEBconfig*, SNMP or Telnet.

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

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

4.2.2

Security for your WLAN

The security of wireless data also can be guaranteed using various techniques:

- Station filter
- Using a closed network
- Data encryption

You can also call up the wizards provided in WEBconfig or LANconfig to configure the basic security settings.

Station filter

When defining an access list, specify which clients are allowed access to the access point. Under the `/Setup/WLAN module/Access list` menu item, add the MAC addresses of the card whose access is to be monitored. Then, under the setting found under

`/Setup/WLAN module/Access mode`, you can define whether clients with these card addresses have access (positive) or are not authorized (negative).

Closed network

On a closed network, the network name is not visible on remote stations. Logging on using the 'ANY' network name is not possible in this case. Therefore, all wireless stations on a closed network have to know the network names and have them entered in their current user profiles.

Use the `/Setup/WLAN module` menu to set the value for a closed network to 'On' (no access with 'ANY') or 'Off' (access with 'ANY' allowed).

Data encryption

The *11-Mbit wireless* network cards support a data encryption based on the WEP method (**W**ired **E**quivalent **P**rivacy). The 'Security' tab in the *AirLancer Client Manager* lets you define four different keys, based on how

- the data received and sent via wireless cards is decoded and
- the data sent via wireless cards is encoded.

The four various keys can contain five alphanumeric characters from the range 'a-z' and '0-9', whereby capitalization and lower case letters are



distinguished. As an alternative to the alphanumeric keys, a 10-digit hexadecimal value can be assigned.

Alphanumeric key	Hexadecimal key
For example: Seku1	For example: 0xABCD1234FE



In order to encode data communication, the same keys must be used for all client stations and access points. Write down the assigned keys and store them in a secure location.

The keys entered in the dialog box are only displayed when data is first input. After closing the window, the values are protected from viewing via an x-string.

4.2.3

Security for your LAN

You certainly would not like any outsider to have easy access to or to be able to modify the data on your computer. A *ELSA LANCOM Wireless L-11* offers various ways of limiting access for incoming and outgoing router connections:

- IP masquerading (also known as NAT/PAT)
- Data packet filtering
- Access protection with Password

Firewall filter

The firewall filters of the *ELSA LANCOM* devices offer filter functions that can apply to individual computers or the entire network. It is possible to set up source and target filters for individual ports or port ranges. Furthermore, individual protocols or any combinations of protocols (TCP/UDP/ICMP) can be filtered.

As soon as a filter condition is met, a definable action can be triggered.

Two tables provide the means for setting up filters. The first, the object list, is used to define computers, networks and protocols as objects. The second, the rule list, is used to describe source, target and action based on individual objects. The actual filter table is generated from these two tables.

As such, you do not need to create the filter list itself; and inconsistent entries are thus prevented in the filter table.

Object list

Use the object list to define the objects to be filtered. The following may apply as objects:

- Protocols
- Individual computers
- Entire networks
- Services

Any and all of these elements may be combined. Furthermore, objects can be defined recursively. In this manner, for example, you could define objects for the TCP and UDP protocols. Later, objects such as those for FTP (= TCP + ports 20 and 21), HTTP (= TCP + port 80) and DNS (= TCP, UDP + port 53) could be added. These in turn could be combined into a single object, which would contain all permissions.

Rule table

Use the rule table to combine individual objects into filter rules. The rule table contains the protocol being filtered, the source object, the target object and the filter action to be executed.

The protocol and the source and target objects can consist of combined objects or contain direct descriptions (such as %P6 for TCP), which are separated by '+' or the space character. Direct descriptions are labeled with '%'. Possible descriptions include:

Description	Function
%A	IP address
%M	Netmask
%S	Service (port)
%L	local net
%H	Host name
%P	Protocol (TCP/UDP/ICMP etc.)

Similar descriptions can form comma-separated lists, such as for host lists and address lists (%A10.0.0.1, 10.0.0.2), or hyphenated ranges, such as port lists (%S20-25). Specifying '0' or an empty string indicates the 'ANY' object:

all computers: %A0.0.0.0
all services: %S0
all protocols: %P0

Host names can be used only if *ELSA LANCOM* can resolve the names into IP addresses. To do so, *ELSA LANCOM* has to have learned the names via DHCP or NetBIOS, or the assignment has to be entered statically in the DNS or IP-routing table. An entry in the IP-routing table can simultaneously assign a host name to an entire net.

Filter list



The filter list is constructed of the object and rule lists. In doing so, the union of sets of all filters defined by the objects and rules is formed.

Note here that incorrect input neither results in a filter being created nor an error message. When configuring filters manually, be sure to verify that the filter you create does what you intend.

