

**ELSA LANCOM™ Wireless IL-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<sup>®</sup>, Windows NT<sup>®</sup> and Microsoft<sup>®</sup> 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](http://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 ISDN network.

## Documentation

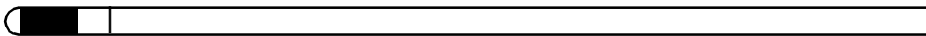
The accompanying documentation comprises:

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



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



# Contents

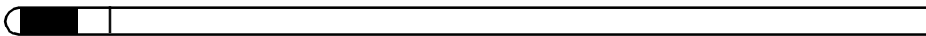
<b>1 Introduction</b>	<b>9</b>
1.1 The basic functions of a wireless network	9
1.2 Operating modes	10
1.3 What does the <i>ELSA LANCOM Wireless IL-11</i> offer?	13
<b>2 Installation</b>	<b>21</b>
2.1 Package contents	21
2.2 System requirements	21
2.3 Install TCP/IP on your workstation	22
2.3.1 Windows 95 and Windows 98	22
2.3.2 Windows NT 4.0	23
2.3.3 Windows 2000	25
2.4 Introducing the <i>ELSA LANCOM Wireless IL-11</i>	26
2.4.1 The front of the unit	26
2.4.2 The status of the ISDN connection	27
2.4.3 The bottom of the unit	29
2.5 How to connect the device	29
2.6 Software installation	29
2.7 Quickstart	30
2.7.1 The wizards	31
2.7.2 Basic settings	31
<b>3 Configuration and management</b>	<b>37</b>
3.1 Radio or wired: configuration approaches	37
3.2 Configuration using <i>ELSA LANconfig</i>	37
3.3 Configuration with <i>ELSA WEBconfig</i>	38
3.4 Configuration using Telnet	39
3.5 Configuration using a dial-up connection	40
3.5.1 This is what you need for remote configuration	40
3.5.2 This is how you prepare the remote configuration	40
3.5.3 The first remote connection using a Dial-up Networking and <i>ELSA LANconfig</i>	40
3.5.4 The first remote connection using a PPP client and Telnet	41
3.5.5 Limiting remote configuration	41
3.6 Configuration using SNMP	43

3.7 New firmware with FirmSafe . . . . .	43
3.7.1 This is how FirmSafe works . . . . .	44
3.7.2 How to load new software . . . . .	44
3.8 What's happening on the line? . . . . .	46
3.9 <i>ELSA LANmonitor</i> . . . . .	46
3.10 <i>DSL firmware for ELSA LANCOM Wireless</i> . . . . .	47

## **4 Operating modes and functions . . . . . 49**

4.1 Establishing wireless connections . . . . .	49
4.1.1 Considerations for setting up a wireless network . . . . .	50
4.1.2 Ad hoc network (peer-to-peer) . . . . .	50
4.1.3 Infrastructure network . . . . .	51
4.1.4 Point-to-point network . . . . .	52
4.1.5 Wireless Internet gateway via ISDN . . . . .	52
4.1.6 Wireless Internet gateway via DSL . . . . .	53
4.2 Security for your configuration . . . . .	54
4.2.1 Security for the device . . . . .	54
4.2.2 Security for your WLAN . . . . .	56
4.2.3 Security for your LAN . . . . .	57
4.3 ISDN routing . . . . .	62
4.3.1 ISDN name list . . . . .	63
4.3.2 Interface settings . . . . .	64
4.3.3 Router interface settings . . . . .	65
4.3.4 Layer list . . . . .	65
4.3.5 Call charge management . . . . .	66
4.4 Automatic address administration with DHCP . . . . .	67
4.4.1 The DHCP server . . . . .	67
4.4.2 DHCP—'on', 'off' or 'auto'? . . . . .	68
4.4.3 How are the addresses assigned? . . . . .	68
4.4.4 Configuring the DHCP server . . . . .	71
4.5 The least-cost router . . . . .	74
4.5.1 Function of the <i>LANCOM Wireless</i> least-cost router . . . . .	74
4.5.2 Setting up the least-cost router . . . . .	77
4.6 <i>ELSA CAPI Faxmodem</i> . . . . .	79
4.6.1 Installation . . . . .	79
4.6.2 Faxing with the <i>ELSA CAPI Faxmodem</i> . . . . .	80
4.7 Office communications and <i>LANCAPI</i> . . . . .	80
4.7.1 <i>LANCAPI</i> interface settings . . . . .	80
4.7.2 <i>The ELSA LANCAPI</i> . . . . .	81

4.8 Accounting .....	86
4.8.1 Configuring accounting .....	87
4.8.2 Reading the accounting data .....	87
<b>5 Technical data .....</b>	<b>89</b>
5.1 Power and ratings data .....	89
5.2 Radio frequency channels .....	91
<b>6 Appendix .....</b>	<b>93</b>
6.1 Declaration of conformity .....	93
6.2 General Warranty conditions .....	94
<b>7 Index .....</b>	<b>97</b>





## 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.

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

## 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

*Wireless network  
adapters WLAN*

of wireless networks introduced. Detailed information on this and other topics can be found in the electronic documentation on the CD.

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.

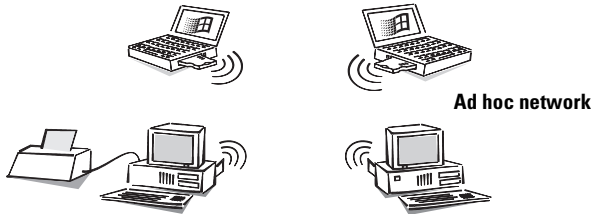
## 1.2 Operating modes

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 + ISDN gateway
- 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.

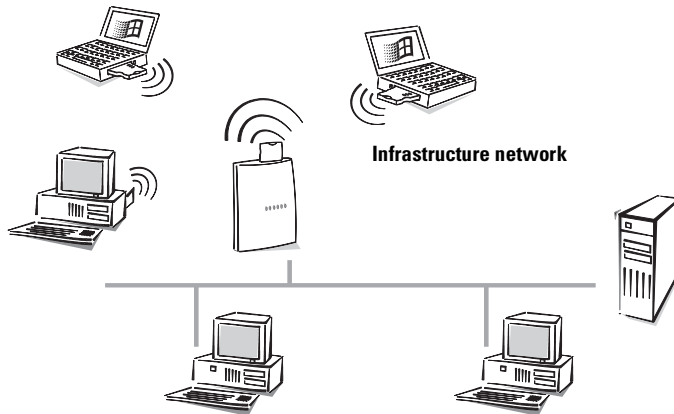


#### *Ad hoc network*

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.

