

Contents

User Manual

Introduction	Chapter 1.1
Introducing the <i>LANCOM Office</i> router	Chapter 1.2
Configuration modes	Chapter 1.3
<i>LANCOM Office</i> router operating modes	Chapter 1.4
Bridge or router?	
The bridge in the network	
The IP router	
The IPX router	
Office communications and <i>LANCAPI</i>	
Automatic address administration with DHCP	
The least-cost router	
Point-to-point protocol	Chapter 1.5
Communications software	Chapter 1.6

Workshop

Foreword	Chapter. 2.1
Internet applications	Chapter 2.2
LAN to LAN couplings	Chapter 2.3
Remote access	Chapter 2.4
PBX and least-cost router	Chapter 2.5
Office communication (<i>LANCOM Office</i> only)	Chapter 2.6
Access to the ELSA test network	Chapter 2.7
Error Search	Chapter 2.8

Reference Manual

Only available as electronic documentation (PDF) on CD

Description of the menu options	Chapter 3.1
<i>LANCOM Office</i> router intern	Chapter 3.2
Messages, numbers, ports	Chapter 3.3

Appendix

Addendum

Supplements to the user manual covering new software and firmware versions and also additional functions.

© 1999 ELSA AG, Aachen (Germany)

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

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from ELSA.

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

Trademarks

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

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

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

ELSA AG
Sonnenweg 11
D-52070 Aachen
Germany
www.elsa.de

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

Aachen, May 1999

Art.-Nr. 20795/0599

Preface

Thank you for placing your trust in this ELSA product.

By selecting the *ELSA LANCOM Office* router you have chosen an ISDN router which you can use to connect local area networks with other networks just as simply as you connect with other remote workstation computers or the Internet. The highest quality standards in manufacturing and stringent quality control are the basis for high product standards and consistent quality of ELSA products.

Documentation

The accompanying documentation comprises:

- Installation Guide

Hardware installation and configuration examples

- Manual

Comprehensive description of the *LANCOM Office* router, further configuration examples, reference manual

Online Services



If you still have questions or require additional help, our online services are at your disposal around the clock. The complete range of support and services provided by ELSA can be found in the "Advice and Help" section in the Appendix.

User Manual

Introduction	1.1.1
What does a <i>LANCOM Office</i> router do?	1.1.2
What does the <i>ELSA LANCOM Office</i> router offer?	1.1.4
What will you find in this documentation?	1.1.9
CE Conformity	1.1.10
Introducing the <i>LANCOM Office</i> router	1.2.1
The <i>LANCOM Office</i> router takes the stage.....	1.2.2
What does the <i>LANCOM Office</i> router look like?.....	1.2.2
How do you connect the <i>LANCOM Office</i> router?.....	1.2.5
Security for your LAN.....	1.2.7
Security check	1.2.7
Login barring	1.2.8
Callback	1.2.9
The hiding place—IP masquerading (NAT, PAT).....	1.2.9
Costs under control	1.2.10
Selecting what's relevant	1.2.10
Faster, faster—data compression and channel bundling	1.2.12
Costs under control—call charge management.....	1.2.12
The least-cost router	1.2.13
Compatible communication	1.2.14
Online or offline—the line used for the connection	1.2.14
Transfer protocols	1.2.14
The chameleon.....	1.2.15
Configuration modes	1.3.1
Many paths lead to the <i>LANCOM Office</i> router.....	1.3.2
The direct method: outband.....	1.3.3
The user-friendly method: inband.....	1.3.4
Remote access: configuration using a dial-up connection.....	1.3.6
Configuration commands	1.3.9
Configuration using SNMP	1.3.10
General.....	1.3.10
Accessing tables and parameters using SNMP	1.3.10
The Management Information Base (MIB)	1.3.12
What's happening on the line?	1.3.13
<i>ELSA LANmonitor</i>	1.3.13
Trace outputs	1.3.14
New firmware with FirmSafe	1.3.17
This is how FirmSafe works.....	1.3.17

How to load new software	1.3.18
LANCOM Office router operating modes	1.4.1
Bridge or router?	1.4.2
The bridge in the network.....	1.4.4
The IP router.....	1.4.6
Naming IP addresses	1.4.6
The IP routing table.....	1.4.7
What happens when data is transmitted on an IP network?	1.4.10
TCP/IP packet filters.....	1.4.11
Proxy ARP	1.4.11
Local routing.....	1.4.12
Dynamic routing with IP RIP.....	1.4.13
IP masquerading (NAT, PAT).....	1.4.15
DNS forwarding	1.4.18
Access verification.....	1.4.18
Policy-based routing.....	1.4.19
The IPX router	1.4.20
Naming IPX addresses	1.4.20
Information about the LAN	1.4.20
IPX routing table.....	1.4.20
What happens when data is transmitted on an IPX network?	1.4.22
RIP and SAP tables.....	1.4.22
So many <i>LANCOM Office</i> routers around here.....	1.4.22
Redundant routes.....	1.4.23
Exponential backoff.....	1.4.23
IPX packet filters	1.4.24
<i>ELSA LANCAPI</i>	1.4.26
Automatic address administration with DHCP.....	1.4.31
DHCP, short and sweet	1.4.31
How are the addresses assigned?.....	1.4.32
Configuring the <i>LANCOM Office</i> router as a DHCP server.....	1.4.35
The integrated PBX	1.4.39
Connecting analog terminals	1.4.39
Configuration with <i>ELSA LANconfig</i> and the Setup Wizard.....	1.4.40
Manual configuration with <i>ELSA LANconfig</i>	1.4.41
Operating the PBX via telephone.....	1.4.49
The least-cost router.....	1.4.56
Point-to-point protocol	1.5.1
The protocol	1.5.2
The PPP list	1.5.4
Everything ok? Checking the line with LCP.....	1.5.5
Assigning IP addresses via PPP	1.5.6

Callback functions.....	1.5.8
Microsoft CBCP callback.....	1.5.8
Fast ELSA callback	1.5.10
Callback as specified in RFC 1570 (PPP LCP extensions).....	1.5.11
Channel bundling with MLPPP.....	1.5.12
Communications software	1.6.1
<i>ELSA-RVS-COM</i>	1.6.2
What does <i>ELSA-RVS-COM</i> offer?	1.6.2
Setup for <i>ELSA-RVS-COM</i>	1.6.2
The installation wizard for <i>ELSA-RVS-COM</i>	1.6.3
LapLink	1.6.5
The 'Take Two' license.....	1.6.5
What can LapLink do?	1.6.5
Connection paths for LapLink.....	1.6.5
Installing and uninstalling.....	1.6.6
<i>ELSA-ZOC</i>	1.6.7
What does <i>ELSA-ZOC</i> offer?	1.6.7
Installing <i>ELSA-ZOC</i>	1.6.7

Workshop

Foreword	2.1.1
Configuration using <i>ELSA LANconfig</i> and the wizards.....	2.1.2
Configuration without wizards.....	2.1.2
Which <i>LANCOM Office</i> router are you using?	2.1.2
Additional information	2.1.2
Internet applications	2.2.1
Internet access for all PCs on the LAN	2.2.2
Intranet with its own Web server on the Internet.....	2.2.7
LAN to LAN couplings	2.3.1
Networks connected with the IP router.....	2.3.2
Two IP routers for four branches	
(static scaling).....	2.3.8
Two IP routers for six branches	
(dynamic scaling)	2.3.16
Networks connected with the IPX router	2.3.25
Several IPX routers in one Network	
(scaling).....	2.3.31
Two networks connected via the bridge	2.3.37
Remote access	2.4.1
Remote access using TCP/IP	2.4.2
Remote access for IPX	2.4.7
PBX and least-cost router	2.5.1
Example: small office.....	2.5.2
The PBX.....	2.5.3
The least-cost router.....	2.5.6
Office communication	2.6.1
Faxing with <i>ELSA-RVS-COM</i>	2.6.2
Telephone and answering machine.....	2.6.4
Computer telecontrol with LapLink.....	2.6.5
Establishing a connection	2.6.5
EuroFileTransfer with <i>ELSA-RVS-COM</i>	2.6.6
Mailboxing with <i>ELSA-ZOC</i>	2.6.8
Access to the ELSA test network	2.7.1
Router mode using PPP	2.7.3
Router mode using the ELSA protocol	2.7.8
Bridge mode.....	2.7.11

Error Search	2.8.1
The Search Methods.....	2.8.2
No Connection to the Internet	2.8.3
Computer in the other Network Cannot Be Reached	2.8.4
Error Search in TCP/IP Networks	2.8.4
Error Search in IPX Networks.....	2.8.5
Unwanted Call Origination	2.8.6

Reference Manual

Only available as electronic documentation (PDF) on CD

Description of the menu options	3.1.1
Status	3.1.3
Status/Connection-state	3.1.4
Status/Current-time	3.1.5
Status/Operating-time	3.1.5
Status/S0-bus	3.1.5
Status/WAN-statistics.....	3.1.5
Status/LAN-statistics.....	3.1.8
Status/PPP-statistics.....	3.1.8
Status/Bridge-statistics	3.1.15
Status/IPX-statistics	3.1.16
Status/TCP-IP-statistics	3.1.21
Status/IP-router-statistics.....	3.1.24
Status/Config-statistics	3.1.26
Status/Queue-statistics	3.1.27
Status/Connection-statistics	3.1.28
Status/Info-connection	3.1.29
Status/Layer-connection	3.1.29
Status/Call-info-table	3.1.30
Status/Remote-statistics	3.1.30
Status/Channel-statistics	3.1.31
Status/Time-statistics.....	3.1.32
Status/Delete-values	3.1.33
Setup	3.1.34
Setup/WAN-module	3.1.35
Setup/Charges-module	3.1.46
Setup/LAN-module	3.1.49
Setup/Bridge-module.....	3.1.50
Setup/IPX-module	3.1.52
Setup/TCP-IP-module.....	3.1.60
Setup/IP-router-module	3.1.64
Setup/SNMP-module.....	3.1.71
Setup/DHCP-module	3.1.72
Setup/Config-module.....	3.1.74
Setup/ab-module	3.1.75
Setup/LANAPI-module.....	3.1.78
Setup/LCR-module	3.1.79
Setup/Time-module	3.1.80

Setup/Other.....	3.1.81
Firmware	3.1.82
Other	3.1.84
LANCOM Office router Internal	3.2.1
Script Processing	3.2.2
General.....	3.2.2
The Script List	3.2.2
CompuServe Select.....	3.2.3
Online Trace Outputs	3.2.5
General.....	3.2.5
Control of Trace Outputs.....	3.2.5
Examples for Control of Trace Outputs.....	3.2.7
Supported Protocols and Functions	3.2.7
Policy Based Routing	3.2.19
General.....	3.2.19
Examples	3.2.20
Messages, Numbers, Ports	3.3.1
Error Messages.....	3.3.2
LANCOM Office router Error Messages	3.3.2
ISDN Error Messages.....	3.3.2
PPP Error Messages	3.3.3
Modem Error Messages.....	3.3.5
Status Displays	3.3.6
Novell SAP Numbers	3.3.8
TCP/IP Ports	3.3.12

Appendix

Appendix	A-1
Technical Data	A-2
Hardware Specifications.....	A-2
Standards:	A-2
Connector Pinouts:	A-4
Frequently Asked Questions and Answers.....	A-5
General.....	A-5
IP-RIP	A-9
PPP	A-11
Bridge	A-13
IPX Router.....	A-14
IP Router.....	A-19
Warranty conditions	A-22
Glossary	A-24
Index.....	A-31



Introduction

The current use of modern ISDN communication is making Internet and Intranet applications more and more important for companies in various industries. On-line services are increasingly being used for professional purposes. Company branch offices are being interconnected to enable fast communications between different sites, and telecommuting is gaining increasing importance.

All these applications are making the use of ISDN router solutions more attractive than ever. *ELSA LANCOM Office* routers connect local networks with the Internet and act as a communications center for handling fax and voice mail services in small and medium-sized companies.

ELSA LANCOM Office router also connect local networks with other LANs and provide access to company data via their remote access function.

What does a <i>LANCOM Office</i> router do?	2
What does the <i>ELSA LANCOM Office</i> router offer?	4
What will you find in this documentation?	9
CE Conformity	10

What does a *LANCOM Office* router do?

An ISDN router such as the *LANCOM Office* router uses ISDN lines to link Local Area Networks (LANs) and individual PCs to form a Wide Area Network (WAN). This allows any computer in this WAN to access the computers and services on the entire network, depending on its access privileges. The router does this by seeking out a path, for example via a telephone connection, over which data can be exchanged between the computers.

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

But that's not all the *ELSA LANCOM Office* router does. Using a special interface called the *ELSA LANCAPI™*, modern office communications functions such as fax, telephone answering machine, online banking etc. can be provided on the entire local network. The corresponding communications programs forward their data via the *LANCAPI* to the *LANCOM Office* router which then takes care of the data transmission. This makes an expensive and maintenance-intensive installation of ISDN adapters in every workstation quite unnecessary.

The *LANCOM Office* router is incorporated into the network in the same way as any normal PC. Any data traveling on the network cable, therefore, is seen by the router too. The router automatically determines whether or not the data needs to be transmitted to another network and, if necessary, establishes a connection to the destination network via the ISDN line. Of course, a dedicated ISDN line does away with the process of establishing a connection.

When precisely should the *LANCOM Office* router be used?

As a matter of fact, wherever computers need to be joined together and a simple modem operation no longer fits the bill. Here are some example applications:

- Internet on the LAN

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

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

- LAN to LAN coupling

When business is going well, the time eventually comes for a sister company or subsidiary to be established in the global markets. Of course, the branch office, too, has its own network and must to be kept up-to-date.

LAN to LAN coupling links the individual LANs to form one large network, even if this means crossing continents. When connecting via a dial-up connection, an intelligent line management function together with sophisticated filter mechanisms keeps connections costs low. Of course, it is also possible to operate a combination of dedicated lines and dial-up connections.

■ Teleworking using remote access

The work of many office workers in modern organizations is less and less dependent on any definite location—the most important factor here is unimpaired access to shared and freely available information.

Remote access is the key to this. The router on the local network at the head office enables colleagues to telecommute from their home offices and traveling staff to access the office while on the road. The *LANCOM Office* router naturally also does everything necessary to protect the company's data holdings during remote access: the callback function uses the names and call numbers entered to provide access to specified users only. And telephone charges are calculated at head office, simplifying the billing process.

■ Office communications using *LANCAPI*

Faxing directly from within applications, voice mail with different announcements according to the time of day, banking without having to leave the office: These functions are made possible by using the *LANCAPI*.

The *LANCAPI* is special type of CAPI 2.0 interface through which applications such as *ELSA-RVS-COM* and *ELSA-ZOC* can access *ELSA LANCOM Office* routers.

■ Telephone functions

In addition to its ISDN router features, the *LANCOM 2000 Office* also contains an integrated private automatic branch exchange with four analog connections (a/b ports). Analog terminal devices such as telephones or fax machines can be connected to these ports, making the expense of acquiring new ISDN terminal devices unnecessary in the transition from an analog telephone connection to a modern ISDN Basic Rate Interface.

The *LANCOM Office* router provides many useful functions such as internal call switching, internal calls, brokering, consultation hold, call redirection, call pickup, call charge metering, etc.

What does the *ELSA LANCOM Office* router offer?

The following is an outline of the principal features of the *LANCOM Office* router giving you a quick overview of its capabilities.

Easy installation

LANCOM Office routers by ELSA are particularly easy to install:

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

LAN connection

ELSA's ISDN routers work on Ethernet networks. Connect the *LANCOM 1000 Office* or *LANCOM 2000 Office* with the 10 Mbit LAN using the 10Base-2 or 10Base-T ports. A *LANCOM 1100 Office* can be connected to a (Fast) Ethernet network using the 10/100Base-T port.

WAN connection

The *LANCOM Office* router is connected to the S_0 interface of an ISDN Basic Rate Interface in point-to-multipoint configuration (multi-device terminal) or in point-to-point configuration (system terminal). The *LANCOM Office* router automatically detects your port type and the D-channel protocol being used.

The *LANCOM Office* router will, of course, also support channel bundling. Switched connections using DSS1 or 1TR6 can also be used, as can leased-line connections.

Compatibility

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

Status displays

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

ELSA LANmonitor

Not only the LEDs give you an indication of the router status. Users of Windows 95, Windows 98 or Windows NT 4.0 have another option. With the *LANmonitor* you have

status information of the *LANCOM Office* router permanently on your monitor. For each device on the local network, the *LANmonitor* displays the most important information, e.g.:

- Connection status for each B channel
- Name of the remote side
- The *LANCOM Office* router module (router, *LANCAPi*, a/b port) connected
- Connection duration and transmission rates
- Excerpts of the device statistics (e.g. PPP negotiation data)

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

Configuration using *ELSA LANconfig*

Setting up and configuring the *LANCOM Office* router to your specific needs is made quick and easy in Windows 95, Windows 98 and Windows NT 4.0 by the configuration tool supplied, *ELSA LANconfig*. Users of other operating systems can use any telnet or terminal program. This means that you can access the *LANCOM Office* router from the WAN, from the LAN or directly via your own configuration interface. TFTP is supported along with SNMP if configuring from the LAN or WAN.

The integrated installation wizards help you to setup the *LANCOM Office* router in just a few steps.

Remote configuration using PPP

One special configuration feature of the *LANCOM Office* router which cannot and should not be setup locally is its ability to be configured remotely via the Dial-Up Network. All you have to do is to plug the new device into the power supply and connect it to the ISDN Basic Rate Interface. Now you can access the *LANCOM Office* router using a PPP connection and configure it from your location. The first time the device is configured, access to it is secured and thereafter it remains inaccessible to unauthorized callers.

Line establishment and management

The *LANCOM Office* router checks whether any data on a network is intended for transmission to another network or another computer. The *LANCOM Office* router automatically establishes the connection if a transmission is required and closes the connection when the transmission is completed. If call charge information is received during the transmission, any partly used call charge units are used up in full.

The *LANCOM Office* router offers various filter options, depending on the operating mode, to save on transfer costs. This enables you to prevent the data from entire networks or parts of networks being transferred. Similarly, data belonging to specific services (print services, for example) can be filtered out of the transfer, too.

Least-cost routing

Even if there is a large selection of telecommunications service providers you can always use the cheapest lines using the least cost router. As a once-off step, you define once the providers who have the lowest rates for your needs. For each connection the *LANCOM Office* router automatically selects the provider with the lowest rate (whether it is used by the router, the *LANCAPi* or the a/b ports).

Intruder protection

Along with password protection and call number recognition, the *LANCOM Office* router offers protection against unauthorized access to the company network by means of a callback function which only permits a connection to be established from the *LANCOM Office* router to previously defined telephone connections. Furthermore, login barring prevents any “brute force attacks” and denies access to the *LANCOM Office* router after a configurable number of login attempts using an incorrect password.

Charge monitoring

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

Software update

The *LANCOM Office* router incorporates a flash ROM. 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, for example, and can be loaded into the *LANCOM Office* router via the LAN, the WAN or the configuration interface.

FirmSafe

There is no risk involved with loading the new firmware: The FirmSafe function enables two firmware files to be managed on one *LANCOM Office* router 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 on the ISDN) the functioning previous version is automatically reactivated.

Statistics

The comprehensive statistics function lets you keep track of your *LANCOM Office* router. These statistics give you all the information you need on the connections established, for example, so that you can optimize the configuration of your ISDN router.

Automatic time check

In order to generate sound statistics and to select the correct connection paths using the least cost router, the *LANCOM Office* router always must have the exact time. The device 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.

Operating modes

The *LANCOM Office* router uses the bridge to link networks using any protocol at MAC address level. Networks using TCP/IP or IPX/SPX can use the router functions. This means that all operating modes can run parallel and simultaneously on the device, if desired.

With the included *ELSA LANCAPI*, furthermore, a *ELSA LANCOM Office* router can be operated as a CAPI server on the network.

Additionally, a complete PBX with four ports is integrated in the *LANCOM 2000 Office*.

DHCP

The *LANCOM Office* router also incorporates the functions of a DHCP server. Thus you can define a certain range of IP addresses which the *LANCOM Office* router then independently assigns to the individual devices on the local network.

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

Office communications using *ELSA LANCAPI*

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*) can access the *LANCOM Office* router.

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

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

The integrated private automatic branch exchange

A *LANCOM 2000 Office* offers yet more. Analog telephones, fax machines or modems can be connected to the four integrated a/b ports.

*LANCOM 2000
Office only*

The a/b ports are of particular use when switching from analog lines to digital connections (ISDN). With a *LANCOM 2000 Office*, analog terminal devices such as telephones and fax devices can continue to be used at the work place. This saves on any additional investment in new digital terminal devices. Additionally, the PBX on the *LANCOM 2000 Office* provides extra ISDN functions such as call forwarding, recall, brokering, holding and three-party conferencing, internal calls, baby monitoring, call charge metering and many more.

What will you find in this documentation?

User Manual

First of all you will find an exhaustive description of the router's functions and characteristics. We will then explain how the *LANCOM Office* router operates and the tools available to you for configuring it.

Workshop

The Workshop introduces you to practical matters. In addition to the special functions and capabilities of bridge, IPX and IP routers, you will learn all you need to know about the router's extensive filtering mechanisms. The practical section concludes with sample applications such as LAN to LAN coupling, Internet hookup, remote access and access to the ELSA test networks. You will also find some additional instructions on analytical troubleshooting using the router's help utilities intended for this purpose (statistics and trace outputs, for example).

Reference Manual

This guide contains a reference section. This provides all the *LANCOM Office* router software commands. The documents contain easy-to-understand explanations for all those who are not professionals in network technology or ISDN and so do not require any in-depth knowledge in advance. The reference manual concludes with notes on script processing and trace outputs.

You will find this part of the documentation only on the *ELSA LANCOM-CD*.

Appendix

In the appendix you will find technical data on the router, contact addresses, conditions of service and warranty conditions. Here you will find answers to frequently asked questions (FAQs), the glossary explains the technical jargon used in this Manual and the index helps you to quickly find the information you are looking for.



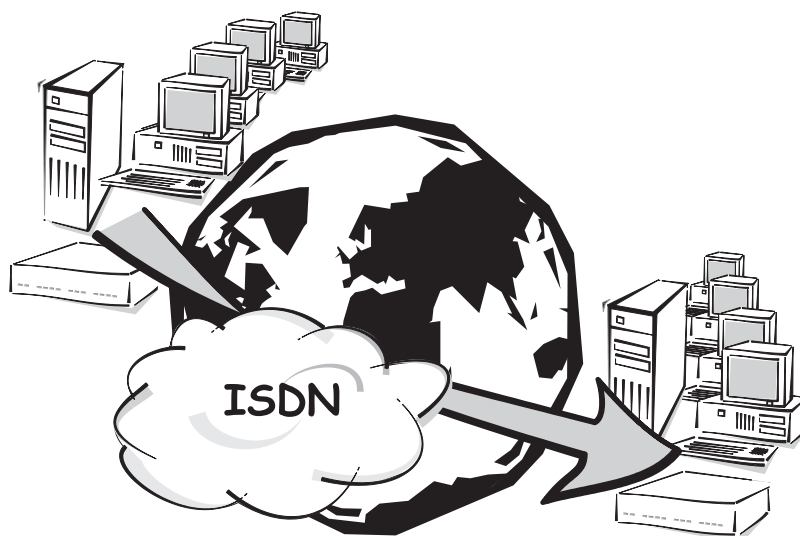
CE Conformity

This equipment has been tested and found to comply with the limits of the European Council Directive on the approximation of the laws of the member states relating to electromagnetic compatibility (89/336/EEC) according to EN 55022 class B.

The operation of this device in a manner not in accordance with the directions or within the proximity of powerful transmitters may lead to its temporary failure.

These limits are designed to provide reasonable protection against radio frequency interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may interfere with radio communications if not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception (this can be determined by turning this equipment off and on), the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between this equipment and the receiver.
- Connect the equipment to an outlet on a circuit other than that to which the receiver is connected.
- Consult your dealer or an experienced radio/TV technician.
- Caution: To comply with the limits for an FCC Class B computing device, always use a shielded signal cable.



Introducing the *LANCOM Office* router

The *LANCOM Office* routers' core function is their data transfer function. Above all, the connections have to be secure, reliable, economical and compatible, as the data is transferred over public telephone lines.

Furthermore, it should be simple to configure, no matter what the computing environment, and offer the user the best possible solution, no matter what the problem...

This section will introduce you to the display elements of the *LANCOM Office* routers, the connectivity they offer and the properties and functions they use to meet the requirements listed above.

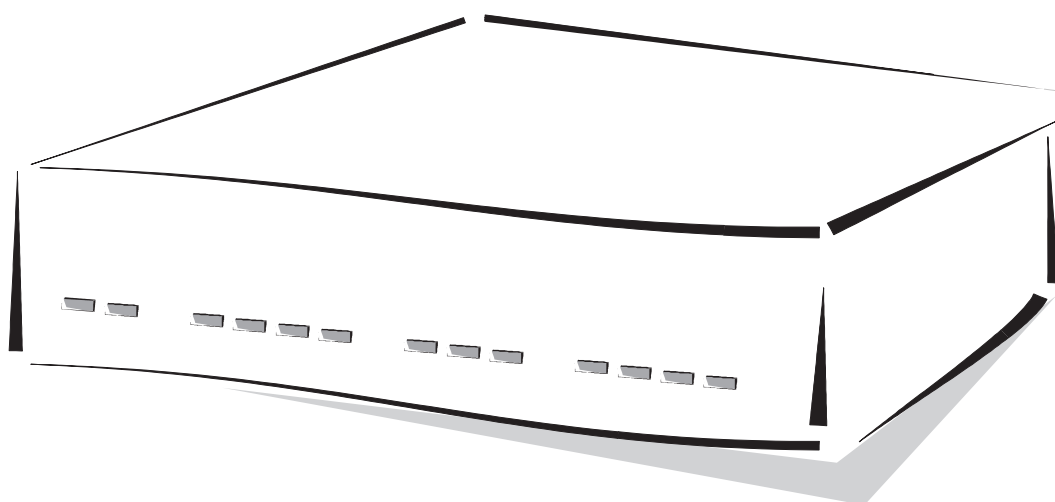
The precise use of the *LANCOM Office* router's features will be explained in the following sections and with the aid of the examples in the 'Workshop'.

The <i>LANCOM Office</i> router takes the stage.....	2
Security for your LAN.....	7
Costs under control.....	10
Compatible communication	14

The *LANCOM Office* router takes the stage



















What does the *LANCOM Office* router look like?

We would first like to familiarize you with the *LANCOM Office* router. You will find a number of LEDs as display elements on the front panel.



Finally, the LEDs tell you what is happening on the LAN and WAN. Starting on the left-hand side, take a look at each of the LEDs:

LED	Color	Meaning	LANCOM 1000 Office	LANCOM 1100 Office	LANCOM 2000 Office
Power/ Power msg	red	'Power On' / 'Self Test' / 'Ready'	☑	☑	☑
S0 status	green	S ₀ bus status (TEI present)	☑	☑	☑
Port 1	red/ green	a/b port 1 activity	☒	☒	☑
Port 2	red/ green	a/b port 2 activity	☒	☒	☑
Port 3	red/ green	a/b port 3 activity	☒	☒	☑
Port 4	red/ green	a/b port 4 activity	☒	☒	☑
WAN-chan1	red/ green	B channel data activity	☑	☑	☑
WAN-chan2	red/ green	B channel data activity	☑	☑	☑
WAN-1+2	green	Channel bundling	☑	☑	☑
LAN-tx	yellow	LAN packet being sent	☑	☒	☑

LED	Color	Meaning	LANCOM 1000 Office	LANCOM 1100 Office	LANCOM 2000 Office
LAN-rx	green	LAN packet being received			
LAN-rx/tx	yellow	LAN packet being received/sent			
LAN-Coll	red	LAN collisions			
LAN-Link	green	LAN connection ok			
LAN-FDpx	green	Full duplex operation			
LAN-Fast	green	Connected to 100Mbit LAN			

The various LEDs show the current operating status with various displays, as described below:

Power
Power msg

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

off		Device off
red	1 x short	Boot procedure (test and load) started
red	flashing	Display of a boot error (flashing light code)
red		Device ready for use
red	inter.	Error message or a charge block prevents outgoing calls

S₀ status

This LED shows the status of the S₀ connection:

off		Not connected or no S ₀ voltage (on ISDN Basic Rate Interfaces the S ₀ voltage is often dropped after a certain period of inactivity)
green	flashing	Initialization (contacting connecting station)
green		Ready for use (S ₀ bus activated, TEI present and D channel protocol checked)
green	once short off	Incoming digital call
green	twice short off	Incoming analog call
green	power off	LED is on and power LED is off: device in boot monitor

a/b 1 to a/b 4 With the *LANCOM 2000 Office*, these LEDs show the status of the analog connections:

off		a/b port idle
green		Connection is established
green	flashing	Outgoing call in progress (port off hook) (standard flashing)
green	flashing	- B channel not available (on bus or internally) - DTMF receiver not present (anymore) - ISDN line not available
red	flashing	Incoming call (LED in ringing sequence)
red	single flash	Incoming call, MSN OK, port blocked for incoming calls

WAN-chan1
WAN-chan2

These LEDs show the status of the corresponding logical WAN channel (in both router operation and in CAPI operation):

off		Channel idle
red	flashing	Incoming call
green	flashing	Outgoing call in progress
red		Channel physically established / protocol being negotiated
green		Associated protocol negotiation (X.75, PPP, etc.) is complete; channel logically online
green/ red	short red flashes (dur. approx. 1/10 sec)	Indicates a sent or received data packet



WAN channels have no fixed assignment to B channels!

WAN 1+2

This LED indicates whether the current connection is a static or dynamic channel grouping.

off	Connection or trunk connection not active
green	Static or dynamic trunk connection active

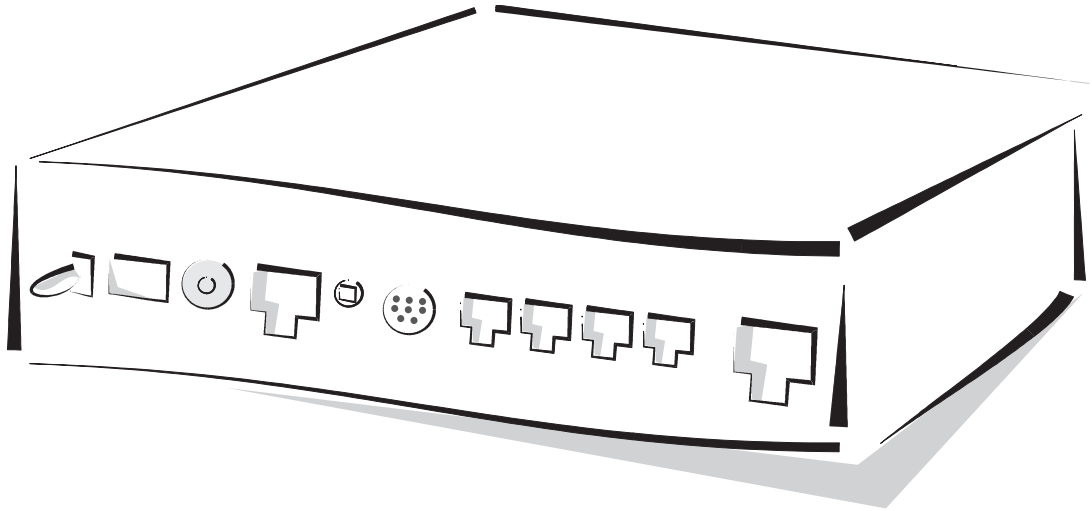
LAN-tx, -rx,
LAN-Coll, -Link

These LEDs show the corresponding network controller status:

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

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

For example:
LANCOM 2000
Office



- On/Off switch
- Connection for power supply unit
- 10Base-2 (BNC), only *LANCOM 1000 Office* or *LANCOM 2000 Office*
- 10Base-T (*LANCOM 1000 Office* or *LANCOM 2000 Office*) for 10 Mbit networks or 10/100Base-TX (*LANCOM 1100 Office*) for 10 Mbit or 100 Mbit networks
- Node/hub selector switch
- V.24 configuration interface
- Four analog terminals (POTS, a/b ports, only *LANCOM 2000 Office*)
- ISDN S₀ port

How do you connect the LANCOM Office router?

Network connection

You can connect the *LANCOM Office* router to your local (Ethernet network at 10 Mbit (as of *LANCOM 1100 Office* also Fast Ethernet at 100 Mbit) very simply like any workstation computer.

LANCOM 1000 Office and *LANCOM 2000 Office* offer 10Base-T and 10Base-2 ports, and the *LANCOM 1100 Office* has a 100Base-TX port.

Node or hub?

If you are using a twisted pair cable (10Base-T or 100Base-TX) to connect the *LANCOM Office* router to the network, you must check the setting of the node/hub switch:

- As the factory default, the switch is set to 'Node'. In this setting, the *LANCOM Office* router acts as a node on a network. The *LANCOM Office* router can, in this case, only be connected to a hub, not directly to the network card of a computer.

- Set the switch to 'Hub' if you do not wish to connect the *LANCOM Office* router to a hub but directly to a workstation. In this setting the lines for sending and receiving the data are crossed.



Look at the link status LED (Link) to check if the node/hub switch is set correctly.

ISDN connection

In addition, the *LANCOM Office* router also requires a basic rate interface in the ISDN in point-to-multipoint configuration (multi-device terminal) or in point-to-point configuration (system terminal). The router supports DSS1 and 1TR6 as D-channel protocols. Leased-line connections using D64S or D64S2 are available for the transfer of large volumes of data. Leased-line support must be activated separately in the device.

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 company's servers. The *LANCOM Office* router offers you various ways of restricting access from outside:

- Access protection using name, password and call number
- Login barring against “brute force attacks”
- Callback to defined call numbers
- Data packet filtering
- IP masquerading (also known as NAT or PAT)

Security check

A caller can be identified by two characteristics: name or call number. You can specify which of the two “identifiers” is used to recognize the caller in the 'Security' menu. You have a choice of the following:

- None: Calls are accepted from any remote station.
- Name: Only calls from those remote stations entered in the name list are accepted.
- 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 name or call number is also sent by the caller.

It is also possible to specify in the name list whether the caller should be called back. This means that the *LANCOM Office* router being called is charged for the connection, but it also means that, if necessary, only certain remote stations, whose call number has been recognized, gain access to the network. The caller also has the option of specifying the call number to be used to call him back, if you are using 'PPP' as the protocol on the B channel.

Standing guard

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

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 Office* router is set to provide security using the telephone number, any calls from remote sites with unknown numbers are denied access.

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

Tell me your 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 *LANCOM Office* 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 name list if the ELSA protocol is being used.

The name sent by the remote station will be checked for its appearance on the PPP list (of device names) if the PPP protocol is being used.

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



Obviously you will not need to use the PAP or CHAP security procedures if you are using the LANCOM Office router 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?

- If you are using the ELSA protocol for the B channel, identification is, in fact, made by name only and without a password. The device name of the router making the call is used as the name.
- If you are using PPP, the name and password are specified when the connection is established with the remote station. This may be in the corresponding window of a dial-up connection. The device name, password and user name in the PPP list are used if the *LANCOM Office* router establishes the connection itself.

Login barring

The configuration of the *LANCOM Office* router is protected against "brute force attacks" by barring logins. Both the maximum number of permissible incorrect login attempts as well as the barring duration may be set.

These parameters apply globally to all configuration options (outband, 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 case of an outband or telnet session:



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

For further information about login barring please refer to the Reference Manual.

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.

By making entries in the names and numbers lists and selecting the protocol (ELSA or PPP) you can control your *LANCOM Office* router's callback behavior:

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

If the *LANCOM Office* 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)

One of today's most common tasks for ISDN routers such as the *LANCOM Office* router is connecting the numerous workstation computers in a LAN to the network of all networks, the Internet. Everyone should have the potential to access the WWW from his workstation and be able to fetch bang up-to-date information for his work.

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 in the Internet. This means that only the *LANCOM Office* router and its IP address (fixed or allocated by the provider) is made known on the Internet. The computers in the LAN then use the *LANCOM Office* router as a gateway so that they themselves cannot be detected. To do this, the *LANCOM Office* router separates Internet and Intranet, as if by a wall. Therefore, IP masquerading is also called a "firewall function".

Costs under control

One thing has been clear to you from the start: To the purely capital costs of the *LANCOM Office* router you have to add the charges for data transfer using ISDN (or analog telephone). And because we know that too we want to help you save money.

But how can we work together to cut costs and keep them in check? The following considerations will help us on our way:

- The lowest costs are incurred by data which is not transferred at all. You should therefore use the line to send only the most important data packets. You can determine this by using routing tables, for example, which only allow the transfer of specified data. The rest can be suppressed using the filters so that entire groups of data can be excluded from the expensive ISDN line, or by “spoofing mechanisms” ensuring that requests to remote networks can be answered locally in your own network.
- If you really need to transfer data, volumes should be as small as possible and arrive as quickly as possible. Data compression is designed for this.
- Furthermore, you should only be paying for the line when data is actually flowing along it. Intelligent line management establishes the connection automatically and closes it once the transfer has been completed. If call charge information is transmitted over the ISDN network **during** the connection (i.e. AOCD), the *LANCOM Office* router uses up any partly used call charge unit fully and only breaks the connection shortly before the next unit is due to start.
- The call charge units that you pay must, of course, be as inexpensive as possible. The competition caused by the privatization of the telephony market means that the cheapest telephone rates are offered by different providers (telephone companies) depending on the time of day and the distance involved. With the least-cost routing functions the *LANCOM Office* router automatically looks for the cheapest rates, for each connection, in a table defined by you. Therefore, you always connect at the lowest possible cost, without even being aware of it.
- Finally, set your *LANCOM Office* router a limit: this far and no further. You can avoid excessive and, most importantly, unexpected phone bills by using the charges budget.

Selecting what's relevant

Seeking out the data packets that are truly important and which really do need to reach a remote station is one of the main tasks of router configuration. Take a look at the *LANCOM Office* router's three different operating modes and see how they can trap superfluous data packets.

IP router

This makes it very simple to select which data should be transferred. The IP router transfers only those data packets to target IP addresses which are not located on the local area network **and** for which a path can be found in the routing table. You therefore use your entries in the IP routing table to determine precisely which data should be transferred and which should not. You can also target which data packet groups should be excluded from transfer by using address and port filters for the WAN and LAN side.

IPX router

The situation is not quite as easy with the IPX router. There is one particularly important characteristic of IPX networks with reference to routing: The individual devices on an IPX network regularly send out special data packets so that they can communicate with one another. These are used to announce the services available on a network (Service Advertising Protocol SAP), to swap information on routes into other networks (Routing Information Protocol RIP) or simply to inquire whether other devices are still active (watchdogs). If an IPX network and another network are connected via a router, these data will also be transferred over the ISDN line as a matter of course and will establish permanent connections.

This can be prevented by excluding individual RIP or SAP data items (or entire groups of them) from the RIP/SAP tables. Another possibility is for SAP or RIP to be transferred only when there has been a change in the information or only if the connection has been established anyway.

Spoofing can be used to reduce the watchdogs on the WAN line. The *LANCOM Office* router does this by answering locally those watchdogs which are actually intended for a device on a remote network, thus preventing the establishment of a connection.

Filter tables for the WAN and LAN side can be kept for an IPX router in a similar way to the port filters for IP routing. No packet originating on the local area or remote network that has been allocated to one of the sockets from the corresponding table will be transferred.

Bridge

A bridge connects two local area networks only. It has the particular characteristic of transferring any data packet which cannot be allocated locally. This is a very expensive and undesirable feature, especially if you are using switched connections. This is why you also have the ability to limit the transfer of these data packets to a certain extent.

You have the choice of three options for broadcast data packets (intended for all accessible devices on a network) and multicast data packets (intended for a specified group of devices on a network): always transfer, never transfer, or only transfer if the connection has already been established.

You can specify further restrictions using the filter tables. The filter tables can be used to determine whether the packets are to be transferred to addresses specified in them or whether these very packets are to be excluded (positive or negative filtering). The physical, fixed addresses of the affected network boards will then be specified in the table.

Faster, faster—data compression and channel bundling

When should I use channel bundling?

If you are establishing an ISDN connection to a party supporting PPP you can really speed up your data: You can compress the data and/or use two B channels for the transfer (channel bundling).

MLPPP (Multilink PPP) is used for channel bundling. Of course, this procedure is only available if PPP is being used as the B-channel protocol. MLPPP is ideal, for example, for accessing the Internet via a provider which also supports MLPPP on its dial-up nodes.

Costs under control—call charge management

It is all well and good that your *LANCOM Office* router can decide for itself when to establish connections. But how do you prevent connections being made too frequently?

Set the *LANCOM Office* router a definite budget in order to avoid a costs explosion on your phone bill (caused by bad configuration, for example): For example, you could limit usage to 830 units per seven days (preset value). You can adjust both the number of days and the charge limit to any setting you wish.

Set the units to zero if you do not wish to place any charge restrictions on the *LANCOM Office* router. But be careful: the *LANCOM Office* router can now establish as many connections as it likes.



*The best way to use the LANCOM Office router's call charge monitoring function is if you have "call charge information enabled **during** the connection" to the ISDN network (i.e. AOCD). If necessary, subscribe to this facility from your telecomms carrier. Charge monitoring with the "Charge information **after** connection" feature is also possible in principle, but in this case continuous connections may not be detected!*



If you have enabled least-cost routing on the router modules, connections may be established to providers who do not transmit any charge information!

Another advantage of charge information transmission during the connection is that the *LANCOM Office* router can detect the length of a call unit. Armed with this information the *LANCOM Office* router can use up the last unit completely before disconnecting (dynamic short hold).