There are several ways of configuring firewall filters:

- *WEBconfig*

Full configuration ► Setup ► IP router module ► Firewall

- *LANconfig*

IP router ► Filter

- Telnet

/Setup/IP-router module/Firewall

ELSA LANconfig provides a very convenient tool for setting up filters. Use the following 'Filter' index card to define filter rules.



Note that configuring filters using LANconfig modifies the form of object tables that have been set up using Telnet or WEBconfig.

- General

Define here the name of the filter service and what is to happen with the data packets (action).

- Stations

Define here the stations for which the filter rule is to apply as sender or addressee.

- Services

Specify here which IP protocols and source and target ports the filter rule applies to.

Security check

The "identifier" to be used for determining the caller can be specified in the 'Communication' configuration section under the 'Call Acceptance' tab, or

under the /Setup/WAN-module/Security menu. You have a choice of the following:

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

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

The hiding place – IP masquerading (NAT, PAT)

This section is only relevant for devices with DSL firmware!!

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

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

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

4.3

Call charge management

This section is only relevant for devices with DSL firmware!!

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

Settings in the charge module

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

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



4.4

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 great.

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

4.4.1

The DHCP server

As a DHCP server, the *ELSA LANCOM Wireless L-11* can administer the IP addresses in its TCP/IP network. In doing so, it passes the following parameters to the workstation computers:

- IP address
- Netmask
- 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 DHCP server then interacts with *ELSA LANconfig* using a wizard and handles all of the address assignments in the local network itself.

4.4.2

DHCP – 'on', 'off' or 'auto'?

The DHCP server can be set to three different states:

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

4.4.3

How are the addresses assigned?

IP address assignment

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

- The IP address can be taken from the address pool selected (start address pool to end address pool). Any valid addresses in the local network can be entered here.

- If '0.0.0.0' is entered instead, the DHCP server automatically determines the addresses (start or end) from the IP address settings in the 'TCP/IP module'.
- If the access point 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.

Subnet mask assignment

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

Broadcast address assignment

Normally, an address yielded from the valid IP addresses and the netmask 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 must also be available to the WLAN, their addresses must be specified. Otherwise, the access point 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. However, because a *ELSA AirLancer* does not have the functions of a gateway, this task must be done by another gateway.

If a gateway in a wired LAN must also be available in the wireless network, enter the IP address of the gateway in the DHCP module as the 'Gateway Address'. Otherwise, the access point 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 that exceeds the maximum length, this will nevertheless be the maximum available validity!

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

- Default lease time in minutes

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

Priority for the DHCP server—request assignment

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

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

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.

This can be performed via the Network Neighborhood properties, for example.

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

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

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

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

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

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

4.4.4

Configuring the DHCP server

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

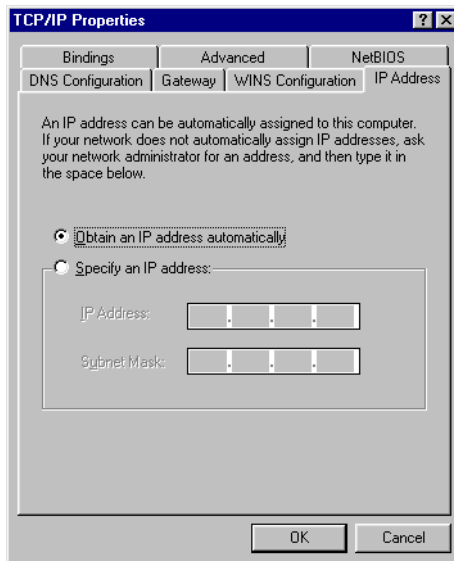
- You have not yet configured a network or your existing local network does not use TCP/IP. The DHCP server in your new ELSA lets you assign IP addresses to all of the computers in the network and to the router in a single operation.
- You are already using TCP/IP but without a DHCP server, and you would 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 device to your local network using a network cable.
- ② Switch the device on. It will not find any other DHCP servers in the network and will thus enable its own DHCP functions.
- ③ If you have not done so already, install the TCP/IP protocol on all computers in the LAN.
 - Usually when the protocol is installed, the default configuration is such that the computers are automatically ready to obtain the IP address from a DHCP server. After rebooting at the end of the protocol installation, the computers automatically request an IP address from the DHCP server.
 - If the protocol is already installed, enable the DHCP function on all of the computers in the local network. Under Windows 95, for example, this is done by selecting **Start ► Settings ► Control Panel ► Network** to open the window for configuring network properties. Double-click the entry for the 'TCP/IP' protocol. Enable the 'Obtain an IP address automatically' option. Switch over to the 'DNS Configuration' tab and delete all of the existing DNS

addresses. Next, delete any entries under the 'Gateway' tab and click **OK** to close all the windows. This change will require a reboot, after which the computer will automatically request an IP address from the DHCP server's address pool.



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

enter an unused IP address from the previously-used address range and activate the DHCP server.