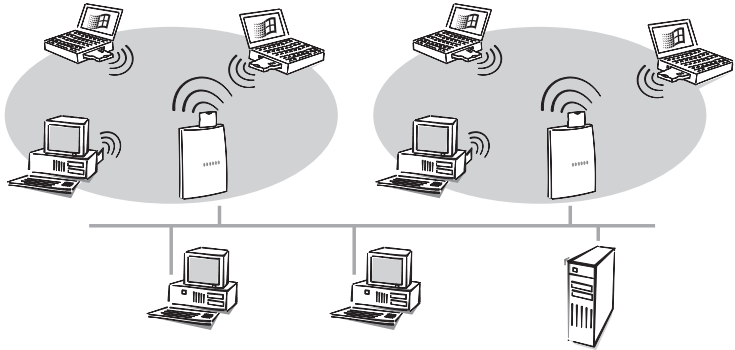


A wireless network with a access point is also referred to as an infrastructure network.

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*

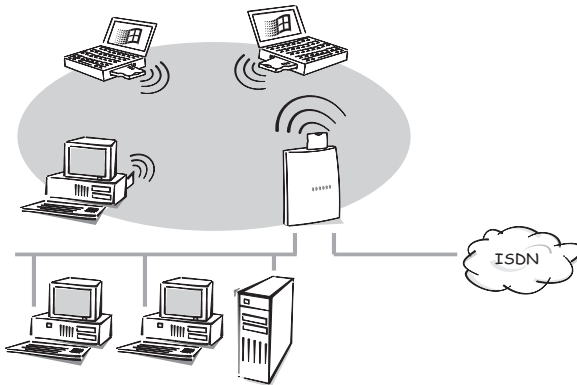
Multiple access points can be used if the range of a cell is not sufficient to link all mobile stations. This makes it possible to switch from one wireless cell to another without interrupting the connection to the network.



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.

*WLAN and  
ISDN/DSL gateway*

The *ELSA LANCOM Wireless IL-11* access point offers a special supplementary function. The access point connects both the wireless network and the ISDN or DSL network simultaneously to the wired network via the ISDN interface.



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

## 1.3

# What does the *ELSA LANCOM Wireless IL-11* offer?

13

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.
- Plug in the ISDN cable.
- 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 IL-11* to a 10 Mbit LAN or to a DSL modem.

### WAN connection

The *ELSA LANCOM Wireless IL-11* is connected to the  $S_0$  interface(s) of an ISDN basic rate interface in point-to-multipoint configuration (multi-device terminal) or in point-to-point configuration (system terminal). The router automatically detects your port type and the D-channel protocol being used. Switched connections using DSS1 or 1TR6 can also be used, as can leased-line connections.

*Operation with an ISDN leased line is not included in the standard delivery scope of the router. The leased line option can be enabled by entering a code.*

### 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.

For access to the device, the TCP/IP protocol has to be installed on the stations. The *ELSA LANCOM* access point can then be configured for a LAN, WLAN or WAN connection. The unit can be maintained remotely via ISDN—even before being configured after delivery.

Access to the device is possible from a WAN (via ISDN), WLAN or LAN. TFTP is supported along with SNMP if configuring from the LAN or WLAN.

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, the WLAN or the WAN (ISDN).

## FirmSafe

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

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

## Intruder protection

Along with password protection and call number recognition (CLIP), the router offers protection against unauthorized access to the company network by means of a callback function which only permits a connection to be established to previously defined ISDN telephone numbers only. Authentication

mechanisms in PPP, firewall filters and IP masquerading complete the security concept. Furthermore, login barring prevents any “brute force attacks” and denies access to the router after a configurable number of login attempts using an incorrect password.

### **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.

### **Charge monitoring**

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

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

### **Least-cost routing**

Even if there is a large selection of telecommunications service providers you can always use the cheapest ISDN lines using the least-cost router.

### **Automatic time check**

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

### **Channel bundling and compression**

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

### ***ELSA LANmonitor***

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

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

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

### ***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 ISDN and 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 IL-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

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

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

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

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

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

Any workstation which has been integrated into the LAN (Local Area Network) can use *LANCAPI* to give unlimited access to office communication functions such as fax and EuroFileTransfer. All functions are made available throughout the network without the need to add hardware to the workstations. The office communications software simply needs to be loaded onto the individual workstations.

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

### 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 IL-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 IL-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)
- ISDN connection cable
- 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 and ELSA LANCAPI require a Windows operating system.*



## 2.3

## Install TCP/IP on your workstation

To establish a connection to a *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.

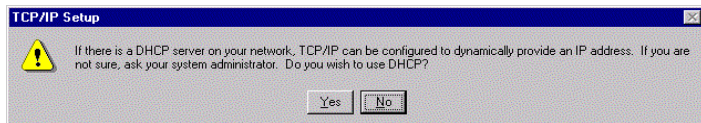
- Entering the gateway and DNS server (not necessary when using DHCP)  
On the workstation computers, specify the address of the local network router as the gateway and as the Domain Name Server (DNS server): **Start ► Settings ► Control panel ► Network ► TCP/IP ► Properties ► Gateway and DNS configuration**. 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.

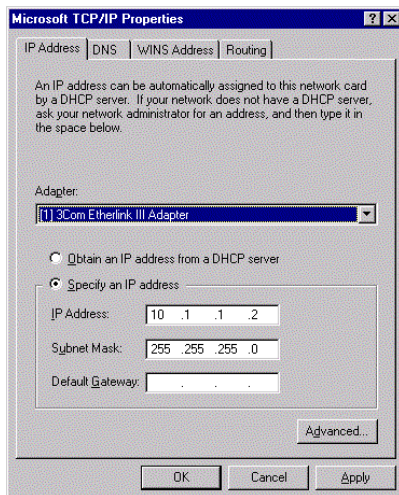
- Installing TCP/IP  
To install TCP/IP, click **Start ► Settings ► Control Panel ► Network ► Protocols ► Add**. Select the 'TCP/IP protocol' network protocol.
- Allocate IP addresses (using DHCP)  
If you are going to use the router as a DHCP server, set the workstations to obtain IP addresses automatically.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

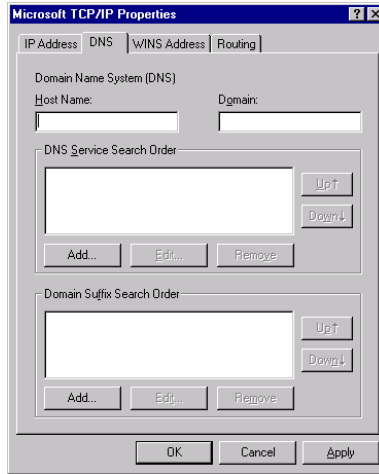


Assign unique IP addresses, for example taken from a reserved range of addresses. For example, the workstations can be assigned addresses from '10.1.1.2' to '10.1.1.253', the router can be given '10.1.1.1' and all can have the subnet mask of '255.255.255.0'. To test whether or not a specific IP address, 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.