The least-cost router

Since the privatization of the telephone market in Germany and Europe, users can choose from telecommunications services provided by a number of providers (network operators) who, at times, charge very different rates.

The least cost router (LCR) is provided with certain telephone number prefixes, weekdays and times as well as the provider to be used for the connection, if suitable.

Every time a number is dialed the least cost router checks the dialed digits to see if they match any of the prefixes in the LCR table and, if so, determines whether this entry is currently active. If this is the case, the LCR adds in the network code of the corresponding provider and thus redirects the call to a different network.

For every call, whether by telephone, fax (*LANCAPi*) or router, the LCR module in the *LANCOM Office* router therefore automatically selects the cheapest provider on a call by call basis.

Compatible communication

Online or offline—the line used for the connection

LANCOM Office routers connect networks and individual PCs via ISDN lines. This means that both dial-up connections and dedicated lines can be used.

The option of communicating over dedicated lines must be enabled separately on the *LANCOM Office* router as an upgrade. You will find details of the upgrade procedure on our web site www.elsa.de.

■ Leased-line connection

A permanent or leased-line connection is mainly used to link networks between which there is a constant exchange of data. It becomes more economical to have a dedicated connection rather than a dial-up connection if more than a given volume of data is being transferred, and it is quicker because there is no dialing process involved.

LANCOM Office routers support leased lines with one or two B channels. Leased lines may need to be activated separately by entering a code.

■ Dial-up connection

A dial-up connection will usually suffice if the flow of data passing through the *LANCOM Office* router is sporadic rather than constant.

The dial-up connection is managed independently by the *LANCOM Office* router, i.e. it is established automatically as required and disconnected once the timeout has expired.

Transfer protocols

Two devices must first be speaking the same language before they can understand one another to transfer data over an ISDN line. The language used on the ISDN network is dictated by protocols. The two devices will only understand each other if they are using the same protocol. ISDN always uses two protocols for the connection: one D-channel protocol and one B-channel protocol.

D channel

The D channel is generally only used to send the control information needed to establish and manage the connection. The *LANCOM Office* router supports DSS1 (Euro ISDN) and 1TR6 (the older, national ISDN in Germany) and leased lines (D64S, D64S2, D64SY). This means that remote stations in a connection can use quite different D-channel protocols.

B channel

The B channel is used to send the data itself for the connection. The method of data transfer is defined in the layer list for the three B-channel protocol layers. This ensures compatibility when transferring data between devices made by different manufacturers.

- On layer 1, either 64 or 56 kbps (USA-ISDN standard) can be selected, both using HDLC.
- On layer 2, you have a choice of transparent or X.75LAPB.
- You have the choice of transparent, synchronous and asynchronous PPP on layer 3. Additionally, a script can be started with the selection of the protocol.

Having these protocols in the layer list will allow you to communicate with the majority of other routers. Use transparent HDLC or data compression if possible, as this will give you the greatest data throughput.

The *LANCOM Office* router makes a great variety of B-channel protocols available to you by using combinations of the different setting values for the communications layers. We have already put together a few commonly used settings and saved them in the layer list. Of course, you can modify these at any time or add new B-channel protocols (layers).

The *LANCOM Office* router supports LZS (Stac) data compression as well as static and dynamic channel bundling. Naturally, the B channels can also be used simultaneously for different connections.

The chameleon

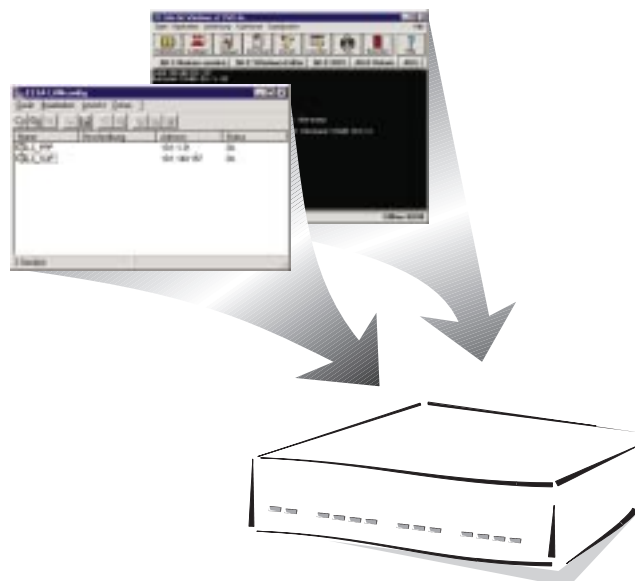
One of the great strengths of *LANCOM Office* routers: They can be adjusted to the environment no matter where they are used. They will find a way of transferring the data, no matter what version of Ethernet, and seek out a suitable path for configuration, no matter what the operating system.

Networks

The *LANCOM Office* router transfers data from networks running TCP/IP or IPX/SPX using the corresponding router modules and therefore always finds a path between different remote networks. The bridge function interconnects networks working on other Ethernet protocols to form a single network.

Operating systems

Nor is the *LANCOM Office* router choosy about the operating system used: A suitable program can always be found in Windows, UNIX, OS/2 or MacOS to adjust the *LANCOM Office* router's software to your needs. Windows users can use the *ELSA LANconfig* configuration tool, an intuitive, easy-to-learn interface with wizards and online help. Terminal or Telnet programs can be used to the same end in other operating systems.



Configuration modes

New *LANCOM Office* router are always dispatched with up-to-date software in which several of the settings have already been made.

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 *LANCOM Office* router 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 onto the *LANCOM Office* router.

Many paths lead to the <i>LANCOM Office</i> router.....	2
The direct method: outband	3
The user-friendly method: inband	4
Remote access: configuration using a dial-up connection	6
Configuration commands	9
Configuration using SNMP	10
What's happening on the line?.....	13
New firmware with FirmSafe	17

Many paths lead to the *LANCOM Office* router

In principle, there are three methods of accessing the *LANCOM Office* router:

- Through the configuration interface (config interface) on the rear of the *LANCOM Office* router (also known as outband)
- Through the LAN or WAN network (inband)
- Through a PPP connection via a dial-up line or similar (remote configuration)

What is the difference between these?

First, whether or not you will need additional software or hardware. For inband configuration you will need one of the computers that are on the LAN or WAN anyway and a suitable type of software; for outband configuration you need the software and one of the computers (with serial interface) and the corresponding configuration cable and remote configuration requires a remote computer with a PPP client, ISDN card or terminal adapter. The easiest method to use is remote configuration using a dial-up connection and *ELSA LANconfig*.

Depending on your access method there are different ways of protecting the configuration:

- Using a password.
- Access lists define the computers that have permission on the network (applies to the inband method only).
- You can set the permitted access rights from the local network (LAN) and remote networks (WAN): From within a particular network, the configuration of the router can either not be accessed at all, read only, or also be written to.
- The configuration block protects against users attempting to access the configuration by repeatedly guessing the password (brute force).
- For remote configuration you can reserve a special configuration call number. This number should not be the same as the numbers used for router functions.

The direct method: outband

Outband configuration gives you direct access to the *LANCOM Office* router via the configuration interface.

You really only need to use the outband configuration method if you cannot access your LANCOM Office router via TCP/IP. Every LANCOM Office router with the original factory settings can be configured directly via inband or using PPP remote access.

Requirements for outband configuration

What's needed?

- A computer running Windows 95, Windows 98 or Windows NT 4.0 and the configuration program *ELSA LANconfig*.
or
A computer using any operating system and a terminal program (e.g. *Telix* or Hyperterminal).
- The configuration cable supplied and, if necessary, the 9/25-pin adapter used to connect the computer and the *LANCOM Office* router (the PC's COM port to the router's configuration interface).

Outband configuration using *ELSA LANconfig*

Start up *ELSA LANconfig* from the Windows Start Menu, for instance, by clicking **Start ► Programs ► ELSAlan ► ELSA LANconfig**. *ELSA LANconfig* will now automatically search for *LANCOM Office* router devices in the local area network (but not on the serial ports). *ELSA LANconfig* displays new routers in the list by their device types, e.g. 'ELSA LANCOM Office'.

If your *LANCOM Office* router is new and has not yet been configured at the configuration interface, you can call up various configuration tools with **Tools ► Setup Wizard**. Select one of the wizards offered and simply answer its questions. This will then set up the *LANCOM Office* router for the task selected.

Alternatively, you can double-click on the new device's name entry (e.g. 'ELSA LANCOM Office') to open the router's configuration in edit mode.

Outband configuration using a terminal program, e.g. *Telix*

After starting the terminal program, press return just a few times to automatically detect the bit rate (up to 230 kbps, 38.4 kbps as standard).

Once you have entered the password, configuration can be carried out using any of the commands contained in section 'Configuration commands'.

The user-friendly method: inband

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

Requirements for inband configuration

TCP/IP or TFTP are used to make configurations using telnet or *LANconfig*. This means that the TCP/IP protocol must be installed on the computer being used and the *LANCOM Office* router must be given an IP address which you will then use when addressing it. The *LANCOM Office* router has the IP address XXX.XXX.XXX.254 until you have configured it. Here the row of Xs denote the network address on your LAN. If the computers on your network have addresses such as 192.110.130.1, then you will be able to address the *LANCOM Office* router using 192.110.130.254.



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

Don't forget: The DHCP server integrated in the *LANCOM Office* router will be happy to lighten your workload!

If it is not absolutely essential that you configure the correct IP addresses "manually", the *LANCOM Office* router will gladly do this task for you automatically. When using the DHCP server you can have all IP addresses on the network assigned automatically, including the one belonging to the *LANCOM Office* router itself (see also chapter 'Automatic Address Administration with DHCP').

Beginning inband configuration using *LANconfig*

Once you have performed the installation (by double-clicking on 'setup.exe') you can call up the *LANconfig* configuration tool from the Windows Start Menu, for example, with **Start ► Programs ► ELSA LAN ► ELSA LANconfig**. *LANconfig* searches the local area network and at the configuration interface for *LANCOM Office* router devices. *LANconfig* will automatically start up the setup wizard if a *LANCOM Office* router which has not yet been configured is found on the local area network.

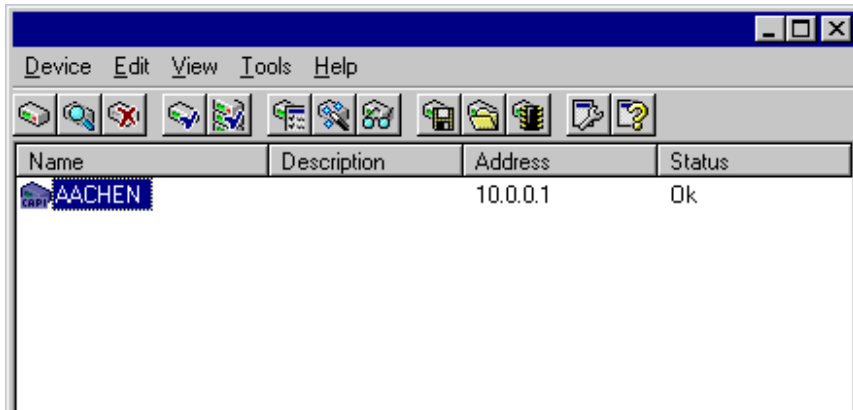
Select one of the wizards offered and simply answer its questions. This will then set up the *LANCOM Office* router for the task selected.



Just click on the Browse button or call up the command with **Device ► Find** to initiate a search for a new router 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.



Double-clicking the entry for the highlighted *LANCOM Office* router 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 *LANconfig* program's operation is pretty much self-explanatory or you can use the online help. You can click on the question mark top right in any window or right-click on an unclear term at any time to call up context-sensitive help.

Start up inband configuration using telnet

Start up inband configuration using telnet with the command:

```
telnet 10.1.250.183
```

Telnet will then establish a connection with the *LANCOM Office* router using the IP address.

Once you have entered the password, configuration can be carried out using any of the commands contained in the section 'Configuration commands'.

Remote access: 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 *LANCOM Office* router is accessible by the administrator immediately without any settings being made after it is switched on and connected to the ISDN basic rate 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.

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
- An ISDN card, a terminal adapter or a *LANCOM Office* router with *ELSA LANCAPI*

This is how you prepare the *LANCOM Office* router for remote configuration

- ① Attach the router to the power supply.
- ② Connect the device to an ISDN basic rate interface.

The first remote connection using a dial-up connection and *ELSA LANconfig*

- ① In the *ELSA LANconfig* program select **Device ► New**, enable 'Dial-Up connection' as the connection type and enter the calling number of the ISDN interface to which the *LANCOM Office* router is connected. If you wish, you can also enter the time period after which an idle connection is to be disconnected automatically.
- ② *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 *LANCAPI*) for the connection and press OK to confirm.
- ③ 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.

- ④ You can configure the *LANCOM Office* router remotely just like all other devices. *ELSA LANconfig* establishes a dial-up connection enabling you to select a configuration.



The first remote connection using a generic PPP client and telnet

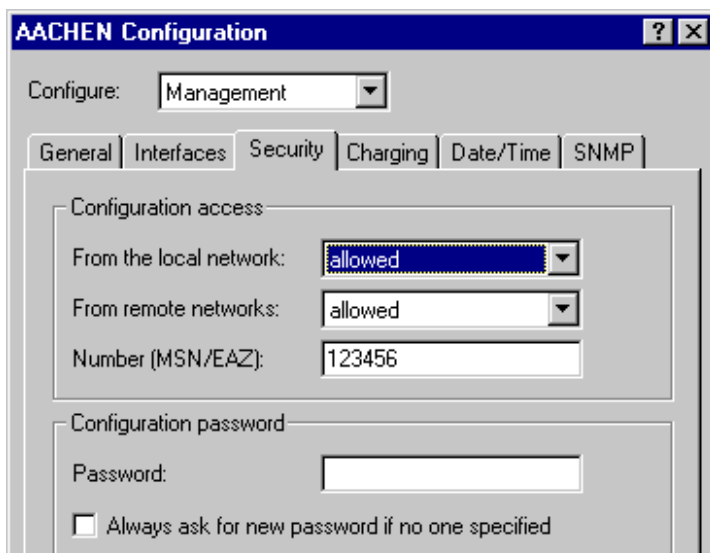
- ① Establish a connection to the *LANCOM Office* router with your PPP client using the following details:
 - User name 'ADMIN'
 - Password as set on the *LANCOM Office* router, factory default setting is no password
 - An IP address for the connection, only if required
- ② Open a telnet session to the *LANCOM Office* router. 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 Office* router 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 Office* router 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 Office* router remotely just like all other devices.

Limiting remote configuration

The PPP connection of any other remote site to the *LANCOM Office* 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 *LANCOM Office* router 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 In the 'Management' configuration group select the 'Security' tab.
- ② In the 'Configuration access' field, choose whether the configuration is fully accessible, read-only or not accessible from remote networks.
- ③ As the calling number in the 'Configuration access' area, enter an MSN or EAZ of your ISDN connection which is not used by the router, the *LANCAPi* or the a/b ports.
- ④ You can protect the configuration of the device by assigning a password.



The screenshot shows the 'AACHEN Configuration' window with the 'Security' tab selected. The 'Configure:' dropdown is set to 'Management'. The 'Configuration access' section has two dropdown menus: 'From the local network:' set to 'allowed' and 'From remote networks:' set to 'allowed'. The 'Number (MSN/EAZ):' text box contains '123456'. The 'Configuration password' section has an empty 'Password:' text box and an unchecked checkbox labeled 'Always ask for new password if no one specified'.




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

Configuration commands

Commands and path specifications are entered using the normal DOS or UNIX conventions if you are using telnet (inband) or a terminal program (outband) to configure the *LANCOM Office* router.

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

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

This command means this for instance:
? or help	Calls up help text	-
dir, list, ll, ls <MENU>, <VALUE> or <TABLE>	Displays the contents of MENU, VALUE or TABLE	dir/status/wan-statistics displays the current WAN statistics
cd <MENU> or <TABLE>	Switches to the MENU or TABLE specified	cd setup/tcp-ip-module (or cd se/tc for short) switches to the TCP/IP module
set <VALUE>	This resets the value.	set IP-address 192.110.120.140 sets a new IP address
	Insert a space between all entries in table rows. An * leaves the entry unchanged.	set name-list/AACHEN 123456 90 30 creates an entry in the name list for the device 'AACHEN' with the call number 123456 and timeouts of 90 and 30 seconds.
set <VALUE> ?	Shows you which values can be specified here	
del <VALUE>	Deletes the specified VALUE (or the whole line)	del setup/name
do <ACTION> (parameters)	Executes the ACTION according to any parameters specified,	do other/manual-dialing/connect ELSA.SUP.1 (or do/ot/m/co ELSA.SUP.1 for short) manually establishes a connection to the ELSA test network.
passwd	Allows a new password to be specified. The old password, if there is one, must be entered first. The new password must then be entered twice in a row and confirmed each time with  .	
repeat <sec> <ACTION>	Repeats the action at an interval of the number of seconds specified. Any key can be used to terminate the repetition.	repeat 3 dir/status/wan-statistics displays the current WAN statistics every 3 seconds
time	sets the system time and date	time 24.12.1998 18:00:00
exit, quit, x	Configuration is terminated.	

Configuration using SNMP

General

The Simple Network Management Protocol (SNMP V.1 as specified in RFC 1157) allows monitoring and configuration of the devices on a network from a single central instance. This instance is commonly termed the "manager" while the devices become "agents". The structure permitted for SNMP information exchange is relatively simple. A manager can access all SNMP-capable devices and services (agents) on the network. The access rights are controlled via "communities".

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

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

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

An agent for SNMP V.1 (as specified in RFC 1157) is implemented in the *LANCOM Office* router's firmware. A part of MIB-2 and a private MIB, included in the product as a separate file, are supported. This MIB must be loaded and translated by an SNMP manager (HP OpenView, for example) to allow you to manage a *LANCOM Office* router completely using SNMP. All menus and parameters of the *LANCOM Office* router remote configuration will then be available to you on a single branch of the SNMP management tree: iso/org/dod/internet/private/enterprises/elsa/ISDN-systems/ISDN-Router/LANCOM-1000 for *LANCOM 1000 Office* or 1.3.6.1.4.1.2356.1.

Accessing tables and parameters using SNMP

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

Access protection in SNMP V.1

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

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

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

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

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

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

Deleting rows in tables using SNMP

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

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

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

IP-address	IP netmask	Router-name	Distance
192.168.0.0	255.255.0.0	0.0.0.0	0
172.16.0.0	255.240.0.0	0.0.0.0	0

IP-address	IP netmask	Router-name	Distance
10.0.0.0	255.0.0.0	ROBERT	0
224.0.0.0	224.0.0.0	0.0.0.0	0
255.255.255.255	0.0.0.0	T-ONLINE	1

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

Appending rows to tables using SNMP

If you need to append a row to a table, you have to 'amend' the index entry for any existing row to the new index value for the new row. The row which has been used as the source for the amendment will itself remain unchanged.

Error messages via SNMP trap

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

SNMP and *ELSA LANmonitor*

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

The Management Information Base (MIB)

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

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

What's happening on the line?

ELSA LANmonitor

The *ELSA LANmonitor* includes a small 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 95, Windows 98 or Windows NT 4.0. Many of the internal messages generated by the device are converted to plain English, 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.

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

During the installation you should activate the 'ELSA LANconfig' option.



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

Checking your internet connection with ELSA LANmonitor

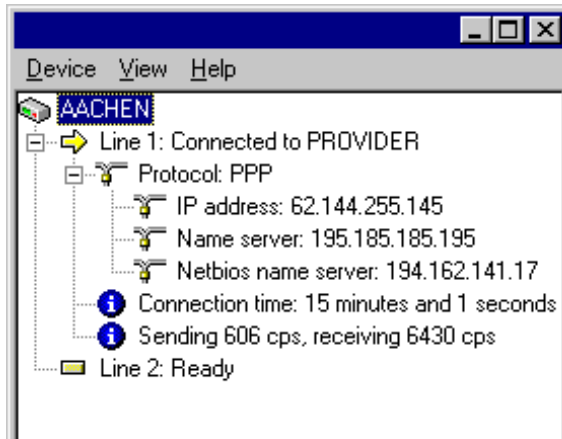
To demonstrate the functions of *ELSA LANmonitor* we will first show you the types of information *ELSA LANmonitor* provides about connections being established to your Internet provider.

- ① So you should setup *LANCOM Office* router to connect to your provider, e.g. with the *ELSA LANconfig* setup wizard. We selected call-by-call access to Arcor for this example.
- ② Start up *ELSA LANmonitor* by clicking **Start ► Programs ► ELSAan ► ELSA LANmonitor**. Generate a new device by selecting **Device ► New** and, in the following window, enter the IP address of the router you wish to monitor. If the configuration of the device is protected by password, enter the password too.

Alternatively, you can select the device in *ELSA LANconfig* and start the monitoring function for a *LANCOM Office* router by selecting **Device ► ELSA LANmonitor**.

- ③ *ELSA LANmonitor* automatically creates a new entry in the device list and initially displays the status of the two B channels. Start your Internet browser and enter any web page you like. You can now see in *ELSA LANmonitor* a connection being established on one channel and the name of the remote site being called. As soon as the

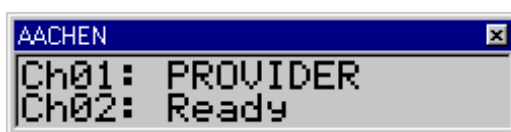
connection is established, a plus sign against the B channel entry indicates that further information on this channel is available. Click on the plus sign to open a tree structure in which you can view various information.



In this example, you can determine from the PPP protocol information the IP address assigned to your *LANCOM Office* router by the provider for the duration of the connection and the addresses transmitted for the DNS and NBNS server.

Under the general information you can watch the transmission rates at which data is currently being exchanged with the Internet.

- ④ To break the connection manually, click on the active channel with the right mouse button.
- ⑤ If, in addition to the information in the *ELSA LANmonitor* device list, you wish to see a minimized status window in the form of an LED display, right-click on the name of the device and select **Line Display**.



Right-click on the line display area to configure this virtual display to remain in the foreground on your monitor.

- ⑥ If you would like to receive a log of the *LANmonitor* results in the form of a file, select 'Options' on the 'View' menu and then the 'Logging' tab. Enable logging and define whether *LANmonitor* should generate a daily, monthly or continuous log file.

Trace outputs

Trace outputs may be used to monitor the internal processes in the *LANCOM Office* router during or after configuration. One such trace can be used to display the individual steps involved in negotiating the PPP. Experienced users may interpret these outputs to trace any errors occurring in the establishment of a connection. A particular advantage

of this is: The errors being tracked may stem from the configuration of your own *LANCOM Office* router or that of the remote site.



The trace outputs are slightly delayed behind the actual event, but are always in the correct sequence. This will not usually hamper interpretation of the displays but should be taken into consideration if making precise analyses.

How to start a trace

The command to call up a trace follows this syntax:

```
trace [code] [parameters]
```

The trace command, the code, the parameters and the combination commands are all separated from each other by spaces. And what is lurking behind the code and parameters?

This code in combination with the trace causes the following:
?	Displays a help text
+	Switches on a trace output
-	Switches off a trace output
#	Switches between different trace outputs (toggle)
no code	Displays the current status of the trace

This parameter brings up the following display for the trace:
Status	Status messages for the connection
Error	Error messages for the connection
ELSA	ELSA protocol negotiation
PPP	PPP protocol negotiation
IPX-router	IPX routing
RIP	IPX Routing Information Protocol
SAP	IPX Service Advertising Protocol
IPX-watchdog	IPX watchdog spoofing
SPX-watchdog	SPX watchdog spoofing
NetBIOS	IPX NetBIOS management
IP-router	IP routing
IP-RIP	IP Routing Information Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
Script	Script processing
IP-masquerading	Processes in the masquerading module
DHCP	Dynamic Host Configuration Protocol

This parameter brings up the following display for the trace:
D-channel	Trace on the D channel of the connected ISDN bus

This combination command	... brings up the following display for the trace:
All	All trace outputs
Display	Status and error outputs
Protocol	ELSA and PPP outputs
TCP-IP	IP-Rt., IP-RIP, ICMP and ARP outputs
IPX-SPX	IPX-Tr., RIP, SAP, IPX-Wd., SPX-Wd., and NetBIOS outputs
Time	Displays the system time in front of the actual trace output
Source	Includes a display of the protocol that has initiated the output in front of the trace.

Any appended parameters are processed from left to right. This means that it is possible to call a parameter and then restrict it.

Examples

This code in combination with the trace causes the following:
trace	Displays all protocols that can generate outputs during the configuration, and the status of each output (ON or OFF)
trace + all	Switches on all trace outputs
trace + protocol display	Switches on the output for all connection protocols together with the status and error messages
trace + all - icmp	Switches on all trace outputs with the exception of the ICMP protocol
trace ppp elsa	Displays the status of the PPP and ELSA connection protocols.
trace # ipx-router display	Toggles between the trace outputs for the IPX router and the display outputs
trace - time	Switches off the system time output before the actual trace output.



You will find notes on the interpretation of trace outputs in the reference section of this guide.

New firmware with FirmSafe

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

This is how FirmSafe works

FirmSafe makes the installation of the new software safe: The existing 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 *LANCOM Office* router 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.
 - The difference to the first option is that the *LANCOM Office* router then waits five minutes for a successful login to the device via outband or inband (via telnet). Only if this login attempt is successful does the new firmware remain active permanently.
 - If the device no longer responds and it is therefore impossible to log in, the *LANCOM Office* router 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 *LANCOM Office* router boots with the new firmware and waits for the defined time period for the loaded firmware to be activated manually and therefore to be made permanently active.



With the introduction of FirmSafe a new boot loader is also required. The boot loader serves to load new firmware versions and to boot the firmware when the device is switched on. The new boot loader, however, only works with firmware versions higher than 1.20. This means that you cannot downgrade to firmware versions lower than 1.20 at a later stage.

How to load new software

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

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



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

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

ELSA LANconfig



If you are using the *LANconfig* configuration tool, highlight the corresponding *LANCOM Office* router in the list box and click on **Edit ► Firmware Management** or simply click on the **Firmware Upload** button. Then select the directory in which the new version is located and mark the corresponding file.

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

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

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

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

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

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

TFTP

How do I configure the Firmsafe parameters when performing a firmware upload via TFTP?

With TFTP you can use the **writeflash** command to install new firmware. To transmit a new firmware version which, for example, is in the LC_1000U.130 file (firmware version 1.30 for *LANCOM 1000 Office*), to a router with the IP address 194.162.200.17, you would enter the following command under Windows NT for example:

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



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

The device is booted up following a successful firmware upload and this activates the new firmware switch directly. If an error occurs during the upload (write error in the flash ROM, TFTP transmission error or similar) the TFTP connection is broken in order to provide the user with information about the problem. In this instance, the device will not boot but will continue to operate with the previous firmware version until the next time it is switched off and then on. The user still has the opportunity to save the device's current configuration, for example.

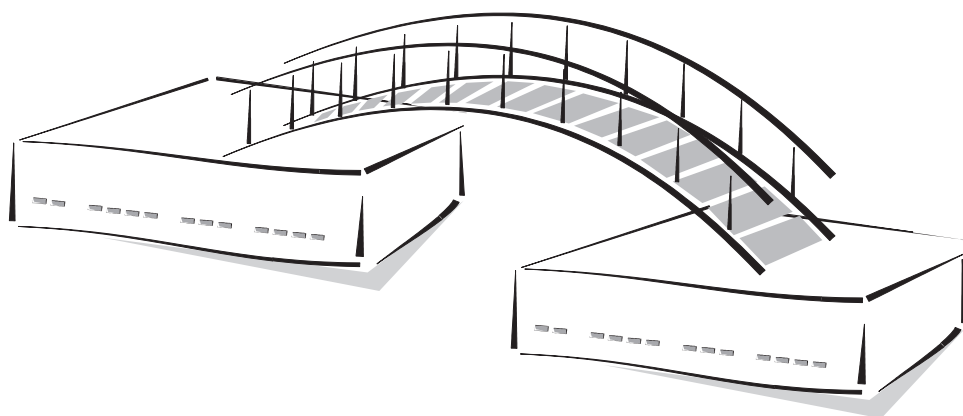
It will only be possible to configure the device locally, i.e. via the outband interface, if it is switched off during TFTP upload. The *LANCOM Office* router will expect a firmware upload via the serial port when it is switched back on.



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

With TFTP, all other *LANCOM Office* router 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



***LANCOM Office* router operating modes**

This section is an introduction to the three operating modes of your ISDN router.

We shall show you the various options and requirements of bridge, IP router and IPX router. You will also see what possibilities exist for filtering data in the individual configurations.

The operation of the *LANCAPi*, the PBX and the least-cost router are also covered in the following sections, as well as the DHCP server function.

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

Bridge or router?	2
The bridge in the network.....	4
The IP router.....	6
The IPX router	20
Office communications and <i>LANCAPi</i>	26
Automatic address administration with DHCP	31
The integrated PBX.....	39
The least-cost router.....	56



Bridge or router?

The *LANCOM Office* router can operate as a bridge or as a router. But what is the difference between the two, or, to put it more succinctly: What does a bridge do and what does a router do?

We must first dwell briefly on the OSI reference model (also known as the 7 layer model). This model organizes the various tasks which occur when information is transported in a network or between several networks into seven ranges or layers. Each layer sits on top of the layer below.

You can find further information on the OSI model in the reference section of the manual.

Only the three lowest layers are of importance in understanding bridges and routers. These three layers handle the following:

- Layer 1 (physical layer):

This is where the purely physical transportation of data is agreed. Which cables are to be used and how will digital information formed with ones and zeros be represented electronically? The answer to such questions is to be found in the lowest layer.

- Layer 2 (Data link layer):

The data is now rather more organized. The individual bits are put together into units in this layer. These, then, are the data packets or frames which networkers are always talking about. The second layer, therefore, tells us, for example, how many bits belong to one frame.

The data packets also have addresses (sender and addresses) allocated to them so that they can be correctly routed. 'Addresses' here mean the fixed addresses of the individual network components. These addresses are also called Media Access Control (MAC) addresses, are absolutely unique and are firmly fixed in virtually all components.

- Layer 3 (Network layer):

Organizing a network using MAC addresses can occasionally be rather difficult and confusing. Thus, for example, it is not possible to tell from the MAC address whether it conceals a server or a workstation computer or to which work group the computer belongs. Thus, arrangements have been made on the network layer to make it possible to use logical addresses specified by the network supervisor. The administrator can thus assign computers to groups which can also be addressed very easily as one.

The third layer is thus the layer for the network protocols such as IP or IPX.

A bridge only uses the physical addresses from the second OSI layer when addressing the data packets. The bridge is independent of the layer 3 protocols (IP, IPX, Apple Talk...)

and can thus be used to interconnect Ethernet networks with any protocol on layer 3 (with the exception of PPP).

The main difference between routers and bridges is that routers use logical addresses to transfer data packets. Logical addresses are assigned—within specific address conventions—by systems administrators from a logical point of view and thus have no direct association with the MAC addresses. The nature of the logical address modes is specified in the third OSI layer, so a router is dependent on the network protocol agreed there. An IP router thus operates with different addresses to an IPX router.

The bridge in the network

In the bridge operating mode, the *LANCOM Office* router transfers all data to computers without locally assigned MAC addresses, between the local network and another LAN or a workstation. The bridge thus learns fairly quickly which MAC addresses are located on its own network and which are located on the other side. After a very high level of initial data traffic which occurs when the two networks introduce themselves to each other, the network load then drops sharply and the connection no longer needs to be established as frequently.

The bridge connects the two participating computers as if they were in fact located in one network. For this reason, however, only those computers which can also theoretically be integrated into a network should be connected. This means that both networks and the network and workstation computer must have the same network addresses.

The bridge is not dependent on the protocol used in layer 3. It operates only with Ethernet addresses (MAC addresses). Please, therefore, ensure that you only use those B-channel protocols in the layer list which have the setting ETHER in the ENCAPS column. Use a protocol other than PPP on layer 3, as this protocol is not supported for the bridge.



It is not possible to use the bridge via 2 B channels, as MLPPP is used for channel bundling.

What do you need to configure the bridge?

First establish which call numbers the *LANCOM Office* router should listen to and which it should itself transfer externally (Setup/WAN-module/Interface).

An entry which includes name and call number must exist in the name list for *LANCOM Office* router to reach the remote station (Setup/WAN-module/Name-list).

You should still inform the bridge which is the correct remote station (Setup/Bridge-module/Remote-ID) since many remote stations will probably be entered in the *LANCOM Office* router over time. This is because the bridge can only connect precisely two networks together, while one router can manage several remote stations. You should also set (Setup/Bridge-module/Operating:On) so that the bridge can function.

The process is now completed. The bridge now sets to work transferring all the data packets for non-local MAC addresses to the remote station set.



You can find more instructions on how to configure the LANCOM Office router as a bridge in the appropriate section of 'Workshop' and in the detailed description of the individual menus in the reference section of the manual.

What are its other capabilities?

You may not always wish to transfer all data. Much of the data which is rattling around in the network is of no interest to remote networks or workstations. For this reason, you can block transfer of the following data packets or only transfer them if the line has been established anyway:

- Broadcast packets: Data directed at all devices reachable in a network (Setup/Bridge-module/LAN-config/Broadcast).
- Multicast packets: Data which is transferred to all devices which are reachable in a group (Setup/Bridge-module/LAN-config/Multicast).
- Unicast packets: This is data directed only at a specific device (meaning a fixed MAC address).

Special filter lists which exclude certain addresses from a transmission or only allow certain addresses can be set up to handle this data. The bridge filters differentiate here between destination and source addresses. You can first establish whether the table belonging to both address types contains the addresses to which data are to be transmitted (Setup/Bridge-module/LAN-config/Dest.-address/Filter-type/pos) or the addresses which to be excluded from the transmissions (.../Filter-type/neg). You then enter the MAC addresses to be filtered into the table itself.



This method of filtering by entering the exact MAC address naturally demands a certain degree of maintenance effort. Should the addresses change when a network adapter is changed, for example, the new addresses must be entered to ensure that the bridge continues to function.

The IP router

The IP router works between networks which use TCP/IP as the network protocol. This only allows data transmissions to destination addresses entered in the router. Up to 64 different remote stations can be named as destination addresses for one IP router.

Naming IP addresses

IP addresses are used in TCP/IP networks to communicate between different devices. The addresses must be unique within an associated network in order to avoid confusion. Since the Internet also uses TCP/IP for its many millions of connected computers and thus uses IP addresses, all Internet addresses must also be unique. There are bodies which exist to monitor these publicly accessible addresses and which manage, distribute and also charge for the IP addresses.

Certain ranges of IP addresses are reserved for private use (Private Address Spaces) so that a company does not have to purchase an IP address for each workstation. These addresses can be used as required in a closed network but must be unique within this network and may not be disclosed externally (on the Internet).

What does an IP address look like? It comprises four bytes separated by points, making a total of 32 bits. Each of the four bytes can take on values from 0 to 255, e.g. 192.168.130.124. The address of both the network and the computer are contained in this address.

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

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

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

You can see from this that an IP address alone is not enough. The computers belong to other logical networks with other network masks. And you can also see that there are

more bits available to identify the individual computer if there are fewer bits in a network mask that contain a one. While only 254 different addresses could be allocated in the first example with the network mask 255.255.255.0 (the final numbers '0' and '255' are reserved), the second example has as many as $254 \times 254 = 64516$ different addresses available!

A range of IP addresses are reserved for private use (Private Address Spaces), which means that companies do not have to purchase individual IP addresses for every workstation. Addresses within this range can be freely used within a closed network. They must be unique within this network, and must not be released to the outside (e.g. the Internet).

The allocation of IP addresses by the IANA (Internet Assigned Numbers Authority) allows for the following address ranges to be used for experimental and private use:

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

There are two considerations when using these IP addresses:

- ① The IP addresses used in a private network should not leave this network, i.e. an Internet connection is only possible with the use of IP masquerading, for example.
- ② These IP addresses will not be routed in the Internet, i.e. backbone routers will simply reject such IP packets. Depending on the provider, consequences may result if such IP packets are released on the Internet.

The IP routing table

Use the IP routing table to tell the *LANCOM Office* router which remote station (which other router or computer) it should send the data for particular IP addresses or IP address ranges to. This type of entry is also known as a "route" since it is used to describe the path of the data packet. This procedure is also called "static routing" since you make these entries yourself and they remain unchanged until you either change or delete them yourself. Naturally, there is also "dynamic routing" too. The routers use the routes in this way to exchange data between themselves and continually update it automatically (see also 'Dynamic routing with IP RIP' auf Seite 1.4.13). The static routing table can hold

up to 64 entries, the dynamic table can hold 128. The IP router looks at both tables when the IP RIP is activated.

You also use the IP routing table to tell the *LANCOM Office* router the length of this route's path so that it can select the most suitable route in conjunction with IP RIP where there are several routes to the same destination. The default setting for the distance to another ISDN router is 2, i.e. the router can be reached directly. All devices which can be reached locally, such as other routers in the same LAN or workstation computers connected via Proxy ARP (see also 'Proxy ARP' auf Seite 1.4.11) are entered with the distance 0. The "quality level" of this route will be reduced if the entry addressed has a higher distance (up to 14). "Unfavorable" routes like this will only be used if no other route to the remote station in question can be found.

This, then, is how an IP routing table might look:

IP address	IP netmask	Router name	Distance
192.168.120.0	255.255.255.0	LANCOM01	2
192.168.125.0	255.255.255.0	LANCOM02	3
192.168.130.0	255.255.255.0	191.168.140.123	0

What do the various entries on the list mean?

■ IP addresses and IP network masks

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

■ Router Name

The *LANCOM Office* router transmits the appropriate data packets to the IP address and network mask to this remote station. A name is entered at this point if the remote station is a router in another network or an individual workstation computer. This is where the IP address of another router which knows the path to the destination network is entered if the *LANCOM Office* router on the network cannot address the remote station itself.

■ Distance

This is the number of routers between the *LANCOM Office* router and the destination. This value is often equated with the cost of the transmission and used to distinguish between inexpensive and expensive call paths. The distance values entered are propagated as follows:

- All networks which can be reached while an ISDN network connection is established to a destination network are propagated with a distance of 1.

- All non-connected networks are propagated with the distance entered in the routing table (but with a minimum distance of 2) as long as a free channel is still available.
 - The remaining networks are propagated with a distance of 16 (= unreachable) if there are no longer any channels available.
 - Remote stations connected using Proxy ARP are an exception to this (see also 'Proxy ARP' auf Seite 1.4.11). These "Proxy hosts" are not propagated at all.
- Following entries have a special meaning:
- IP address 255.255.255.255 with a network mask of 0.0.0.0: This is the default route. Any data packets which cannot be routed by other routing entries are transmitted to the remote station listed here.
 - Network mask 255.255.255.255: Entries with completed network masks frequently only identify individual workstation computers (remote access) and not actual networks. A network which is only visible by a single IP address using IP masquerading (see also 'IP masquerading (NAT, PAT)' auf Seite 1.4.15) may sometimes be concealed behind this.
 - Router name 0.0.0.0: Exclusion routes. Data packets for this "zero route" are rejected and are not routed any further by *LANCOM Office* router. This is how routes which are forbidden on the Internet (private address spaces, e.g. 10.0.0.0), for example, are excluded from transmission.

Examples with explanatory notes:

IP address	IP netmask	Router name	Dist.	This is what happens:
192.168.1.9	255.255.255.255	FIELD SERVICE	2	The FIELD SERVICE remote station can be reached at IP address 192.168.1.9.
192.168.120.0	255.255.255.0	ROUTER01	2	All data packets with destination IP addresses 192.168.120.x are transmitted to ROUTER01.
192.168.125.0	255.255.255.0	ROUTER02	3	All data packets with destination IP addresses 192.168.125.x are transmitted to ROUTER02.
192.168.130.0	255.255.255.0	192.168.140.123	0	All data packets with destination IP addresses 192.168.130.x are transmitted to the router with the IP address 192.168.140.123.
10.0.0.0	255.0.0.0	0.0.0.0	0	Excludes transmission of all data packets to networks using private address spaces.
255.255.255.255	0.0.0.0	INTERNET	2	All data packets which cannot be allocated to the entries listed above are transmitted to the INTERNET remote station.



The sequence of the entries is important here: They are processed from top to bottom. The LANCOM Office router sorts entries automatically: Firstly by network masks, in descending order. Then by the IP addresses, in ascending order. This places the 'INTERNET' entry at the very end of the list. If this entry were at the top of the list, LANCOM Office router would send every data packet which did not belong in its own network to the Internet!

What happens when data is transmitted on an IP network?

If a device in an IP network wishes to send a data packet to another device it requires its physical MAC address to do this. It can use the IP address and the network mask to discover whether the destination is located on the same network as the transmitting device. If this is the case, it first asks all devices on the network which MAC address is concealed behind the IP address desired. This round robin is also known as an ARP request (address resolution protocol request). When it gets the answer, the device which wants to send information knows which MAC address it must send the data packet to. In addition to this, it notes this assignment of MAC address and IP address for the next time in its internal ARP table to avoid having to carry out unnecessary requests thus relieving the network of some of the load.

If, however, the transmitter determines from network masks that the destination is located on another network, a router is required. The router for this must have an IP address in the same network as the sender so that the sender can find it in the first place. The sender requests the MAC address of the relevant remote router via ARP from the routing table of the sender's 'own' router (e.g. default gateway). The packets are then sent to that address. This, then, is how the routing table might look:

IP address	IP netmask	Router name	Distance
192.168.120.0	255.255.255.0	LANCOM01	2
192.168.125.0	255.255.255.0	LANCOM02	2
192.168.130.0	255.255.255.0	192.168.140.123	0

If the router (with IP address 192.168.110.50, network mask 255.255.255.0) now receives a packet with the destination address 192.168.125.123, it can detect that this address is located on another network. It therefore searches the routing table from top to bottom for an IP address for the correct destination network. This would be the second entry in this example which contains the destination network 192.168.125.0. The entry in the 'router name' column displays which name on the name list the LANCOM Office router must look under to find the information to establish a connection, while the entry under distance displays how many routers the path passes through.