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

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

Manual configuration

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

4.5

Accounting



This section is only relevant for devices with DSL firmware!!

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

The data collected include the following:

- User (name, IP address, MAC address)

The online times and data transfer volumes are assigned the MAC addresses of the system network interfaces in the LAN. The router can supply additional information regarding the assignments of MAC addresses and computer names from the DHCP or DNS server modules, if available. In this case, online times can be assigned directly to computer names. If the assignment of MAC addresses to computer names is not possible, other existing information is recorded to identify the user, such as the IP address.

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

- Remote site to which the connection was established
- Type of connection
- Sent and received data volumes
- Online time

The entire connection time of a dial-up connection that is used by several users at a time can be longer than the amount of time a user actually uses it. So in such cases, the length of the connection is determined based on the first and last user actions plus the valid hold time for the connection.

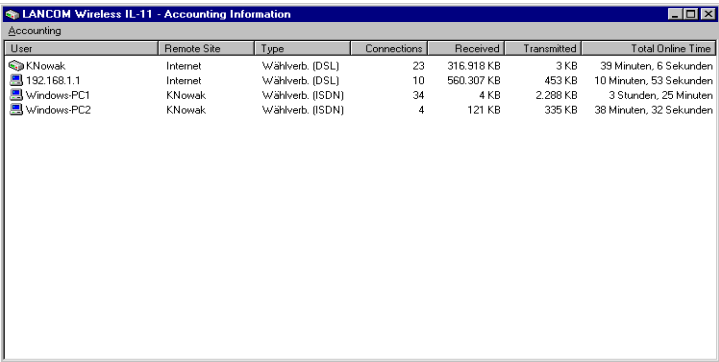
- Number of connections
- This field specifies how often a user's action led to the establishment of a connection.

4.5.1 Configuring accounting

Settings for accounting are found under */Setup/Accounting*. From there, you can enable or disable accounting and enable storage to flash ROM. Furthermore, you can influence the sorting of the accumulated table based on online time or transfer volume.

4.5.2 Reading the accounting data

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



User	Remote Site	Type	Connections	Received	Transmitted	Total Online Time
KNowak	Internet	Wahlverb. (DSL)	23	316.918 KB	3 KB	39 Minuten, 6 Sekunden
192.168.1.1	Internet	Wahlverb. (DSL)	10	560.307 KB	453 KB	10 Minuten, 53 Sekunden
Windows-PC1	KNowak	Wahlverb. (ISDN)	34	4 KB	2.288 KB	3 Stunden, 25 Minuten
Windows-PC2	KNowak	Wahlverb. (ISDN)	4	121 KB	335 KB	38 Minuten, 32 Sekunden

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

Organized by user name and remote site, the following information is listed:

- Username
The name of the user or his or her layer-3 address (IP address, IPX address or, in bridge mode, the MAC address again)
- Remote site
The remote site with which the user exchanged data
- Connection type
Type of connection
- Rx-bytes, Tx-bytes
Data volumes on the interface
- Total amount of time
Total online time for this user to this remote site
- Connections
The number of counted connections for this user to this remote site

If a user establishes a connection to another remote site, a new entry is created in the table. All of the transfer volumes and online times incurred by one user to one remote site are recorded in a single entry.

Depending on how the list is sorted, the 512 entries with the largest transfer volumes or longest online times are included in the table.



5 Technical data

5.1 Power and ratings data

Frequency band-width	2400-2483.5 MHz (ISM)
Standard	IEEE 802.11b, DSSS (Direct Sequence Spread Spectrum)
Transfer throughput	High: 11 Mbps Medium: 5,5 Mbps Standard: 2 Mbps Low: 1 Mbps The transmission rate is automatically determined. It is also possible to adjust the transmission rate manually.
Range	About 150–400 meters across open terrain and about 30–50 meters in closed buildings (typical range)
Bit error ratio	Better than 10^{-5}
Transmitting power	15 dBm
Radio channels	Up to 13 channels, max. 3 non-overlapping
Network protocols	Any network protocols can be transmitted between wireless LAN and ethernet LAN by bridge; protocols for WAN: PPPoE (DSL); routed protocols via ISDN/DSL: TCP/IP, IPX, NetBIOS/IP
Security	Password protection, address and protocol filters: WEP encryption, Closed Wireless Network, IP masquerading (NAT/PAT), firewall filters
Connects	10-base-T, external power adapter (9V)
Package contents	<ul style="list-style-type: none"> – Extensive documentation in German, English, French and Italian – Patch network cable (UTP) – Plug-in power adapter – Software bundle CD with <i>ELSA RVS-COM</i>, Laplink Pro – CD with management software
Standards/Approvals	ETSI, ETS 300328, ETS 300826, EN 55022, EN 55024, EN 60601-1-2, EN 60950, CE marked; radio approval for all EU countries and Switzerland
Warranty	6 years for the access point, 2 years for the <i>AirLancer</i> wireless adapter
Support	Hotline and Internet, free software updates

5.2

Radio frequency channels

Up to 13 DSSS channels are available within the utilizable frequency range of 2400 to 2483 MHz. Each channel has a bandwidth of 22 MHz, so that a maximum of three independent channels are possible within the ISM frequency band. Not all channels are utilizable in all countries. The following table shows the medium frequencies and what channels are permitted in what country.