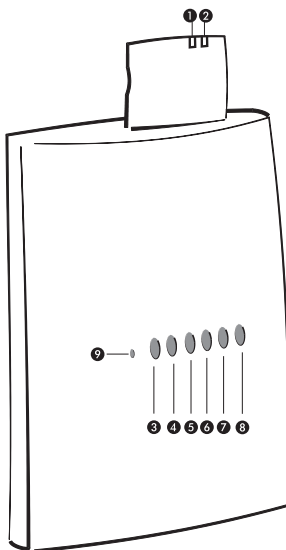
## 2.4 Introducing the *ELSA LANCOM Wireless IL-11*

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/receive status of the card:
  - Off—no wireless activity
  - Blinking—wireless data being sent/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 'S<sub>0</sub> Status' LED on the access point shows the activity on the D-channel.
- 5 The 'WAN Channel-1' LED on the access point shows the activity on the first B-channel on the ISDN port.
- 6 The 'WAN Channel-2' LED on the access point shows the activity on the second B-channel on the ISDN port.
- 7 The 'LAN Tx/Rx' LED on the access point indicates activity on the wireless network and 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 status of the ISDN connection

This LED shows the status of the S<sub>0</sub> connection:

off		Not connected or no S <sub>0</sub> voltage (often, the S <sub>0</sub> voltage is disabled at ISDN connections after certain length of inactivity)
green	flashing	Initializing (establishing contact with the connection point)

WAN  
Chan1  
Chan2

green		operational (S <sub>0</sub> bus activated, TEI exists and D channel protocol checked)
green	Power off	LED is on, but power LED is off: unit in boot monitor

These LEDs indicate the status of the corresponding logical ISDN-WAN channels (in both router and CAPI modes):

off		Channel idle
red	flashing	incoming call pending
green	flashing	outgoing call being executed
red		Channel is physically established/protocol negotiation in process
green		Corresponding protocol negotiation (X.75, PPP, etc.) completed; channel is logically online
green/red	short red flashes (duration approx. 1/10 s)	Indicate a received data packet

The ISDN WAN channels do not have any fixed assignments to B channels!

*The connection is active and incurring charges so long as the 'Chan1' or 'Chan2' LED is green!*



WAN  
Chan 1+2

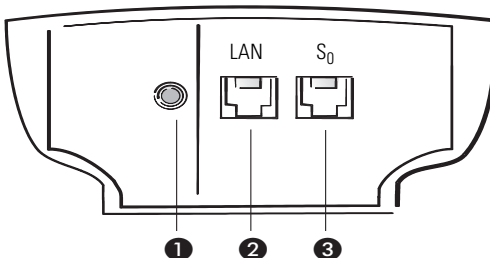
This LED indicates whether the current ISDN connection is static or using dynamic channel bundling.

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

### 2.4.3

## The bottom of the unit

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



- ❶ Connection for power supply unit
- ❷ 10Base-T network connection
- ❸ ISDN S<sub>0</sub> port

## 2.5

## How to connect the device

- ❶ Connect your *ELSA LANCOM Wireless IL-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.
- ❷ Connect your *ELSA LANCOM Wireless IL-11* to the ISDN network. To do so, connect the supplied ISDN line connection cable to the ISDN/S<sub>0</sub> terminal on the unit and to an ISDN/S<sub>0</sub> multi-device terminal or system terminal (point-to-multipoint or point-to-point configuration).
- ❸ 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 sys-

tem. 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 IL-11*, are available in *ELSA LANconfig* and *ELSA WEBconfig*:

- Basic settings
- Changing security settings
- Setting up Internet access
- Selecting the Internet provider
- Preparing remote access service (RAS)
- Connecting two local networks

#### Wizards in *ELSA LANconfig*

- ① Start the software *ELSA LANconfig* with **Start ► Programs ► ELSAlan ► *ELSA LANconfig***.
- ② Select your *ELSA LANCOM Wireless IL-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 IL-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.

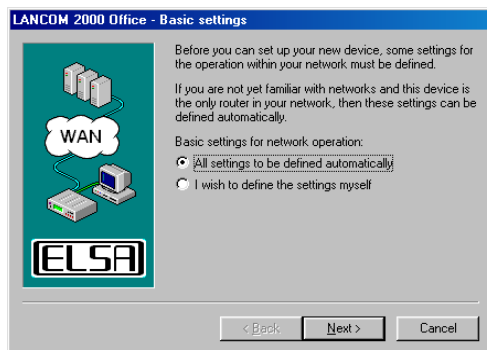
#### *ELSA LANconfig*

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 automat-

ically 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 ► ELSAlan ► 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 `winipcfg` 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 network mask '255.255.255.0'. At the same time you will set the address range that the DHCP server uses for the other devices in the network (so long as the DHCP server is not switched off).
  - You have previously used IP addresses 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 adr. 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 operating 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

123

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

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

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

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

### 3.1

## Radio or wired: configuration approaches

With the configuration via WLAN and LAN or the remote configuration via ISDN, you can access the access point from any computer on the WLAN, LAN or WAN (ISDN). However, you can restrict or block the access altogether by using the IP access list.

The configuration of *ELSA LANCOM Wireless IL-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

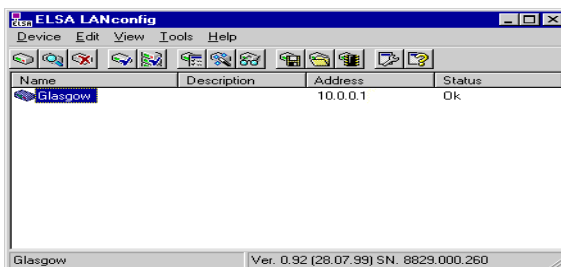
## Configuration using *ELSA LANconfig*

Start *ELSA LANconfig* e.g. via the Windows taskbar with **Start ► Programs ► ELSA!an ► 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 IL-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 a dial-up connection

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

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

### 3.5.1

### This is what you need for remote configuration

- A computer with a PPP client, e.g. Windows Dial-up Networking
- A program for inband configuration, e.g. *ELSA LANconfig* or Telnet

### 3.5.2

### This is how you prepare the remote configuration

- ① Attach the router to the power supply.
- ② Connect the device to a WAN interface.

### 3.5.3

### The first remote connection using a Dial-up Networking and *ELSA LANconfig*

- ③ In the *ELSA LANconfig* program select **Device ► New**, enable 'Dial-up connection' as the connection type and enter the calling number of the WAN interface to which the *LANCOM Wireless* is connected. If you wish, you can also enter the time period after which an idle connection is to be disconnected automatically.
- ④ *ELSA LANconfig* now automatically generates a new entry under Dial-up Networking. Select a device that supports PPP (e.g. the NDIS-WAN driver included with the *LANCAP*) for the connection and press **OK** to confirm.
- ⑤ Then the *ELSA LANconfig* program will display a new device with the name 'Unknown' and the dial-up call number as the address in the device list.





Once the entry appears in the device list the Dial-up Networking connection is broken.

- ⑥ You can configure the device remotely just like all other devices. *ELSA LANconfig* establishes a dial-up connection enabling you to select a configuration.

### 3.5.4

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

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

### 3.5.5

#### Limiting remote configuration

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

You may, however, want to change the default layer for LAN-to-LAN connections, for example, to a different protocol after the first configuration run.