The distance is listed as '2' if the router can reach the destination directly by an ISDN connection. The distance is reduced to '1' if the router has established a connection. The routers on a network may thus exchange information between themselves once (using IP

RIP, see also 'Dynamic routing with IP RIP' auf Seite 1.4.13) as to which particular device has already established a connection to a remote station which other devices may also be able to use.

If the router finds an IP address in the 'Router-name' field (and no remote station name), as can be seen on the last entry in the example, this router is not responsible for the destination network and routes the packet to the IP address entered.

TCP/IP packet filters

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

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

The *LANCOM Office* router can check the source and destination ports of data packets using the TCP or UDP protocols. It can then deduce the purpose of the data from these ports. For example, FTP accesses or Telnet sessions can be identified. The appropriate filter table can be used to determine that certain data is not to be transferred from the LAN to the remote station. Data for particular ports can also be blocked from entering the LAN from the WAN in the same way. The filter tables can use the filter type along with the definition of the port ranges and associated protocols to determine whether the data in question should never be transmitted or whether it should simply not lead to a call being established (i.e. only be transmitted if a connection already exists).

The *LANCOM Office* router has two separate filter tables, for packets coming from the LAN and from the WAN.

Proxy ARP

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



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

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

IP address	IP netmask	Router name	Distance	Masquerade
192.168.110.123	255.255.255.255	Teleworker01	0	Off

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

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

Local routing

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

How else can you assist the workstation computer?

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

Certain computers, however, do not know how to handle ICMP redirects. Use local routing (Setup/IP-router-module/Loc.-routing:On) to allow the data packets to be delivered nevertheless. This is how you tell the *LANCOM Office* router to send the data packet to the other router itself. The router will then no longer send any ICMP redirects.

This may seem to be a good idea in principle, but local routing should still only be used as a last resort, since this function leads to doubling of the number of data packets being

sent to the destination network required. The data is first sent to the default router and is then sent on from here to the router which is actually responsible.

Dynamic routing with IP RIP

In addition to the static routing table (see also 'The IP routing table' auf Seite 1.4.7) *LANCOM Office* router also has a dynamic routing table containing up to 128 entries. Unlike the static table, you do not fill this out yourself, but leave it to be dealt with by the *LANCOM Office* router itself. The *LANCOM Office* router uses the Routing Information Protocol (RIP) for this purpose. This protocol is used by all routers with RIP in a local network to exchange information regarding the reachable routes.

What information is propagated by IP RIP?

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

- Rejected routes with the '0.0.0.0' router setting.
- Routes referring to on other routers in the local network.
- Routes linking individual computers to the LAN by proxy ARP (see also 'Proxy ARP' auf Seite 1.4.11).

Although the entries in the static routing table are set manually, this information changes according to the connection status of the *LANCOM Office* router and so, therefore, do the RIP packets transmitted.

- If the *LANCOM Office* router has established a connection to a remote station, it propagates all the networks which can be reached via this route in the RIPs with the distance '1'. Other routers in the LAN are thus informed by these means that a connection to the remote station has been established on this *LANCOM Office* router which they can use. This saves on charges and also prevents additional connections being established by routers that also happen to know a route to the destination.
- If this *LANCOM Office* router cannot establish a further connection to another remote station, all other routes are propagated with the distance '16' in the RIPs. The number '16' stands for "This route is not reachable at the moment." A *LANCOM Office* router may be prevented from establishing a connection in addition to the present one may be due to one of the following causes:
 - Another connection has already been established on the other channel
 - Another connection has already been established on the other channel (also via the *LANCAPI* or a/b ports).
 - Y connections for the S_0 port have been explicitly excluded in the interface table.

- The existing connection is using both B channels (channel bundling).
- The existing connection is a leased-line connection. It is not possible to establish a parallel dial-up connection in this case.



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

Routers with RIP capabilities dispatch the RIP packets approximately every 30 seconds. The LANCOM Office router is only set up to send and receive RIPs if it has a unique IP address. The IP RIP module is deselected in the default setting using the IP address XXX.XXX.XXX.254.

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

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

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

What do the entries mean?

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

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

- The route is incorporated if it is not yet listed in the table (as long as there is enough space in the table).
- The route exists in the table with a time of '5' or '6'. The new route is then used if it indicates the same or a better distance.
- The route exists in the table with a time of '7' to '10' and thus has the distance '16'. The new route will always be used.

- The route exists in the table. The new route comes from the same router which notified this route, but has a worse distance than the previous entry. If a router notifies the degradation of its own static routing table in this way (e.g. releasing a connection increases the distance from 1 to 2, see below), the LANCOM Office router will believe this and include the poorer entry in its dynamic table.



RIP packets from the WAN will be ignored and will be rejected immediately. RIP packets from the LAN will be evaluated and will not be propagated in the LAN.

The interaction of static and dynamic tables

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

Routers without IP RIP support

Routers which do not support the Routing Information Protocol are also occasionally present on the local network. These routers cannot recognize the RIP packets and look on them as normal broadcast or multicast packets. Connections are continually established by the RIPs if this router holds the default route to a remote router. This can be prevented by entering the RIP port in the filter tables.

Scaling with IP RIP

If you use several routers in a local network with IP RIP, you can represent the routers outwardly as one large router. This procedure is known as “scaling”. A router like this, with its supposedly inexhaustible supply of routes is created by the continual exchange of information between the routers.



Further instructions on scaling several LANCOM Office routers in one network may be found in Workshop.

IP masquerading (NAT, PAT)

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

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

Two addresses for the *LANCOM Office* router

Masquerading pits two opposing requirements of the *LANCOM Office* router against one another: While it must have an IP address which is valid on the local network, it must also have an address valid on the Internet. Since these two addresses may not in principle be located on the same logical network, there is only one solution: two IP addresses are required. The *LANCOM Office* router is therefore assigned an **Internet** address and an **Intranet** address, each with its own fitting network mask. Use the 'Masquerade' option in the routing table to inform the *LANCOM Office* router which of the two addresses to use when transferring the packets.

- 'Off': No masquerading.
- 'Dynamic': This entry requests a random IP address valid in the Internet from your provider which is then used for the connection and masquerading.
- 'Static': This entry requests a specific IP address entered under /setup/TCP from your provider which is then used for the connection and masquerading.

There are now two options for assigning the actual address:

- The provider assigns the desired address to the *LANCOM Office* router. The network mask now decides how many computers are masked behind the *LANCOM Office* router.
 - IP address with full '255.255.255.255' network mask: This is your own unique IP address, registered by the NIC. None of the other computers on the network have valid Internet addresses and are masked behind the *LANCOM Office* router's fixed address.
 - IP address with an incomplete network mask, e.g. '255.255.255.248': You have several registered IP addresses, one of which you assign to the *LANCOM Office* router. The remaining IP addresses are assigned permanently to devices on the Intranet, which can then use unmasked connections to access the Internet. The other devices can still access the Internet using masked connections.
- The provider assigns another address to the *LANCOM Office* router. Then **all** computers in the local network are masked behind the assigned address.

How does IP masquerading work?

Masquerading makes use of a characteristic of TCP/IP data transmission, which is to use port numbers for destination and source as well as the source and destination addresses. When the *LANCOM Office* router receives a data packet for transfer it now notes the IP address and the sender's port in an internal table. The *LANCOM Office* router then gives the packet its unique IP address and a new port number, which could be any number. It also enters this new port on the table and forwards the packet with the new information.



The response to this new packet is now sent to the IP address of the *LANCOM Office* router with the new sender port number. The entry in the internal table allows the *LANCOM Office* router to assign this response to the original sender again.

You can view these tables in detail in the LANCOM Office router statistics (see also 'Status').

Simple and inverse masquerading

This masking operates in both directions: The local network behind the IP address of the *LANCOM Office* router is masked if a computer from the LAN sends a packet to the Internet (simple masquerading).

If, on the other hand, a computer sends a packet from the Internet to, for example, an FTP server on the Intranet, from the point of view of this computer the *LANCOM Office* router appears to be the FTP server. The *LANCOM Office* router knows the Intranet address of the server from the entry in the service table (Setup/IP-router-module/Masquerading/Service-table). The packet is forwarded to this computer. All packets that come from the FTP server in the local network (answers from the server) are hidden behind the IP address of the *LANCOM Office* router.

The only small difference is that:

- Access to a service (port) in the intranet from outside must be defined in advance by specifying a port number. The destination port is specified with the Intranet address of, for example, the FTP server, on a service table to achieve this.
- When accessing the Internet from the Intranet, on the other hand, the *LANCOM Office* router itself makes the entry in the port and IP address information table.

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

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

Which protocols can be transmitted using IP masquerading?

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

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

- FTP
- TCP
- UDP

- ICMP

DNS forwarding

Names rather than IP addresses are generally used to access a server over the Internet. Who knows what address location could be hiding behind 'www.elsa.de'? The DNS server, of course.

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

If a computer calls up the home page of ELSA from the intranet, it first sends out a DNS request: "What IP address belongs to www.elsa.de?" This request is dealt with as follows if the *LANCOM Office* router is registered as the DNS server for the workstation computers:

- The *LANCOM Office* router first searches in its own settings to see if a DNS server has been registered. If it finds one it connects to this server and retrieves the information required.
- If no DNS server is entered in the *LANCOM Office* router, the router will attempt to reach a DNS server over a PPP connection (e.g. from the Internet provider) to get the IP address assigned to the name from there. This can only succeed if the address of a DNS server is sent to the *LANCOM Office* router during PPP negotiation.
- The default route is established and the DNS server searched for there if no connection exists.

This procedure does not require you to have any knowledge of the DNS server address. Entering the Intranet address of your router as the DNS server for the workstation computers is sufficient to enable you obtain the name assignment. This procedure also automatically updates the address of the DNS server. The *LANCOM Office* router always receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

Access verification

Access to the internal functions of the *LANCOM Office* router through TCP/IP can be restricted using a special filter list. Internal functions in this case means Telnet or TFTP sessions to configure the *LANCOM Office* router.

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

can be expanded by inputting further entries. The filter entries can describe both individual computers and whole networks.

Policy-based routing

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

You can find more information on policy based circuit routing in the 'Description of the menu options'.



The IPX router

The IPX router transmits data from networks using IPX/SPX as the network protocols (e.g. Novell networks). A remote network is notified to the computers in the local network by its entry in the IPX routing table. A maximum of 16 different networks can be entered in the routing table.

Naming IPX addresses

A complete IPX network address comprises three parts: A network number, the MAC address of the network adapter and the socket number.

- The network number can be freely selected. It must, however, be unique on all the addressable IPX networks to ensure correct assignment.
- The MAC address is burnt into each network component. A different address is only used inside the network in special cases.
- An IPX network uses the socket numbers to address a specific service on a computer rather than just the computer itself. Socket numbers identify the various services uniquely.

Information about the LAN

Several separate LANs required at one location do not necessarily need to have their own cabling. Different logical networks can share one cable. They use different formats for the Ethernet packets to ensure that the data belonging to the various networks does not clash and that one network remains invisible to the others. These formats are determined by the binding belonging to a unique network number on this cable.

You must provide the *LANCOM Office* router with the network number and the binding associated with it to ensure that it too now knows which network it belongs to. If we leave the network address at the default setting '00000000', the *LANCOM Office* router provides the address and the binding itself. It does this by searching on the attached cable for the network from which it receives the most SAP replies.

IPX routing table

Use the IPX routing table to tell the *LANCOM Office* router which remote stations (i.e. which other routers or computers) can be reached by the local network and to give it some parameters for connection purposes. The table, which can hold up to 16 entries has the following structure:

Remote site	Network	Binding	Propagated	Backoff
FILIALE01	00000245	802.3	Route	On
FILIALE02	00000320	SNAP	Filt.	On

Remote site	Network	Binding	Propagated	Backoff
HEAD OFFICE	00000420	802.2	Filt.	Off

■ Remote site:

The name of the remote station registered as the device name in the corresponding router on the remote side.

■ Network:

The address of the WAN. This is not the address of the destination network, but a third address which represents the network between the two networks to be connected. Thus the following applies:

LAN address 1 \neq WAN address 1 = WAN address 2 \neq LAN address 2 \neq LAN addr.1

■ Binding:

This is where you set which Ethernet binding is to be used on the WAN. This entry is only effective if the layer for this connection supports Ethernet encapsulation. 802.3 is assumed if the entry is missing.

■ Propagated:

A filter for type 20 IPX packets (NetBIOS propagated frames). The Network Basic Input/Output System was originally developed for IBM, and has since also been used by Microsoft in a modified form. This protocol provides services such as name resolution, data protection and correct packet sequencing (secure protocol) in layers 3 and 4 of the OSI model. NetBIOS packets have a special packet type and socket (propagated packets). NetBIOS is primarily used to exchange data between stations on a local network (LAN).

These IPX packets can be excluded from transmission or routed using the 'Filter' property. The 'Route' property transmits the packets if a connection to the remote station concerned is active or a free channel is available for the establishment of an additional connection. The propagated frames are rejected if all the lines to other remote stations are busy.

■ Backoff:

The IPX router uses a special algorithm (exponential backoff) to keep the connection costs arising in the case of erroneous configurations as low as possible.

The backoff function should be switched off if there is no server available on the remote station network (e.g. in the case of remote access from a workstation) (see also 'Exponential backoff' auf Seite 1.4.23).

The default setting is 'On'.

What happens when data is transmitted on an IPX network?

When a device logs on to an IPX network, it first sends a request for the Service Advertising Protocol (SAP) and locates the nearest available server (get nearest server request) in the network numbered '00000000'. A router or server located on this network responds to this request and sends the correct network number.

The servers also regularly transmit information regarding which services they offer and which other networks they can reach. They use the special data packets complying with the Service Advertising Protocol or the Routing Information Protocol (RIP).

Once the IPX router is fully configured in the *LANCOM Office* router and is ready for operation, the *LANCOM Office* router proceeds to establish connections to all remote stations which can be reached via the routing tables and then exchanges SAP and RIP information with these networks. The *LANCOM Office* router saves this data to its internal SAP and RIP tables.

RIP and SAP tables

RIP and SAP information is sorted alphabetically in the relevant tables. RIPs are thus only ordered by network and SAPs by service type first, then by server name.

The RIP and SAP tables are updated with each new RIP or SAP packet. The *LANCOM Office* router only incorporates in its table SAP information for which it also has a corresponding RIP entry to ensure that only those services are offered (SAP) which can also be reached (RIP). The entries on the tables indicate, in addition to the information on reachable routes and services, how many routers the path to the destination (hops) passes through or how much time a data packet needs in the destination network (tics = approx. 1/18 of a second), for instance. The *LANCOM Office* router selects the path with the fewest tics and the lowest hop count from the tables and stores only this route if the RIP information offers several different routes to a destination network, for instance.

RIP tables can hold 64 entries and SAP tables 128. If each new packet updates the tables, it stands to reason that the old entries must also disappear at some stage. Entries are artificially aged to do this. The age of all entries on RIP/SAP tables derived from local data transfers is incremented by 1 point every 60 seconds. A new RIP or SAP packet for an entry resets the age to zero. The route or service can be designated unreachable (down) once a selectable age of between 1 and 60 is reached. The entry is deleted when this elapsed time doubles. Additionally, any RIP and SAP information related to this remote station is deleted from the tables and replaced with new information when a connection is established.

So many *LANCOM Office* routers around here...

If the establishment of simultaneous network connections to a greater number of remote stations is required than the number of B channels available to the *LANCOM Office* rout-

er, then it's time for a second (third...) router. The same entries are made in the routing tables for all routers to ensure that the brothers function in perfect harmony with each other and that the network really can always find a contact. The same routing information is then sent in the RIP packets to each *LANCOM Office* router, albeit with a higher tic and hop count (`Setup/IPX-module/LAN-config/RIP-SAP-scal. activate`). This marks these routes as a sort of stand-by in the event that all channels are busy on the *LANCOM Office* router addressed.

Redundant routes

A *LANCOM Office* router receiving information in a RIP packet relating to routes with the same tic and hop counts as its own routes (redundant routes) does not, of course, have to reannounce these routes itself to the sender. The *LANCOM Office* router, therefore, only sends these routes to the routers which did not propagate the route. This procedure is known as a "split horizon".

The Propagate loop (`SETUP/IPX-MODULE/LAN-CONFIGURATION/LOOP-PROP.`) can be used if it is nevertheless necessary to notify redundant routes to the local network. The routes learned in this way are then flagged in the RIP table with 'LOOP'. Although the propagation of redundant routes is not prohibited by the Novell specification, it should still be avoided as much as possible. Therefore, the default setting is 'Off'.

Exponential backoff

When switched on, the unit's IPX router attempts to establish suitable connections to receive routing information (RIP and SAP information) required for operation from the remote IPX stations. If this is not possible, due perhaps to a faulty configuration of the IPX router, the exponential backoff algorithm prevents connections constantly being established and thus saves charges.

The *LANCOM Office* router will attempt to reach a remote station again with ever increasing wait times if the first attempt is unsuccessful. The wait time for this is determined as follows:

- The first attempt takes place after $10 + x$ seconds. x being a number from 0 to 10.
- The second attempt will be made $10 + x$ seconds after the first attempt has failed. x now standing for a number from 0 to 20 seconds.
- The higher value for x will now be doubled with each repeated attempt. The *LANCOM Office* router finally gives up after the 16th unsuccessful attempt. The continual increase in the wait time means that 16 attempts will take a maximum of one day.

The route will be blocked if all attempts to call the remote station are unsuccessful. You can then only make further attempts at connection by amending the entry in the routing table.



The time to the next attempt and the number of attempts to establish a connection can be found in the network statistics using (Status / IPX-statistics / IPX-router-statistics / Networks).

IPX packet filters

The entries in the routing table determine which other networks will be accessible. However, they are then also accessible for data packets which are not actually required in the network of the remote station. These packets can also lead to unwanted connections being established which cost money.

Suitable filters are therefore required. These enable you to exclude from transmission over the WAN or at least restrict data packets which are only used in internal network communications, for example:

- Propagated frames

These special data packets use protocols which cannot in fact be routed. This data is encapsulated in normal IPX packets and sent as broadcast so that they can nevertheless participate in common routing.

These packets are sometimes not desirable in routing. For this reason, you can specify explicitly whether this type of packet is to be routed or filtered.

- Socket filter

Every packet in an IPX network contains destination and source sockets along with destination and source addresses. Sockets identify the processes for which the data in the packet is intended.

There is a filter table each for sockets from local and remote networks containing the filters which can be used to exclude individual or entire groups of destination sockets. Certain sockets which are known frequently to be the cause of unwanted connections have already been entered in the socket filter table as default settings.

- RIP and SAP information

A router uses the RIPs to inform the other routers of all the routes (paths to the other networks) known to it using the split horizon principle. This includes the entries from its own routing table and all routes which the *LANCOM Office* router has derived from other routers. The *LANCOM Office* router gets its information for this purpose from routers on both local and remote networks. The *LANCOM Office* router enters all available routing information in its internal RIP table.

The servers offer their services in the SAP information. The various services are represented within the SAP information as numbers. Each service (e.g. file server or print server) has a unique number. The *LANCOM Office* router incorporates the information on the services available in its internal SAP table and registers which ser-

vice is available on which network at which MAC address. At the same time the *LANCOM Office* router also establishes whether the service offered is located in a local or remote network and whether it can propagate the service without first establishing a connection.



You can look at the RIP and SAP tables and their current values in the IPX module (set-up/IPX-module/RIP-config or SAP-config) of the LANCOM Office router.

RIP and SAP information are extremely important for devices communicating on a network, which is why there are various different options for setting up the transmission of these packets.

- A LAN and WAN filter table can be used to tell the *LANCOM Office* router not to include information on routes to particular networks or on certain available services in internal or external tables. The affected routes are thus not used by your *LANCOM Office* router, information on them is not provided and the services are not offered in the local network.
- RIP and SAP packets are always transmitted, i.e. no filters are used. These packets, however, must occupy a part of the connection.
- RIP and SAP packets will only be sent if the information they contain has been modified in some way.
- RIPs and SAPs can be transferred at regular, selectable intervals. Information is usually sent out in one minute intervals. The time interval between blocks can be stretched to up to 60 minutes.
- The most economical handling of RIP and SAP packets involves transmitting the information only once, when a connection is established.

■ IPX and SPX watchdogs:

These data packets are used by the server to determine whether workstation computers, for example, are still active or if they can be logged off. To ensure that these "Are you there?" packets for computers on a remote network do not continually result in connections being established, you can set the responses to these requests as follows:

- Do not respond to IPX watchdogs. The computers are logged off after a time specified on the server.
- IPX and SPX watchdogs can be responded to locally. This procedure is known as spoofing. The *LANCOM Office* router responds in place of the computers addressed, which are then never logged off. It is also recommended that a time is set on the server after which the devices in question are always logged off.
- IPX and SPX watchdogs may of course be routed as normal but this frequently results in a connection being established.



Further information on IPX, the IPX router and the associated parameters can be found in chapter 'Setup/IPX-module'.

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

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

ELSA LANCAPI

What are the advantages of *LANCAPI*?

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

For example, faxes are sent by simulating an ISDN fax machine at the workstation. The PC uses *LANCAPI* to transfer the fax across the network to the *LANCOM Office* router, which establishes the connection to the recipient via ISDN.

LANCAPI's dynamic design also means that communications paths are easily scaled. When more B channels are needed to handle a larger number of jobs, another *LANCOM Office* router is simply installed in the network. All *LANCOM Office* router present in the local network then share the pending tasks.



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

Installing the *LANCAPI* client

The *LANCAPI* is made up of two components, a server (in the *LANCOM Office* router) 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 'autorun.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.

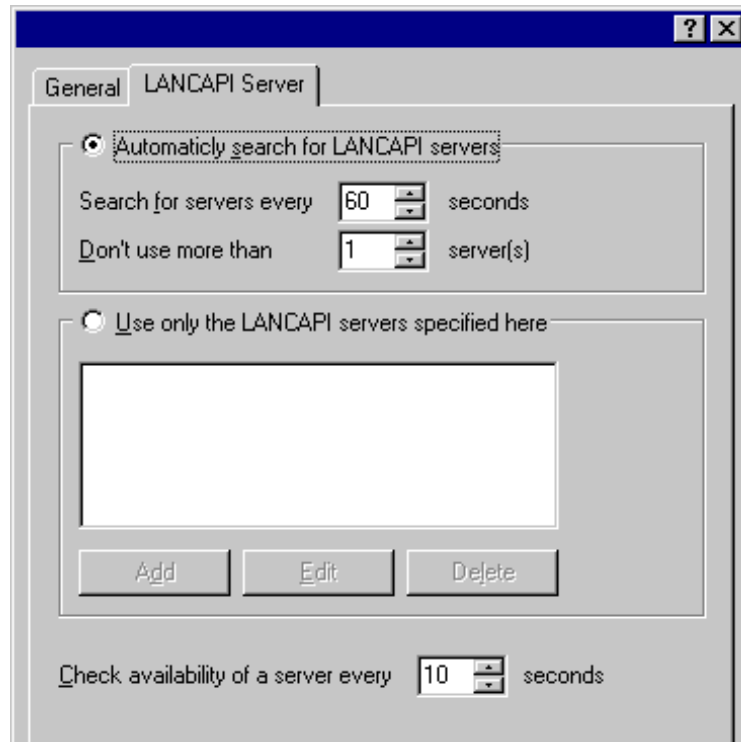
If necessary, the system is restarted and *LANCAPI* is then ready to accept all jobs from the office communications software. After successful installation, an icon for *LANCAPI* will be available in the Start Menu. A double-click on this icon opens a status window that permits current information on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

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



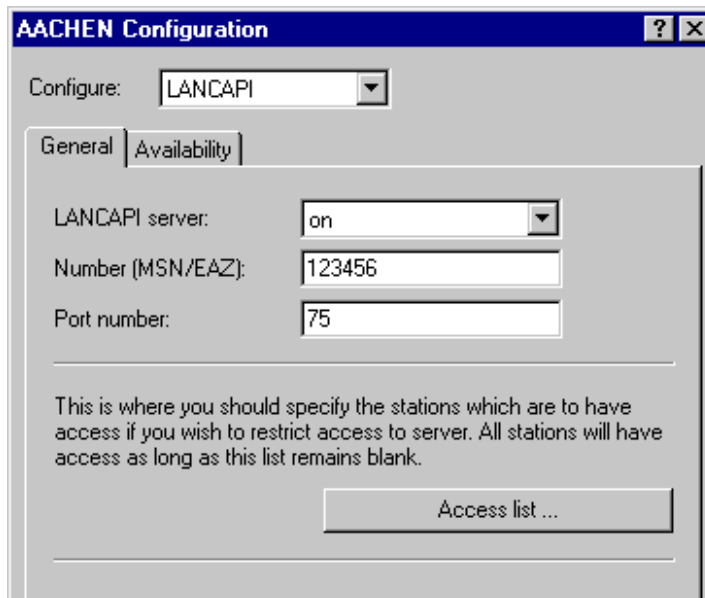
Configuring the *LANCAP* server

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

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

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 'LANCAP' section.

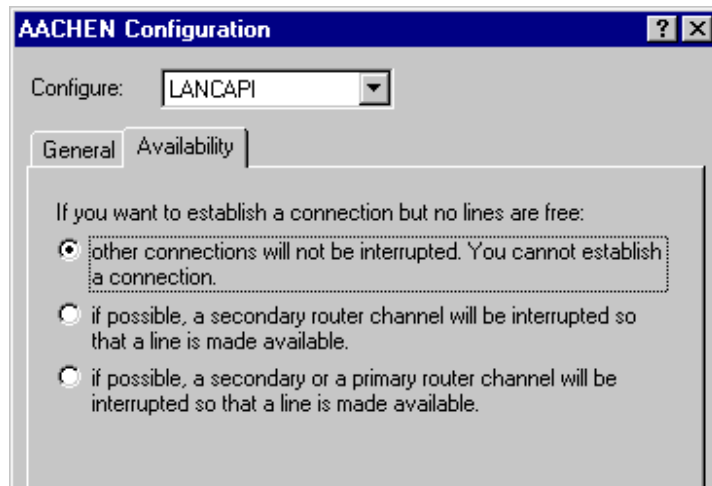


- ② Activate the *LANCAPI* server, or set it to permit outgoing calls only. In the latter case, the *LANCAPI* will not respond to incoming calls—to receive faxes, for example. Permitting outgoing calls only is useful if you do not have a specific call number available for the *LANCAPI*.
- ③ When the *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 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 *LANCOM Office* router should respond if a connection is to be established via the *LANCAP* (incoming or outgoing) when both B channels are already busy (priority control). The available options are:



- The connection cannot be established via the *LANCAP*. A fax program using the *LANCAP* will then probably attempt to send again at a later time.
- The connection via the *LANCAP* 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. The *LANCAP* must wait if two router connections are established to separate remote stations (two main channels busy).
- A connection can always be established via the *LANCAP*; 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 *LANCAP*

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

- You may use software which interacts directly with a CAPI (in this case, the *LANCAP*) 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 *LANCAP*, select the entry 'ELSA ISDN WAN Line 1'.

Automatic address administration with DHCP

The 'Point-to-point protocol' chapter describes a method for assigning IP addresses across the WAN.

But it is also convenient to be able to distribute IP and other addresses automatically to the individual computers within a local network.

Instead of the PPP negotiation used for assigning addresses via the WAN, DHCP serves the same purpose within a LAN.

DHCP, short and sweet

What is 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 DNSs and NBNSs as well as that of a default gateway through which the data packets are to be routed from addresses that are not available locally. In a smaller network, it is still conceivable that these addresses could be entered manually in all the computers in the network. In a larger network with many workstation computers, however, this would simply be too enormous of a task.

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

The *LANCOM Office* router as a DHCP server

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

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

The *LANCOM Office* router takes the IP addresses either from a freely defined address pool or determines the addresses automatically from its own IP address.

In DHCP mode, a completely unconfigured *LANCOM Office* router 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 *LANCOM Office* router to a network without other DHCP servers and switch it on. The *LANCOM Office* router then interacts with *ELSA LANconfig* using a wizard and handles all of the address assignments in the local network itself.

DHCP—on, off or auto?

The DHCP server in the *LANCOM Office* router 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 *LANCOM Office* router will be available to the network as a DHCP server.
 - In the event of an incorrect configuration (e.g. invalid pool limits), the DHCP server is disabled and switches to the 'off' state.
- 'off': The DHCP server is permanently disabled.
- 'auto': The server is in automode. When the *LANCOM Office* router is switched on in this state, it searches the local network for other DHCP servers (this can be seen by the brief flicker of the Tx LED when switching the unit on).
 - The *LANCOM Office* router then disables its own DHCP server if any other DHCP servers are found. This prevents the unconfigured *LANCOM Office* router from assigning addresses not in the local network when switched on.
 - If no other DHCP servers are found, the *LANCOM Office* router enables its own DHCP server.

Whether the server is active or not can be seen in the DHCP statistics.

The default state is 'auto'.

How are the addresses assigned?

IP address assignment

Before the *LANCOM Office* router 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 assigned can be taken from the address pool selected (start address pool to end address pool). Any valid addresses in the local network can be entered here.
- If '0.0.0.0' is entered instead, the *LANCOM Office* router automatically determines the particular addresses (start or end) from the IP or Intranet address settings in the 'TCP-IP-module' using the following procedure:
 - If only the IP address or only the Intranet address is entered, the start or end of the pool is determined by means of the associated network mask.

- If both addresses have been specified, the Intranet address has priority for determining the pool.

From the address used (IP or Intranet address) and the associated network mask, the *LANCOM Office* router determines the first and last possible IP address in the local network as a start or end address for the address pool.

- If the *LANCOM Office* router has neither an IP address of its own nor an intranet address, the *LANCOM Office* router will go into a special operating mode. It then uses the IP address '10.0.0.254' for itself and the address pool '10.x.x.x' for the assignment of IP addresses in the network. In this state, the *LANCOM Office* router only assigns IP addresses and their validity to the computers in the network, but not the other information.

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

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

Network mask assignment

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

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. Incorrect configuration of this section can result in the undesired establishment of connections subject to connect charges!

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 *LANCOM Office* router passes its own IP address as a DNS address. This address is determined as described under 'IP address

assignment'. The *LANCOM Office* router then uses DNS-forwarding (also see 'DNS-forwarding'), to resolve DNS or NBNS requests from the host.

Default gateway assignment

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

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

Period of validity for an assignment

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

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

- Maximum lease time in minutes

Here you can enter the maximum period of validity that the *LANCOM Office* router assigns a host.

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

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

- Default lease time in minutes

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

Priority for *LANCOM Office* router—requesting an 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 *LANCOM Office* router, simply delete the corresponding entries.

Under the 'WINS Address' tab, the 'Use DHCP for WINS Resolution' option must also be activated if you wish to use Windows networks via IP with name resolution via NBNS. In this case, the *LANCOM Office* router must also have an NBNS entry.

Priority for computer—overwriting an assignment

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

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

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

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

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

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

- new
The computer has made its initial request. The *LANCOM Office* router 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 *LANCOM Office* router has no means of obtaining additional information on this computer.
- status
A computer has informed the *LANCOM Office* router that it has a fixed IP address. This address can no longer be used.
- dynamic
The *LANCOM Office* router assigned an address to the computer.

Configuring the *LANCOM Office* router as a DHCP server

Basically, two starting points are possible when the *LANCOM Office* router is 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 the *LANCOM Office* router lets you assign IP addresses

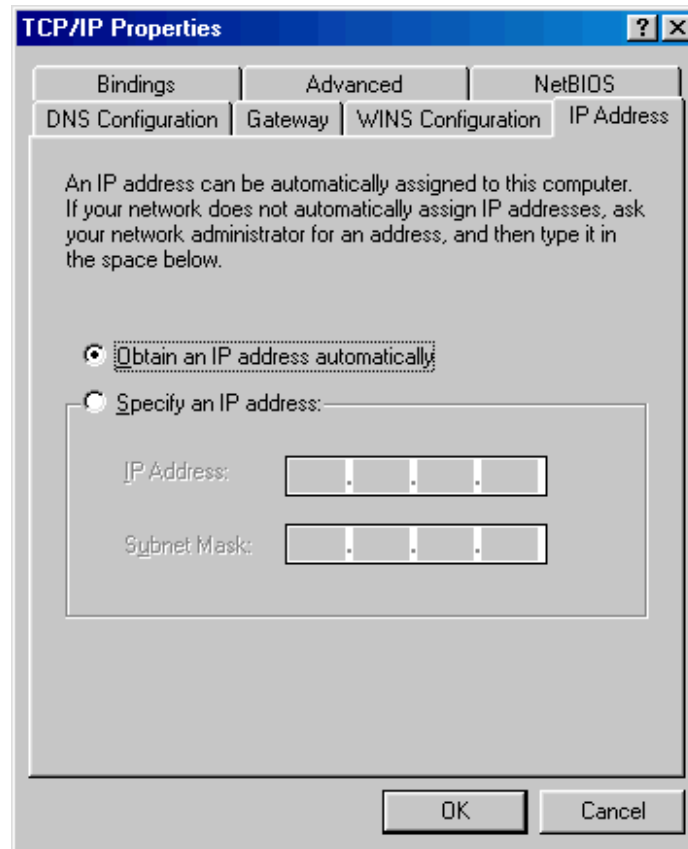
to all of the computers in the network and to the *LANCOM Office* router in a single operation.

- You are already using TCP/IP but without a DHCP server, and you would now like to convert to DHCP operation using the *LANCOM Office* router.

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

- ① Connect the unconfigured *LANCOM Office* router to your local network using a network cable. If you are connecting the *LANCOM Office* router to a hub, the node/hub switch must be set to 'Node'. If you are connecting the *LANCOM Office* router directly to the network adapter of a computer in your network, set the switch to the 'Hub' position.
- ② Switch on the *LANCOM Office* router. The router will not find any other DHCP servers in the network and will thus enable its own DHCP functions.
- ③ If you have not done so already, install the TCP/IP protocol on all computers in the LAN.
 - Usually when the protocol is installed, the default configuration is such that the computers are automatically ready to obtain the IP address from a DHCP server. After rebooting at the end of the protocol installation, the computers automatically request an IP address from the *LANCOM Office* router.
 - 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 router's address pool.



You will learn how to install a network protocol under, for example, Windows 95 or Windows NT in the Workshop. For instructions on how to install ELSA LANconfig, please refer to the Installation Guide.

- ④ Install the *ELSA LANconfig* on a computer in the network.
- ⑤ Start the *ELSA LANconfig* from the 'ELSAan' program group. When loading, the *ELSA LANconfig*, will detect an unconfigured *LANCOM Office* 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 *LANCOM Office* router and enables the DHCP server. On the basis of this IP address, the *LANCOM Office* router then determines the valid address pool for the DHCP assignment.
 - In the event that IP addresses were already in use in your network before converting to DHCP operation, select the option 'I would like to adjust the settings

manually' in the wizard. In the next window, enter an unused IP address from the previously-used address range and activate the DHCP server.

The wizard now assigns the selected IP address and associated netmask to the *LANCOM Office* router. On the basis of this IP address, the *LANCOM Office* router 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 *LANCOM Office* router as required. The computers also receive additional parameters such as the broadcast address, DNS server, default gateway, etc.

The integrated PBX

When migrating from analog lines to digital connections (ISDN), users often ask whether they can continue to use their existing analog terminals. Analog devices such as telephones, fax machines, answering machines or modems can be connected to the four integrated a/b ports of the *LANCOM 2000 Office*.

Consequently, you can also continue to use your analog terminals at the workstation, thus eliminating the necessity of additional investments in new digital terminals. Furthermore, the a/b ports of the *LANCOM 2000 Office* ensure the availability of the latest ISDN add-on functions such as call forwarding, consultation hold, brokering, hold and three-party conferencing.

What's more, the functions of a small PBX system are also available to the devices connected to the a/b ports. For example, it's possible to make internal calls, transfer calls to a different terminal device or broker between internal and external calls.

Please also note the functions of the least-cost router in this context!

Connecting analog terminals

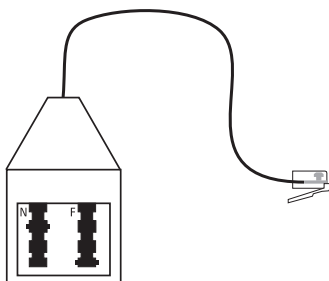
Which devices can be connected?

Basically, you can connect all analog terminals to the a/b ports of the *LANCOM 2000 Office*:

- Telephones
- Group 3 fax machines
- Answering machines
- Modems
- Multipurpose devices

Telephone adapter (RJ11)

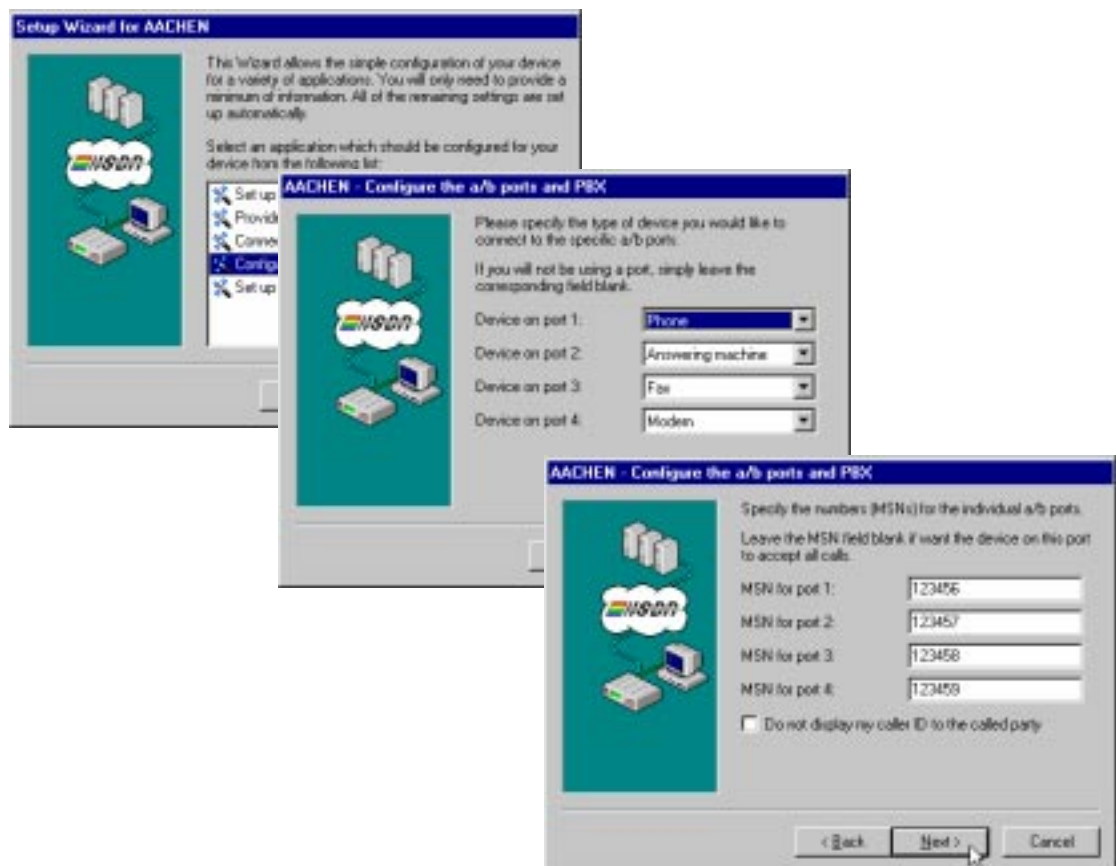
In order to allow you to continue using your analog terminals (e.g. telephones, answering machines, fax machines), ELSA supplies the appropriate adapters.



Configuration with *ELSA LANconfig* and the Setup Wizard

A wizard is available in the *ELSA LANconfig* to configure the a/b ports and the PBX of the *LANCOM 2000 Office* and to take care of all of the settings of the *LANCOM Office* router software for you. Basically, you only need to specify which device is connected to which a/b port and the MSNs to be assigned to the individual devices.

- ① Start the *ELSA LANconfig* in the 'ELSAIan' program group.
- ② In the Device List, mark the *LANCOM Office* router which you would like to set up. Click on **Tools** ► **Setup Wizard** and select the entry 'Configure the a/b ports and PBX'.



- ③ In the following steps, specify which device is connected to which a/b port and assign MSNs to the a/b ports.
- ④ Next, specify whether you are going to use the *LANCOM Office* router as a PBX, or whether you will continue using it as a normal telephone connection.
- ⑤ You have already taken care of everything with these settings. Click on **Finish** in the next window to close the wizard and save the new settings to your *LANCOM Office* router.

What have you achieved with this wizard? The results vary according to the device types selected for the individual ports. In addition to the MSNs and the fixed internal calling numbers, the following special settings apply:

■ Telephone

If you have a telephone connected to an a/b port with this setting, a further call for that port will be signaled by a call-waiting tone.

■ Answering machines

Call waiting does not apply to the answering machine setting, but it is possible to accept the call. If the answering machine is already responding to a call by the time that you reach the telephone, simply pick up the receiver to take the call yourself.

■ Fax and modem

The wizard automatically disables the options described above, as neither call waiting nor the internal transfer of calls is desirable for these devices.