Frequency band	2400-2500 MHz			
Channel no.	USA (FCC)	EU (ETSI)	France *	Japan
1	2412	2412	—	2412
2	2417	2417	—	2417
3	2422	2422	—	2422
4	2427	2427	—	2427
5	2432	2432	—	2432
6	2437	2437	—	2437
7	2442	2442	—	2442
8	2447	2447	—	2447
9	2452	2452	—	2452
10	2457	2457	2457	2457
11	2462	2462	2462	2462
12	—	2467	2467	2467
13	—	2472	2472	2472

* In France, the entire ISM band will be cleared for use by radio networks by 2001. Please read the information on this provided in the 'Readme' file on the CD.

The boldface values are set as the defaults for the *ELSA LANCOM Wireless L-11*.

6

Appendix

6.1

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-11

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, 14. April 2000

Aachen, 14th April 2000

i.V. Stefan Kriebel
Bereichsleiter Entwicklung
VP Engineering

6.2

General 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 the *ELSA LANCOM Wireless L-11* access point is six years. The warranty period for the *ELSA AirLancer* wireless adapter is two 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.

7 Index

- **A**
 - Access control 46
 - Access point 8
 - Access protection 48
 - name 51
 - name or number 51
 - number 51
 - Accounting 13
 - Ad hoc network 8, 42
 - Address administration 52
 - Address pool 53, 58
 - AirLancer Client Manager 12
- **B**
 - Barring 46
 - Bridge mode
 - see Point-to-point network
 - Broadcast 54
 - Brute force 46
- **C**
 - Call charge information 13
 - Call charge management 51
 - CD 15
 - Channel bundling 11
 - Closed network 47
 - Configuration 10
 - SNMP 34
 - Connection duration 11
- **D**
 - Data encryption 47
 - Data volume 13
 - DHCP 52, 53
 - DHCP mode 53
 - DHCP server 52
 - configuration 57
 - DNS server 13, 52, 54
 - DSL 44
- **E**
 - Electronic documentation 15
 - End address 53
 - Ethernet 10
 - 10Base-T 10
 - Ethernet connection 8
- **F**
 - Factory defaults 22
 - Filter 48
 - Firewall 48
 - Filter list 50
 - Object list 49
 - Rule table 49
 - Firewall function 51
 - FirmSafe 11, 34
 - Firmware 11
 - Firmware upload 35
 - using TFTP 36
 - with LANconfig 35
 - Flash ROM 11, 34
- **G**
 - Gateway 51, 52, 55
- **H**
 - High telephone costs 51
- **I**
 - Identifying the caller 51
 - Inband
 - using Telnet 33
 - Infrastructure network 9, 43
 - Install software 34

Installation	10
IP access list	31
IP address	51
IP masquerading	48, 51

L

LAN	8
LAN connection	10
LAN connector cable	15
LANCAPI	13
LANconfig	23, 31, 35, 37
LANmonitor	11, 37
LED	21
LAN Collision	22
LAN Status, received	22
LAN Status, send	22
Power/Msg	22
Wireless network activity	22
Line connection	13
Line management	13
Local area network	8
Login	34, 46
Login barring	46

M

Mode	53
Monitoring	37

N

NAT	48, 51
NBNS server	52, 54
NetBIOS	13

O

Online media	31
Online time	13
Operating modes	41

P

Package contents	15
------------------------	----

Password	48
Password protection	45
PAT	48, 51
Peer-to-peer network	8, 13
Period of validity	52, 55
Point-to-point network	44
Power adapter	15
Proxy	13

R

Radio cell	8
Radio frequency channels	64
Range	9
Reset button	22
Roaming	9

S

Security	45, 48, 51
Device	45
WLAN	47
Single user access	51
SNMP	34
Software update	11
Specifications	63
Start address	53
Station filter	47
Statistics	12
Status displays	12
Subnet mask	54

T

TCP/IP	23
Transfer costs	13
Transmission rates	11
Troubleshooting	37

U

Upload	11, 34
--------------	--------

W

Warranty conditions	66	Wireless Internet gateway	44
WEBconfig	35, 36	Wireless LAN	8
WEP	47	Wireless network	7
Windows networks	13	Wireless network adapter	8
Winipcfg	26	WLAN	8
		WWW	51