Then the device will no longer take calls on the dial-up connection using the PPP settings. The solution to this is to agree upon a special calling number for configuration access. If the device receives a call on this number, it will always use PPP, regardless of any other settings made on the router. Only a specific user name which is automatically entered by the *ELSA LANconfig* program during call establishment will be accepted during the PPP negotiations.

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

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

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

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

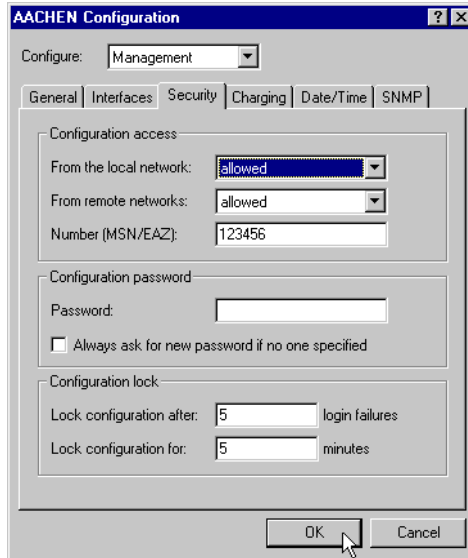
- ③ Enter a calling number of your connector as the calling number in the 'configuration access' area, which is not used for other purposes.

Alternatively, enter the following command:

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

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





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

```
passwd
```

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

## 3.6 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.

## 3.7 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.

### 3.7.1

## 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.

### 3.7.2

## How to load new software

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

- *ELSA LANconfig*
- *ELSA WEBconfig*
- 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 **writelflash** 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 writelflash
```



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

The device is booted up following a successful firmware upload and this activates the new firmware switch directly. If an error occurs during the upload (write error in the flash ROM, TFTP transmission error 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.

## 3.8

### 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.

## 3.9

### **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 'auto-run.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.*

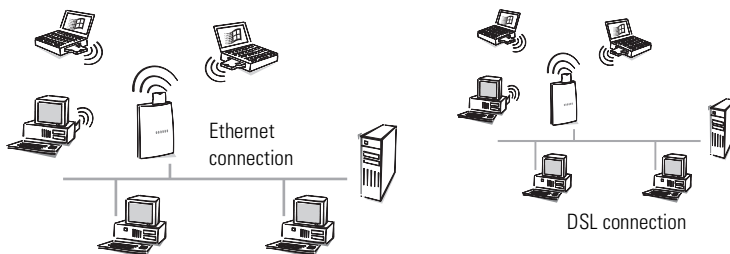
## 3.10

### DSL firmware for *ELSA LANCOM Wireless*

With the accompanying DSL firmware, the *ELSA Wireless* router can be configured for communication via DSL.



*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_IL-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
- ISDN connections
- Automatic address administration with DHCP
- DHCP server
- Least-cost router
- *ELSA LANCAPi*
- Time check

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 ISDN
- 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 54.

*Before configuring a network connection manually, check whether one of the available wizards might be applied to this purpose ('The wizards' 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 50, 'Considerations for setting up a wireless network'). 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, 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 ISDN

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

Only a few steps are required to set up Internet access for all network users via the integrated ISDN router. The easiest method to set up Internet access is by using the setup wizard provided in *Webconfig* or *LANconfig*. You can then fine-tune the settings manually in the individual router tables:

- **Layer list**

The layer list contains predefined protocols, which you can customize as needed (e.g. for channel bundling). The standard protocol is PPPHDL, which you can use in most cases. Here, assign a layer name for the ISDN gateway. That defines it for the Internet connection to be configured.

- **Name list**

Data for remote stations and the phone numbers. Here, for example, enter the Internet provider you call for an ISDN connection. The recommended idle time is about 90 seconds. Apply the layer names that you have created in the layer list.

- **PPP list**

Here enter the device name and/or user name of the remote station and the password for the connection. If the user name is different from the device name, enter the user name here as well. Be sure that authentication is set to 'None'. This refers to the local authentication of the remote station. The *LANCOM*, not the provider, has to log on.

- **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).

The corresponding menu commands are as follows:

*WEBconfig:*

**Advanced configuration ► Setup ► WAN module and**

**Advanced configuration ► Setup ► IP router module**

*LANconfig:*

► **Communication ► Remote stations and Protocols**

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

## 4.1.6

### 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 IL-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 IL-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 network mask is entered and from that point on only those IP addresses contained in this initial entry will be permitted to use the internal functions. The circle of authorized users can be expanded by inputting further entries. The filter entries can describe both individual computers and whole networks.

The access list can be found in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'General' tab, 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 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 distin-



guished. 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 IL-11* offers various ways of limiting access for incoming and outgoing router connections:

- IP masquerading (also known as NAT/PAT)
- Data packet filtering
- Verification of incoming connections (callback to specified call numbers)

### Firewall filter

The firewall filters of the *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 labelled with '%'. Possible descriptions include:

Description	Function
%A	IP address
%M	Network mask
%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 *LANCOM* can resolve the names into IP addresses. To do so, *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.

*Verification of  
name*

When using the ELSA or PPP layer on the B channel, the name of the calling party can also be transmitted. This requires a connection to be established first, since the name cannot be transferred over the D channel.

The name of the remote station can also be transferred in PPP connections.

This requires a connection to be established first, since the name cannot be transferred over the D channel.

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

The name sent by the remote station will be checked for its appearance on the PPP list of user names if the PPP protocol is being used. If the user name is not available, the device name is accepted and verified as the name of the remote station. The PPP list can be found in the *ELSA LANconfig* in the 'Communication' configuration section on the 'Protocols' tab, or in the `/Setup/WAN-module/PPP-list` menu.

Addition security is provided by a password. PPP offers password protection through three different login protocols: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) and MS-CHAP (the Microsoft variation of CHAP). All of these protocols serve the same purpose. The calling device determines which protocol is used.



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

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

*Checking the  
number*

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

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

### Callback

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

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

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

And all the while you can use the settings to dictate how the cost of the connection is to be apportioned. The router accepts all unit charges, except for the unit required to send the name, if call back 'With name' is set in the name list. Likewise, a unit is charged to the router, if the caller is not identified by means of CLIP. On the other hand, the caller incurs no costs if identification of the caller's number is possible and is accepted.

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

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

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

IP masquerading provides a hiding place for every computer while connected with the Internet. Only the router module of the unit and its IP address are visible on the Internet. The computers in the LAN then use the router as a gateway so that they themselves cannot be detected. To do this, the router

separates Internet and intranet, as if by a wall. Therefore, IP masquerading is also called a "firewall function".

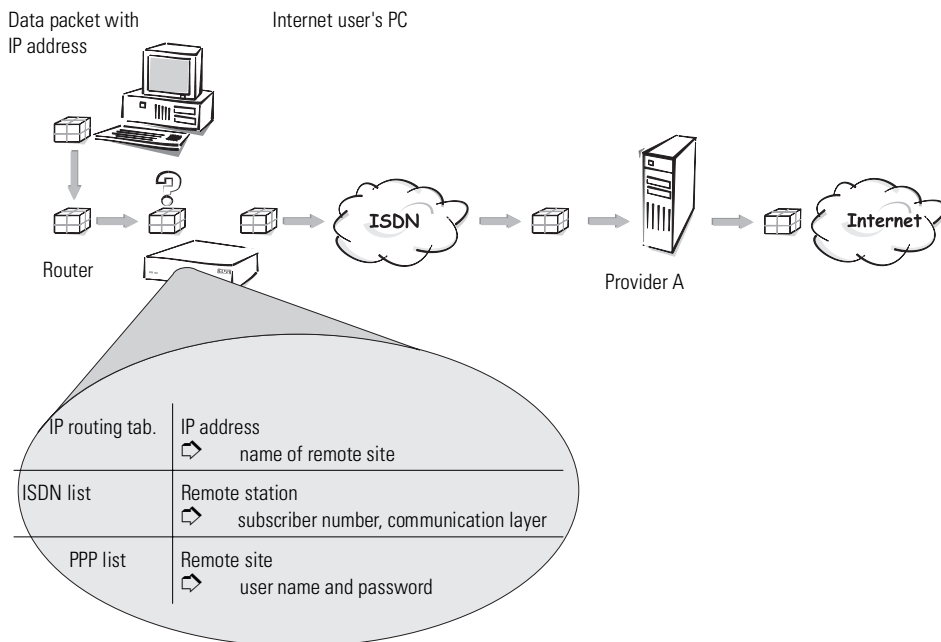
For further information, see the 'IP routing: IP masquerading' section.

## 4.3 ISDN routing

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

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

A simplified example will clarify this process.



A data packet from a computer initially finds the path to the Internet through the IP address of the recipient. The computer sends the packet with this