■ External call

- With the *LANCOM 2000 Office* set as a PBX, you are initially connected to the *LANCOM Office* router when picking up the telephone handset. You can make internal calls immediately, or dial zero to get a dial tone for external calls.

If your LANCOM 2000 Office is connected to a PBX, dialing zero will naturally only access the superordinate PBX, after which another zero may be required to get a dial tone!

Please also note that the leading zero must be added to the telephone books or speed-dial entries of telephones, modems and other devices.

- With the *LANCOM 2000 Office* set as a normal telephone connection, you will hear the dial tone of the external exchange (or that of the PBX to which the *LANCOM 2000 Office* is connected) immediately upon picking up the telephone handset. Internal telephone calls via the *LANCOM 2000 Office* are not possible in this mode.

If you are not satisfied with one or more points of the configuration set by the wizard, the configuration can be subsequently modified as described in the following section.

Manual configuration with *ELSA LANconfig*

The response of each of the four a/b ports to incoming and outgoing calls can also be set up precisely by hand if necessary.

Select the 'Telephony' configuration section. On the 'a/b Ports' tab, select the country in which you are using your *LANCOM 2000 Office*. You may also set up the response to calls which can be taken by multiple devices: Do all of the units ring individually and consecutively, in pairs or all at the same time?

Please bear in mind the high power requirements, especially for older telephones. If several such devices are set to ring at the same time, the power supply of the LANCOM



Office router may be overloaded. In that case, select the 'one at a time' or 'two by two' setting.



The configuration of each individual port can now be edited in the pulldown list for the a/b port settings. The symbol next to the entry shows the type of device for which the port is set up. Select the entry from the list for which you would like to modify the settings.

General settings

Specify the following settings for each a/b port used on the 'General' tab:

a/b Port settings - Port 1

General | Public exchange access | Class of service | Availability

Number (MSN/EAZ): 123456

Internal calling number: 11

Description: Phone

Capability: Telephony analog

☐ Don't ring on incoming calls (do-not-disturb service)

☐ Let hear knocking tone on incoming call during a conversation

☐ Generate metering pulse (for phones with charging display)

☐ Suppress transmission of own phone number to the remote site

☐ Allow automatic adoption of an established connection by another port (for answering machines)

☐ Automatically interconnect two external calls when hanging up

☐ Dial the following number whenever the phone is picked up:

Number: 123666

OK Cancel

- Assign a 'Number' to the connection: MSN (multiple subscriber number) for point-to-multipoint connections using DSS1 as the D-channel protocol, DDI (direct dial-in) for point-to-point connections or EAZ (terminal selection digits) for 1TR6 connections.
 - For the a/b to respond to several numbers, enter the numbers separated by semi-colons.
 - The first of these numbers is displayed to the exchange and the remote station during outgoing calls.
 - If you do not enter a number, the a/b port will respond to all incoming calls and will display the primary number of your connection to the exchange and remote station.
- The internal number of the a/b port is fixed and cannot be modified.
 - '11' for a/b port 1
 - '12' for a/b port 2
 - '13' for a/b port 3
 - '14' for a/b port 4
- Provide a description for the port. This description has no effect on the function of the ports or the attached devices, but is only intended to simplify the identification of the attached terminal equipment. The available choices:

- No description
- Telephones
- Group 3 fax machines
- Answering machines
- Modems
- Combined devices
- Select the service that the a/b port itself reports to the remote station during call establishment. This setting does not specify the acceptance of incoming calls according to service! Possible settings are:
 - Analog 3,1 kHz (default setting)
 - Speech
 - Fax Group 2/3
- Enable or disable the following options as required:
 - 'Don't ring...' toggles the ring of the connected terminal device.
 - 'Let hear knocking tone on incoming call...' enables additional calls for a specific port to be signalized during an existing connection.
 - 'Generate metering pulse' generates a charge pulse on the basis of the ISDN connect-charge information and sends it to the device attached to this port. The charges for the current call can thus be monitored on analog telephones equipped with a connect-charge display. Disable this option for ports used by modems or fax machines, as the charge pulse may interfere with data transmission.



The charge pulses only function correctly on 'AOCD' lines (advice of charges during call). The connect charge information of 'AOCE' lines is not transferred until the connection has been terminated, in which case the telephone will no longer be able to count the charge pulses correctly.

- 'Suppress transmission of own phone number...' prevents your number from being transmitted to the remote station if you would like to prevent your call from being identified on the basis of your number. The number is always transmitted to the exchange. Your telecommunications provider will thus be able to provide an itemization of connect charges according to subscriber numbers even with the caller ID suppressed.



The "Individual suppression of call number" option is a feature which may require a specific application to your telecommunications provider.

- 'Allow automatic adoption...' permits a call to be taken over after it has already been accepted by a device on another port. This option is generally only activated for ports with an answering machine.

- 'Automatically interconnect...' permits the connection of external callers. While making two external calls, it is possible to connect the two external parties to one another by simply hanging up.

This feature may also require a specific application to your telecommunications provider.

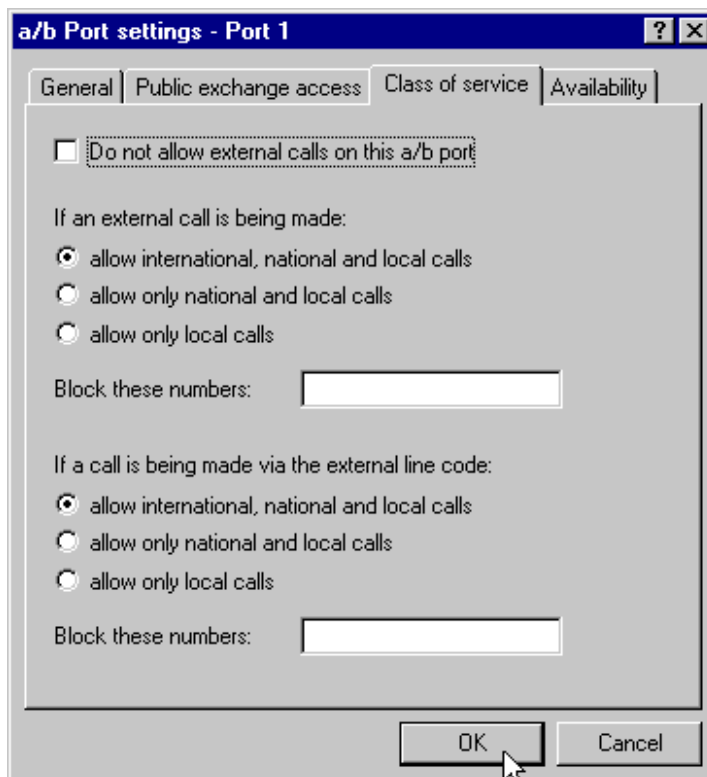
Please note that you will bear connect charges for this type of connection, even if you are no longer participating in the call yourself!

- 'Dial the following number...': Enter the call number to be used for the auto connection function. The number entered here will be dialed automatically five seconds after lifting the receiver if no other number is dialed during that time.

This function can also be programmed using the keypad of your telephone. This will overwrite the settings made in ELSA LANconfig.

External call settings

Change over to the 'Public exchange access' tab. Here you can configure the response of the a/b port to the off-hook telephone and the flash key. Please take "off-hook" literally, since a modem or fax machine on this port would initiate the dialing process in a different manner.



Three options are available for the off-hook response:

- In Option 1, lifting the receiver only initiates a connection to the *LANCOM Office* router. You can now make an internal call, i.e. to a device on one of the other a/b

ports. Please distinguish between the two following methods for placing external calls:

- If the *LANCOM Office* router is connected directly to the ISDN, dial a '0' to place an external call.
 - If the *LANCOM Office* router is itself connected to a further large PBX system, it may be necessary to also dial the external-calling prefix of this PBX to get an external dial tone.
- In Option 2, lifting the receiver establishes a connection to the ISDN or superordinate PBX to which your *LANCOM Office* router is connected. This corresponds to an internal connection to the *LANCOM Office* router, for which the '0' for an external line has been dialed automatically. You now have the following possibilities:
- If the *LANCOM Office* router is connected directly to the ISDN, place an external call without dialing any additional prefixes.
 - If the *LANCOM Office* router is itself connected to a further large PBX system, it may be necessary to also dial the external-calling prefix of this PBX to get an external dial tone.
- In Option 3, lifting the receiver establishes a connection to the ISDN or superordinate PBX to which your *LANCOM Office* router is connected, i.e. a '0' is dialed automatically once the connection to the *LANCOM Office* router has been established. In addition, the number entered in the field at the bottom of this window is also dialed automatically. This setting gives you the following possibilities:
- If the *LANCOM Office* router is itself connected to a further large PBX system, you can automatically dial the external-calling prefix of this PBX to get an external dial tone.
 - If you would like to make long-distance calls from this telephone with specific long-distance carriers on a call-by-call basis, enter the prefix of the long-distance carrier here (e.g. 0101x) in addition to any other required prefixes. This will automatically give you the dial tone of your long-distance carrier each time you pick up the receiver.

Flash key (R key) functions

The options for the effect of the flash key can be found in the lower section of the 'Public exchange access' tab.



On most telephones, the flash key is the consultation-hold or R key. The function of this key is often configurable. Please consult the documentation of your telephone for the default settings of the key and for information on reprogramming its function. Signals of a length between 70 and 300 ms are identified by the LANCOM Office router as a flash.

One of three options for the response to the flash key may also be selected. The options are the same as those for the off-hook response:

- With Option 1, pressing the flash key establishes a connection to the internal PBX of the *LANCOM Office* router. You can now place an internal call or dial '0' to establish a connection to the ISDN (or the superordinate PBX).
- With Option 2, pressing the flash key establishes a connection to the ISDN (or the superordinate PBX) directly.
- With Option 3, pressing the flash key automatically dials the specified external number.

The interaction of the off-hook and flash settings can be used to adapt the PBX in your *LANCOM Office* router to your specific needs. Examples:

- Your *LANCOM Office* router is connected directly to the ISDN. Select Option 2 for the off-hook response and Option 1 for the flash key. You can now make external calls by lifting the receiver; pressing the flash key enables internal calls.
- Your *LANCOM Office* router is connected to a superordinate PBX. Select Option 1 for the off-hook response and Option 3 for the flash key. Enter the number required by your PBX to place external calls in the 'External line code' field. You can now make internal calls by lifting the receiver; pressing the flash key automatically dials the required prefixes to place an external call.

The flash key functions vary according to whether a connection is currently active, an opposite party is on consultation hold, or a number is currently being dialed. The following table shows the specific effect in a variety of situations. It is generally safe to assume that using the flash key will perform the function that you need in any given situation.

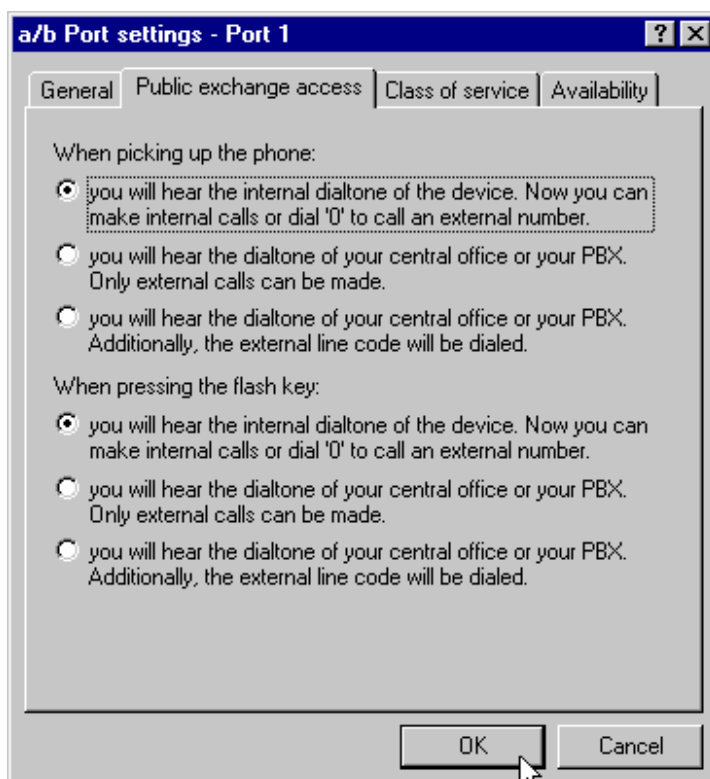
The following occurs in detail:

Connection state	Status	Effect of flash key
No active connection	<ul style="list-style-type: none"> - Dial tone - Incomplete dialing - Timeout during dialing - Remote station ringing - Timeout during ringing 	Dialing/call establishment canceled, the preset function is executed.
Active connection		Connection is held, the preset function is executed.
Connection is being held	- Dial tone	Returns to held connection.
	<ul style="list-style-type: none"> - Incomplete dialing - Timeout during dialing 	Dialing canceled, the preset function is executed.
	<ul style="list-style-type: none"> - Remote station ringing - Timeout during ringing 	Call establishment canceled, return to held connection.
One connection active, another connection held, or waiting		Flash + '0': held/waiting connection is disconnected. Flash + '1': active connection is disconnected, held/waiting connection activated. Flash + '2': transfer from active to held/waiting connection. Flash + '3': establish three-party conference.

Connection state	Status	Effect of flash key
Active three-party conference		Flash + '2': three-party conference is returned to one active and one held connection.

Configuration of the external calling authorization

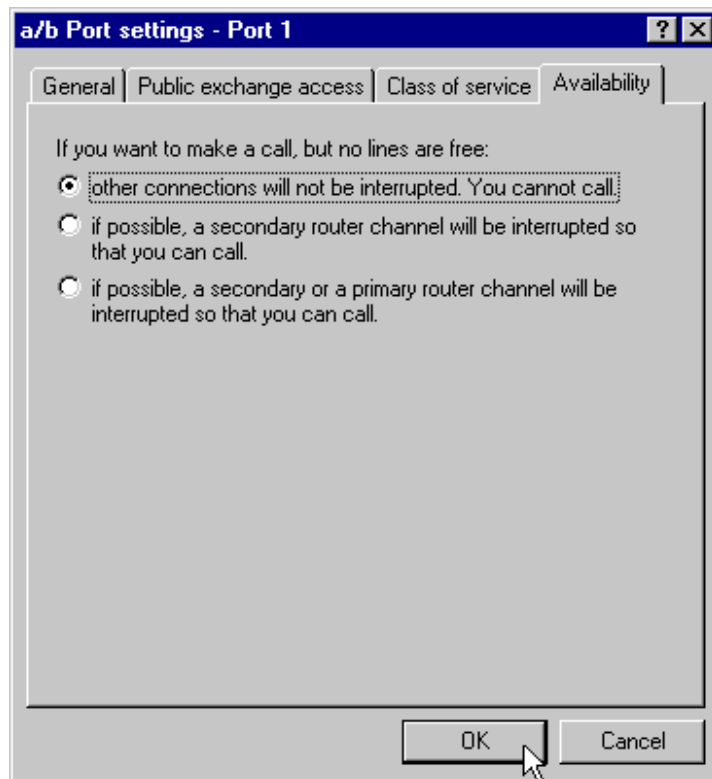
Use the 'Class of service' tab to set the authorization for outgoing external calls for the devices on each a/b port.



This does not affect the acceptance of external calls. External calls can also be restricted to local or domestic long-distance calls. Access to specific external numbers can also be locked.

Configuring availability

Use the 'Availability' tab to determine how the *LANCOM Office* router should respond if a connection is to be established via the a/b ports (incoming or outgoing) when both B channels are already busy (priority control). The available options are:



- Termination of other connections not permitted. The connection cannot be established via the a/b port.
- Permit termination of secondary channels, e.g. those in use for channel-bundled connections. The connection via the a/b port can then be established when a primary channel is free.
- Permit termination of primary channels. A connection can always be established via the a/b port; an existing router connection will be terminated for the duration of the call if required. The telephone is thus always available.

Call waiting must be enabled to ensure that the LANCOM 2000 Office can identify incoming calls during existing connections.

Operating the PBX via telephone

The *LANCOM 2000 Office* allows you to use certain enhanced features (e.g. brokering). This requires that you have a telephone suitable for tone dialing (DTMF dialing) and an R key (consultation key with hook-flash function).

If you are not certain whether your telephone works with tone or pulse dialing, it is generally easy to find out by listening to the sounds in the receiver when dialing normally: If



you hear a clicking after each dialed digit, your phone uses pulse dialing; if you hear different beeping tones, it uses tone dialing.



Some features (such as call waiting) are features that you must specifically apply for from your telephone company.

Call waiting

With this function, you hear a signal tone whenever a second call is pending. You can then decide whether you wish to continue your current conversation or terminate this call and answer the waiting call. To answer a waiting call, do the following:

- ① Checking the activation
 - To check whether this feature is activated, lift the receiver and press *** # 4 3 #**.
 - If you hear two clear tones, the function is activated. If you hear two faint tones, the function is not activated.
- ② Activating call waiting
 - Lift the receiver and wait for the dial tone.
 - Press the following series of keys on your telephone: *** 4 3 #**.
 - When you hear the announcement, replace the receiver.
- ③ Answering a waiting call
 - Press the **flash** key within 30 seconds of hearing the signal in the receiver.
 - Press key **2**. The first call is now deactivated and the second call is activated.
 - Press the flash key and **2** to toggle between the two callers (brokering).
- ④ Terminating an existing call
 - Press the **flash** key.
 - Press **1** to terminate the activated call.



Make sure that you replace the receiver or hold down the hookswitch for at least half a second between telephone calls.

- ⑤ Deactivating call waiting
 - Lift the receiver and wait for the dial tone.
 - Press the following series of keys on your telephone: **# 4 3 #**.
 - When you hear the announcement, replace the receiver.

Three-party conference

This function allows you to speak to two parties simultaneously. You can either call both conference parties yourself or add a call-waiting party to an existing call.



A three-party telephone conference can only be held between two external callers and one internal connection. In other words, two internal participants cannot establish a conference with an external caller.

To establish a three-party conference, do the following:

- ① three-party conference with call-waiting party
 - Press the **flash** key within 30 seconds of hearing the signal in the receiver.
 - Press key **2**. The first call is now deactivated and the second call is activated.
 - Press the **flash** key once again.
 - Press **3** to activate the three-party conference.
- ② Three-party conference with two independent connections
 - Establish a connection to the first party.
 - Next, press the **flash** key. Depending on the external calling configuration, you will now hear an internal or external dial tone.
 - Enter the call number for the second party. The first call is now deactivated and the second call is activated.
 - Press **3** to activate the three-party conference.
- ③ Terminating an active connection
 - Press the **flash** key.
 - Press **1** to terminate the activated call.
- ④ Terminating both connections
 - Hanging up the receiver will terminate both connections of the three-party conference simultaneously.



Please bear in mind the setting of the 'Automatically interconnect two external calls when hanging up' option for the relevant a/b port. If this option is enabled, the connections will not be terminated when you hang up, but the two external participants will remain connected with one another.

Please note that you will bear connect charges for this type of connection, even if you are no longer participating in the call yourself!

Consultation hold/brokering

This function allows you to establish a second call parallel to an existing connection in order, for example, to ask a question. To initiate consultation hold, do the following:

- ① Establishing a second call
 - Press the **flash** key.

- Enter the relevant call number. The first call is now deactivated and the second call is activated (consultation).



The second call can be established to an internal or external remote station.

② Brokering

- Press the flash key and **2** to toggle between the two calls (brokering).

③ Connection

- Hanging up the receiver will connect the two caller to one another.



Please bear in mind the setting of the 'Automatic transfer of external calls on hang-up' option for the relevant a/b port. It is also possible to connect two external callers with one another when this option is enabled.

④ Terminating an existing call

- Press the **flash** key.
- Press **1** to terminate the activated call.



When terminating the active connection by hanging up, the phone will ring again immediately to remind you of the held connection.

Accepting calls from another phone

If you have telephones connected to more than one a/b port, you can use this function to redirect calls for another telephone to your own telephone.

- ① Pick up your receiver while the other telephone is ringing.
- ② When you hear the internal dial tone of the *LANCOM 2000 Office*, dial the internal number of the a/b port currently being called. If you do not automatically receive the internal dial tone of the *LANCOM 2000 Office*, you may have to press the **flash** key to establish the connection to the *LANCOM 2000 Office*.
- ③ Next, press the **8** key to transfer the call from the other a/b port to your telephone.



*If you are currently making a call yourself, press the **flash** key (depending on the configuration of the *LANCOM 2000 Office*) to place your own call on hold before transferring the other call to your telephone using the internal number and the **8**.*

Call forwarding

This function makes you available under your call number wherever you go. You only need enter the relevant destination call number and all calls are automatically forwarded to this number. Forwarding can be performed either immediately, after 15 seconds or when the line is busy. To activate the function, do the following:



Before you can use this enhanced feature, you must assign an MSN to the a/b ports. Use ELSA LANconfig to assign an MSN.

① Activating call forwarding

- Lift the receiver and wait for the dial tone.
- Press the following series of keys on your telephone:
 - * 2 1 *** (for immediate call forwarding)
 - * 6 1 *** (for call forwarding after 15 seconds)
 - * 6 7 *** (for call forwarding when busy)
- Enter the relevant destination call number and press #.
- If you hear two clear tones, the function is activated and you can replace the receiver.



*If you have not assigned an MSN to the a/b port, use the key combination *** x y * destination call number * MSN of the a/b port #** to enable call forwarding, or **# x y * MSN of the a/b port #** to disable it (in this case, x y stands for the codes for the 'immediate', 'after 15 seconds' or 'when busy' options).*

*To check whether this service is active, pick up the receiver and wait for the dial tone, then dial **# * x y * MSN of the a/b port #**. If you hear two clear tones, the function is activated. If you hear two faint tones, the function is not activated.*

② Deactivating call forwarding

- Lift the receiver and wait for the dial tone.
- Press the following series of keys on your telephone:
 - # 2 1 #** (for immediate call forwarding)
 - # 6 1 #** (for call forwarding after 15 seconds)
 - # 6 7 #** (for call forwarding when busy)
- Two high tones indicate that the function was active and has been disabled. You may hang up now. If you hear a single low tone, the function was either not enabled or you entered an incorrect MSN!

Hotline

This function allows you to dial a special destination call number (e.g. emergency services) automatically. If no call number is dialed within five seconds of lifting the receiver, this destination number is automatically dialed.

For example, if you go out for the evening you can enter the call number under which you can be reached. Your child simply needs to lift the receiver and the number is dialed automatically.



This function can also be configured using ELSA LANconfig. This will overwrite the settings made using the telephone keypad.

To activate the function, do the following:

- ① Checking the activation
 - To check whether this feature is activated, lift the receiver and (after listening for the dial tone) press *** # 5 3 #**.
 - If you hear two clear tones, the function is activated. If you hear two faint tones, the function is not activated.

Please note that you may have to dial the prefix '0' depending on the external calling configuration of the a/b port.
- ② Activating hotline
 - Lift the receiver and wait for the dial tone.
 - Press the following series of keys on your telephone: *** 5 3 ***.
 - Enter the relevant call number and press **#**.
 - If you hear two clear tones, the function is activated and you can replace the receiver.
- ③ Deactivating hotline
 - Lift the receiver and wait for the dial tone.
 - Press the following series of keys on your telephone: **# 5 3 #**.
 - If you hear two clear tones, the function is activated and you can replace the receiver.



*Once you have entered a number for the hotline function and disabled the function, you can reactivate the stored hotline number at any time by dialing *** 5 3 #**.*

Activating an a/b port for calls

This function allows you to determine whether your telephone will ring when you receive a call. It is particularly useful when you do not wish to be disturbed. The caller will then receive a busy signal. To activate the function, do the following:

- ① Checking the activation
 - To check whether this feature is activated, lift the receiver and (after listening for the dial tone) press *** # 9 9 #**.
 - If you hear two clear tones, the function is activated. If you hear two faint tones, the function is not activated.
- ② Activating a/b port
 - Lift the receiver and wait for the dial tone.
 - Press the following series of keys on your telephone: *** 9 9 #**.
 - If you hear two clear tones, the function is activated and you can replace the receiver.
- ③ Deactivating a/b port

- Lift the receiver and wait for the dial tone.
- Press the following series of keys on your telephone: **# 9 9 #**.
- If you hear two clear tones, the function is activated and you can replace the receiver.

Call number suppression

This function allows you to suppress the display of your multiple subscriber number (MSN) at the remote station.



The “Individual suppression of call number” option is a feature which may require a specific application to your telecommunications provider.

To activate the function, do the following:

- ① Checking the activation
 - To check whether this feature is activated, lift the receiver and (after listening for the dial tone) press *** # 3 1 0 #**.
 - If you hear two clear tones, the function is activated. If you hear two faint tones, the function is not activated.
- ② Activating call number suppression
 - Lift the receiver and wait for the dial tone.
 - Press the following series of keys on your telephone: *** 3 1 0 #**.
 - If you hear two clear tones, the function is activated and you can replace the receiver.
- ③ Deactivating call number suppression
 - Lift the receiver and wait for the dial tone.
 - Press the following series of keys on your telephone: **# 3 1 0 #**.
 - If you hear two clear tones, the function is activated and you can replace the receiver.

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. *LANCOM Office* router 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 *LANCOM Office* router automatically selects the most economical provider for you, regardless of whether you are using the router, the *LANCAPI* or the a/b ports.

Function of the *LANCOM Office* router least-cost router

The LCR in the *LANCOM Office* router analyzes the digits dialed by the router, the *LANCAPI* or by a connected device such as a telephone or fax machine in the case of the *LANCOM 2000 Office*.

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

The LCR also requires the following information:

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

Initial tests

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

You know, for example, that considerable savings can be had by selecting a provider on a call-by-call basis for long distance and international calls, as well as calls to mobile

telephone networks. 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
089	01097	Sat + Sun	0:00 AM to 11:59 PM
089	01098	Mon + Tue + Wed + Thu + Fri	8:00 AM to 6:00 PM
0172	01099	Every day	0:00 AM to 11:59 PM
00	01097	Sun	0:00 PM to 11:59 PM

These four entries mean that all calls 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 '01098'. Calls to the D2 mobile network ('0172') will be made via the provider with the network prefix '01099', and international calls placed on Sundays will use the provider with the network prefix '01097'.

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 *LANCOM Office* router LCR table. A variety of approaches are possible:
- Combinations leading to definite savings can be entered directly, e.g. the prefixes '0177', '0171', '0172' for mobile networks in Germany, or '00' for international calls.
- 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', '0190', 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 tele-

phone company (e.g. '01033' for the Deutsche Telekom network). If the entry for the network prefix is left empty, the entry will not be rerouted.

- Perhaps a large number of your long-distance calls go to the same area codes. If your whole family lives in one city, for example, you may wish to use one specific provider for all of your family-related calls.
- 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.billiger-telefonieren.de'.

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.billiger-telefonieren.de' or 'www.focus.de' in Germany, for example, contain complete, up-to-date listings for all types of telephone connections. With this information on hand, you can now begin feeding your least-cost router...

Setting up the least-cost router

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

- Which operating modes of the *LANCOM Office* router 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 (IP, IPX and bridge)
 - a/b ports (*LANCOM 2000 Office* only)
 - *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.

- 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?
- 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 or the a/b ports. Use the dialed number to verify whether the LCR settings suit your requirements. For router connections, check the log file for the number dialed (**View** ► **Options** ► **Logging** ► **View**).*

Please refer to the 'PBX and least-cost router' chapter in the Workshop for a comprehensive LCR configuration example.

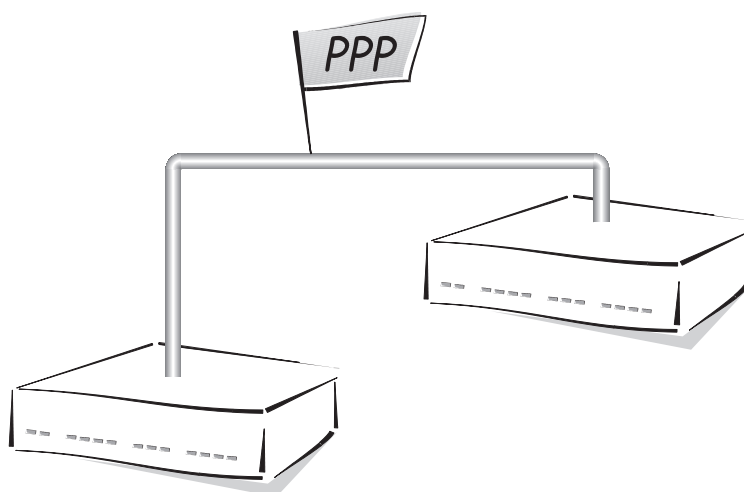
Time for the selection

It goes without saying that the internal clock of the LANCOM Office router 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 *LANCOM Office* router 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 LANCOM Office router, which would impair the function of the least-cost router!



Point-to-point protocol

As mentioned in the 'Transfer protocols' chapter, the *LANCOM Office* router also supports the point-to-point protocol (PPP). PPP is a generic term for a whole series of WAN protocols which enable the interaction of routers made by different manufacturers since this protocol is supported by practically all manufacturers. PPP is used with both the IP router and the IPX router in the *LANCOM Office* router.

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

The protocol	2
The PPP list	4
Everything ok? Checking the line with LCP	5
Assigning IP addresses via PPP	6
Callback functions.....	8
Channel bundling with MLPPP	12

The protocol

What is PPP?

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

- Password protection according to PAP or CHAP
- Callback functions
- Negotiation of the network protocol to be used over the connection established (IP or IPX, for example). Included in this are any parameters necessary for these protocols, for example IP/IPX addresses. This process is carried out using IPCP and IPXCP protocols (IP Control Protocol and IPX Control Protocol).
- Verification of the connection through the Link Control Protocol (LCP)
- Channel bundling (Multilink PPP)

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

What is PPP used for?

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

- for reasons of compatibility when communicating with external routers, for example
- remote access from remote workstation computers with ISDN adapters
- Internet access (when sending addresses)

PPP as implemented in the *LANCOM Office* router can be used synchronously or asynchronously and over both a transparent HDLC connection and an X.75 connection.

The phases of PPP negotiation

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

- Establish phase

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

This ascertains whether the remote station is also ready to use PPP, and the packet sizes and authentication protocol (PAP, CHAP or none) are determined. The LCP then switches to the “opened” status (also see 'Status/PPP-statistics').

■ Authenticate phase

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

There may also be negotiation on a callback using CBCP (Callback Control Protocol) during this phase.

■ Network phase

The IPCP and IPXCP protocols have been implemented in the *LANCOM Office* router.

The IPCP and/or IPXCP network layers can be established following a successful transfer of the password.

IP and/or IPS packets can be transferred from the router modules to the opened line if the negotiation of parameters is successful for at least one of the network layers.

■ Terminate phase

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

PPP negotiation in the *LANCOM Office* router

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

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

```
trace + ppp
```

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

If you are using a computer running Windows 95, Windows 98 or Windows NT for remote access using PPP and an ISDN terminal adapter or an ISDN PC card, there are exhaustive troubleshooting guides in the online media which can serve as an introduction to configuring such connections.

The PPP list

You can specify a custom definition of the PPP negotiation for each of the remote stations that contact your *LANCOM Office* router.

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

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

Everything ok? Checking the line with LCP

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

The reliability of the line can be constantly monitored using the LCP once the connection has been established. This is achieved within the protocol by the LCP echo request and the associated LCP echo reply. The LCP echo request is a query in the form of a data packet which is transferred to the remote station along with the data. The connection is reliable and stable if a valid response to this request for information is returned (LCP echo reply). This request is repeated at defined intervals so that the connection can be continually monitored.

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



We recommend that you switch off regular LCP queries in the case of remote access from individual workstation computers using Windows 95, Windows 98 or Windows NT since these operating systems do not respond to LCP echo requests.

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



Assigning IP addresses via PPP

In order to connect computers using TCP/IP as the network protocol, all participating computers require a valid and unique IP address. In the event that a remote station does not have an IP address of its own (e.g. an individual computer belonging to a teleworker), the *LANCOM Office* router can assign an IP address for the duration of the connection to permit communications.

This mode of assigning addresses is run during the PPP negotiation and is used only for connections over the WAN. The assignment of addresses via DHCP (also see 'Automatic address management via DHCP'), on the other hand, is used only within the LAN.

Assignment of an IP address will only be possible if the LANCOM Office router can identify the remote station by its call number or name when the call arrives, i.e. the authentication process has been successful.

■ Example: Remote access

Address assignment is made possible by a special entry in the IP routing table. 255.255.255.255 is specified as the network mask as the IP address to be assigned to the remote station in the 'Router-name' field. In this case the router name is the name the remote station uses to identify itself to the *LANCOM Office* router.

In this configuration, the addresses of the DNS and NBNS servers (Domain Name Server and NetBIOS Name Server), including those of the backup servers based on the entries in the TCP/IP module are sent to the remote station in addition to the IP address.

For the whole thing to work it follows that the remote station should be configured to take the IP address and the name servers (DNS and NBNS) from the *LANCOM Office* router. This can be done under Windows Dial-Up Networking, for example, using the 'TCP-settings' under 'IP-address' or 'DNS-configuration'. Enable the 'Server-assigned IP-address' and 'Server-assigned name server addresses' options.

■ Example: Internet access

The assignment of IP addresses can take place the other way round if the *LANCOM Office* router is used to provide access to the Internet for a local area network. In this case it is possible to configure the *LANCOM Office* router so that it has no valid Internet IP address of its own but has one assigned to it by the Internet provider for the duration of the connection. The *LANCOM Office* router also receives information on DNS servers at the provider in addition to the IP address during PPP negotiation.

The *LANCOM Office* router is only known by its internally valid Intranet address on the local area network. This means that all workstation computers on the local area network can access the same Internet account and reach the same DNS server, for example.

Windows users can view the assigned addresses in the *LANmonitor*. In addition to the name of the remote station, the current IP address as well as the addresses of DNS and NBNS servers can be found there. Options such as channel bundling or the duration of the connection are also displayed.



The ELSA LANmonitor is generally installed automatically during the installation of the ELSA LANconfig. Its description can be found in the 'Configuration modes' chapter in the 'What's happening on the line?' section.

Callback functions

In addition to callback via the D channel and via the ELSA protocol, the *LANCOM Office* router also supports callback via CBCP as specified by Microsoft and via PPP in accordance with RFC 1570 (PPP LCP extensions). There is also the option of a particularly fast callback using a process developed by ELSA.

PCs running Windows 95, Windows 98 or Windows NT can only be called back through the CBCP. The following values have been made available to you in the name list for the callback entry so that additional call number verification is also possible on the *LANCOM Office* router:

This entry is used to...	...to set the callback so that:
Off	No callback occurs.
Auto (not Windows 95, Windows 98 or Windows NT, see below)	If the remote station is found in the number list, it will be called back. The call is initially rejected and the return call placed as soon as the channel is free (approx. 8 seconds later). If the remote station is not found in the number list, the call is initially accepted as the DEFAULT remote station and the callback is negotiated during the callback protocol negotiation (ELSA or PPP). A charge of one unit is incurred for this.
Name	A protocol negotiation is always performed before the return call is placed, even if the remote station is found on the number list (e.g. for computers using Windows that have dialed into the device). A charge of one unit is incurred for this.
ELSA	If the remote station is found in the number list, a fast callback is performed; i.e. the <i>LANCOM Office</i> router sends a special signal to the remote station and returns the call immediately once the channel is free. The connection is established in approx. 2 seconds. If the remote station does not cancel the call immediately upon receiving the signal, a fallback to the standard callback procedure is performed after 2 seconds (duration of call establishment approx. 8 seconds). This process is only available for DSS1 connections.
Looser	Use the 'Looser' option if a return call is being expected by the remote station. This setting simultaneously fulfills two tasks. It ensures that the call establishment is canceled locally for incoming calls from a remote station just called, as well as enabling the response to the fast-callback process. In other words, to take advantage of the fast callback, the caller must be in 'Looser' mode, while the station being called must be set to the 'ELSA'.



Greatest security is offered by the 'Name' setting if an entry exists in both the number list and the PPP list. The 'ELSA' setting ensures the fastest callback method between two ELSA routers.

*The 'Name' setting **must** be selected for Windows remote stations.*

Microsoft CBCP callback

Microsoft CBCP provides a number of options to determine callback numbers:

- The party called does not call back.
- The party called allows the caller to specify the callback number itself.
- The party called knows the callback numbers and **only** calls these back.

It is possible to use the CBCP from a PC running Windows 95, Windows 98 or Windows NT to establish a connection to the *LANCOM Office* router have it call you back. The callback entry and the call numbers entry in the name list are used to select these three possible settings.

Name list - New Entry

Name:

Phonenumber:

Short hold time: seconds

Short hold time (bundle): seconds

Layer name:

Automatic callback:

☒ No callback

☐ Call back the remote site

☐ Call back the remote site (fast procedure)

☐ Call back the remote site after name verification

☐ Wait for callback from remote site

OK Cancel

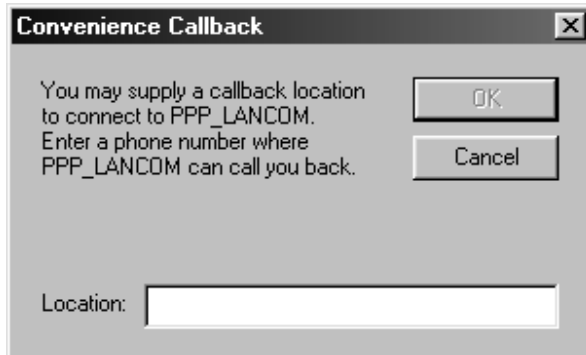
No callback

For this setting, the callback entry must be set to 'Off' during configuration with a terminal program or via telnet.

Choose select callback number

The remote station is called back after the name has been verified. The callback entry must have the value 'Name' for this setting and **no** call number may be specified in the name list.

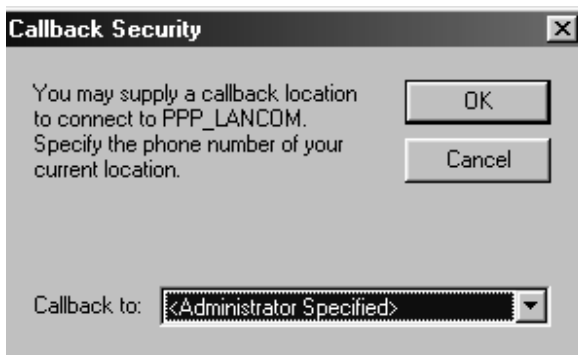
Following the authentication process, the dialog box below will appear in Windows 95 in which the user can specify his call number:



Callback number specified by the *LANCOM Office* router

The remote station is called back after the name has been verified. The callback entry of the appropriate remote station must have the value 'Name' for this setting and **one** call number must be specified in the name list.

Following the authentication process, the message below will appear in Windows 95 which the user can only confirm:



Callback to a Windows 95, Windows 98 or Windows NT workstation is initiated approximately 15 seconds after the connection is dropped. This delay is specified by Windows and cannot be shortened.

Fast ELSA callback

This fast, ELSA-specific process is ideal if two *LANCOM Office* router are to communicate with one another via callback.

- The caller who would like to be called back sets 'Wait for callback from remote site' in the name list ('Looser' when configuring via a terminal program or Telnet).
- The return caller selects 'Call back the remote site (fast procedure)' in the name list and sets the number ('ELSA').

Callback as specified in RFC 1570 (PPP LCP extensions)

There are five methods of demanding a callback specified in RFC 1570. All versions are accepted by the *LANCOM Office* router. All versions will be processed in the same way, however:

The *LANCOM Office* router drops the connection to the remote station after authentication and then calls it back three seconds later.

Channel bundling with MLPPP

If you are establishing an ISDN connection to a party supporting PPP you can really speed up your data: You can compress the data and/or use two B channels for the transfer (channel bundling).

Connections using channel bundling differ from “normal” connections inasmuch as they use not only one, but two B channels in parallel for transmitting the data.

MLPPP (Multilink PPP) is used for channel bundling. Of course, this procedure is only available if PPP is being used as the B-channel protocol. MLPPP is ideal, for example, for accessing the Internet via a provider which also supports MLPPP on its dial-up nodes.

■ Static channel bundling

If a connection is established with static channel bundling, the *LANCOM Office* router tries to establish the second B channel immediately after setting up the first B channel. If this does not work because, for example, this channel is already taken by another device or a different connection within the *LANCOM Office* router, the connection attempt is automatically and regularly repeated until the second channel is available for it.

■ Dynamic channel bundling

In the case of a connection with dynamic channel bundling, the *LANCOM Office* router first only establishes one B channel and begins transmitting data. If, during this connection, it determines that the throughput rate lies above a certain threshold value, it tries to add the second channel.

If the second channel is established and the data throughput rate drops below the threshold value, the *LANCOM Office* router waits for the set B2 timeout period and then automatically closes the channel again. Any partly used call charge units are used up fully if call charge information is transmitted during the connection. Therefore, the *LANCOM Office* router only uses the second B channel if and as long as it really needs it.

How to configure channel bundling

Three settings are required to configure a channel-bundled connection:

- ① Create an entry in the name list for the connection to be established with channel bundling. Select a layer which has set the bundling in the layer-2 options.
 - **compr.** When using the LZS data compression procedure (Stac), the data volume is reduced provided it was not already compressed before. This process is also supported by routers from other manufacturers and by ISDN adapters under Windows operating systems.

- **bundle** uses two B channels per connection. The channel bundling method is determined by the configuration of the layer 2 options in the layer list, the timeouts in the names list and the setting for the Y connection in the interface table.
 - **bnd+compr** uses both compression and channel bundling and therefore provides maximum possible transmission performance.
- ② Enter the holding times for this connection in the name list as well. Please observe the following rules:
- Depending on the application, the B1 holding time should be long enough to ensure that the connection is not prematurely terminated by the brief absence of data packets. Experience has shown that values between 60 and 180 seconds are a good basis which can be adapted as required during operation.
 - The B2 holding time determines whether static or dynamic channel bundling will be used (see above). A B2 holding time of '0' or '9999' ensures that the bundling will be static; values in between that are lower than the B1 holding time permit dynamic channel bundling.
- ③ Use the entry for the Y connection in the interface list to determine what should happen if a second connection to a different remote station is requested during an existing connection using channel bundling.
- Y connection **On**: The router interrupts the bundled connection to establish a connection to the other remote station. When the second channel is free again, the originally bundled connection automatically takes the channel back (always in the case of static bundling, only as required when using dynamic bundling).
 - Y connection **Off**: The router maintains the existing bundled connection; the establishment of the new connection must wait.



Please note that if channel bundling is used, the cost of two connections is charged. Furthermore, no simultaneous telephone calls via the a/b ports on the LANCOM 2000 Office or other connections via the LANCAP1 can be made! So you should only use channel bundling if the double transmission capacity can really be used in full.



Telephone calls and CAPI connections can interrupt routing connections (see 'service priority' as described in the corresponding chapters)!

Communications software

Your *LANCOM Office* router is supplied not only with software for the configuration and monitoring of your device, but also with various other applications for opening up the whole wide world of ISDN data communications.

ELSA-RVS-COM advances your *LANCOM Office* router to a full ISDN adapter with EuroFile Transfer, fax and answering machine. LapLink provides access to remote computers via ISDN or LAN, and *ELSA-ZOC* connects you with BBSs and other terminal programs.

This section gives you a brief introduction to these applications and information on their installation. If you have further questions, just use the help function. Practical examples of uses for this software can be found in the 'Workshop' section.

<i>ELSA-RVS-COM</i>	2
LapLink	5
<i>ELSA-ZOC</i>	7



ELSA-RVS-COM

What does **ELSA-RVS-COM** offer?

ELSA-RVS-COM provides you with a powerful and universal communications program that renders the implementation of the most important data communications applications both comfortable and convenient.

Your ELSA LANCOM Office router is supplied with one license for ELSA-RVS-COM. If this should not be sufficient for operation in your LAN, please refer to the separate information sheet included with your unit for information regarding multiple licenses.

In combination with *ELSA LANCOM Office* router, *ELSA-RVS-COM* offers you the following options:

Fax

- Fax Group 3 and Group 4 via software
- Fax operation at up to 14,400 bps
- Faxes sent directly from a Windows application via a Windows printer driver
- Delayed fax transmission
- Fax polling

Data transmission

- Convenient file transfer from PC to PC
- EuroFileTransfer with Explorer-compatible user interface

Telephone and answering machine

- Full ISDN telephony features (in conjunction with a full-duplex sound card)
- Digital answering machine (requires sound card)

Virtual COM ports

- Virtual COM ports permit the use of conventional data communications software such as *Telir for Windows*.

CommCenter

- Universal ready-to-receive state via CommCenter.

Setup for **ELSA-RVS-COM**

The setup program for *ELSA-RVS-COM* copies the required files to the selected drive and creates a program group on your Windows desktop.

System requirements

The following minimum system requirements must be fulfilled for the use of *ELSA-RVS-COM*:

Operating system	Microsoft Windows 95, Windows 98, Windows NT 4.0
Processor	Fully compatible to Pentium or higher
RAM	Min. 16 MB; min. 32 MB for fax mode
Hard disk	Min. 25 MB free memory space before installation Min. 12 MB during operation for virtual main memory (swap file)
Graphics card	Min. VGA (640*480 pixels, 16 colors/grayscales) 256 colors min.
Other	Sound card & microphone for answering machine and telephony

Install *ELSA-RVS-COM* as follows:

Double-click the 'ELSA-RVS-COM' entry in the installation program on your *ELSA LANCOM* CD. Follow the instructions for the installation program.

When entering the serial number, make sure you use the correct format, uppercase letters, etc. The installation wizard then starts automatically.

The installation wizard for *ELSA-RVS-COM*

The installation wizard will support you in configuring the services you require such as fax and answering machine functions and in entering the subscriber numbers of your ISDN line. You are then instantly ready to begin communication.

- With 'Express Configuration', you can set up a fully functional ISDN system while supplying very little required information. For example, you only need to enter a calling number, without having to assign the numbers to services such as fax, answering machine, etc.
- The 'User-Defined Configuration' is only required if you have specific configuration requirements (e.g. different numbers for fax, EFT, etc.). You can then enter various numbers and assign individual functions.

You can also call the installation wizard again at any time in the future to change or expand the configuration.



ELSA-RVS-COM has an 'In Box' for managing faxes and voice messages. No Microsoft Exchange or Outlook components are required if you do not expressly activate this option when setting up ELSA-RVS-COM using the 'User/defined Installation'.



If you should run into any difficulties when configuring ELSA-RVS-COM, you can obtain support and further instructions at any time from ELSA-RVS-COM's comprehensive help function.

Entering the subscriber numbers

During the 'User-Defined Installation', you will be prompted for your ISDN line's subscriber number(s). Different dialog boxes are provided for the Euro-ISDN port and national ISDN port.

■ Euro-ISDN port

Generally speaking, with the Euro-ISDN port you need only enter the call numbers for your port as MSN1 to MSN3 (MSN = multiple subscriber number).

For PBXs, you must enter the master number and DID numbers separately. If necessary, find out about your ISDN port's special features.

■ National ISDN port

In the case of a national ISDN port, MSN1 to MSN3 must be assigned to the EAZs (terminal selection codes). If you leave the EAZ fields empty, the last digit of the MSN will automatically be used as an EAZ.

LapLink

LapLink is a fully comprehensive program for telecontrol and data transmission between remote computers.

The 'Take Two' license

Before you can use the LapLink services, Laplink must be installed on all the computers that are to be linked. But don't panic: The LapLink license, that you received with your *ELSA LANCOM Office* router allows you to install the software on two computers.

What can LapLink do?

LapLink provides you with everything you need to connect two remote computers. Under the categories "data transmission" and "remote control", LapLink offers you the following services:

- Data transmission allows you to copy and move files from one computer to another.
- With data transmission, it is also possible to synchronize folders. The Xchange service is a convenient means of reorganizing individual files, folders, or even entire directory structures. In order to keep from interrupting your work for file synchronization, Xchange accomplishes its tasks automatically as desired, even under the cover of night....
- In the case of telecontrol, one computer user guarantees another free access to the first user's own files, programs, services, etc. The guest at the controlling computer can work on the host (the controlled computer) just as though it were his or her own.
- The dialog function allows users to exchange short messages on the two linked computers.
- You use the security settings to specify exactly who may have access to your computer. The security settings have been preset during the installation to ensure that your data cannot be accessed by unauthorized persons.

Connection paths for LapLink

Using LapLink, you have various possibilities for linking to other computers. The following connection options are available:

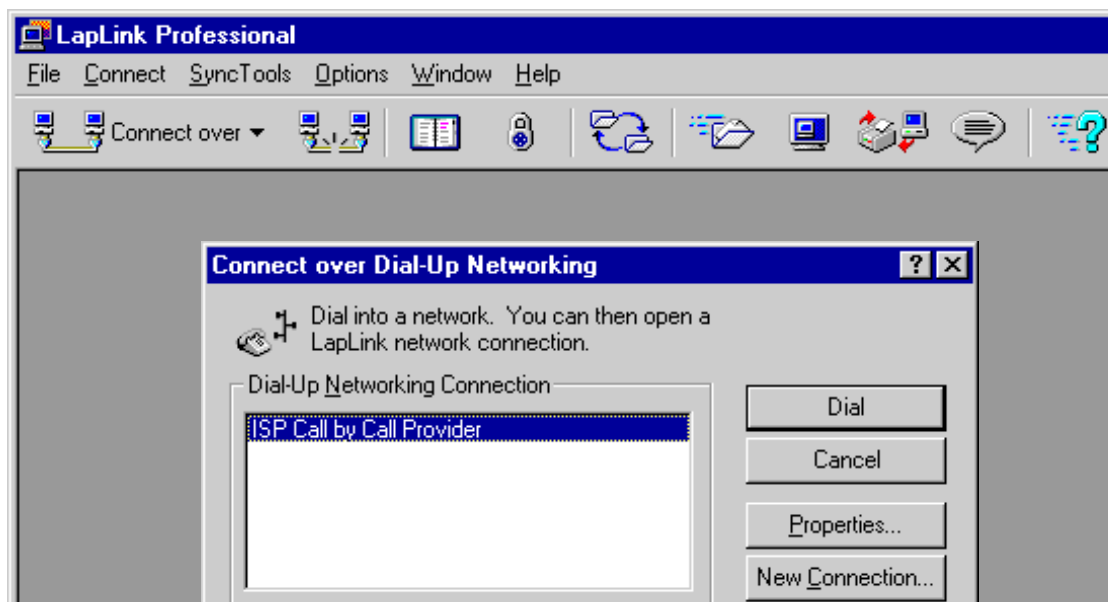
- Cable connection
- Wireless connection
- Modem connection
- Network connection
- Connection via the Windows Dial-Up Network

Configuring a port

Each connection accesses a 'port'. These ports might be called, for example, 'Win95' for the modem connections, 'TCP/IP' for the network connections or 'LPT1' for the cable connections. With the default installation, the port for network connections is immediately available for your use.

Initiating a connection

In order to set up this connection to another computer, simply click on the icon for the relevant connection type at the top of the LapLink window:



When connecting via the network you can, for example, specify an IP address and initiate the connection to this remote station.

Installing and uninstalling

Install LapLink as follows:

You can install LapLink by double-clicking the **LapLink** entry in the installation program on your *ELSA LANCOM* CD. Then follow the instructions for the installation program and within a few minutes, you will have access to LapLink's full range of functions.

If at any time you decide you no longer wish to use LapLink on your computer, simply click **Start ► Programs ► LapLink ► Uninstall**. LapLink then removes all associated files and system entries.

ELSA-ZOC

ELSA-ZOC is a powerful, advanced terminal program, that provides you with direct access under Windows to BBS systems and other computers using different terminal programs.

ELSA-ZOC is a powerful, advanced terminal program, that provides you with direct access under Windows to BBS systems and other computers using different terminal program via the CAPI port (*LANCAPI*).

ELSA-ZOC can also be used to configure the *ELSA LANCOM Office* router (also see 'Configuration modes').

What does *ELSA-ZOC* offer?

ELSA-ZOC is a special version of ZOC that is bundled with ELSA products (ISDN terminal adapters, ISDN cards, and ISDN router). Among other things, *ELSA-ZOC* has the following functions and properties:

- Support for most transport protocols (including V.120, X75, etc.)
- Connection, for example, via Capi 2.0 and Windows modems
- Convenient telephone directory with import options (e.g. for *Tel*ix telephone directories)
- Chat mode

ELSA-ZOC is fully operational; ZOC/Pro contains the following additional, add-on functions: REXX, DDE, Telnet and Rlogin, Named Pipes, VT52, VT220, Kermit and CompuServe Transfer, online image viewer (during downloading). A special upgrade from *ELSA-ZOC* to the ZOC/Pro version is available from the manufacturer. Please refer to the program's online help for details.

Installing *ELSA-ZOC*

ELSA-ZOC is extremely easy to install. Within a few minutes, you can initiate your first call, e.g. to a mailbox.

Install *ELSA-ZOC* as follows:

- ① Start Windows.
- ② Place the *ELSA LANCOM* CD in your CD-ROM drive. If the setup program does not start automatically, double-click 'autorun.exe' on the *ELSA LANCOM* CD.
- ③ Start the installation by clicking on **ELSA-ZOC** in the welcome screen selection. The installation screen for *ELSA-ZOC* is displayed.

- ④ If desired, select the paths under which you would like to configure the various expansions and click **Install**. The program can be started after the installation has completed successfully.

Starting *ELSA-ZOC*

In the Start Menu, select **Start ► Programs ► ELSA-ZOC for Windows ► ZOC** to start the program.

Foreword

We would like to show you how to get the most out of your *LANCOM Office* router using the examples in the following sections.

All the configurations assume the *LANCOM Office* router has the factory settings. You should therefore reset your *LANCOM Office* router to its original configuration using a system reset if necessary if you want to make full sense of an example.

This section is intended to familiarize you with the icons and symbols used.

Our development team is constantly seeking to incorporate new features into the *LANCOM Office* router and to make the use of *LANconfig* even simpler. This may result in minor differences between the appearance of screens as depicted in the Workshop and their actual appearance in the software; this will not, however, affect the functions provided in the menus.

The basic settings, such as the specification of your own call numbers, are repeated each time they appear in the examples so that each individual section forms a complete description. This means that descriptions will be included for settings which may not be required for the basic function.



Configuration using *ELSA LANconfig* and the wizards

Paragraphs marked with this symbol explain to you how to use *LANconfig* and its wizards to set up configurations in Windows 95 or Windows NT both quickly and easily.



Configuration without wizards

The step-by-step instructions provide precise instructions on the menus in which the settings are entered using either *LANconfig* or via a terminal or telnet connection.

	Setup/WAN-module	
	Interface	S0 DSS1 0 123456 123456 123456




You can enter the values shown directly during a configuration session, for example:

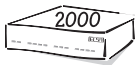
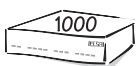
```
cd setup/WAN-Module/Interface
```

```
set S0 DSS1 123456 123456
```

You will find further instructions on configuration using telnet or terminal programs in the section headed 'Configuration Modes'.

You will find the following symbols elsewhere in the step-by-step instructions:

	Menu	Indicates a submenu
	Value	Indicates a value which can be modified
	Table	Indicates a table whose entries can be modified.



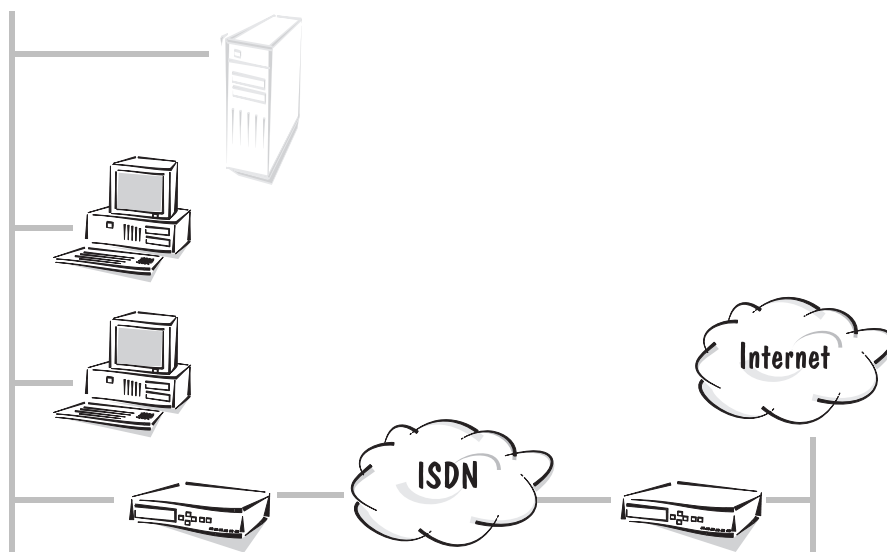
Which *LANCOM Office* router are you using?

You can work through the tasks in Workshop described using a number of models from the *LANCOM Office* router family. Any restrictions with regard to specific models are indicated by the symbol shown here.

Additional information



This symbol tells you if a setting is optional and is not an essential requirement for the simple functioning of the example configuration. This category includes, for example, filter settings which prevent specific data packets being transferred or security measures which restrict access to the *LANCOM Office* router.



Internet applications

This first section on the practical uses of the *LANCOM Office* router will introduce you to applications involving the Internet.

The first example shows a company seeking to use a *LANCOM Office* router on its network to connect up to the Internet. This will give all workstation computers on the LAN access to the services and possibilities offered by the Internet through a single account with a service provider. At the same time the *LANCOM Office* router used in this way will also act as a firewall to protect the local area network against access from outside and to make the workstation computers inaccessible from the Internet.

The second example depicts a company who not only wishes to make use of the services offered on the Internet as a passive subscriber, but also wishes to be an active provider of its own information. This is done by installing a web server on the company's local area network connected to the provider by a leased-line connection. While this server must obviously be accessible from the Internet, all other computers on the network must remain protected behind the firewall.

Internet access for all PCs on the LAN	2
Intranet with its own Web server on the Internet	7

Internet access for all PCs on the LAN

The motivation

Many companies would like to have an Internet connection for all computers on their local area network. Up to now there have been two reasons for arguing against this in several instances:

- Having separate accounts with an Internet service provider (ISP) for each individual computer or even buying IP addresses registered and valid on the Internet is, in most cases, much too expensive. In addition there is the cost of setting up and maintaining Internet access for each computer.
- A further worry is not knowing whether you are flinging wide the gates for access onto the company's network from outside when you connect each individual computer to the WWW.

The *LANCOM Office* router solves both problems in a single function: IP masquerading. In short, this is what happens:

The *LANCOM Office* router is the only device on the LAN to have a valid Internet IP address. This can be allocated dynamically on dial-up by the Internet service provider using PPP for instance (as with CompuServe etc). The network computers use addresses from a protected range (addresses in the tens, for example). The entire local area network is now "hidden" by IP masquerading behind the registered IP address of the *LANCOM Office* router.

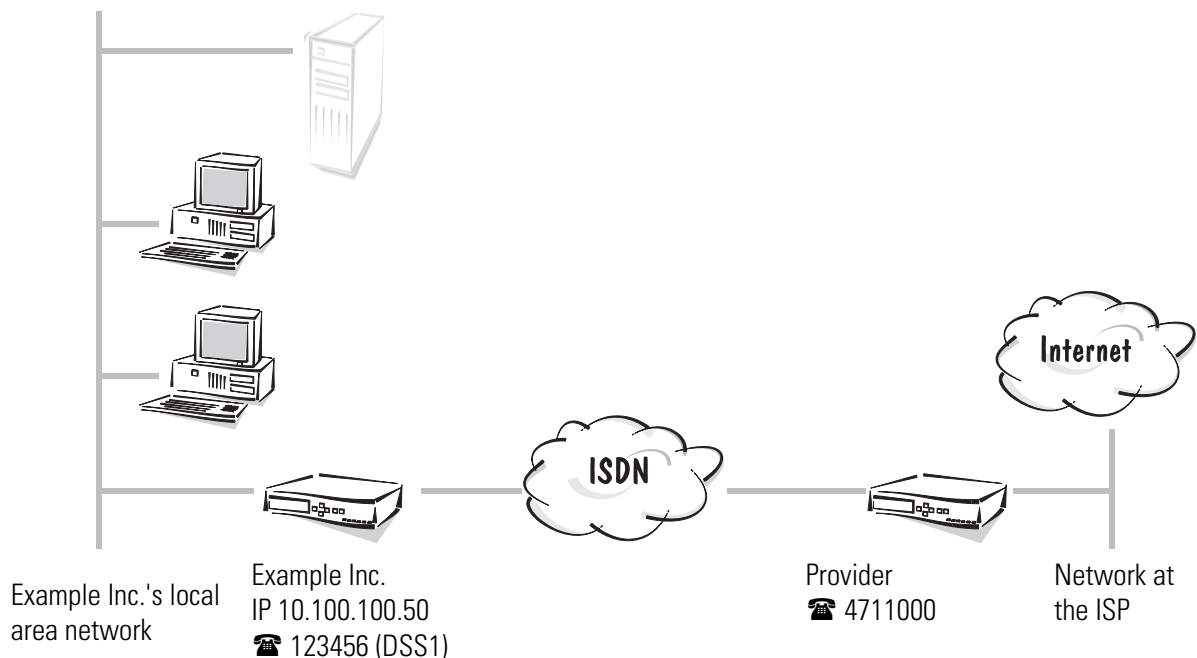
This process has even more benefits:

- IP masquerading makes Internet access simple.
Only one device needs to be configured, namely the *LANCOM Office* router. And the *ELSA LANconfig* setup wizards will even help you do this.
- IP masquerading makes Internet access cost-effective.
All the computers on the local area network can use the IP address of the *LANCOM Office* router to the outside and so have access to the Internet. This means that many users will only need a single account with the service provider. Furthermore, the *LANCOM Office* router manages the ISDN line automatically and only establishes a link to the service provider when there is actually a need to transfer data.
- IP masquerading makes Internet access secure.
The computers in the local area network become invisible from outside. Only the IP address of the *LANCOM Office* router will be known on the Internet. It is therefore not possible to access the local area network from outside; IP masquerading acts as an effective firewall, separating Internet from Intranet. Besides, the *LANCOM Office* router is the only interface with the Internet, making it simpler to monitor than numerous individual workstation machines.

An example of the task

On the one side we have a local area network in a company which has several workstation computers and a *LANCOM Office* router on a Euro-ISDN connection. There may be a server in this network, but this is not necessary.

On the other side we have the Internet service provider with a network using an ISDN router as a dial-up node for the users. This dial-in node demands to be addressed using PPP and also requires 'CHAP' security. The access data take the form of 'WEB_USER' as the user name and 'Surfing' as the password.



The table below shows how all the important data are assigned as used in the example. We recommend that you create a table such as this for each *LANCOM Office* router application. It will assist you in your work of configuring, troubleshooting and when requesting support information.

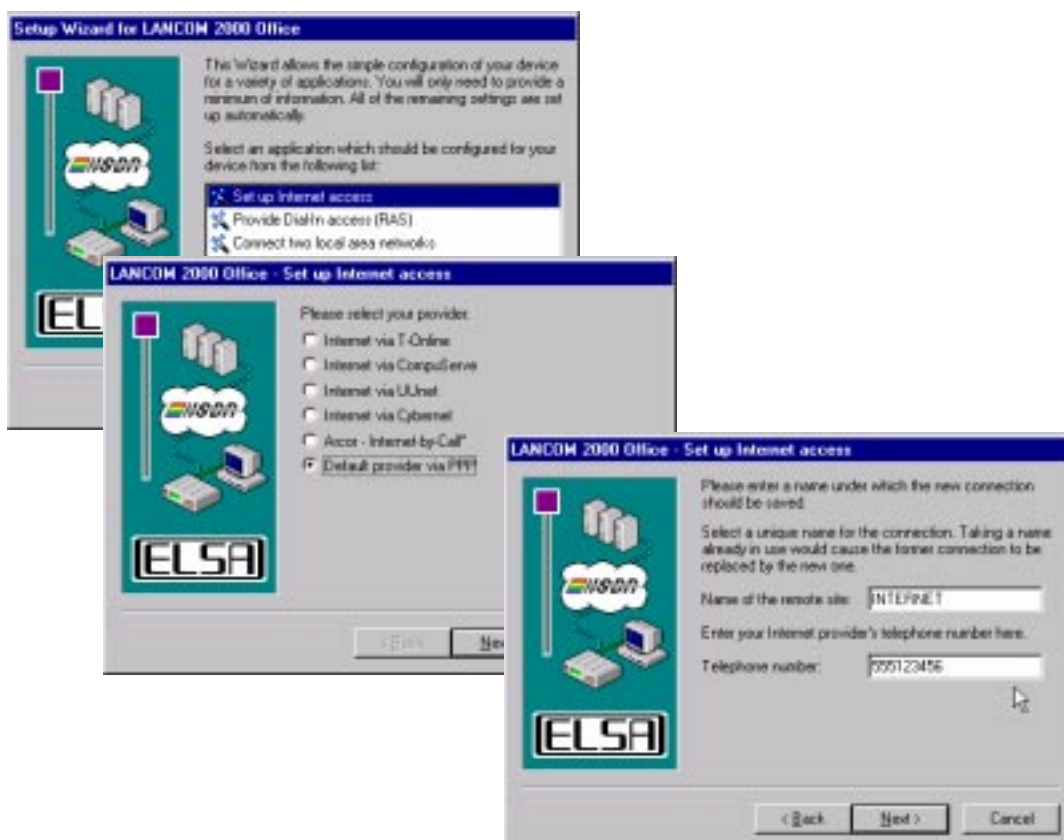
	Example Inc.'s local area network	Service provider's local area network
IP address of the LAN	10.100.100.0	
IP address for the <i>LANCOM Office</i> router	10.100.100.50	
IP network mask	255.255.255.0	
Device name	Example Inc.	Service provider
Call number	123456	4711000



Really easy access to the Internet using *LANconfig* and its wizards

Various wizards have been put together in the *LANconfig* which make all the settings in the *LANCOM Office* router software required to configure the *LANCOM Office* router for

access to the Internet for you. Once you have started up the wizard (automatically or by clicking **Tools ► Setup Wizard**), select the setup wizard you require. For our example we have not opted for one of the major online services, but rather for another ISP which offers dial-up nodes using PPP. Select the 'Internet using PPP' entry. The wizard will now prompt you for a few pieces of data it requires and will then instruct you on what settings still need to be made on the workstation computers.



Step by Step: What settings do you enter for the LANCOM Office router?

- ① First specify in the Router-interface-list (configuration area 'Communication', 'General' tab) the call number for incoming and outgoing calls:

	Setup/WAN-module/Router-interface-list	
	Interface	S0 123456 ON or OFF



The setting for the 'Y connection' will depend on whether a connection is to be established simultaneously to another remote station using the second B channel.

- ② A new entry in the name list (configuration area 'Communication', register 'Remote sites') with identification of the remote stations and the call numbers with selection

of one layer available in all routers (here for example the preset DEFAULT layer) enables the *LANCOM Office* router in the central office to call the routers at the ISP:

	Setup/WAN-module	
	Name-list	Provider 4711000 * * PPPHDL OFF

- ③ The user name and password to be sent when the remote station is dialed up are stored in the PPP list. The PPP negotiation has 'no' security from this end because only the ISP requests your name and password, but you do not request these from the ISP.





	Setup/WAN-module	
	The PPP-list	Provider no Surfing * * WEB_USER

The password 'Surfing' will be replaced by several asterisks (*) when entered. The other asterisks (*) in this entry stand for the values which are to be used without alteration.



Please note that user name and password are case-sensitive.



- ④ Now all that is needed is to clarify the addresses. The *LANCOM Office* router requires a free IP address from the Intranet so that it can be found in its own TCP/IP network. It receives this as part of the entry for the Intranet address together with the associated network mask (configuration area 'TCP/IP', 'General' tab).

	Setup/TCP-IP-module	
	Intranet-address	10.100.100.50
	Intranetmask	255.255.255.0
	State	On

The entries for the IP address and the IP network mask are empty because in this example the LANCOM Office router obtains the IP address dynamically from the ISP. If, on the other hand, there are IP addresses available which are registered and are valid on the Internet, you would enter one of these here together with the associated network mask (see also 'Intranet with its own Web server on the Internet').

- ⑤ The settings thus far have practically integrated the *LANCOM Office* router into the Internet, but the computers on the LAN are not yet able to surf. To achieve this you must create an entry in the routing table (configuration area 'TCP/IP', 'Routing' tab)

so that any packet destined for addresses which cannot be reached locally is routed into the Internet (DEFAULT route).

	Setup/IP-router-module	
	IP-routing-table	255.255.255.255 0.0.0.0 Provider 2 ON

The route to the IP address '255.255.255.255' with the network mask '0.0.0.0' intercepts all packets which cannot be assigned locally. 'Provider' identifies the remote station to which the relevant data is to be sent. The remote station can be accessed directly from our *LANCOM Office* router so the distance is set at '2'. Setting the option for IP masquerading to 'ON' hides all the computers in the LAN behind the *LANCOM Office* router's address so that they will not appear on the Internet.

- ⑥ Now all that is needed is to switch the IP router on and the *LANCOM Office* router is ready for the WWW.

	Setup/IP-router-module	
	State	On

- ⑦ What's left to do? Obviously the computers in the LAN will also need to know that the *LANCOM Office* router is the gateway to the Internet. This will require the *LANCOM Office* router's Intranet address being specified as the default gateway and DNS server for the workstation computers.

The result

When an employee starts up a browser on a workstation computer and enters a Web address (www.elsa.de, for instance), then the DNS server specified in the operating system (in this case the *LANCOM Office* router) will try to determine the associated IP address. The *LANCOM Office* router, being the Internet gateway, passes this request on to the ISP DNS server, which finally determines the IP address for this name (e.g. 168.192.156.100) and returns to the workstation computer via the *LANCOM Office* router. The *LANCOM Office* router will then send all the packets for this IP address by the default route to the Internet since this address was not found in the local area network.

Intranet with its own Web server on the Internet

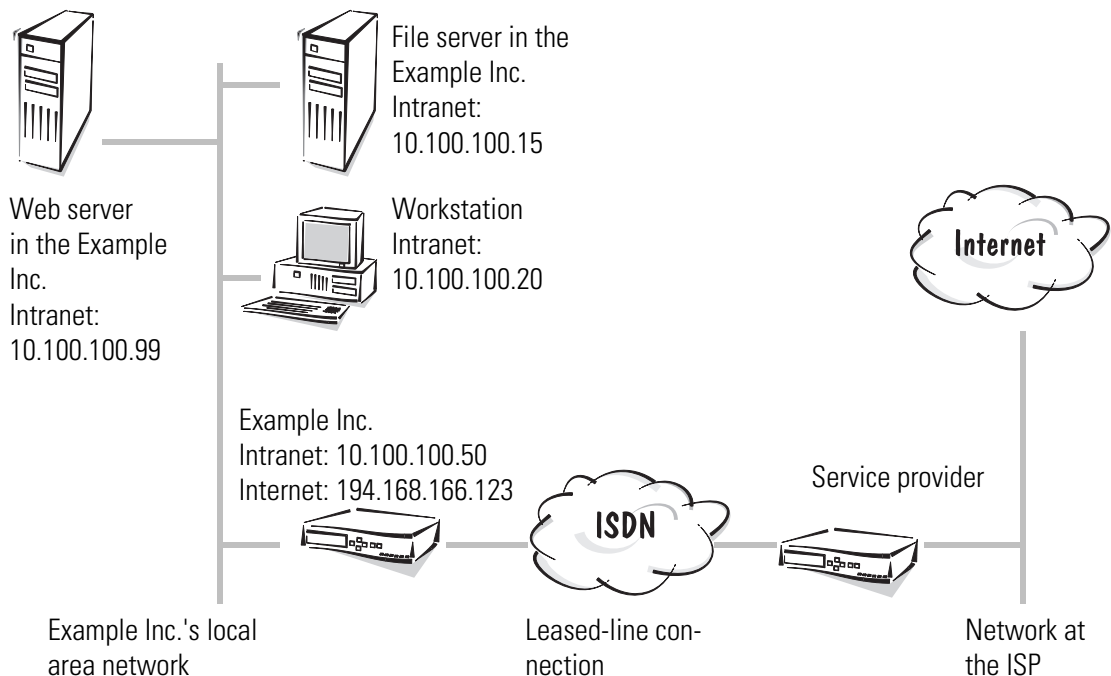
The motivation

In the example 'Internet access for all PCs on the LAN' you have seen how to connect a complete TCP/IP network to the Internet using a *LANCOM Office* router (with IP masquerading).

In the following example the LAN in the Example Inc. adds its own Web server which is to be accessible from the Internet. For this you will require a permanent IP address as well as the account with the ISP. This registered IP address is assigned to the *LANCOM Office* router. The *LANCOM Office* router then translates the registered address to the Web server's Internet address. This makes the Web server visible on the Internet under its registered address (inverse IP masquerading). All computers in the local area network will remain hidden as before.

An example of the task

On the one side we have a local area network in the Example Inc. which has several workstation computers and a *LANCOM Office* router on a Euro-ISDN connection. There is also a Web server on this network in addition to the local servers.



On the other side we have the Internet service provider with its network. In principle there are two options commonly used to connect to this network:

- You may wish to have a dedicated connection (leased-line connection) to the service provider if the Web server is very busy (D64S with a B channel with no D channel, for example). In this case you should install a second *LANCOM Office* router at your ISP and configure both routers for the leased-line connection used.

- A single *LANCOM Office* router in your local area network will be sufficient if a leased-line connection is not required. Set your *LANCOM Office* router to callback for the service provider so that the ISP is not charged for the connection to your Web server.

With the second option, connections are established to the ISP each time your Web site is accessed and your phone bill will be charged. We prefer the first of these two options since it is not possible to control these charges (except by using charge budgeting, which makes no sense in this instance; see 'Setup/Charges-module').



This example only applies if you are using ELSA MicroLink LANCOM MPR devices since neither the LANCOM 1000 Office nor the LANCOM 2000 Office ISDN router supports leased-line connections.

The table below shows how all the important data are assigned as used in the example. We recommend that you create a table such as this for each *LANCOM Office* router application. It will assist you in your work of configuring, troubleshooting and when requesting support information.

	Example Inc.'s local area network	Service provider's local area network
IP address for the <i>LANCOM Office</i> router	194.168.166.123	
IP network mask for the <i>LANCOM Office</i> router	255.255.255.255	
Intranet address of the LAN	10.100.100.0	
Intranet address for the <i>LANCOM Office</i> router	10.100.100.50	
Intranet address for the Web server	10.100.100.99	
Intranet network mask	255.255.255.0	
Device name	Example Inc.	Service provider

Leased-line connection: What settings do you enter for the *LANCOM Office* router?

The settings for the two *LANCOM Office* routers are very similar. We will use the settings for the *LANCOM Office* router at the Example Inc. as our basis and indicate any differences for the *LANCOM Office* router at the service provider.



- ① First set the *LANCOM Office* router in the interface table for a leased-line connection using D64S (configuration area 'Management', 'Interfaces' tab):

	Setup/WAN-module	
	Interface	SO GRPO 1

The *LANCOM Office* router at the ISP will be set as the 'slave', the B channel used in the *LANCOM Office* router must be the same, i.e. this must also be a '1'.

These settings alone allow the two *LANCOM Office* routers to establish a connection independently once they have been connected to a leased-line connection and switched on. They will automatically use the 'DEFAULT' layer for this.

- ② The layer in the layer list (configuration area 'Communication', register 'General') for both *LANCOM Office* routers must be the same and can be set up as you wish using, for instance, the X.75ELSA protocol:

	Setup/WAN-module	
	Layer-list	DEFAULT ETHER ELSA X.75ELSA compr. HDLC64K

- ③ A new entry in the namelist (configuration area 'Communication', 'Remote Sites' tab) identifying the remote station allows the *LANCOM Office* router to identify the router in the remote network. Specify the identifier as the call number for a leased-line connection on the first B channel:

	Setup/WAN-module	
	Name-list	Provider F:1 0 0 DEFAULT Off

The timeouts will be set to '0' since the establishment of unnecessary connections could cause delays.







The *LANCOM Office* router at the service provider specifies 'Example Inc.' as the name, also with the leased-line connection on the first B channel.

- ④ Name the *LANCOM Office* router appropriately so that the *LANCOM Office* routers can also send and recognize the names from the namelist (configuration area 'Communication', register 'General'):

	Setup	
	Name	Example Inc.



- ⑤ Now all that is needed is to clarify the IP addresses. The *LANCOM Office* router in the Example Inc. requires a free IP address from the Intranet so that it can be found in its own TCP/IP network. The *LANCOM Office* router receives this as part of the entry for the Intranet address together with the associated network mask (configuration area 'TCP/IP', 'General' tab). It will also receive the registered IP address, in-

cluding the network mask as negotiated. Enable the TCP/IP module so that these specifications can also take effect.

	Setup/TCP-IP-module	
	IP-address	194.168.166.123
	IP-netmask	255.255.255.255
	Intranet-address	10.100.100.50
	Intranetmask	255.255.255.0
	State	On



By analogy, the other *LANCOM Office* router is assigned a permanent IP address and (if using IP masquerading) an Intranet address from the address range at the ISP.

- ⑥ Setting the IP address practically integrates the Example Inc.'s *LANCOM Office* router into the Internet, but the computers on the LAN are not yet able to surf. You must create an entry in the routing table (configuration area 'TCP/IP', 'Routing' tab) so that any packet destined for addresses which cannot be reached locally is routed into the Internet (DEFAULT route) to allow your company's employees to access the Internet.

	Setup/IP-router-module	
	IP-routing-table	255.255.255.255 0.0.0.0 provider 2 On

The route to the IP address '255.255.255.255' with the network mask '0.0.0.0' intercepts all packets which cannot be assigned locally. 'Provider' identifies the remote station to which the relevant data is to be sent. The remote station can be accessed directly by the *LANCOM Office* router in the Example Inc. so the distance is set at '2'. Setting the option for IP masquerading to 'ON' hides all the computers in the LAN behind the *LANCOM Office* router's address so that they will not appear on the Internet.



- ⑦ The *LANCOM Office* router at the ISP must have the same entry in the routing table. This route contains the registered IP address of the *LANCOM Office* router in the Example Inc. and the name of the remote station. 'IP masquerading' remains disabled for this route since the direction must be routed and not be masked.

	Setup/IP-router-module	
	IP-routing-table	194.168.166.123 255.255.255.255 Example Inc. 2 Off

The 'Proxy-ARP' function must be enabled since this IP address falls within the service provider's own address range:

	Setup/IP- router-module	
	Proxy-ARP	On

- ⑧ The web server is made visible on the Internet by an entry in the service table for the Example Inc.'s *LANCOM Office* router (configuration area 'TCP/IP', 'Masquerading' tab):

	Setup/IP-router-module/masquerading	
	Service-table	80 10.100.100.99

Specifying '80' as the value indicates that the service visible to the outside is HTTP (WWW) and the address '10.100.100.99' selects the computer with this special Intranet address as the web server.



You will find a list containing further services in the section headed 'TCP/IP Ports' auf Seite 3.3.13.

- ⑨ Now activate the IP router only (configuration area 'TCP/IP', 'Routing' tab), and the *LANCOM Office* router is ready for the WWW.

	Setup/IP-router-module	
	State	On

- ⑩ What's left to do? Obviously the computers in the LAN will also need to know that the *LANCOM Office* router is the gateway to the Internet. This will require the *LANCOM Office* router's Intranet address being specified as the default gateway on the workstation computers. The IP address of the relevant server at the ISP is also identified as the DNS server.

The Internet service provider must then see to it that your Web server, together with its registered IP address and domain name, is entered in his DNS server, for example 'www.example.co.uk'.

The Result

The aim of these settings is to allow data exchange with the Internet in both directions: requests for information from the local area network to the Internet and, vice versa, requests for information from the Internet to the web server on the local area network. This is what you have now achieved:

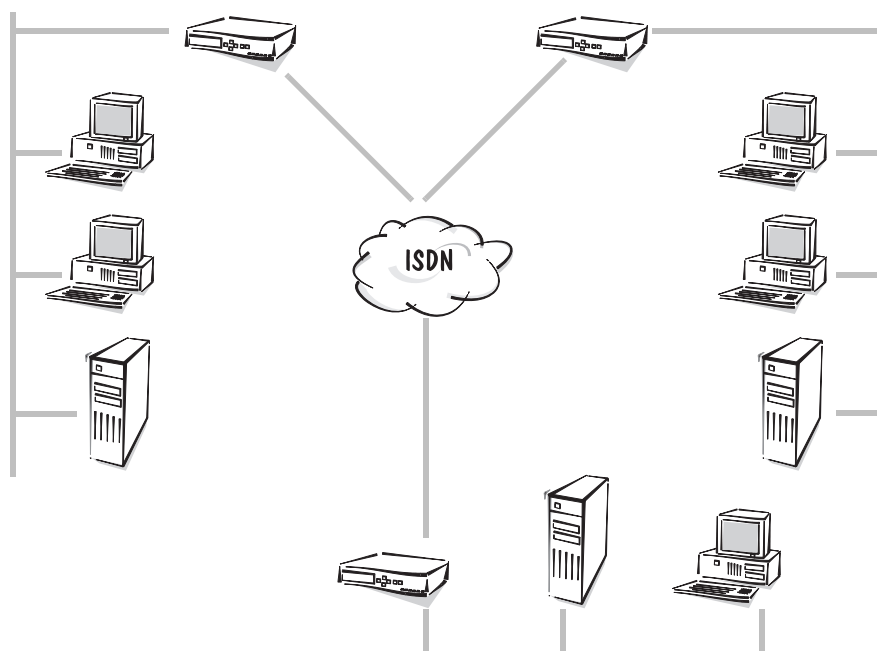
- Internet access for your company's employees:

When an employee starts up a browser on a workstation computer and enters a web address (www.elsa.de, for instance), the DNS server specified in the operating system will try to determine the associated IP address. The *LANCOM Office* router, being the Internet gateway, passes this request on to the ISP DNS server, which finally determines the IP address for this name (eg 168.192.156.100) and returns to the workstation computer via the *LANCOM Office* router. The *LANCOM Office* router will then send all the packets for this IP address by the default route to the Internet since this address was not found in the local area network.

- Company web site on the Internet

If an Internet subscriber somewhere in the world starts up a browser and specifies your web address (www.example.co.uk, for instance), the IP address of the *LANCOM Office* router in your company will be returned to the subscriber's computer by the DNS server (194.168.166.123). The web user's computer will then be able to use this IP address to communicate directly with the *LANCOM Office* router. The *LANCOM Office* router then automatically maps the requests for information on port 80 (WWW) to the Intranet address of the web server and so gives access to your company's web site.

Obviously there are other services offered on the Internet, such as FTP and Gophers, which will need to be added to the service table. You can use the service table to determine whether one or several servers will be used for the various services.



LAN to LAN couplings

When the business of Example Inc. is going really well, it is time to add a subsidiary or a branch in the global market. At the same time the branch office has its own local network and wants to be kept up-to-date.

LAN to LAN coupling links the individual LANs to form one large network, even if this means crossing continents. Intelligent line management uses switched line connections in conjunction with sophisticated filter mechanisms to keep connection costs down. Naturally, operation over dedicated lines in combination with switched lines is also possible.