address over the LAN to the router. Using the IP address, the router then searches the IP routing table and finds the remote station that belongs to the address, for example 'Provider\_A'. Using this name, the router then checks the ISDN name list and finds the call number for the corresponding remote station that can be reached by ISDN, including the communication layer that is to be used. The router also obtains the user name and password required for login to Provider A from the PPP list.

When this is done, the router can establish a connection to the router of the provider over the ISDN line. Once the connection has been established, the router can forward the data packet to the Internet over the ISDN line.

*You can find more information on IP networks, etc. in the technical documentation provided on the CD.*



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

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

### 4.3.1

#### ISDN name list

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

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

- **Name**  
This name is used to identify the remote site in the router modules.
- **Subscriber number**  
This number should be dialed when the router actively establishes a connection to the remote station.  
  
If the remote station can be reached under a variety of subscriber numbers, enter the other numbers in the round-robin list.  
  
If the remote station is available via a leased line, the number for a dial-up backup connection can be entered here.

- Timeouts

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

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

- Layer name

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

- Callback

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

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

## 4.3.2

### Interface settings

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

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

- D channel protocol used on the  $S_0$  port

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

- Leased line option

B channel to be used for the leased-line connection



- Dialing prefix

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

### 4.3.3

## Router interface settings

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

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

- Subscriber numbers (MSN/terminal device selection numbers)

The router responds to incoming calls for these numbers. Multiple numbers are separated by semicolons. If no subscriber number is specified, the router will respond to all incoming calls.

The first subscriber number specified will be transmitted to the remote station during the active establishment of a connection. If no number is specified, the main MSN of the connection will be transmitted.

- Option for Y connections

Enable this option if it should be possible for both B channels of the connection to establish parallel connections to different remote stations.

- Suppression of own subscriber number

Enable this option in order to suppress the display of your own subscriber number to the remote station during call establishment.

This function must be supported by the network operator.

### 4.3.4

## Layer list

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

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

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

### 4.3.5

## Call charge management

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

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

### **Broadcast address assignment**

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

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

### **DNS and NBNS assignment**

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

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

### **Default gateway assignment**

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

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



## Period of validity for an assignment

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

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

- **Maximum lease time in minutes**

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

If a host requests a validity 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:

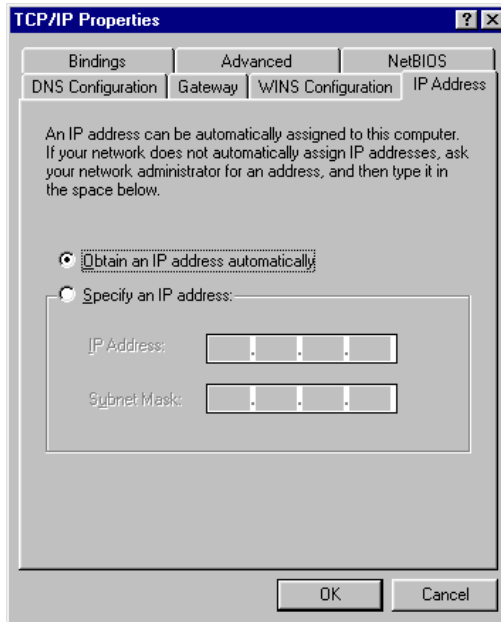
- You have not yet configured a network or your existing local network does not use TCP/IP. The DHCP server in your new ELSA lets you assign IP addresses to all of the computers in the network and to the router in a single operation.
- You are already using TCP/IP but without a DHCP server, and you would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

mask 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 The least-cost router

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

Unfortunately, the most inexpensive rates vary from provider to provider depending on the time of day and region. In the morning Provider 1, Provider 2 in the afternoon and possibly Provider 3 for international calls. To always have the most economical connection for telephone calls, surfing the Internet or transferring data to other networks, it would be necessary to decide which provider is the least expensive before each connection. A *ELSA LANCOM Wireless IL-11* does this for you. Least-cost routing (LCR) is the function for this task. You define once which providers have the most favorable charges for your purposes, and the device automatically selects the most economical provider for you, (regardless of whether you are using the router, the *LAN-CAPI* etc.).

### 4.5.1 Function of the *LANCOM Wireless* least-cost router

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

The unit checks the LCR table after each digit for a correspondence to a previously dialed number (prefix). If a suitable entry is found which is even valid

for the current time and date, the network identification prefix for the connection's detour will be entered before the area code. The number is not sent out to the exchange until it has been completed in this manner.

The LCR also requires the following information:

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

### Initial tests

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

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

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

These four entries mean that all connections to Munich (or other numbers with the prefix '089') on weekends will be made using the provider with the network prefix '01097'. Between 8:00 AM and 6:00 PM on weekdays, these calls will be made using the provider with the network prefix '0800'. International calls on Sundays will be made using the provider with the network prefix '4'.

### For advanced users: systematic use of the LCR

- The first example has shown how connect charges can be reduced with only a few entries. If you would like to put the least-cost router to optimal use, detailed information is required with regard to the connect-charge structure of the call-by-call providers. Next, decide how these rates and rate zones can be best organized in the *ELSA LANCOM Wireless IL-11* LCR table. A variety of approaches are possible:
  - Obvious options for saving telephone charges can be entered directly:
    - '00' for international connections
  - Entering a single '0' will initially reroute all numbers starting with a zero. However, as neighboring local exchanges may also start with a '0' and yet be billed as local calls, their prefixes should be listed separately to prevent these calls from being rerouted. This strategy should also be applied to special prefixes such as '0800' etc.
  - Another strategy aims to achieve the highest possible level of control over the routing activities. Start with the prefixes of the local area and then define the next larger zones. The closer, and thus less expensive, tariff zones are set with longer prefixes, the remaining more distant prefixes with a smaller number of digits.

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

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

Once you have found the area codes that you would like to reroute, you can start assigning them to call-by-call providers. For this, you need the current rates of as many telephone providers as possible. These can also be found in the Internet. Addresses such as 'www.cheap-calls.com' (or 'www.focus.de' in Germany), for example, contain complete, up-to-date list-