And if one router in headquarters is no longer sufficient to meet data requests from several branches, additional *LANCOM Office* routers are set up and connected to form one large router (scaled).

Networks connected with the IP router.....	2
Two IP routers for four branches (static scaling).....	8
Two IP routers for six branches (dynamic scaling)	16
Networks connected with the IPX router	25
Several IPX routers in one Network (scaling).....	31
Two networks connected via the bridge	37

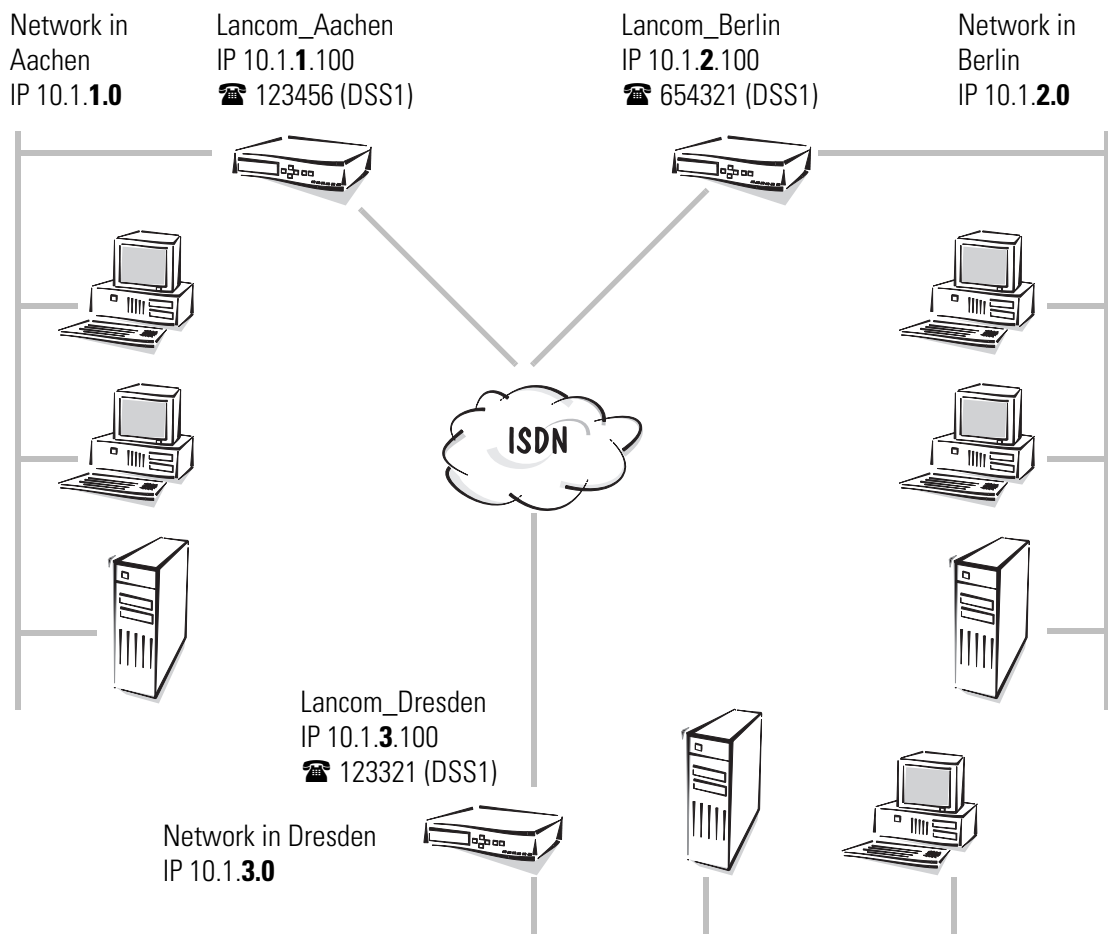
Networks connected with the IP router

The motivation

We can connect networks that use TCP/IP as network protocol using the IP router. In contrast to Internet access with IP masquerading ('Internet access for all PCs on the LAN' auf Seite 2.2.2), when networks are coupled, **all** IP addresses in the associated networks become visible over the IP router in the other coupled networks, not just those of the router.

An example of the task

In this example we shall couple three networks. The structure is then easy to extend to several networks.



The following table shows the assignment of device names, addresses and telephone numbers as used in the example:

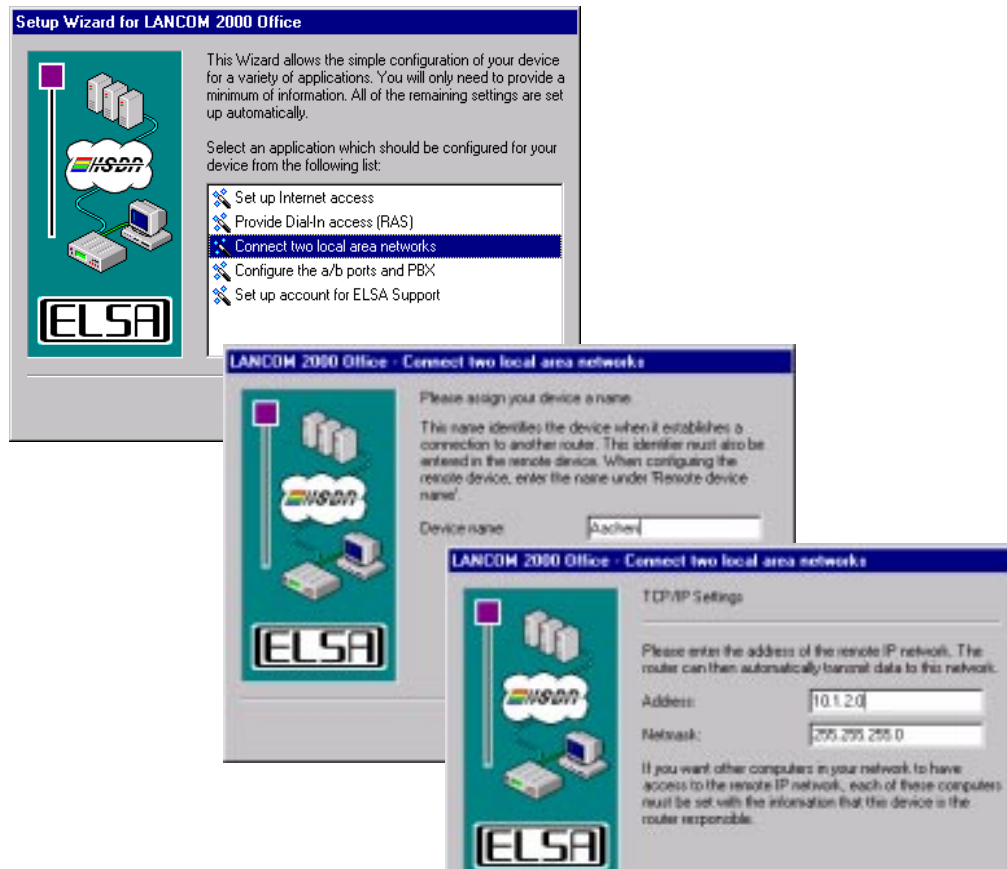
	Network in Aachen	Network in Berlin	Network in Dresden
IP address of the LAN	10.1.1.0	10.1.2.0	10.1.3.0
IP address for the <i>LANCOM Office</i> router	10.1.1.100	10.1.2.100	10.1.3.100
IP network mask	255.255.255.0	255.255.255.0	255.255.255.0
Device name	Aachen	Berlin	Dresden
Call number	123456	654321	123321



IP routing made simple with *LANconfig* and the wizards

For the *LANCOM Office* router configuration on LAN to LAN coupling, there is a wizard in *LANconfig* which makes all required settings in the *LANCOM Office* router software for you and takes the peculiarities of TCP/IP networks into account. Once you have started up the wizard (automatically or by clicking **Tools ► Setup Wizard**) select the entry 'Connect two local area networks'. The wizard will now prompt you for the required data (including the network protocol in use) and will then instruct you on what settings still need to be made on the workstation computers.



Because you wish to couple three networks in this example, run the wizard twice in succession for every *LANCOM Office* router. This will generate the entries for two remote stations.



Step by Step: What settings are made in the *LANCOM Office* routers?

The settings are in principle the same for all *LANCOM Office* routers. We are looking at the first *LANCOM Office* router here, the others are set correspondingly.

- ① First specify in the Router-interface-list (configuration area 'Communication', 'General' tab) the call number for incoming and outgoing calls:




	Setup/WAN-module/Router-interface-list	
	Interface	SO 123456 ON

When specifying several call numbers the first number is used for outgoing calls.



The 'Y connection' option must be activated in every case to enable simultaneous connections to two different remote stations.

- ② A new entry in the name list (configuration area 'Communication', 'Remote Sites' tab) with identification of the remote stations and the call numbers with selection of one layer available in all routers (here for example the preset 'DEFAULT' layer) enables the *LANCOM Office* router in the central office to call the routers in the other





networks. Every network should bear its own telephone costs, therefore the call-back entry remains set to OFF:

	Setup/WAN-module	
	Name-list	Berlin 654321 * * DEFAULT OFF
	Name-list	Dresden 123321 * * DEFAULT OFF




- ③ To ensure that the *LANCOM Office* routers also forward the names from the name list and they are detected, name the *LANCOM Office* router appropriately (configuration area 'Management', 'General' tab):

	Setup	
	Name	Lancom_Aachen

- ④ Now the addresses must still be clarified. To enable the *LANCOM Office* router in its own TCP/IP network to be found, it needs a free IP address from the Intranet. It receives this as part of the entry for the Intranet address together with the associated network mask (configuration area 'TCP/IP', 'General' tab). For these entries to become effective, activate the TCP-IP module.

	Setup/TCP-IP- module	
	Intranet-address	10.1.1.100
	Intranetmask	255.255.255.0
	Status	On

- ⑤ And what IP addresses should the *LANCOM Office* router route where? In the routing table (configuration area 'TCP/IP', 'Routing' tab) enter the IP addresses and network masks of the other networks with the associated remote station:

	Setup/IP-router-module	
	IP- routing-table	10.1.2.0 255.255.255.0 Berlin 2 OFF
	IP-routing-table	10.1.3.0 255.255.255.0 Dresden 2 OFF



The IP masquerading remains deactivated here so every device in the networks with its own IP address participates in the network traffic and is not hidden behind the address of the LANCOM Office router.

The remote stations may be directly reached from our *LANCOM Office* router, therefore the distance is set to '2'.

- ⑥ Now activate the IP router only, and the first *LANCOM Office* router is ready for connection to the other networks.

	Setup/IP-router-module	
	Status	On

- ⑦ What must still be done? Naturally, the computers in the LAN also need to know that the *LANCOM Office* router is the switching centre for the other networks. For this purpose the Intranet address of the *LANCOM Office* router is entered as default gateway for the workstations and servers. Under Windows 95 open the network neighborhood properties and double-click on the entry for the 'TCP/IP' protocol. On the 'Gateway' tab you can then add the desired address of the *LANCOM Office* router.

The result

Every computer in the associated networks can now be entered as the standard gateway *LANCOM Office* router to send an ARP query to IP addresses not locally known in the corresponding target network. The *LANCOM Office* router receives the ARP request and answers it if it is responsible for the target network with its own MAC address. This enables all following data packets for this remote station to be sent directly to the *LANCOM Office* router and routed by it. The workstations save the MAC address of the default gateway (*LANCOM Office* router) in the ARP cache and eventually no longer require any more ARP requests to reach the remote station. This procedure does not unnecessarily load the local network.

Test

To check the functioning of the connection to the other networks, you can send a “ping” to an IP address in the remote network. In the network in Aachen enter the following command for the network in Berlin in the command line of a workstation:

```
ping 10.1.2.99
```

You should receive an answer (Reply) to this request from the network in Berlin, if a server there has the Intranet address 10.1.2.99.

Two IP routers for four branches (static scaling)

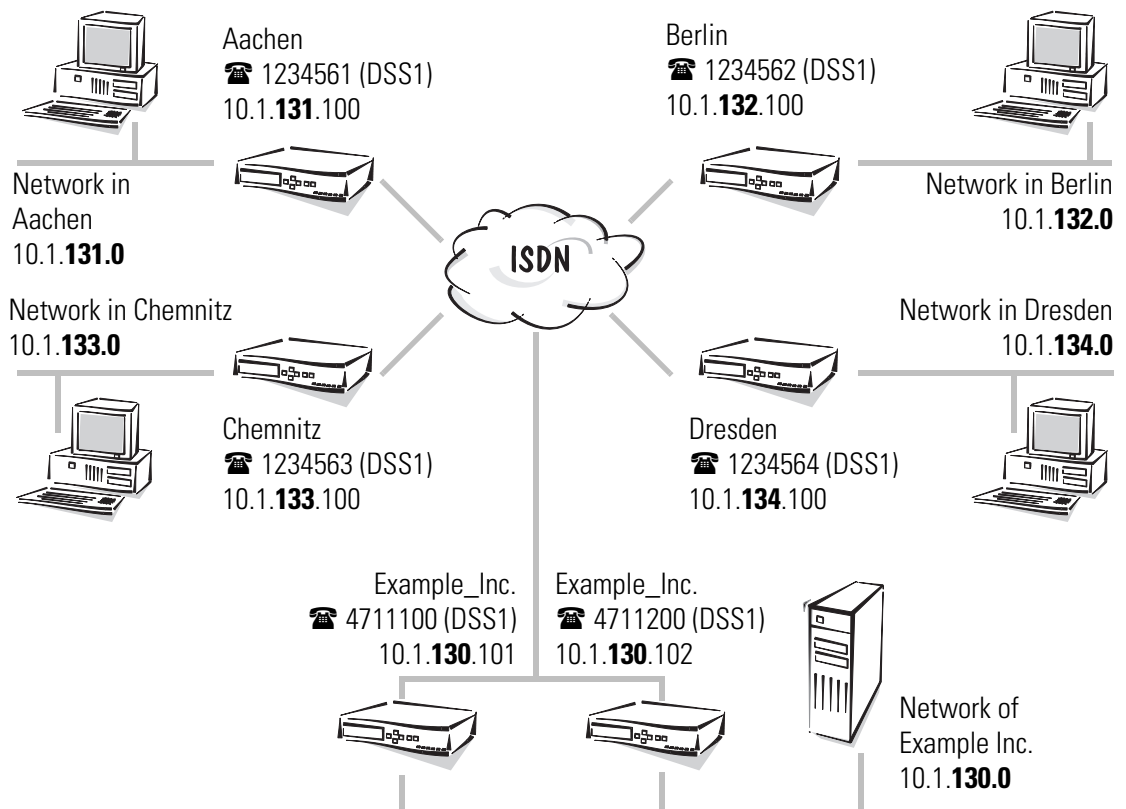
The motivation

As seen in the example 'Networks connected with the IP router', we can connect networks with the IP router, which use TCP/IP as network protocol. If the Example Inc. central office now establishes a few more branches, a *LANCOM Office* router in the central office network may no longer be sufficient. This is the time to use several IP routers in one local network.

The *LANCOM Office* routers in this case are in effect switched together to one large router (scaled). Every router is made responsible for a section of the remote stations with entries in the routing table.

An example of the task

In this example the central office has four branches. A connection between central office and branches should be possible at any time. For this purpose the network in the company central office is equipped with two *LANCOM Office* routers, each of which is connected to one Euro-ISDN terminal (each with two B channels). With the total of four B channels in the central office, the availability of the central office for all branches is guaranteed.



The following table shows the assignment of device names, addresses and telephone numbers as used in the example:

Network	Example Inc.	Aachen	Berlin	Chemnitz	Dresden
IP-address-LAN	10.1.130.0	10.1.1310.0	10.1.132.0	10.1.133.0	10.1.134.0
IP-address for the <i>LANCOM Office</i> router	a) 10.1.130.101 b) 10.1.130.102	10.1.131.100	10.1.132.100	10.1.133.100	10.1.134.100
IP-network-mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Device-name	Example_Inc.	Aachen	Berlin	Chemnitz	Dresden
Call-number	a) 4711100 b) 4711200	1234561	1234562	1234563	1234564



Step by Step: What settings are made in the *LANCOM Office* routers?

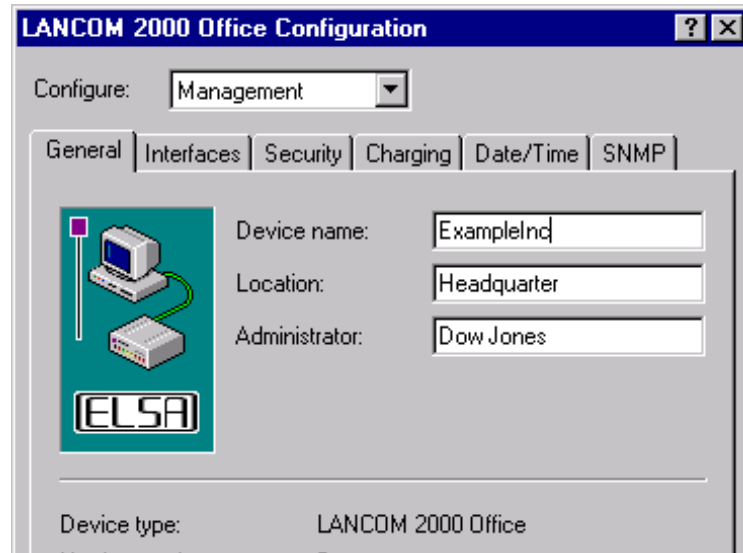
We can set the two routers in the central office almost identically for the *LANCOM Office* router configuration for the static scaling in the IP router operation. The *LANCOM Office* routers in the branches are set slightly differently, but their configurations generally correspond with one another.

Because there are no wizards for the scaled router operation, this example will be run through complete with *LANconfig*.

In the following configuration steps, beginning with the routers in the central office, we show exactly what is set the same and provide information on the deviations in the other *LANCOM Office* routers.

- ① For the names that are used in the name list to be also forwarded and detected by the *LANCOM Office* routers, name the devices appropriately (configuration area 'Management', 'General' tab). Both *LANCOM Office* routers in the network at the central office receive the same name. This ensures that they appear externally as

one large router. With a different entry in the field 'Location', both can be distinguished in the device list of *LANconfig*:

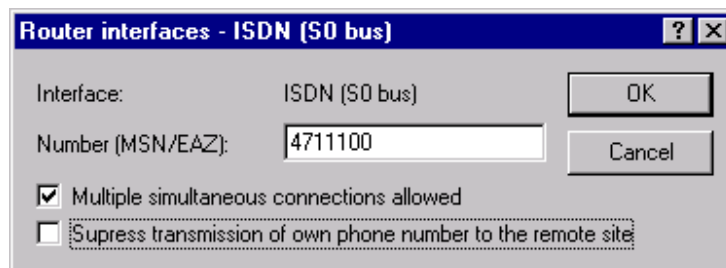


Enter the names of the devices directly in the 'Setup' menu with configurations with other aids:

	Setup	
	Name	Example_Inc.

The *LANCOM Office* routers in the branches receive the names 'Aachen', 'Berlin', 'Chemnitz' and 'Dresden'.

- ② Then enter the **specific** call number of the first *LANCOM Office* router in the central office (configuration area 'Communication', 'General' tab):



	Setup/WAN-module/Router-interface-list	
	Interface	S0 4711100 ON



The 'Y connection' option must be activated in every case to enable simultaneous connections to two different remote stations.

The other *LANCOM Office* routers correspondingly receive their own call numbers (4711200, 1234561, 1234562, 1234563 and 1234564).

- ③ New entries in the name list (configuration area 'Communication', 'Remote Sites' tab) with identification of the remote stations and the call numbers with selection of one layer available in all routers (here for example the preset DEFAULT layer) enables the *LANCOM Office* router to call the routers in the other networks. Every network should bear its own telephone costs, therefore the call-back entry remains set to OFF:

Name list - New Entry

Name: AACHEN OK

Phonenumber: 1234561 Cancel

Short hold time: 20 seconds

Short hold time (bundle): 20 seconds

Layer name: DEFAULT

Automatic callback:

- ☒ No callback
- ☐ Call back the remote site
- ☐ Call back the remote site (fast procedure)
- ☐ Call back the remote site after name verification
- ☐ Wait for callback from remote site

	Setup/WAN-module	
	Name-list	Aachen 1234561 * * DEFAULT, OFF
	Name-list	Berlin 1234562 * * DEFAULT OFF

The second *LANCOM Office* router in the central office acquires the corresponding entries for the Chemnitz and Dresden branches.

	Setup/WAN-module	
	Name-list	Chemnitz 1234563 * * DEFAULT OFF
	Name-list	Dresden 1234564 * * DEFAULT OFF

The *LANCOM Office* routers in the branches enter only the router 'Example_Inc' and the call number of one of the two scaled *LANCOM Office* routers (eg Aachen and Berlin the '471110', Chemnitz and Dresden the '4711200').

- ④ Now the addresses must still be clarified. So that the *LANCOM Office* routers in the internal TCP/IP networks are found, one free IP address at least from the Intranet is required (configuration area 'TCP/IP', 'General' tab). This is acquired with the entry

of the Intranet address with the associated network mask. For these entries to become effective, activate the TCP-IP module.

Example Configuration

Configure: TCP/IP

General | DHCP | DNS | Routing | Filtering | Masquerading

☒ TCP/IP module active

IP address: 0.0.0.0

Netmask: 255.255.255.0

Intranet IP address: 10.1.130.101

Intranet netmask: 255.255.255.0

	Setup/TCP-IP-module	
	Intranet-address	10.1.130.101
	Intranetmask	255.255.255.0
	Status	On

The other *LANCOM Office* routers each receive the corresponding address from the table at the beginning of the example.

- ⑤ To enable exchange of information over the available routes between the scaled *LANCOM Office* routers to function, the IP-RIP must be activated (configuration area 'TCP/IP', 'Routing' tab). If possible, select the option 'RIP-2'. Only with older versions of Novell NetWare (to 3.12) set 'RIP-1' or 'RIP1komp'.

	Setup/IP-router-module/RIP-config	
	RIP-type	RIP-2



Ensure that the RIP functions are also activated in the servers in the local network.

- ⑥ And what IP addresses should the *LANCOM Office* routers route where? Enter the IP addresses and network masks of the two first branches with their remote stations

(without IP masquerading!) into the routing table of the first router in the central office:

Routing table - New Entry

IP address:

10.1.131.0

OK

Netmask:

255.255.255.0

Cancel

Router:

AACHEN

Distance:

2





IP masquerading:

☒ IP Masquerading switched off





☐ masking with the IP address assigned by the remote station

☐ masking with the router's own IP address







The remote stations can be reached directly from every *LANCOM Office* router, therefore the distance is set to 2. Finally, activate the IP routers, and then the first *LANCOM Office* router is ready for connection to the other networks.

	Setup/IP-router-module	
	IP-routing-table	10.1.131.0 255.255.255.0 Aachen 2 OFF
	IP-routing-table	10.1.132.0 255.255.255.0 Berlin 2 OFF
	Status	On

The second *LANCOM Office* router in the central office receives the corresponding entries for the Chemnitz and Dresden branches:

	Setup/IP-router-module	
	IP-routing-table	10.1.133.0 255.255.255.0 Chemnitz 2 OFF
	IP-routing-table	10.1.134.0 255.255.255.0 Dresden 2 OFF
	Status	On

The *LANCOM Office* routers in the branches each acquire an entry for the central office. The remote station in this case is however always that in the central office. A WAN to WAN routing is established in this way in which the branches can exchange data with each other. The entry for the *LANCOM Office* router in Aachen looks like the example below:

	Setup/IP-router-module	
	IP-routing-table	10.1.130.0 255.255.255.0 Example_Inc. 2 OFF
	IP-routing-table	10.1.132.0 255.255.255.0 Example_Inc. 2 OFF
	IP-routing-table	10.1.133.0 255.255.255.0 Example_Inc. 2 OFF
	IP-routing-table	10.1.134.0 255.255.255.0 Example_Inc. 2 OFF
	Status	On

- ⑦ What must still be done? Naturally, the computers in the LAN also need to know that the *LANCOM Office* router is the switching centre for the other networks. For this purpose the Intranet address of the *LANCOM Office* router is entered as default gateway for the workstations and servers.

The result

Access from a computer to a branch to the network in the central office is possible at any time, because a router in the central office with two B channels is responsible for exactly two remote stations. When transferring data to the network in another branch the data packets are forwarded over the same router, if this is responsible for the corresponding branch. Otherwise the packets are forwarded over the local network to the other *LANCOM Office* router, which can establish the connection to the target network.

When establishing a connection from the central office, the dynamic routing table completed with routing information is used over IP RIP. By exchanging the RIP information the first *LANCOM Office* router in the central network (IP 10.1.130.101) notes that in the second *LANCOM Office* router (IP 10.1.130.102) routes to the branches in Chemnitz and Dresden are available. The first *LANCOM Office* router enters these routes in its own dynamic routing tables, but cannot reach the corresponding remote stations because the entries in the name list are missing.

The great advantage of this configuration is in the low maintenance requirement for the routing tables. If, for example, the central office acquires two new branches that are added to the network over another router, the entries for the new branches needs only to be included in the *LANCOM Office* router. The routing tables in the routers previously in place remain the same.



Additional filter possibilities

If one of the linked networks is an NT network, filtering for the NetBIOS data packets on the LAN of the NT network may prove difficult. However, if the central office still wants to protect itself from these data packets, an entry in the WAN filter table of the *LANCOM Office* router in Example Inc. will help:

	Setup/IP-router-module	
	WAN-filter-table	137 139 tcp

Two IP routers for six branches (dynamic scaling)

The motivation

In example 'Two IP routers for four branches (static scaling)' we have assumed that for every branch in the central office LAN there is one B channel in one *LANCOM Office* router and therefore communication between central office and branches is possible at any time.

However, if this continuous availability is not really required, the two routers in the central office may be sufficient for more than four branch networks. Because it is not possible to assign the *LANCOM Office* routers unambiguously to the branches, the scaled router in the central office must independently find a new B channel to establish a connection. The routers exchange the information required for this via IP-RIP.

An example of the task

In this example the central office has six branches, which are linked via two *LANCOM Office* routers to the central office. The branches then share the total of four B channels in the central office. The following table shows the assignment of device names, addresses and telephone numbers as used in the example:

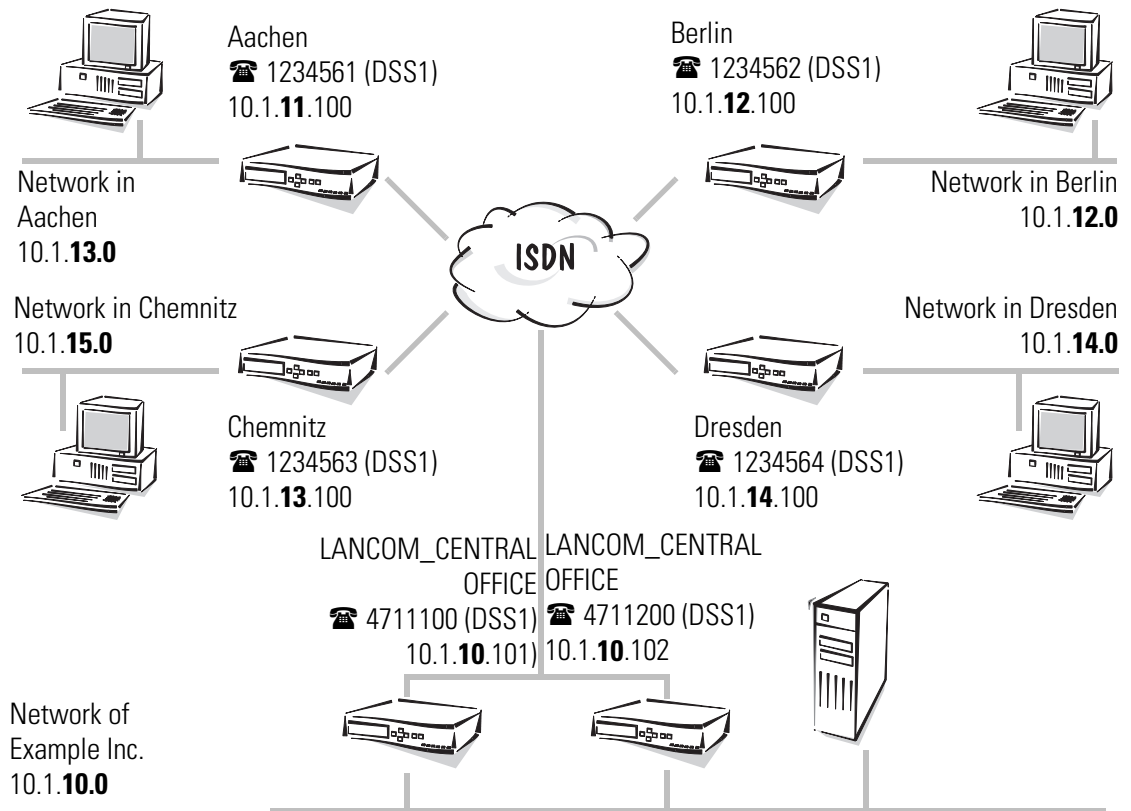
Network	Example_Inc.	Aachen	Berlin	Chemnitz	Dresden	Frankfurt	Gera
IP-address LAN	10.1.10.0	10.1.11.0	10.1.12.0	10.1.13.0	10.1.14.0	10.1.15.0	10.1.16.0
IP-address for the <i>LANCOM Office</i> router	a) 10.1.10.101 b) 10.1.130.102	10.1.11.100	10.1.12.100	10.1.13.100	10.1.14.100	10.1.15.100	10.1.16.100
IP-network-mask	255.255.255.0						
Device-name	Example_Inc.	Aachen	Berlin	Chemnitz	Dresden	Frankfurt	Gera
Call-number	a) 4711100 b) 4711200	1234561	1234562	1234563	1234564	1234565	1234566



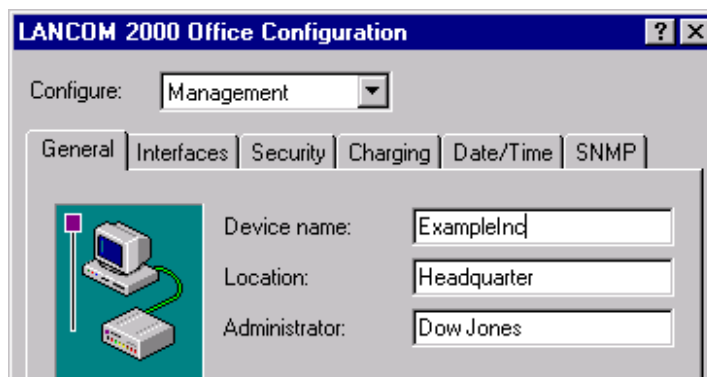
Step by Step: What settings are made in the *LANCOM Office* routers?

For the *LANCOM Office* router configuration for the dynamic scaling with IP-RIP we can set the two routers in the central office identically down to the call number. Important difference to static scaling: the scaled routers have almost identical entries in the routing table, which can be distinguished only by the distance. The *LANCOM Office* routers in the branches are set slightly differently, but their configurations generally correspond with one another.

In the following configuration steps we show, beginning with the routers in the central office, exactly what is set the same, and provide information on the deviations in the other *LANCOM Office* routers.



- ① For the names that are used in the name list to be also forwarded and detected by the *LANCOM Office* routers, name the devices appropriately (configuration area 'Management', 'General' tab). Both *LANCOM Office* routers in the network at the central office receive the same names. This ensures that they appear externally as one large router. With a different entry in the field 'device location', both can be distinguished in the device list of *LANconfig*.

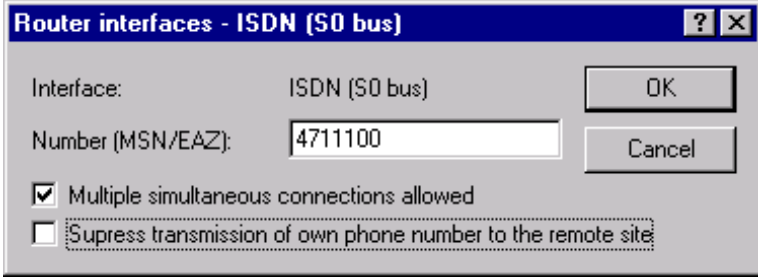




Enter the names of the devices directly in the 'Setup' menu with configurations with other aids:

	Setup	
	Name	Example_Inc.

The *LANCOM Office* routers in the branches correspondingly acquire the names 'Aachen' to 'Gera'.

- ② Then enter the **specific** call number (incoming and outgoing) and the D-channel protocol on the S_0 port of the first *LANCOM Office* router in the central office (configuration area 'Communication', 'Router interfaces' tab):



	Setup/WAN-module/Router-interface-list	
	Interface	S0 4711100 ON

The other *LANCOM Office* routers correspondingly acquire their own call numbers (4711200 and 1234561 to 1234566).

- ③ New entries in the name list (configuration area 'Communication', 'Remote Sites' tab) with identification of the remote stations and the call numbers with selection of one layer available in all routers (here for example the preset DEFAULT layer) enables the *LANCOM Office* router in the central office to call the routers in the other networks. With the standard values for the B1 and B2 hold times, the *LANCOM Office* router automatically disconnects every connection if there is no data flow on this line for 20 seconds.

Every network should bear its own telephone costs, therefore the call-back entry remains set to OFF:

Name list - New Entry

Name: OK

Phonenumber: Cancel

Short hold time: seconds

Short hold time (bundle): seconds

Layer name:

Automatic callback:

☒ No callback

☐ Call back the remote site

☐ Call back the remote site (fast procedure)

☐ Call back the remote site after name verification

☐ Wait for callback from remote site

	Setup/WAN-module	
	Name-list	Aachen -1234561 * * DEFAULT OFF
	Name-list	Berlin -1234562 * * DEFAULT OFF
	Name-list	Chemnitz -1234563 * * DEFAULT OFF
	Name-list	Dresden -1234564 * * DEFAULT OFF
	Name-list	Frankfurt -1234565 * * DEFAULT OFF
	Name-list	Gera -1234566 * * DEFAULT OFF

The second *LANCOM Office* router in the central office acquires the same entries.

The other *LANCOM Office* routers enter only the router 'Example_Inc.' and the call number of one of the two scaled *LANCOM Office* routers (e. g. -471110). The hyphen before the call number signals that there are still other call numbers for this network in the RoundRobin list.

Name list - New Entry

Name: OK

Phonenumber: Cancel

Short hold time: seconds

Short hold time (bundle): seconds

Layer name:

Automatic callback:

☒ No callback

- ④ The RoundRobin list is given below. The call numbers of the *LANCOM Office* routers in the central office, which have not previously been entered in the name list, are entered here in the routers of the branches.

RoundRobin list - New Entry

Remote site: EXAMPLEINC

RoundRobin: 4711200

Begin with:

☒ the last successfully reached number

☐ the first number

OK Cancel

Setup/WAN-module	
Round-Robin-list	-4711200

In selecting according to RoundRobin there are two possible procedures:

- In the setting '**Begin with: the last successfully reached number**' the call number with which the last connection was established is tested first. If this terminal is busy, the next number on the list is tried. At the end of the list, the first number on the list is selected (that is the one entered in the name list). If all call numbers are busy and the router returns to the number that was tried first, the data packet is rejected. A new dialing attempt will take place only when a new data packet is sent to the router.
 - In the setting '**Begin with: the first number**' the call number from the name list is always tried first. If this terminal is busy, the following numbers from the RoundRobin list are tried until the data packet can either be sent or has to be rejected (because all terminals are busy).
- ⑤ Now the addresses must still be clarified. So that the *LANCOM Office* routers in the internal TCP/IP networks are found, one free IP address at least from the Intranet is required. They receive them with the entry of the Intranet address with the associ-

ated network mask (configuration area 'TCP/IP', register 'General'). For these entries to become effective, activate the TCP/IP module.

Example Configuration

Configure: TCP/IP

General | DHCP | DNS | Routing | Filtering | Masquerading

☒ TCP/IP module active

IP address: 0.0.0.0

Netmask: 255.255.255.0

Intranet IP address: 10.1.130.101

Intranet netmask: 255.255.255.0

	Setup/TCP-IP-module	
	Intrane-address	10.1.130.101
	Intranet-network-mask	255.255.255.0
	Status	On

The second *LANCOM Office* router in the central office acquires the IP address 10.130.1.102, the *LANCOM Office* routers in the branches 10.131.1.100 to 10.136.1.100, all with the network mask 255.255.255.0, as shown in the diagram and the overview.

- ⑥ To enable exchange of information over the available routes between the scaled *LANCOM Office* routers to function, the IP-RIP must be activated (configuration area 'TCP/IP', 'Routing' tab). If possible, select the option 'RIP-2'. Only with older versions of Novell NetWare (to 3.12) set 'RIP-1' or 'RIP1komp'.

	Setup/IP-router-module/RIP-config	
	RIP-type	RIP-2











Ensure that the RIP functions are also activated in the servers in the local network.

- ⑦ And what IP addresses should the *LANCOM Office* routers route where? In the routing table of the routers in the central office enter the IP addresses and network masks of all branches with the remote station (without IP masquerading!):









Half of the remote stations should be directly reached from every *LANCOM Office* router, therefore the distance is set to 2. The other scaled *LANCOM Office* router is responsible for the remaining routes, therefore the distance there is set to 3. Finally, activate the IP router, and then the first *LANCOM Office* router is prepared for the connection to the other networks.

	Setup/IP-router-module		
	IP-routing-table	10.1.131.0 255.255.255.0 Aachen	2 OFF
	IP-routing-table	10.1.132.0 255.255.255.0 Berlin	2 OFF
	IP-routing-table	10.1.133.0 255.255.255.0 Chemnitz	2 OFF
	IP-routing-table	10.1.134.0 255.255.255.0 Dresden	3 OFF
	IP-routing-table	10.1.135.0 255.255.255.0 Frankfurt	3 OFF
	IP-routing-table	10.1.136.0 255.255.255.0 Gera	3 OFF
	Status	On	

The second *LANCOM Office* router in the central office has the same entries, except with reversed distribution of the distance values:

	Setup/IP-router-module	
	IP-routing-table	10.1.131.0 255.255.255.0 Aachen 3 OFF
	IP-routing-table	10.1.132.0 255.255.255.0 Berlin 3 OFF
	IP-routing-table	10.1.133.0 255.255.255.0 Chemnitz 3 OFF
	IP-routing-table	10.1.134.0 255.255.255.0 Dresden 2 OFF
	IP-routing-table	10.1.135.0 255.255.255.0 Frankfurt 2 OFF
	IP-routing-table	10.1.136.0 255.255.255.0 Gera 2 OFF
	Status	On

The *LANCOM Office* routers in the branches each acquire one entry for the central office *LANCOM Office* router in Aachen for example, the list looks as follows:

	Setup/IP-router-module	
	IP-routing-table	10.1.130.0 255.255.255.0 Example_Inc. 2 OFF
	IP-routing-table	10.1.132.0 255.255.255.0 Example_Inc. 2 OFF
	IP-routing-table	10.1.133.0 255.255.255.0 Example_Inc. 2 OFF
	IP-routing-table	10.1.134.0 255.255.255.0 Example_Inc. 2 OFF
	IP-routing-table	10.1.135.0 255.255.255.0 Example_Inc. 2 OFF
	IP-routing-table	10.1.136.0 255.255.255.0 Example_Inc. 2 OFF
	Status	On

In this way all connections between the branches are routed over the *LANCOM Office* routers in the central office.

Alternatively, the central offices can also communicate directly. For this purpose they first acquire the same entries in the name list as in the routers in the central office. In addition, the same entries are contained in the routing table as in the *LANCOM Office* routers in the central office, where the routing entry for the internal network is replaced by the entry for the central office network.

- ⑧ What must still be done? Naturally, the computers in the LAN also need to know that the *LANCOM Office* router is the switching centre for the other networks. For this purpose the Intranet address of the *LANCOM Office* router is entered as default gateway for the workstations and servers. In the local network at the central office there are also two gateways with the *LANCOM Office* routers available, which both have to be entered.



The result

With the access from a computer in a branch to the central office network, it is now possible to deviate to the other router via the entry in the RoundRobin list, if the first one dialed is busy. However, with this configuration it can occur that the central office is fully occupied when four branches are simultaneously dialed.

The great advantage of this configuration is in the use of IP-RIP information. By exchanging the RIP information the first *LANCOM Office* router in the central office network (IP 10.1.130.101) finds that routes to the branches are also available in the second *LANCOM Office* router (IP 10.1.130.102). According to the connection status of the two *LANCOM Office* routers, the routes are propagated with different distances, and the scaled router adapts itself to the situation:

- If a *LANCOM Office* router has established a connection to a remote station, it propagates this route with the distance '1'. The other *LANCOM Office* router places another hop on this distance for the detour via another router and enters the route with the distance '2' in its dynamic table. Because this route is better than its own entry in the static table, the *LANCOM Office* router will forward all packets for this route to the router that propagated this route.
 - If a *LANCOM Office* router has already established connections to two remote stations, it marks all other routes from its own static table as "not available" with the distance '16'. In this way the routes propagated by the other routers are better than its own. If this *LANCOM Office* router receives more packets, it automatically forwards them to the free channels on the other scaled routers.
- If the second router is also busy, all other routes are marked with the distance '16'. IP packets that cannot be rerouted are rejected.

Networks connected with the IPX router

The motivation

We can connect Novell networks (or networks with IPX protocol) with the IPX router. A server may be in each of the networks or in only one of the two.

An example of the task

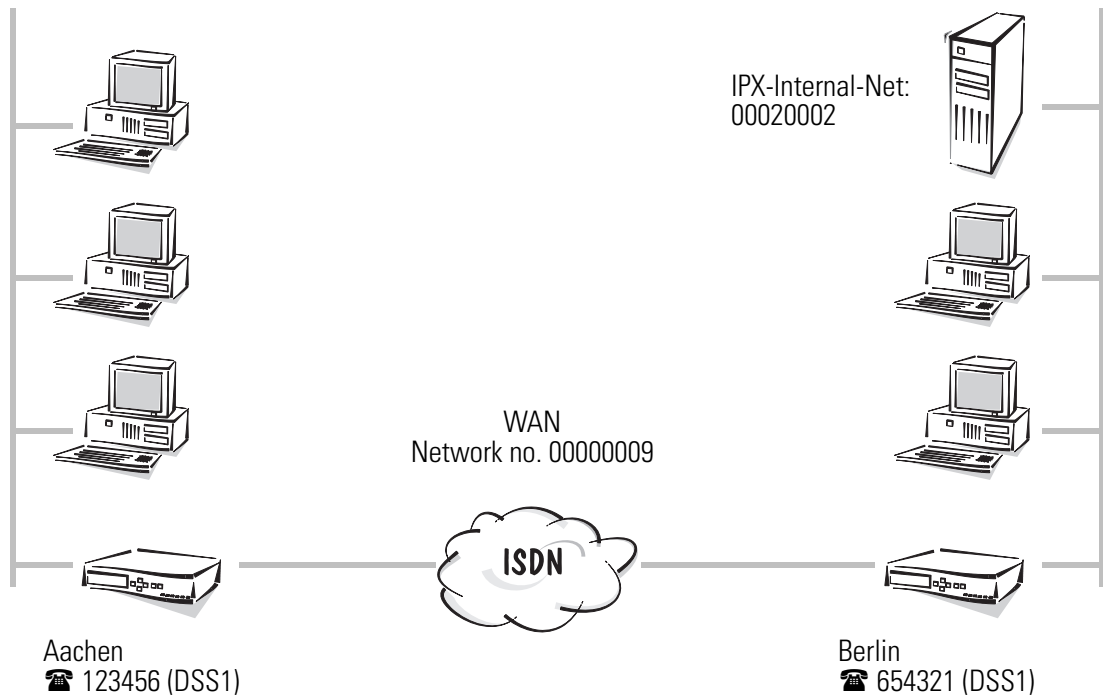
In this example we shall couple two networks and then it can easily be extended to several networks. There is a server in one network and not in the other. The two networks must have different network addresses, and we need another different common network number for the WAN between the two LANs. All these network addresses must also be different from the internal net addresses of the IPX server.

The following table shows the assignment of device names, addresses and telephone numbers as used in the example:

Network	LAN in Aachen	LAN in Berlin	WAN
Network address	00000001	00000002	00000009
IPX internal net		00010002	
Device name	Aachen	Berlin	
Call number	123456	654321	

Network in Aachen
Network no. 00000001

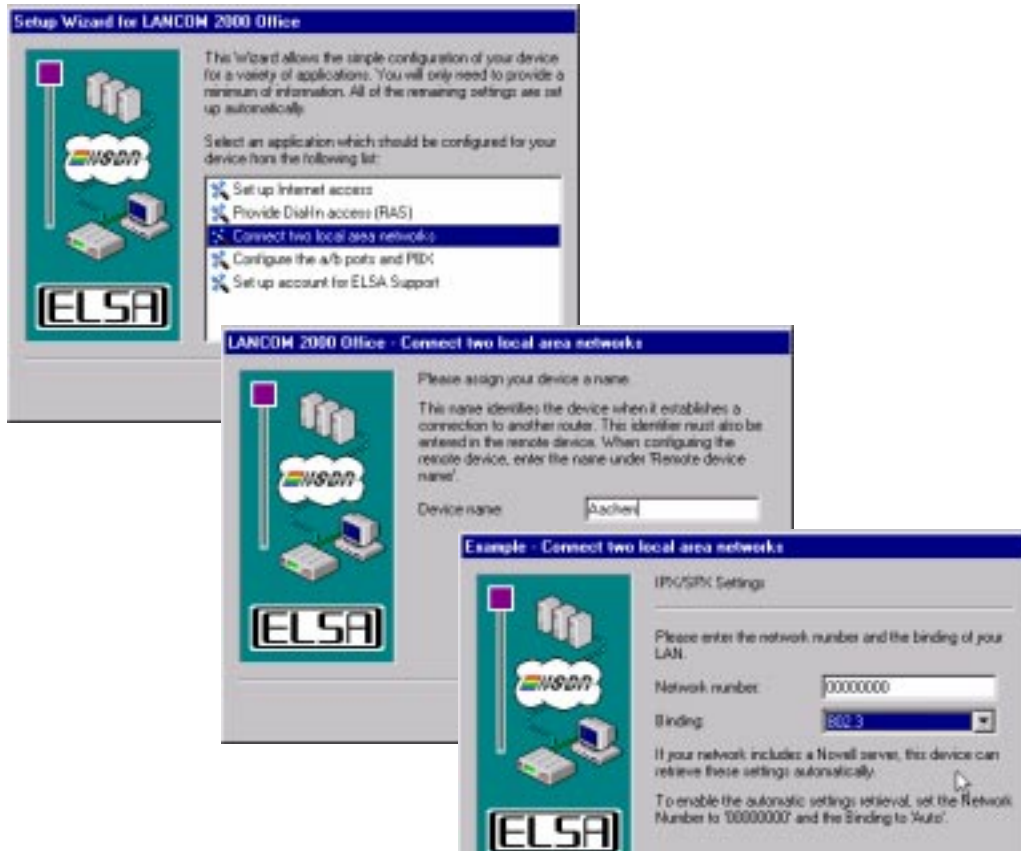
Network in Berlin
Network no. 00000002



IPX routing made simple with *LANconfig* and the wizards

For the *LANCOM Office* router configuration of LAN to LAN coupling there is a wizard in the *LANconfig* which makes all required settings in the *LANCOM Office* router software for you and at the same time takes the peculiarities of IPX networks into account. Once you have started up the wizard (automatically or by clicking **Tools ► Setup Wizard**) select the entry 'Connect two local area networks'. The wizard will now prompt you for the



required data (including the network protocol in use) and will then instruct you on what settings still need to be made on the workstation computers.



Step by Step: What settings are made in the LANCOM Office routers?

The settings are in principle the same for both LANCOM Office routers.



- ① First enter the **internal** call number (incoming and outgoing) and the D-channel protocol in the S_0 port of the LANCOM Office router 'Aachen' in the Router-interface-list (configuration area 'Communication', register 'General'):

	Setup/WAN-module/Router-interface-list	
	Interface	S0 123456 ON or OFF

When specifying several call numbers the first number is used for outgoing calls.

Setting the option 'Y connection' depends on whether a connection to another remote station is to be established simultaneously via the second B channel.

The entry for the LANCOM Office router 'Berlin' is as follows:

	Setup/WAN-module/Router-interface-list	
	Interface	S0 654321 ON or OFF

- ② A new entry in the name list (configuration area 'Communication', 'Remote Sites' tab) with identification of the remote station and the call number with selection of a layer with all routers (here for example the preset DEFAULT layer) enables the *LANCOM Office* router 'Aachen' to call the router in the other network. Every network should bear its own telephone costs, therefore the call-back entry remains set to OFF:

	Setup/WAN-module	
	Name-list	Berlin 654321 * * DEFAULT, OFF

The entry for the *LANCOM Office* router 'Berlin' is as follows:

	Setup/WAN-module	
	Name-list	Aachen 123456 * * DEFAULT, OFF




- ③ For the names used in the name list, including by the *LANCOM Office* routers to be forwarded and detected, name the *LANCOM Office* router 'Aachen' appropriately (configuration area 'Management', 'General' tab):

	Setup	
	Name	Aachen




The entry for the *LANCOM Office* router 'Berlin' is as follows:

	Setup	
	Name	Berlin

- ④ Now the addresses must still be clarified. So the *LANCOM Office* router can distinguish its own LAN from the other LANs and the WAN, enter the network address and the binding for the network in Aachen (configuration area 'IPX/SPX', 'General' tab). This network does not have a server, therefore the network no. and the binding must be explicitly entered.



	Setup/IPX-module/LAN-config	
	Network	00000001
	Binding	802.3

There is a server in the network in Berlin. If only one logical network is in use on the Ethernet string, the network no. with the entry '00000000' and the binding can be automatically determined:

	Setup/IPX-module/LAN-config	
	Network	00000000
	Binding	Auto



The network in which the most RIP information can be detected is automatically selected.

- ⑤ And where should the *LANCOM Office* routers route to? Enter the remote stations into the routing table (configuration area 'IPX/SPX', 'Routing' tab) with an **internal** network address for the WAN (not that of another LAN). The entry for the Aachen network is as shown below:

	Setup/IPX-module/WAN-config	
	Routing-table	Berlin 00000009 802.3 route ON

'Berlin' is the device name of the router in the network at the remote station, '00000009' is the network address of the WAN on which the binding '802.3' is used. Because from the point of view of the network in Aachen there is a server on the remote side, the 'exponential backoff' mechanism is activated.

The entry for the network in Berlin is shown below:

	Setup/IPX-module/WAN-config	
	Routing-table	Aachen 00000009 802.3 route OFF

Network address of the WAN and the binding '802.3' are the same. But, because from the point of view of the network in Berlin there is not a server on the remote side, the 'exponential backoff' mechanism is deactivated here.



Further information on the function of the 'exponential backup' mechanism is found in 'Exponential Backoff'.

- ⑥ What must still be done? Some settings can still be made to extend the communication budget, e. g. transmission of RIP or SAP packets can be permitted only when there are changes ('trig.') or when there is already a connection ('pBack', standard setting, configuration area 'IPX/SPX', 'RIP settings' or 'SAP settings' tab):

	Setup/IPX-module/RIP-config	
	Spoofing	Trig. or pBack



	Setup/IPX-module/SAP-config	
	Spoofing	Trig. or pBack

Further information on the filter functions for RIP and SAP packets is found in Chapter 'IPX packet filters'.

- ⑦ Finally, activate the IPX router (configuration area 'IPX/SPX', 'General' tab), and then the first *LANCOM Office* router is prepared for the connection to the other network.

	Setup/IPX-module	
	IPX-router	On

What has been achieved now?

By activating the IPX router the *LANCOM Office* router 'Aachen' establishes a connection to all available remote stations and exchanges RIP and SAP information with them. Ultimately both networks behave as one large network, in which, for example, servers on the network in Berlin are also available on the Aachen network.



Networks with Windows 95 or Windows NT

To avoid unnecessary connections in network with Windows 95 or Windows NT, include the following entries in the socket filter table:

	Setup/IPX-module/LAN-config	
	Socket-filter	0455 0457

This entry will filter the Microsoft NetBIOS packets.

NetWare-NetBIOS packets are filtered with the following entry:

	Setup/IPX-module/LAN-config	
	Socket-filter	0550 0555

Several IPX routers in one Network (scaling)

The motivation

As seen in example 'Networks connected with the IPX router', networks can be connected with the IPX routers, which use IPX/SPX as network protocol. However, if the central office of a company establishes more branches, one *LANCOM Office* router in the central office network may not be sufficient. It is then time to use several *LANCOM Office* routers in one local network.

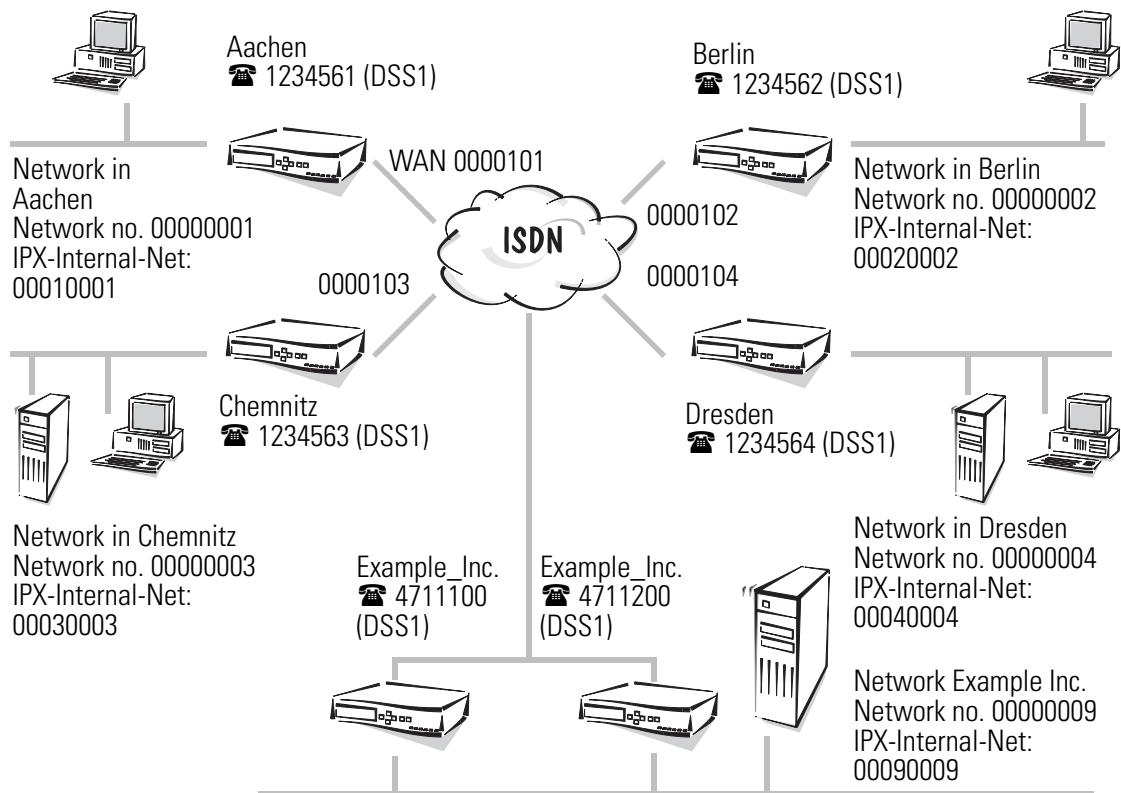
The *LANCOM Office* routers in this case are virtually switched together into one large router (scaled). Every router is made responsible for a section of the remote stations with entries in the routing table.

An example of the task

In this example the central office has four branches. A connection between central office and branches should be possible at any time. For this purpose the network in the company central office is equipped with two *LANCOM Office* routers, each of which is connected to one Euro-ISDN terminal (each with two B channels). With the total of four B channels in the central office, the availability of the central office for all branches is guaranteed. Data exchange among the branches is also possible via the scaled routers in the central office (eg as reserve line for the direct connection).

The following table shows the assignment of device names, addresses and telephone numbers as used in the example:

Network	LAN Example Inc.	LAN Aachen	LAN Berlin	LAN Chemnitz	LAN Dresden
Network address	00000009	00000001	00000002	00000003	00000004
IPX internal net	00090009	00010001	00020002	00030003	00040004
Binding	802.3	SNAP	SNAP	802.3	802.3
Device name	Example_Inc.	Aachen	Berlin	Chemnitz	Dresden
Call number	a) 4711100 b) 4711200	1234561	1234562	1234563	1234564
WAN networks		00000101	00000102	00000103	00000104



Step by Step: What settings are made in the *LANCOM Office* routers?

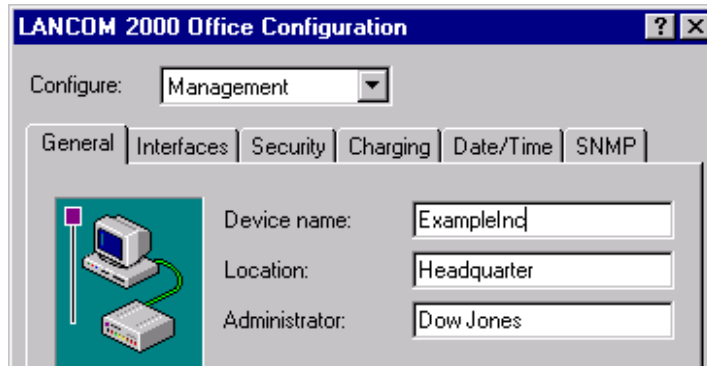
Both routers in the central office may be set almost identically for the *LANCOM Office* router configuration for static scaling in the IPX router operation. The *LANCOM Office* routers in the branches are set slightly differently, but their configurations generally correspond with one another.

Because there are no wizards for the scaled router operation, this example will be run through complete with *LANconfig*.

In the following configuration steps we show, beginning with the routers in the central office, exactly what is set the same, and provide information on the deviations in the other *LANCOM Office* routers.

- ① For the names that are used in the name list to be also forwarded and detected by the *LANCOM Office* routers, name the devices appropriately (configuration area 'Management', 'General' tab). Both *LANCOM Office* routers in the network at the central office receive the same names. This ensures that they appear externally as

one large router. With a different entry in the field 'Location', both can be distinguished in the device list of *LANconfig*:

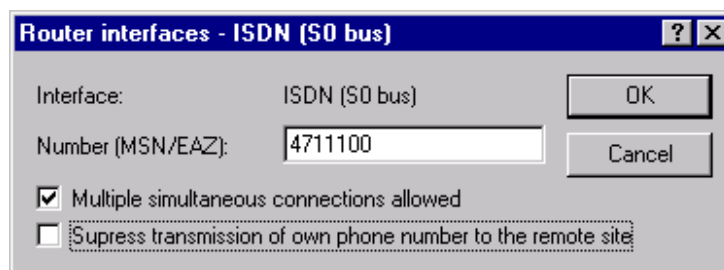




Enter the names of the devices directly in the 'Setup' menu with configurations with other aids:

	Setup	
	Name	Example_Inc.

The *LANCOM Office* routers in the branches receive the names 'Aachen', 'Berlin', 'Chemnitz' and 'Dresden'.

- ② Then enter the **specific** call number (incoming and outgoing) in the central office (configuration area 'Communication', 'General' tab):



	Setup/WAN-module/Router-interface-list	
	Interface	S0 4711100

The other *LANCOM Office* routers correspondingly receive their own call numbers (4711200, 1234561, 1234562, 1234563 and 1234564).

- ③ New entries in the name list (configuration area 'Communication', 'Remote Sites' tab) with identification of the remote stations and the call numbers with selection of a layer available on all routers (here for example the preset DEFAULT layer) enable the *LANCOM Office* routers in the central office to call the routers in the other

branch networks. Every network should bear its own telephone costs, therefore the call-back entry remains set to OFF:

	Setup/WAN-module	
	Name-list	Aachen 1234561 * * DEFAULT OFF
	Name-list	Berlin 1234562 * * DEFAULT OFF
	Name-list	Chemnitz 1234563 * * DEFAULT OFF
	Name-list	Dresden 1234564 * * DEFAULT OFF







The *LANCOM Office* routers in the branches have only the router 'Example_Inc.' ON and therefore the call number of one of the two scaled *LANCOM Office* routers (e. g. Aachen and Berlin the '471110', Chemnitz and Dresden the '4711200').

- ④ Now the addresses must still be clarified. Specify the network address and the binding for the Example Inc.'s network so that the *LANCOM Office* router can differentiate its own LAN from other LANs and the WAN: (configuration area 'IPX/SPX', 'General' tab):






	Setup/IPX-module/LAN-config	
	Network	00000009
	Binding	802.3

The network in the central office has one server. If the network number is not known, this can be automatically found with the setting '00000000' as network number. The binding can also be automatically found. Because the LANCOM Office router always dials the network in which most RIP/SAP information is exchanged in this case, this procedure can for example be used when only one logical network is in use on the Ethernet string.

Also enter the appropriate network address with the binding 'Auto' for the *LANCOM Office* routers in the branches in Chemnitz and Dresden, and the binding, e. g. 'SNAP', and the direct network number must be explicitly entered for the networks in Aachen and Berlin, because there is no server in these networks:

	Setup/IPX-module/LAN-config	
	Network	00000003 or 00000004
	Binding	Auto
	Setup/IPX-module/LAN-config	
	Network	00000001 or 00000002
	Binding	SNAP

- ⑤ And where should the *LANCOM Office* routers route to? Enter the remote stations into the routing table (configuration area 'IPX/SPX', 'Routing' tab) with an **internal** network address for the WAN (not that of another LAN). For the two *LANCOM Office* routers in the network in the central office the table appears as below:

	Setup/IPX-module/WAN-config	
	Routing-table	Aachen 00000101 802.3 Route Off
	Routing-table	Berlin 00000102 802.3 Route Off
	Routing-table	Chemnitz 00000103 802.3 Route ON
	Routing-table	Dresden 00000104 802.3 Route ON

In addition to the device names of the router in the network at the remote station, every entry in the routing table receives its own WAN address. Network address of the WAN on which the binding '802.3' is used. Because, seen from the network in the central office, there is a server for the remote stations in Chemnitz and Dresden, the 'exponential backoff' mechanism is activated.



Further information on the function of the 'exponential backup' mechanism is found in 'Exponential backoff'.

The entry for the network in the Aachen branch, for example, is as follows:

	Setup/IPX module/WAN-setting	
	Routing-table	Example_Inc. 00000101 802.3 Route ON

The network address of the WAN is the same as the entry for the branch network in the *LANCOM Office* router at the central office. '802.3' is always used as binding on the WAN. Because from the point of view of the networks in the branches there

is always a server on the remote side, the 'exponential backoff' mechanism is activated here.

The result

When a computer in a branch accesses the central office network, it is now possible to divert to the other router in the RoundRobin list if the first one dialed is busy.

Two networks connected via the bridge

The motivation

If more Ethernet-based network protocols are to be transmitted between two networks as well as IP and IPX, the router section of the *LANCOM Office* router can no longer cope. IP and IPX use logical addresses to identify the individual devices in the network that can manage a router. Other network protocols operate with other addresses and therefore cannot be routed by the *LANCOM Office* router.

This function is the solution

The bridge in the *LANCOM Office* router only operates on the second level of the OSI model. Therefore, it does not need the logical addresses of the network participants and is oriented only to the physical (MAC) addresses. The bridge is a hardware-oriented solution and also transmits other network protocols as well as IP and IPX between logically **non**-separate networks.



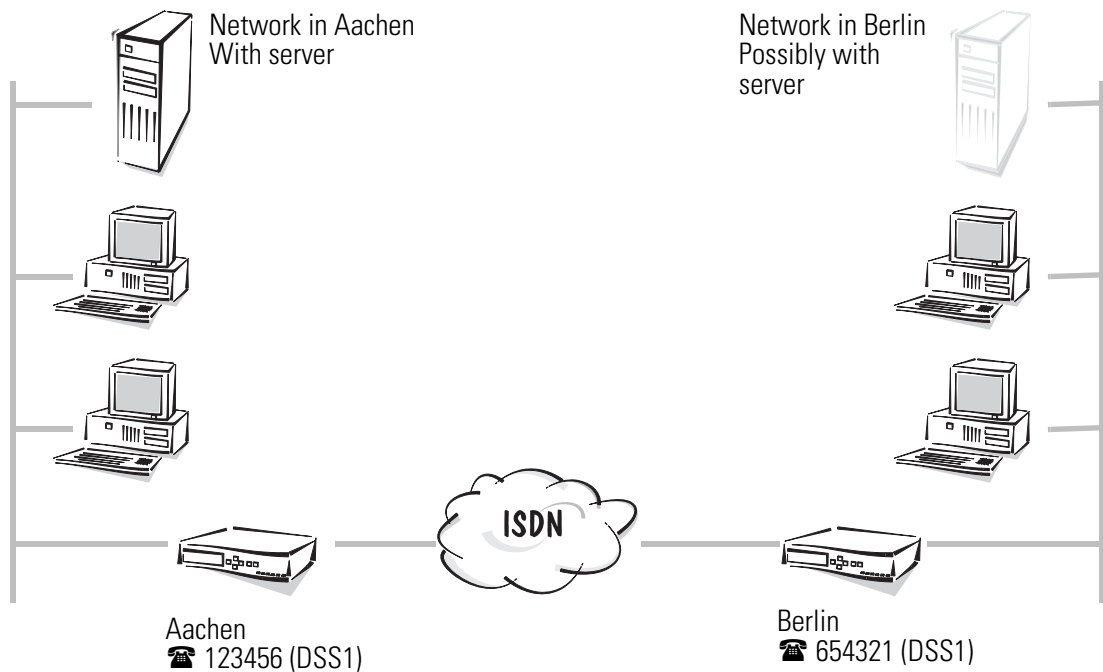
However, always use the corresponding router for transmission of data packets from IP and/or IPX networks.

With simultaneous usage of IP and/or IPX routers with the bridge the router functions always have precedence over those of the bridge. Data packets that can be routed or that have been filtered by the router setting are not for transmission by the bridge.

An example of the task

There is a network on one side in Aachen with one or more servers. On the other side there is a network in Berlin that does not have a server. The network protocol in use is optional, in both networks a *LANCOM Office* router ('Aachen' and 'Berlin'). To connect the two networks, an ISDN switched line is used. The first *LANCOM Office* router has

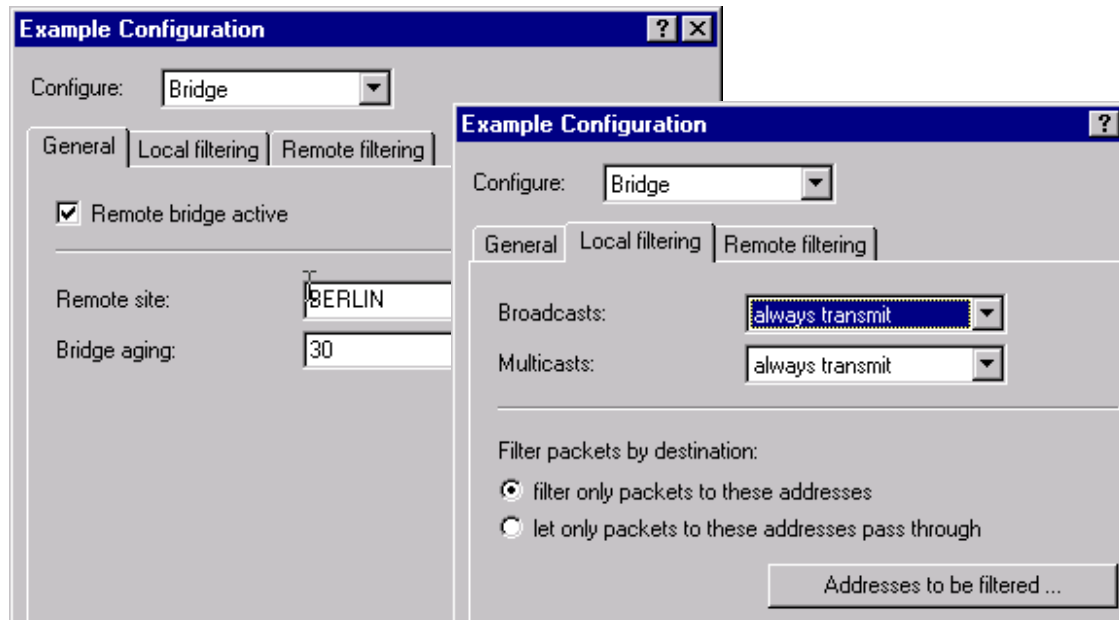
the call number 123456, the second 654321. Both are connected on S_0 ports with Euro-ISDN (DSS1) on the D channel.



Bridging with *LANconfig*

For the *LANCOM Office* router configuration as bridge set the ISDN terminal in the *LANconfig* in the interface settings (configuration area 'Communication', 'Router interfaces' tab) and place a new entry for the remote station in the name list (configuration area 'Communication', 'Remote Sites' tab). The layer used must in every case have the setting 'Ether' in the column 'Encapsulation' (configuration area 'Communication', 'Connect' tab)! Select the remote station for the bridge, (configuration area 'Bridge' 'General' tab), and set the filter for the transmission of broadcast and multicast packets and for individual MAC addresses from the LAN and the WAN (configuration area 'Bridge', '...filtering' tab).

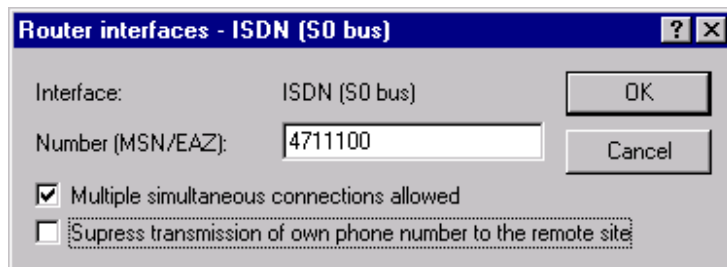
Do not forget to activate the bridge also once the changes have been made.



If data packets from an IP network are to be transmitted over the bridge, the IP router must also be deactivated. The IP router is activated in the standard settings.

Step by Step: What is set on the LANCOM Office router 'Aachen'?

- ① Enter the **internal** call number (configuration area 'Communication', 'General' tab):



	Setup/WAN-module/Router-interface-list	
	Interface	S0 123456

- ② For the names that are used in the name list to be also forwarded and detected by the LANCOM Office routers, name the devices appropriately:

	Setup	
	Name	Aachen

- ③ A new entry in the name list with identification of the remote station and the call number with selection of a layer with the setting 'Encaps=Ether' (here for example the preset layer Bridge_BC with channel bundling and data compression) enables the LANCOM Office router to call the routers in the other network. Every network

should bear its own telephone costs, therefore the call-back entry remains set to OFF:

	Setup/WAN-module	
	Name-list	Berlin 654321 * * Bridge_BC Off

- ④ Finally, enter the new entry from the name list as remote station for the bridge and activate the bridge:

	Setup/Bridge-module	
	Remote-station	Berlin
	Status	On

What is set on the LANCOM Office router 'Berlin'?

In principle the same as on the LANCOM Office router 'Aachen', but of course with the corresponding values of the remote station in the bridge module and in the name list...

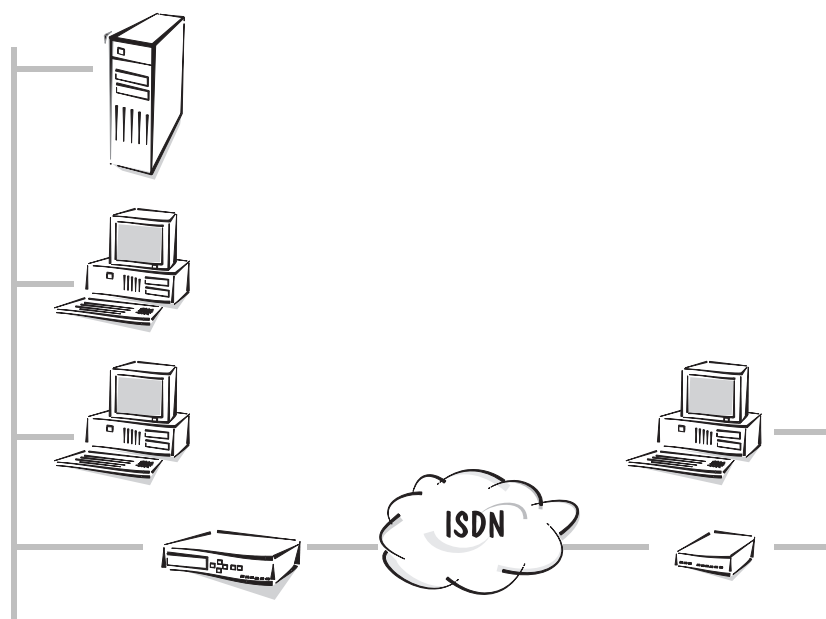
The result

Both networks have now been connected as if they were actually coupled at the hardware level (e. g. by a long Ethernet cable).

The bridge transmits all data back and forth between the two networks. In this process, it learns relatively quickly what MAC addresses are in its own network and what have been found on the other side. After a very high level of initial data traffic which occurs when the two networks introduce themselves to each other, the network load then drops sharply and the connection no longer needs to be established as frequently.



In addition, some settings to filters can be made to improve transmission behavior even more. More on this subject can be found in Chapter 'The Bridge in the network' and in the menu description in section 'Setup/Bridge-module'.



Remote access

The work of many employees in modern organizations depends less and less on any definite location—the most important factor here is constant access to shared and freely available information.

Remote access is the key to this. The ability of employees to telework from their home office or of field staff to contact head office while on the move is made possible by the *LANCOM Office* router in central office's local area network. The *LANCOM Office* router naturally also does everything necessary to protect the company's data during remote access: The callback function uses the names and call numbers entered to give the open sesame to specified users only. And telephone charges are calculated at head office, simplifying the billing process.

Remote access using TCP/IP	2
Remote access for IPX	7

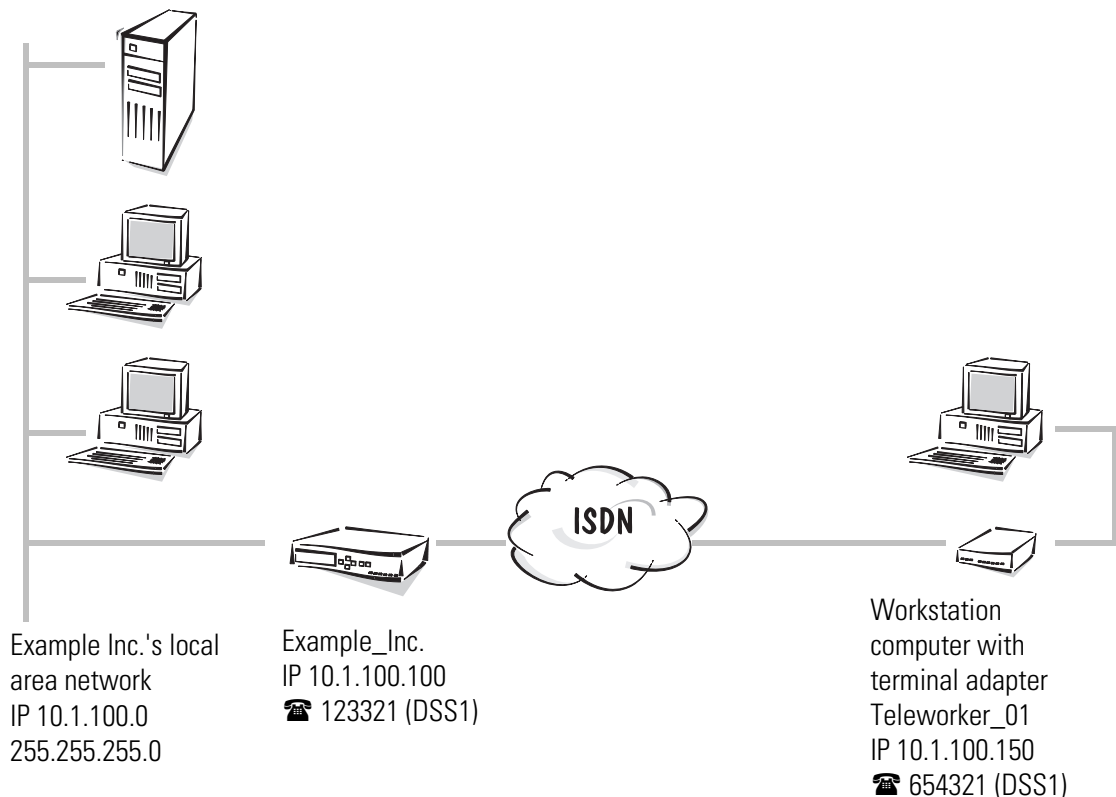
Remote access using TCP/IP

The motivation

A company employs staff in field service or as teleworkers who do not come into the office on a daily basis. Nevertheless they still need to have access to the company's local area network (Intranet) from their computer to allow them to exchange data and information (e-mails, for example). PPP is used as the data transmission protocol since all common devices and operating systems support it.



An example of the task

Staff using remote access will have a workstation computer with an ISDN terminal adapter or an ISDN card. A PPP client is installed on the remote computers, in this example Windows 95 Dial-Up Networking using the TCP/IP protocol. A *LANCOM Office* router is installed on the company's LAN to call back the workstation computers on demand.



Step by Step: What settings do you enter for the LANCOM Office router?



- ① First of all specify your **own** call number for incoming and outgoing calls in the Router-interface-list (configuration area 'Communication', 'General' tab):

	Setup/WAN-module/Router-interface-list	
	Interface	S0123321 ON

When specifying several call numbers the first number is used for outgoing calls.

The 'Y connection' option is enabled in this instance so that simultaneous connections to two different teleworkers are also possible.



- ② Remote access should be possible without verification of the incoming call number since field service employees at least will require access to the company network from different locations. It is therefore not possible to assign call number recognition to a layer which uses PPP. Setting the values for the 'DEFAULT' layer to the pre-set values for the 'PPPHDLIC' layer will greet any caller who cannot be assigned using the number list with PPP negotiation.

	Setup/WAN-module	
	Layer-list	DEFAULT trans PPP trans none HDLC64K

- ③ The entry in the name list identifying the remote station, 'DEFAULT' layer and the 'Name' callback option allows the LANCOM Office router to call back the workstation computer of the field service employee. This forces a protocol negotiation using PPP, the call number for callback remains blank in the name list and can be specified by the field service employee himself:

	Setup/WAN-module	
	Name-list	Teleworker_01 * * * DEFAULT Name

- ④ Since you are using PPP to access the remote computers, you can set the user names (e. g. Anybody) and password (e. g. ELSA) in the PPP list for the 'Teleworker_01' remote station. Use PAP as a security procedure for this:




	Setup/WAN-module	
	PPP-list	Teleworker_01 PAP ELSA 0 0 Anybody

The password "ELSA" will be replaced by several asterisks (*) when entered.

Please note that user name and password are case-sensitive.

- ⑤ You must still clarify the addresses. The LANCOM Office router requires a free IP address from the company network so that it can be found in its own TCP/IP net-



work. It receives this when the Intranet address and associated network mask are entered:

	Setup/TCP-IP-module	
	Intranet-address	10.1.100.100
	Intranet-mask	255.255.255.0



The company's own DNS server IP address and network mask can be specified in the TCP IP module as well. The address of the DNS server will then automatically be sent to the teleworker's computer.

- ⑥ What about the IP address for the computer making the call? This will be assigned by the *LANCOM Office* router for the duration of the connection. For this you will need an IP address which is available on the company's LAN but not yet in use there. You must specify this address in the routing table, with the network mask completed and the remote station name of the computer making the call (without IP masquerading):

	Setup/IP-router-module	
	IP-routing-table	10.1.100.150 255.255.255.255 Teleworker_01 0 OFF

This entry will achieve two things: Firstly the calling computer will be assigned the IP address 10.1.100.150 from the company's LAN, and secondly all packets for this address will be routed to the 'Teleworker_01' remote station.

According to its IP address, the remote station is now located in the same local area network as the *LANCOM Office* router so the distance is 0.

- ⑦ The Proxy ARP must be enabled so that the *LANCOM Office* router will be able to route data for a remote computer using an address from its own logical network.

	Setup/IP-router-module	
	Proxy-ARP	On

- ⑧ Now enable the IP router and the first *LANCOM Office* router is ready for connection to other networks.

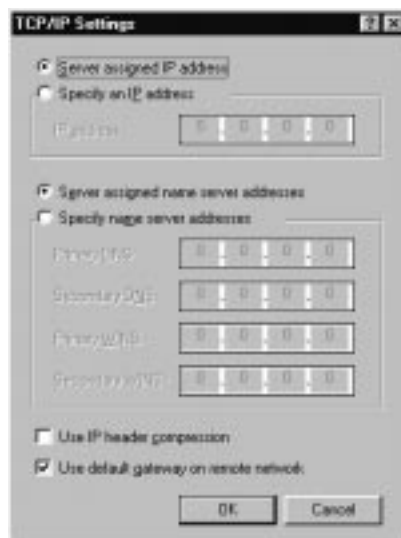
	Setup/IP-router-module	
	Status	On

- ⑨ What's left to do? The field service employee's workstation computer must be set up so that access to the company's network is also possible from his side. This will require the following settings which are only described in brief here:

- Dial-Up Networking correctly set up
- TCP/IP installed and bound to the Dial-Up adapter
- New connection in Dial-Up Networking with the call number of the *LANCOM Office* router
- Terminal adapter or ISDN card set to PPPHDL
- PPP selected as the Dial-Up server type, 'Enable software compression' and 'Require data encryption' unchecked
- TCP/IP selected as the network protocol

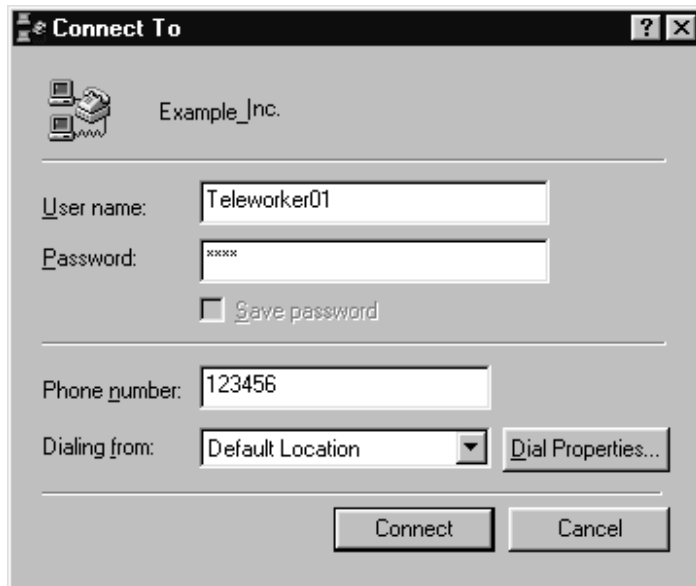


- Assignment of IP address and name server address checked, 'IP header compression' unchecked



What has this achieved?