ings for all types of connections. With this information on hand, you can now begin feeding your least-cost router...

## 4.5.2

### Setting up the least-cost router

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

- Which operating modes of the *ELSA LANCOM Wireless IL-11* should the services of the least-cost router use?
- Which calls should be routed over which provider?

To answer these questions, proceed as follows:

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



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

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

the LCR will start at the beginning after unsuccessfully trying the last network prefix.

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



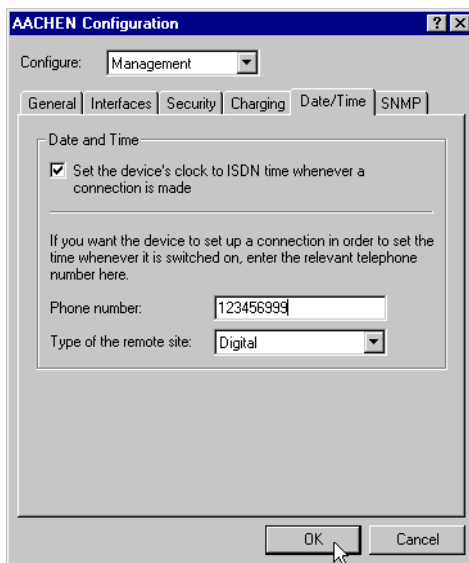
*Build the LCR table one step at a time and check your results. Open the ELSA LANmonitor, for example, and establish connections to the remote stations to be rerouted according to the table using the ELSA LANCAPI. Use the dialed number to verify whether the LCR settings suit your requirements. For router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

### Time for the selection

It goes without saying that the internal clock of the *ELSA LANCOM Wireless IL-11* must be set properly to ensure that the least-cost router correctly applies the information in the table. The router can also help itself in this respect as well, however: It can synchronize its internal clock with the time in the ISDN, either when switched on, or during each call establishment.

- ① In *ELSA LANconfig*, switch to the 'Date/Time' tab in the 'Management' configuration section.
- ② Activate the option for automatic synchronization at each call establishment. If you would rather enter the time manually, disable this option.

- ③ The current time is lost when the unit is switched off. Enter the number of a random remote station if you would like the device to establish a connection immediately upon being switched on, in order to synchronize the time with that of the ISDN network. Specify whether the remote station is digital (e.g. BBSs or Internet providers) or analog (telephone message or voice services).



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

## 4.6

### **ELSA CAPI Faxmodem**

The *ELSA CAPI Faxmodem* provides a Windows fax driver (Fax Class 1) as an interface between the *ELSA LANCAPI* and applications, permitting the use of standard fax programs with an *ELSA LANCOM Wireless IL-11*.

### 4.6.1

#### **Installation**

The *ELSA CAPI Faxmodem* can be installed from the CD setup. Always install the *ELSA CAPI Faxmodem* together with the current version of *ELSA LANCAPI*. After restarting, the *ELSA CAPI Faxmodem* will be available to you

system. Under Windows 95 or Windows 98, it can be found under **Start ► Control Panel ► Modems**.

## 4.6.2

### Faxing with the *ELSA CAPI Faxmodem*

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



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

## 4.7

### Office communications and *LANCAPI*

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

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

### 4.7.1

#### *LANCAPI* interface settings

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

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

- Subscriber numbers (MSN/terminal device selection numbers)

The *LANCAPI* responds to incoming calls for these numbers. Multiple numbers are separated by semicolons. If no subscriber number is specified, the router will respond to all incoming calls.



- Access to *LANCAPi*

Here you can completely disable the *LANCAPi* functions for the interface, or enable it only for incoming or outgoing calls.

- Transfer of own subscriber number

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

## 4.7.2

### The *ELSA LANCAPi*

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

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

#### Installing the *LANCAPi* client

The *LANCAPi* is made up of two components, a server (in the *ELSA LANCOM Wireless IL-11*) and a client (on the PCs). The *LANCAPi* client must be installed on those computers in the LAN that will be using the *LANCAPi* functions.

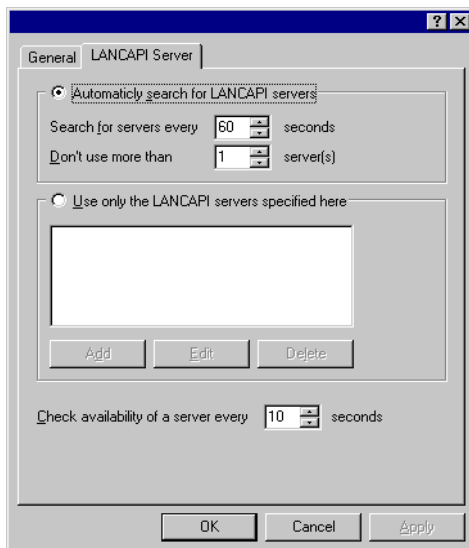
- ① Place the *ELSA LANCOM* CD in your CD-ROM drive. If the setup program does not automatically start when you insert the CD, simply click 'auto-run.exe' on the *ELSA LANCOM* CD in the Windows Explorer.
- ② Select the 'Install LANCOM software' entry.
- ③ Highlight the 'ELSA LANCAPi' option. Click **Next** and follow the instructions for the installation routine.

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

### Configuring the *LANCAPi* client

The configuration of the *LANCAPi* client is used to determine which *LANCAPi* servers will be used and how these will be checked. All parameters can remain at their default settings if you are using only one *ELSA LANCOM Wireless IL-11* in your LAN as a *LANCAPi* server.

- ① Start the *LANCAPi* client in the 'ELSAlan' program group. Information regarding the drivers for the available service can be found on the 'General' tab.
- ② Switch to the 'LANCAPi Server' tab. First, select whether the PC should find its own *LANCAPi* server, or specify the use of a particular server.
  - For the former, determine the interval at which the client should search for a server. It will continue searching until it has found the number of servers specified in the next field. Once the required number of servers has been found, it will stop searching.
  - In the event that the client should not automatically search for servers, list the IP addresses of the servers to be used by the client. This can be useful if you are operating several *ELSA LANCOM Wireless IL-11* in your LAN as *LANCAPi* servers and you would like to specify a server for a group of PCs, for example.
  - It is also possible to set the interval at which the client checks whether the found or listed servers are still active.



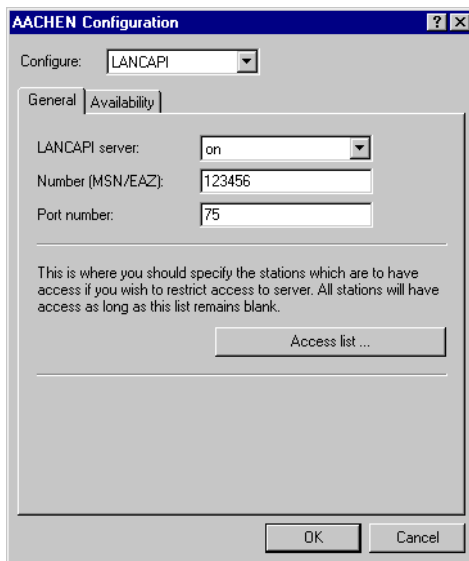
### Configuring the *LANCAPi* server

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

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

Set the relevant parameters as follows:

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

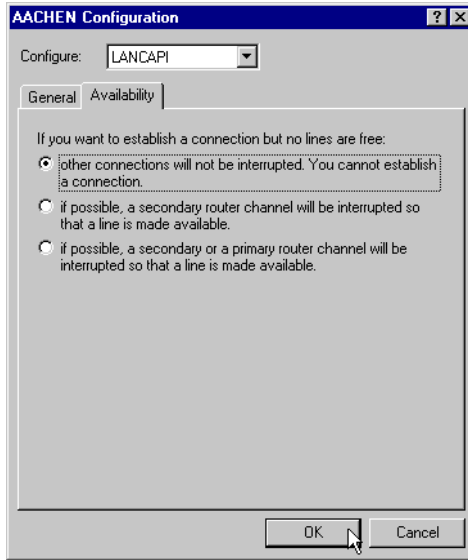


- ② Activate the *LANCAPi* server, or set it to permit outgoing calls only. In the latter case, the *LANCAPi* will not respond to incoming calls—to receive faxes, for example. Permitting outgoing calls only is useful if you do not have a specific call number available for the *LANCAPi*.
- ③ When the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



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

Switch to the 'availability' tab. Here you can determine how the *ELSA LANCOM Wireless IL-11* should respond if a connection is to be established via the *LANCAPI* (incoming or outgoing) when both B channels are already busy (priority control). The available options are:



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

### Using the *LANCAPI*

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

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

## 4.8

## Accounting

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.

## 4.8.1

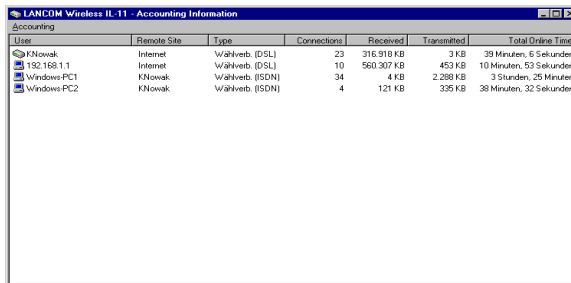
### Configuring accounting

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 time or transfer volume.

## 4.8.2

### 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	VaHVerb. (DSL)	23	318.919 KB	3 KB	39 Minuten, 6 Sekunden
192.168.1.1	Internet	VaHVerb. (DSL)	10	560.307 KB	453 KB	10 Minuten, 53 Sekunden
Windows-PC1	KNowak	VaHVerb. (ISDN)	34	4 KB	2.288 KB	3 Stunden, 25 Minuten
Windows-PC2	KNowak	VaHVerb. (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: PPP/MLPP (ISDN), PPPoE (DSL); routed protocols via ISDN/DSL: TCP/IP, IPX, NetBIOS/IP, LANCAPI (virtual CAPI 2.0)
ISDN	ISDN-S <sub>0</sub> bus, DSS1, 1TR6, autosense, optional fixed line available, CAPI server
Security	Password protection, address and protocol filters: WEP encryption, Closed Wireless Network, IP masquerading (NAT/PAT), firewall filters
Connects	10-base-T, ISDN S <sub>0</sub> , external power adapter (9V)
Package contents	<ul style="list-style-type: none"> <li>– Extensive documentation in German, English, French and Italian</li> <li>– Patch network cable (UTP)</li> <li>– ISDN S<sub>0</sub> cable</li> <li>– Plug-in power adapter</li> <li>– Software bundle CD with <i>ELSA RVS-COM</i>, Laplink Pro</li> <li>– CD with management software</li> </ul>

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 Switzer- land
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	<b>2462</b>	<b>2462</b>	<b>2462</b>	<b>2462</b>
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 IL-11*.



## 6

## Appendix

## 6.1

## Declaration of conformity

**KONFORMITÄTSERKLÄRUNG**

gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen  
(FTEG) und der Richtlinie 1999/5/EG (R&TTE)

EC- DECLARATION OF CONFORMITY appropriate to the law of radio and telecom terminalequipment and  
Directive 1999/5/EC (R&TTE)

Die Firma:  
The Company:

**ELSA AG**  
**Sonnenweg 11**  
**52070 Aachen**

erklärt, daß das Produkt:  
declares that the product:

**ELSA LANCOM Wireless IL-11**

Telekommunikations (TK-) Endeinrichtung  
telecommunications terminal equipment radio equipment

Verwendungszweck:  
intended purpose:

**Router**

den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG  
(Artikel 3 der R&TTE) entspricht.  
complies with the appropriate essential requirements of the FTEG (Article 3 of R&TTE) and the other relevant provisions.

Harmonisierte Normen:  
Harmonised Standards:

Gesundheit und Sicherheit gemäß §3 (1) 1. (Artikel 3 (1) a))  
Health and Safety requirements contained in §3 (1) 1. (Article 3 (1) a))

**EN 60 950: 1992 +A1: 1993 +A2: 1993 +A3: 1995 +A4: 1996 +A11: 1998**

Harmonisierte Normen:  
Harmonised Standards:

Schutzanforderungen in Bezug auf die EMV §3 (1) 2, Artikel 3 (1) b))  
Protection requirements with respect to EMC §3 (1) 2, (Article 3 (1) b))

**EN 50 082-1: 1992 Teile/parts: EN 61 000-4-2,3,4,6,**  
**EN 50 081-1: 1992 Teile/parts: EN 55 022: 1994, EN 61 000-3-2,3**

Schnittstellenspezifikation:  
Interface specification:

Netzabschluß eines öffentlichen Tk-Netzes  
Termination point of a public telecom. network

Spezifikation  
specification:

**TBR 3**

Diese Erklärung wird verantwortlich abgegeben durch:  
This declaration is submitted by:

Aachen, 14. April 2000  
Aachen, 14<sup>th</sup> 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-IL11* 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

- **Ziffern**
  - 1TR6 ..... 13
- **A**
  - Access control ..... 55
  - Access protection ..... 14
    - name ..... 60
    - name or number ..... 60
    - number ..... 60
  - Accounting ..... 18
  - Ad hoc network ..... 11, 50
  - Address administration ..... 67
  - Address pool ..... 68, 73
  - Advice of charge ..... 15
  - AirLancer Client Manager* ..... 16
  - AOCD ..... 15
  - Automatic synchronization ..... 78
  - Availability ..... 85
- **B**
  - B channel
    - connection status ..... 16
  - BACP ..... 15
  - Barring ..... 55
  - Base Station ..... 10
  - B-channel protocol ..... 60
  - Broadcast ..... 69
  - Brute force ..... 15, 55
- **C**
  - Call charge information ..... 18
  - Call charge management ..... 62, 66
  - Call number recognition ..... 14
  - Callback ..... 57, 61
    - fast call back ..... 61
  - Callback function ..... 14
  - Call-by-call ..... 74, 75
  - CAPI Faxmodem* ..... 17, 79
  - CAPI interface ..... 80
  - CD ..... 21
  - Challenge Handshake Authentication Protocol ..... 60
  - Channel bundling ..... 15
    - dynamic ..... 15
    - static ..... 15
  - CHAP ..... 60
  - Charge monitoring ..... 15
  - charges ..... 74
  - CLIP ..... 14
  - Closed network ..... 56
  - Compression ..... 15
  - Configuration ..... 14
    - SNMP ..... 43
  - Connect-charge structure ..... 76
  - Connection duration ..... 16
- **D**
  - Data encryption ..... 56
  - Data volume ..... 18
  - Days of the week ..... 75
  - Detour ..... 75
  - DHCP ..... 67, 68
  - DHCP mode ..... 67
  - DHCP server ..... 67
    - configuration ..... 71
  - Dialing prefix ..... 75
  - Dial-up connection ..... 40
  - Dial-up Networking ..... 61
  - DNS server ..... 17, 67, 69
  - DSL ..... 53
  - DSS1 ..... 13
  - Dynamic channel bundling ..... 15

- **E**
  - Electronic documentation .....21
  - End address .....68
  - Ethernet .....13
    - 10Base-T .....13
  - Ethernet connection .....10
  - EuroFileTransfer .....17
- **F**
  - Factory defaults .....27
  - Fast Call Back .....61
  - Fax .....17, 79
  - Fax Class 1 .....79
  - Fax driver .....79
  - Fax transmission .....80
  - Faxmodem .....17
    - LANCAPi* .....80
  - Filter .....57
  - Firewall .....15, 57
    - Filter list .....59
    - Object list .....58
    - Rule table .....58
  - Firewall function .....62
  - FirmSafe .....14, 43
  - Firmware .....14
  - Firmware upload .....44
    - using TFTP .....45
    - with LANconfig .....45
  - Flash ROM .....14, 43
- **G**
  - Gateway .....61, 67, 69
- **H**
  - High telephone costs .....66
  - holidays .....75
- **I**
  - Identifying the caller .....60
  - Inband
    - using telnet .....39
  - Infrastructure network .....11, 51
  - Install software .....43
  - Installation .....13
  - Internal clock .....78
  - International calls .....74
  - IP address .....61
  - IP masquerading .....15, 57, 61
  - ISDN .....52
  - ISDN cable .....13
  - ISDN connection cable .....21
  - ISDN time .....15
  - ISDN-S<sub>0</sub>-Anschluß .....29
- **L**
  - LAN .....10
  - LAN connection .....13
  - LAN connector cable .....21
  - LANCAPi* .....17, 80
  - LANCAPi-Client* .....81
  - LANCAPi-Server* .....83
  - LANCOM
    - LED indicators .....16
  - LANconfig* .....30, 37, 40, 44, 47
  - LANmonitor* .....16, 46
  - LCR .....15, 74
  - LCR table .....74
  - Least-cost router .....74, 77
    - automatic fallback .....77
    - connect-charge monitoring .....77
    - operating modes .....77
  - Least-cost routing .....15
  - LED .....26
    - LAN Status .....27
    - Power/Msg .....27
  - Line connection .....18
  - Line management .....18
  - Local area network .....10
  - Local calls .....76
  - Login .....44, 55

Login barring .....	55
Long distance calls .....	75

## ● M

MLPPP .....	15
Mode .....	67
Monitoring .....	46
Multi-device terminal .....	13

## ● N

NAT .....	57, 61
NBNS server .....	67, 69
Neighboring local exchanges .....	76
NetBIOS .....	18
Network identification prefix .....	74
Network operators .....	74

## ● O

Office communications .....	80
Online media .....	37
Online time .....	18
Operating modes .....	49
Options for saving telephone charges .....	76

## ● P

Package contents .....	21
PAP .....	60
Password .....	42, 60, 61
Password protection .....	14, 54
PAT .....	57, 61
Peer-to-peer network .....	11, 18
Period of validity .....	67, 70
Point-to-multipoint configuration .....	13
Point-to-point configuration .....	13
Point-to-point network .....	52
Port .....	84
Power adapter .....	21
PPP .....	61
PPP client .....	40
PPP connection .....	41

PPP list .....	60
PPP negotiation .....	42
Prefix .....	74
Preselection .....	74
Priority control .....	85
Provider .....	74
Proxy .....	18

## ● R

Radio cell .....	10
Radiofrequency channels .....	91
Range .....	11
Rate zones .....	76
Remote connection .....	40
Reset button .....	27
Roaming .....	11

## ● S

S <sub>0</sub> Status .....	27
S <sub>0</sub> -Schnittstelle .....	13
Security .....	54, 57, 61
Device .....	54
WLAN .....	56
Security procedures .....	60
Single user access .....	61
SNMP .....	43
Software update .....	14
Special prefixes .....	76
Specifications .....	89
Standard fax programs .....	79
Start address .....	68
Static channel bundling .....	15
Station filter .....	56
Statistics .....	16
Status displays .....	16
Subnet mask .....	69
System terminal .....	13

## ● T

TCP/IP .....	30
--------------	----

Telephone provider .....	76
Telnet .....	40
Time .....	75, 78
Time check .....	15
Time in the ISDN .....	78
Time of day .....	75
Transfer costs .....	18
Transmission rates .....	16
Troubleshooting .....	46

## U

Upload .....	14, 44
User name .....	42, 61

## W

WAN Chan1 .....	28
WAN Chan2 .....	28
WAN connection .....	13
Warranty conditions .....	94
<i>WEBconfig</i> .....	44, 45
WEP .....	56
Windows networks .....	18
Winipcfg .....	32
Wireless Internet Gateway .....	52, 53
Wireless LAN .....	10
Wireless network .....	9
Wireless network adapter .....	10
WLAN .....	10
WWW .....	61