The employee at the remote workstation computer now use Dial-Up Networking to establish a connection to the company network. This is done by specifying the user name set in the PPP list and its associated password.



He can now access the shared server on the TCP/IP network. He can find this server by clicking on **Start ► Find ► Computer** in the Windows Start menu, for instance.

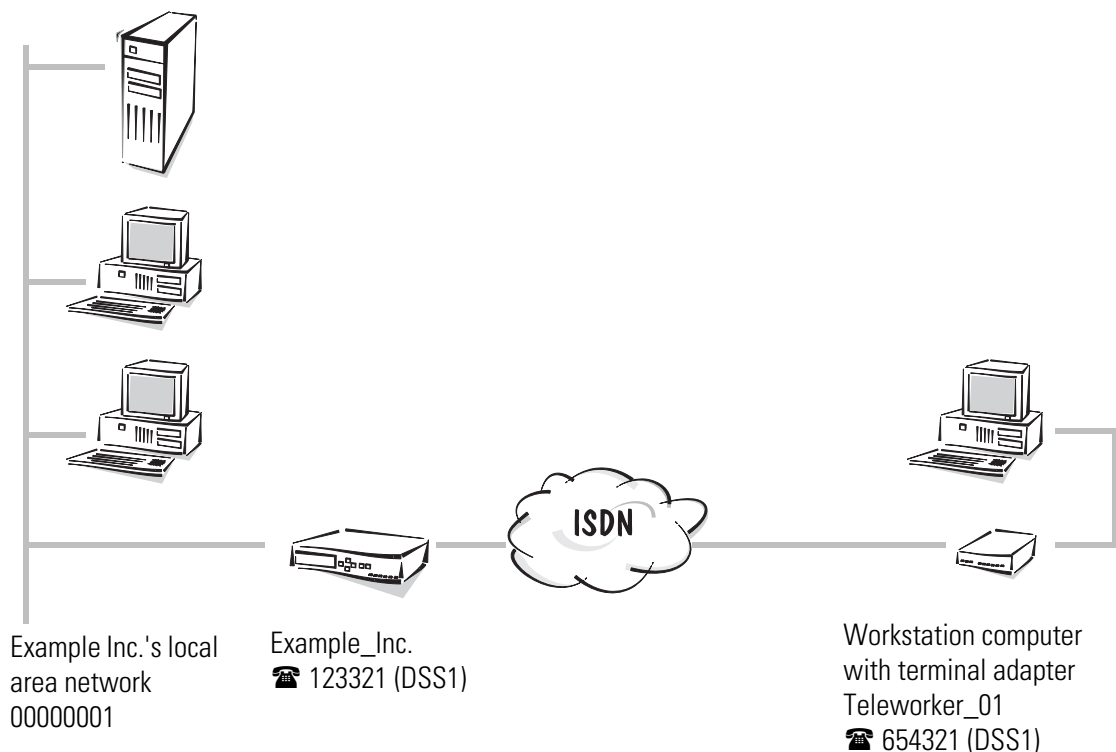
Remote access for IPX

The motivation

A company employs staff in field service or as teleworkers who do not come into the office on a daily basis. Nevertheless they still need to have access to the company's local area network (Intranet with IPX) from their computer to allow them to copy data from Novell NetWare servers, for example. PPP is used as the data transmission protocol since all common devices and operating systems support it.

An example of the task

Staff using remote access will have a workstation computer with an ISDN terminal adapter or an ISDN card. A PPP client is installed on the remote computers, in this example Windows 95 Dial-Up Networking using the TCP/IP protocol. A *LANCOM Office* router is installed on the company's LAN to call back the workstation computers on demand.





Remote access for IPX made simple with *LANconfig* and its wizards

Various wizards for configuring the *LANCOM Office* router have been put together in the *LANconfig* which make all the necessary settings for you in the *LANCOM Office* router software, at the same time taking into account the characteristics of IPX networks. Once you have started up the wizard (automatically or by clicking **Tools ► Setup Wizard**),

select the appropriate entry. The wizard will now simply ask for the necessary data and will then instruct you what settings still need to be made for the workstation computers.

Step by Step: What settings do you enter for the *LANCOM Office* router?

- ① First specify in the interface table (configuration area 'Communication', 'General' tab) the call number for incoming and outgoing calls in the Router-interface-list:

	Setup/WAN-module/Router-interface-list	
	Interface	SO 123321 ON

When specifying several call numbers the first number is used for outgoing calls.





The 'Y connection' option is enabled in this instance so that simultaneous connections to two different teleworkers are also possible.



- ② Then set which calls the *LANCOM Office* router should answer. You can protect your local area network against calls from remote stations that are not entered together with name and password by using the 'by name' setting.

	Setup/WAN-module	
	Protect	Name

- ③ Remote access should be possible without verification of the incoming call number since field service employees at least will require access to the company network from different locations. It is therefore not possible to assign call number recognition to a layer which uses PPP. Setting the values for the 'DEFAULT' layer to the pre-set values for the 'PPPHDLC' layer will greet any caller who cannot be assigned using the number list with PPP negotiation.



	Setup/WAN-module	
	Layer-list	DEFAULT trans PPP trans none HDLC64K

- ④ The entry in the name list designating the remote station, DEFAULT layer and which callback option has been activated allows the *LANCOM Office* router to call back the workstation computer of the field service employee:

	Setup/WAN-module	
	Name-list	Teleworker_01 654321 * * DEFAULT ON

- ⑤ Since you are using PPPHDLC to access the remote computer, you can agree the user name (e. g. Anybody) and password (e. g. TEST) in the PPP list for the

'Teleworker_01' remote station. You should use PAP as a security procedure for this:




	Setup/WAN-module	
	PPP-list	Teleworker_01 PAP TEST 0 0 Anybody

The password "TEST" will be replaced by several asterisks (*) when entered.

Please note that user name and password are case-sensitive.





- ⑥ You must still clarify the addresses. Specify the network address and the binding for the Example Inc.'s network so that the *LANCOM Office* router can differentiate its own LAN from other LANs and the WAN:

	Setup/IPX-module/LAN-config	
	Network	00000001
	Binding	802.3

Head office's network has one server. If you do not know the network number, you can have this determined automatically by setting the network number to '00000000'. You can also have the binding determined automatically. This procedure is useful if only one logical network is being used on the Ethernet line since the LANCOM Office router will always select the network on which the most RIP/SAP data is being exchanged.

- ⑦ And where should the *LANCOM Office* router route to? Enter the remote station with any network address of its own for the WAN (not the other LANs) in the routing table: an:

	Setup/IPX-module/WAN-config	
	Routing-table	Teleworker_01 00000099 802.3 Route Off

The binding of '802.3' has also been chosen freely. The 'exponential backoff' mechanism is disabled in this case because there is no server on the remote site from the point of view of the company network.

- ⑧ What's left to do? The field service employee's workstation computer must be set up so that access to the company's network is also possible from his side. This will require the following settings which are only described in brief here:
- Dial-Up Networking correctly set up
 - IPX installed and bound to the dial-up adapter
 - New connection in Dial-Up Networking with the call number of the *LANCOM Office* router
 - Terminal adapter or ISDN card set to PPPHDLC

- PPP selected as the Dial-Up server type, IPX selected as the network protocol

What has this achieved?

The employee at the remote workstation computer can now use Dial-Up Networking to establish a connection to the company network. This is done by specifying the user name set in the PPP list and its associated password. He can then use an IPX network client (Novell or Microsoft, for example) to log onto the IPX network. He can find the server on this network by clicking on **Start ► Find ► Computer** in the Windows Start menu, for instance.



If the user name and password for the LANCOM Office router match the login name and password for the server, the 'Log on to network' option may be enabled in the Dial-Up connection properties. The user will now not only have access to the local area network but he will also be logged directly onto his server.

PBX and least-cost router

One of the *LANCOM 2000 Office*'s special features is the option of connecting four analog end devices such as telephones, fax devices and telephone answering machines to it. With the functions of a small PBX the device presents itself as a complete communications center, e.g. for small companies or offices.

In this chapter we will use an example, to show you how you can set up your telephone system and also, how you can save yourself a lot in call charges with the least-cost router.

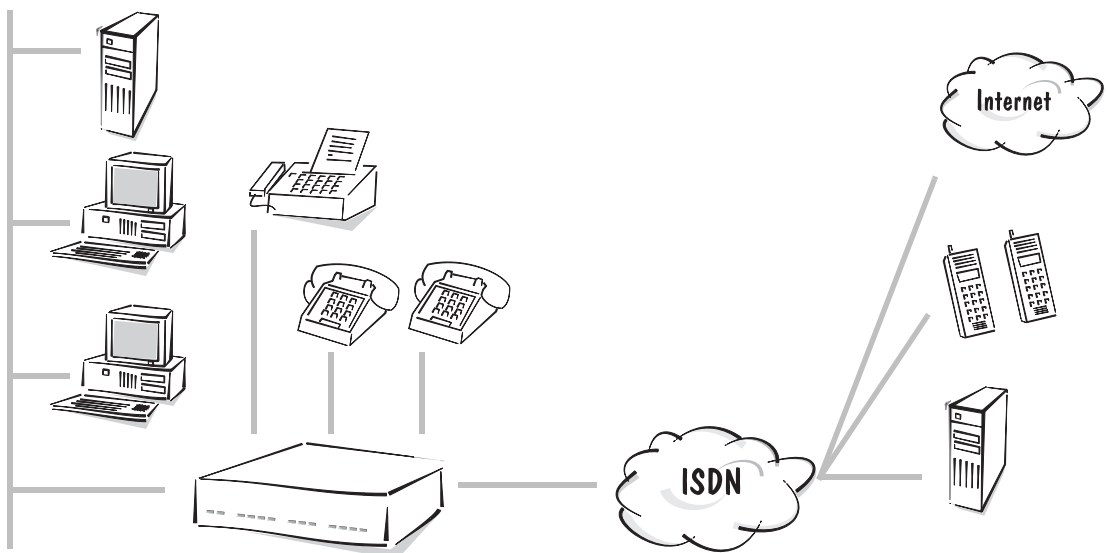
Although not demonstrated in this example, the LCR functions can also be used for router modules in the *LANCOM Office* router and for the *ELSA LANCAPI*.

Example: small office.....	2
The PBX.....	3
The least-cost router.....	6

Example: small office

Let's take a small engineering office with two work places (a branch office of a larger planning office) as an example. There is a fax device and an answering machine and each of the two work places has a telephone. As the office only switched to an ISDN connection recently, these are analog devices.

The two employees travel a lot and always take their cell phones with them as they want to be reachable at all times if possible. Call forwarding to the cell phone number while they are on the road ensures that they both do not miss any important information.



The customers and business partners of the office are located all over the country, some of them are also based abroad. Long distance calls and connections to cellular networks are therefore commonplace.

The two employees in this office also use the other functions of the *ELSA LANCOM Office* router:

- They were able to setup their access to the Internet through a provider in a flash with the *ELSA LANconfig* and its wizards. This function uses the IP router.
- Data exchange with the head office takes place via a LAN-to-LAN connection using the functions of the IPX router.
- To send fax messages directly from the PC they use *ELSA-RVS-COM* via the *LANCAPI*.

You may ask why these details are important. Well, we would like to use this example to explain, among other functions, the least-cost router. The LCR can basically not only be used for the PBX but also for the router modules and the *LANCAPI*. A further aspect is the "service priority" with which you can define those tasks of the *ELSA LANCOM Office* router which are particularly important.

The PBX



PBX with *ELSA LANconfig*

You can configure the basic functions of the PBX using the setup wizard in *ELSA LANconfig*. After that, you can manually set the parameters for the individual a/b ports, if necessary.

How to set up the PBX:

- ① Connect the four devices to the a/b ports of the *LANCOM 2000 Office*.
- ② Start the setup wizard by selecting **Tools ► Setup Wizard ► Configure the a/b ports and PBX**.
- ③ For each port, set the device type attached to it. This selection defines the basic settings for the corresponding port. In the case of a telephone, for example, call waiting is activated, for answering machines the transfer of calls in progress is activated and for fax devices both these options are disabled.
- ④ Then define the call numbers to which the individual ports should respond. If you assign several call numbers to a port, separate them with semicolons.
 - The two telephones are assigned to the call numbers '123456' and '123457'.
 - The fax, of course, receives its own number '123458'.
 - The answering machine must respond for both telephones and thus is assigned '123456;123457'.
- ⑤ Because the engineers each have their own office, they also need to be able to telephone each other internally. Therefore, you should now activate the option to use the PBX function.

And that was it, the PBX is now ready for operation. The two colleagues can speak to each other internally, for external calls they first dial zero. Both telephones can also be called from outside and if nobody takes the call the answering machine steps in for both devices.

The two following steps add extra sophistication:

- ① Open the configuration of the device in *ELSA LANconfig* by double-clicking the entry on the device list and select the 'Telephony' configuration area.
- ② In sequence, open the settings for the a/b ports to which the telephones are attached. For each one, activate the option on the 'Availability' tab that permits main and secondary channels to be disconnected. This ensures that the two employees in the office can always make telephone calls even if a download from the web with channel bundling is taking place or a data exchange with head office is scheduled.

- ③ For the port the fax device is attached to you should configure the availability options such that only secondary channels may be disconnected. In this office, faxing is more important than fast data transfers, but access to the Internet should not be ruled out completely if lengthy tenders are being transferred by fax. The faxes can wait a little.
- ④ Another setting for the fax device: On the 'Public exchange access' tab, enable access to an outside line once the receiver is lifted. The fax does not require any internal telephony so the call numbers entered should be dialed directly on an outside line.
- ⑤ This concludes the settings to be configured on the *LANCOM 2000 Office*. Now you only have to take care of call forwarding to the cell phones when the engineers are outside the office. The calls should be forwarded immediately so that the caller does not have to wait unnecessarily.
 - Lift the receiver of the telephone for which you want to forward calls.
 - Press, for example, . Now all calls will be forwarded to the desired telephone number.
 - When you return to the office, lift the receiver and press . This cancels the call forwarding command.



Step by step PBX

If you cannot use the *ELSA LANconfig* configuration tool, you can achieve the same results by configuring the device via telnet (or a terminal program) using the following commands:

Menu	Parameter	Comment or value
Setup/ab-module/ Port-list	Port	Number of port for which the following parameters are valid.
	Device	Type of device attached, e.g. telephone or fax
	Capab.	Detection of capabilities on this port
	Mode	Port behavior for incoming calls
	CLIP	Report own telephone number to remote site
	Example	'set 1 phone 123456 speech 3 YES' 'set 2 phone 123457 speech 3 YES' 'set 3 fax 123458 speech 0 YES' 'set 4 answ-mach. 123456;123457 speech 16 YES'
Setup/ab-module/ Public-exchange-list	Offhook-line	Action when receiver lifted
	Flash-line	Action when flash button pressed
	Example	'set 3 private intern' sets the fax port such that a zero does not have to be dialed first

Menu	Parameter	Comment or value
Setup/ab-module/ Priority-list	Prio-out	Availability of the port if the router is occupying a channel.
	Example	'set 1 3' allows the telephone to disconnect main or secondary channels of the router. 'set 3 2' allows the fax to disconnect secondary channels of the router.

The least-cost router

Of course, the office in this chapter's example also needs to make connections as cheaply as possible when telephoning, faxing, accessing the Internet or exchanging data with head office. The least-cost router which automatically searches for the cheapest connection for every call, is used for this purpose. You will find information about rates in magazines, brochures or on the Internet, for example.

Our example office is located in Aachen and it has a telephone account with the Deutsche Telekom. The following entries on the least-cost router have been compiled according to these local circumstances and based on information on zones and rates from the Internet.



Please note that you cannot necessarily apply these entries to different situations, they should only serve as an example.



Configuring the least-cost router with the **ELSA LANconfig**

With the following steps you can turn your *ELSA LANCOM Office* router into a bargain hunter:

- ① Open up the configuration of the device in *ELSA LANconfig* by double-clicking the entry in the device list and select the 'least-cost router' configuration area.
- ② On the 'General' tab activate the LCR function for all operating modes provided. Because the office does not require any call charge monitoring, the use of the LCR for the router module is not a problem.
- ③ Edit the public holiday table on the 'Time periods and public holidays' tab.
 - First enter any annually recurring holidays by supplying the day and month but not the year. These entries will be set automatically each year.
 - Then enter the variable holidays by supplying the day, month and year. It is best to enter them for the next two or three years while you are at it.
- ④ Now we get to the core of the matter: The entries in the LCR table. For some entries there are several network codes. These are dialed in sequence if the previously dialed numbers are engaged. To ensure that a connection can, however, always be established quickly, an automatic fallback number is enabled (in this case Deutsche Telekom) for all entries.

First create the entries for calls to cellular networks:

Prefix	Call-by-call number	Days	Time	Fallback
0161	01049;01079	Mon - Fri	0:00 am - 8:59 am	YES
0161	01028	Mon - Fri	9:00 am - 5:59 pm	YES

Prefix	Call-by-call number	Days	Time	Fallback
0161	01049;01079	Mon - Fri	6:00 pm - 11:59 pm	YES
0161	01049;01079	Sat, Sun, Public holidays	0:00 am - 12:59 pm	YES
017	01049;01079	Mon - Fri	0:00 am - 8:59 am	YES
017	01028	Mon - Fri	9:00 am - 5:59 pm	YES
017	01049;01079	Mon - Fri	6:00 pm - 11:59 pm	YES
017	01049;01079	Sat, Sun, Public holidays	0:00 am - 11:59 pm	YES

By this example, you can already see how you can make your life easy when making entries in the table: The entry '017' stands for the D1 , D2 and E network!

- ⑤ National calls are next. With this entry you can divert all national calls to another provider, depending on the time of day they are made:

Prefix	Call-by-call number	Days	Time	Fallback
0	01015	Mon - Fri	0:00 am - 1:59 am	YES
0	01033	Mon - Fri	2:00 am - 4:59 am	YES
0	01015	Mon - Fri	5:00 am - 7:59 am	YES
0	01050	Mon - Fri	8:00 am - 8:59 am	YES
0	01028	Mon - Fri	9:00 am - 5:59 pm	YES
0	01015	Mon - Fri	6:00 pm - 11:59 pm	YES
0	01015	Sat, Sun, Public holidays	0:00 am - 7:59 am	YES
0	01050	Sat, Sun, Public holidays	8:00 am - 8:59 am	YES
0	01013;01090	Sat, Sun, Public holidays	8:00 am - 8:59 pm	YES
0	01015	Sat, Sun, Public holidays	9:00 pm - 11:59 pm	YES

- ⑥ International calls are relatively rare. In this example, therefore, just one entry applies to all international connections:

Prefix	Call-by-call number	Days	Time	Fallback
00	01015;01028	All days	0:00 am - 11:59 pm	YES

- ⑦ You may be able to dial some of the exchanges near you at the local rate even though a prefix is required. These calls should not be interpreted as national calls and redirected, they are therefore “retrieved” by leaving the network code blank. The office in the example is situated in Aachen. On the Internet, the employees have found out which exchanges belong to the local zone. The following entries are now added:

Prefix	Call-by-call number	Days	Time	Fallback
02408		All days	0:00 am - 11:59 pm	YES
02464		All days	0:00 am - 11:59 pm	YES
02404		All days	0:00 am - 11:59 pm	YES
02401		All days	0:00 am - 11:59 pm	YES
02403		All days	0:00 am - 11:59 pm	YES
02454		All days	0:00 am - 11:59 pm	YES
02451		All days	0:00 am - 11:59 pm	YES
02406		All days	0:00 am - 11:59 pm	YES
02407		All days	0:00 am - 11:59 pm	YES
02429		All days	0:00 am - 11:59 pm	YES
02465		All days	0:00 am - 11:59 pm	YES
02423		All days	0:00 am - 11:59 pm	YES
02471		All days	0:00 am - 11:59 pm	YES
02456		All days	0:00 am - 11:59 pm	YES
02473		All days	0:00 am - 11:59 pm	YES
02409		All days	0:00 am - 11:59 pm	YES
02402		All days	0:00 am - 11:59 pm	YES
02405		All days	0:00 am - 11:59 pm	YES

After completing the first entry you can simply copy it and just change the prefix for each entry.

- ⑧ Some special telephone numbers can also be exempted from redirection, e.g. '0130', '0180', '0190' and '0800':

Prefix	Call-by-call number	Days	Time	Fallback
01		All days	0:00 am - 11:59 pm	YES
0800		All days	0:00 am - 11:59 pm	YES

- ⑨ That's it! Now you have configured your least-cost router very precisely. Initially, you can use *ELSA LANmonitor* to check if the LCR is doing its job properly and keep

an eye on your telephone bill at the end of the month. You may find some additional prefixes you could add to the LCR table if you receive itemized bills.



Step by step least-cost router

If you cannot use the *ELSA LANconfig* configuration tool, you can achieve the same results by configuring the device via telnet (or a terminal program) with the following commands:

Menu	Parameter	Comment or value
Setup/LCR-module	Router-usage	Activation of the LCR module for the individual operating modes.
	LANCAPI-usage	
	ab-port-usage	
	Example	'set router on' 'set lancapi on' 'set ab-port on'
Setup/LCR-module/ Timetable	Index	Complete index of the entries in the table.
	Prefix	Prefix to be redirected.
	Days	Validity of the entry for weekdays and holidays in the form of an 8-bit mask: Bit 0 stands for Monday, bit 7 for holidays. The entry '31' therefore indicates all weekdays, '192' stands for Sundays and holidays.
	Start	Time at which validity of entry on the defined days starts.
	Stop	Time at which validity of the entry on the defined days ends.
	Number-list	Network code of the call-by-call provider.
	Fallback	Automatic fallback to your own telephone company if all call-by-call numbers are engaged.
	Example	'set 1 02 31 1:00 11:59 01033;01090;01070 on' diverts all national calls in the '02' region between one and twelve o'clock to a provider with the network code '01033'. If this number is engaged, the network codes '01090' and '01070' are tried. If these are also not available the connection is directed to the regular telephone company.

Create all the entries in accordance with this example, using the tables in *ELSA LANconfig* as a reference.

Office communication

The examples in this section are intended to show you how quickly and easily you can use the *LANCOM 1000 Office* and *LANCOM 2000 Office* and the accompanying office communication software in practical applications.

The main focus will be on the *LANCOM Office* router's function as a fax and answering machine (e.g. with *ELSA RVS COM*) and telecontrol using LapLink for Windows.

Finally, you will be introduced to data transmission via EuroFileTransfer as well as mailbox and terminal program access using *ELSA-ZOC*.

In addition, please refer to the instructions for the installation and use of *ELSA LAN-CAPI* in the section entitled 'Office communication and LANCAPI' of the User Manual.

Faxing with <i>ELSA-RVS-COM</i>	2
Telephone and answering machine	4
Computer telcontrol with LapLink.....	5
EuroFileTransfer with <i>ELSA-RVS-COM</i>	6
Mailboxing with <i>ELSA-ZOC</i>	8

Faxing with *ELSA-RVS-COM*

With *ELSA LANCAPI*, the computers in the LAN can also be used as convenient fax machines for ISDN ports.

Sending a fax with *ELSA-RVS-COM*

When it was installed, *ELSA-RVS-COM* configured a special printer driver (RVS Fax) for your standard application programs (e.g. word processing) that will allow you to print your faxes. When you send a document to the printer, the Fax Assistant takes over its further transmission.

As an alternative, you can initiate fax transmission by clicking on the **Create new fax** button in the 'ELSA-RVS-COM' program group. In this case as well, the Fax Assistant takes charge of the further processing of the fax. It asks you to enter the recipient's name and call number and, further along in the process, offers to enter additional text and use a prepared cover sheet.

Before sending the fax, you can view it using the RVS FAXViewer. You then have the option of either sending the fax immediately or placing it in the Out Box if, for example, you wish to send a number of faxes at a later point in time.

Receiving a fax

There are basically two possibilities for receiving faxes:

- Another person would like to send you a fax.
- You would like to retrieve a prepared fax directly (fax polling).

In the first case, you simply need to switch on your fax machine (i.e. *ELSA-RVS-COM*) and wait for the incoming fax. Your computer is ready to receive faxes if you have configured fax reception using the *ELSA-RVS-COM* Installation Assistant and the ComCenter is started (also see communication software).

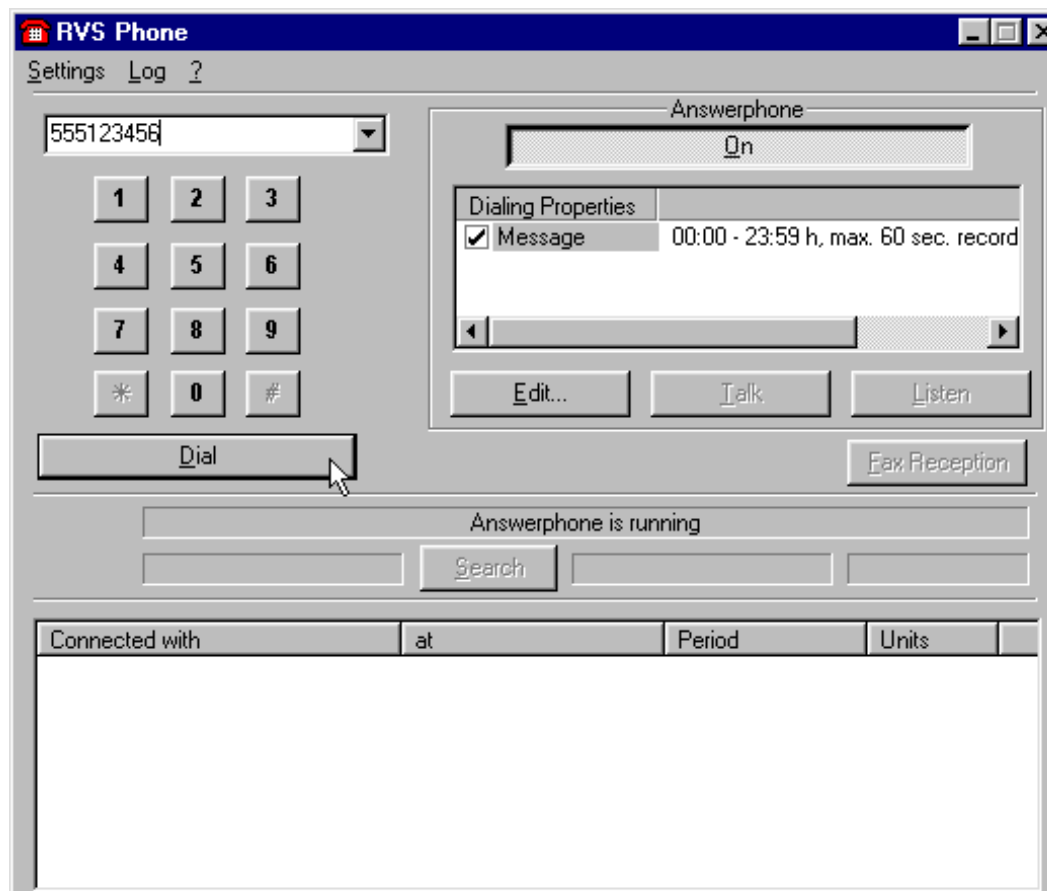
For fax polling, proceed as follows:

- ① Start the 'RVS Telephone' in the 'ELSA-RVS-COM' program group.
- ② Dial the call number of the fax machine from which you would like to retrieve the fax.
- ③ As soon as the connection is established, click the fax reception button.

The remote station's fax machine now transmits the fax to your computer. The call number of the other fax machine and the current connection time are displayed on the status line of the RVS telephone.

Telephone and answering machine

ELSA LANCAPI also allows you to use the computer in the LAN as a convenient ISDN telephone and answering machine.



This requires:

- Communication software with an answering machine function (e.g. *ELSA-RVS-COM*)
- A sound card with corresponding speakers
- A microphone for recording announcement texts

When installing *ELSA-RVS-COM*, enter a call number to which the answering machine (and thus the telephone as well) is to respond.

The following are some of the options that *ELSA-RVS-COM*'s answering machine offers you:

- Recording of several announcement and closing texts
- Management of different announcement texts by means of a schedule
- Definition of a maximum recording time per call



Your computer is not ready to receive telephone calls until you have started the ELSA-RVS ComCenter.

Computer telecontrol with LapLink

This Workshop will help you over the first hurdles you will encounter when using telecontrol with remote computers. As an example, we propose a computer that is set up in a company and that the company's field personnel and teleworkers can access. With the aid of LapLink, users who do not work directly on company premises can, for example, use special programs on the company's computer.

Establishing a connection

Using LapLink, you can link your computer to other computers using various means. Among your options is the 'network connection'. Since the *LANCOM Office* router also allows you, for example, to link the workstations of teleworkers and field personnel to the company's local network via TCP/IP, we would like to use this option in our example.

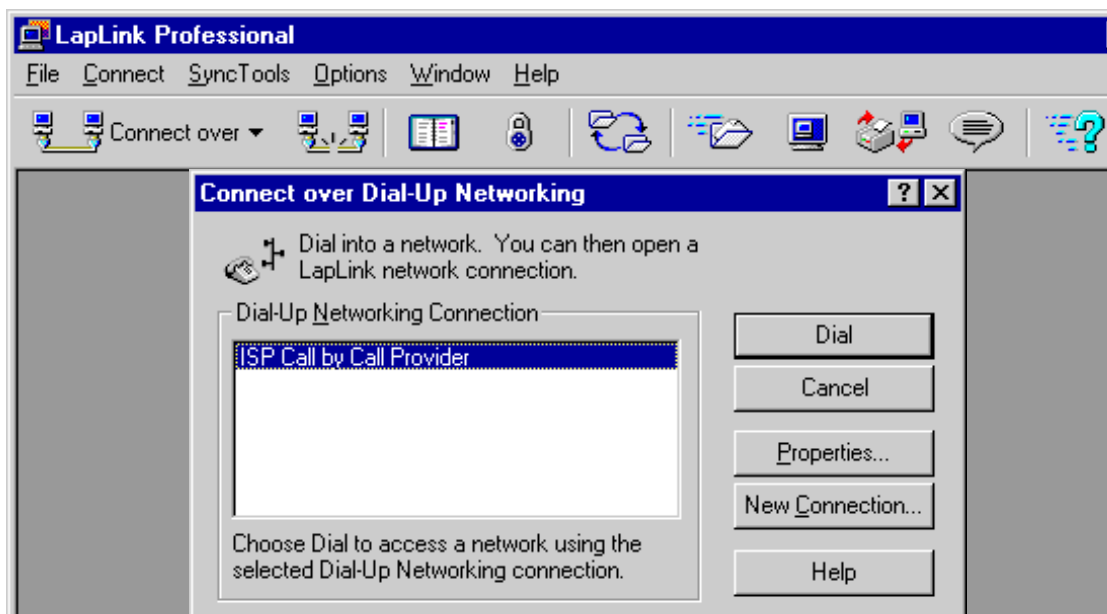
In addition to the existing TCP/IP connection between the remote computer and the LAN, LapLink must be started on both of the participating computers.

Configuring a port

With the default installation, the port for network connections is immediately available for your use.

Initiating a connection

In order to set up this connection to another computer, simply click on the icon for the relevant connection type at the top of the LapLink window:



When connecting via the network you can, for example, specify an IP address and initiate the connection to this remote station.

EuroFileTransfer with *ELSA-RVS-COM*

The Transfer Master from *ELSA-RVS-COM* provides you with a very convenient option for transferring files from one PC to another via ISDN. It simply requires that the ready-to-receive state for EuroFileTransfer be activated on the other PC (e.g. with ComCenter from *ELSA-RVS-COM*).

Setting up EuroFileTransfer

In order to allow other users to access your computer via EuroFileTransfer, set up the access in the *ELSA-RVS-COM* ComCenter by making a few entries.

- ① Activate the ready-to-receive state in the properties for the ISDN port and select the call number to which EuroFileTransfer is to respond.
- ② On the 'Mailbox' card, define a user name and password and select the directory to be open to this user. The user can then read all the files in this directory and in all subdirectories as well as write to them (if the appropriate option has been activated).
- ③ Deactivate the guest access.

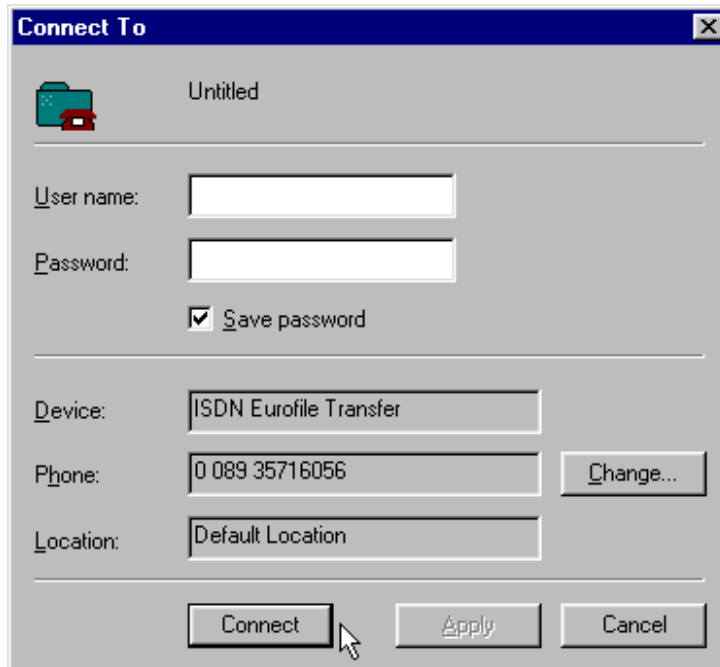
As long as the ComCenter is activated, your computer is ready for EuroFileTransfer.

Transferring files with EuroFileTransfer

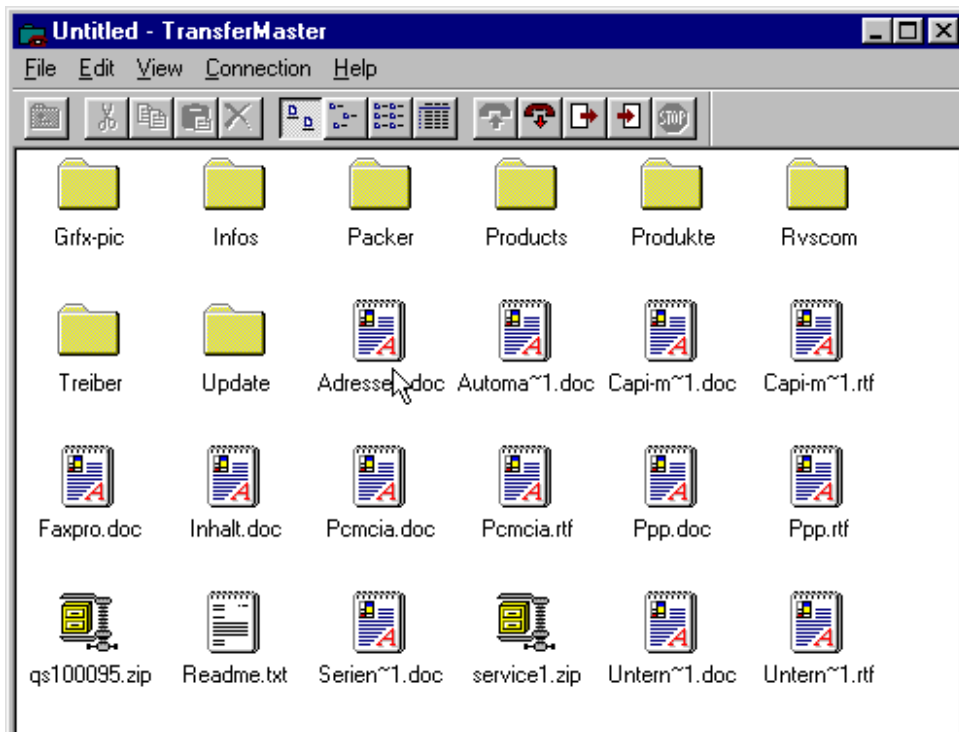
To transfer files from your computer to another (or vice versa), proceed as follows:

- ① Start the TransferMaster by double-clicking the appropriate icon.
- ② Open a folder (e.g. RVS Mailbox: ISDN Eurofile) or a saved connection, or open a window for a new remote station by selecting **Connection ► Connect**.

- ③ If appropriate, enter the user name (none) and password (none) as well as the call number for the remote station (default setting) and click **Connect**.



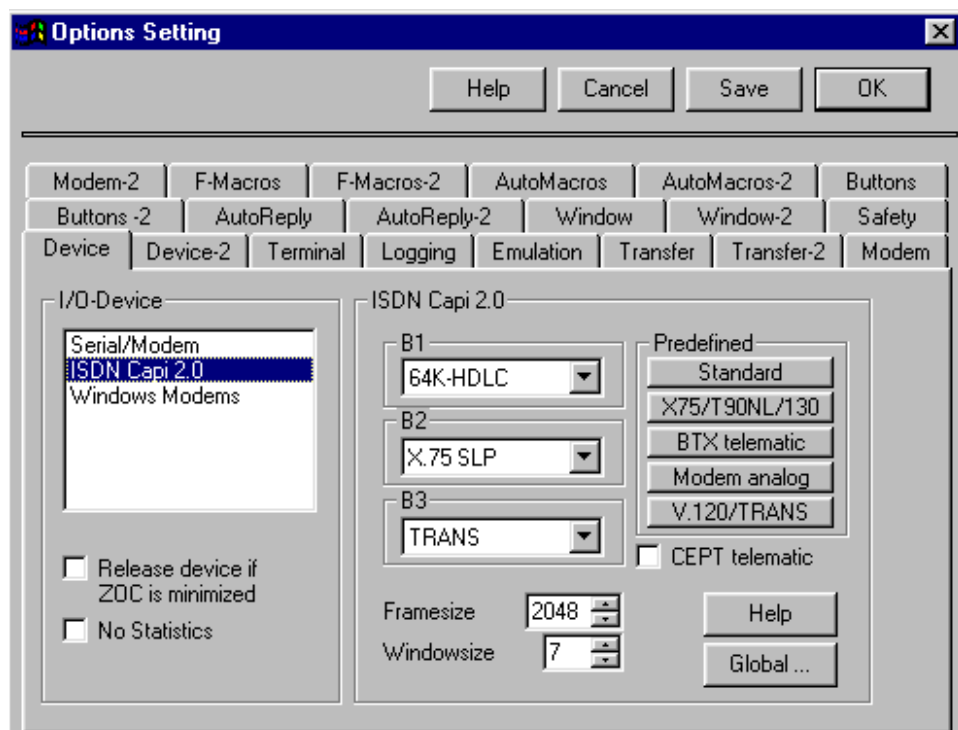
- ④ Once the connection has been successfully established, the files on the other computer are available to you as an additional folder on your own computer. You can now transfer files between the two computers in either direction by dragging and dropping them. You can also open files on the other computer, provided that the relevant application is installed on your own computer.



Mailboxing with *ELSA-ZOC*

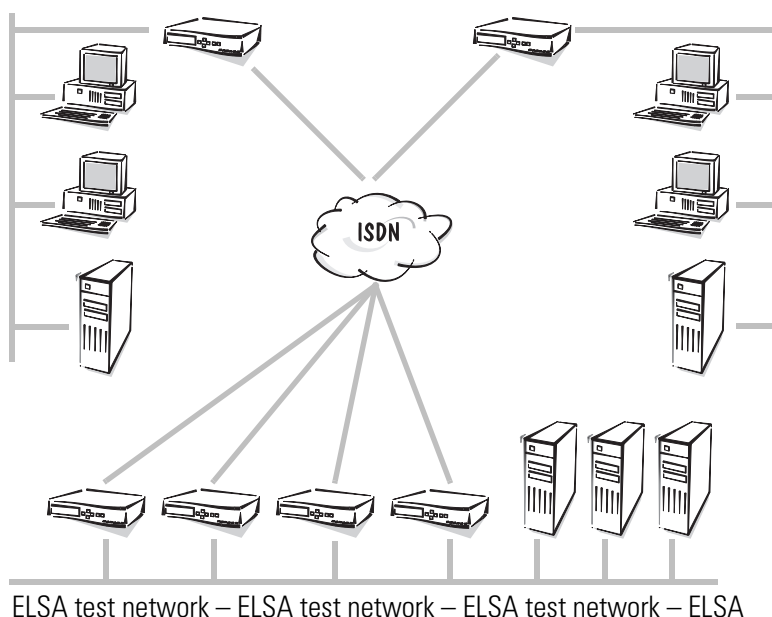
In the default configuration, *ELSA-ZOC* is set up so that you can immediately initiate your first connection on most systems.

- ① Start *ELSA-ZOC* by selecting the appropriate entry from the Windows Start menu.
- ② From the menu line under 'Options', click the 'Settings' entry. This window displays the settings for the transmission devices used (modems, etc.) and all program-specific parameters.



Under the 'Device' tab, 'ISDN CAPI 2.0' is already selected with the default settings; your *LANCOM* is instantly ready for its first file transfer via *ELSA LANCAPI*.

- ③ From the 'Device' entry on the menu line, start 'Manual Dialing...'. Enter the call number of the relevant mailbox in its entirety, including the exchange code (e.g. 0 for many PBXs), country code and local area code and click **OK**. Within a few seconds, you are greeted by the initial page of the mailbox.



Access to the ELSA test network

The ELSA test network offers you a simple and easy means of testing that your *LANCOM Office* router is functioning and that your configurations are correct. The ELSA test network is a small local area network with several *LANCOM Office* routers and terminal adapters which have been pre-configured for specific tasks. You can use this equipment to test the operation of your *LANCOM Office* router as an IP or IPX router with both the ELSA protocol and PPP, for example. You can also test the transmission between two bridges or dialing in to a remote computer in a LAN.

The following examples will give you a full explanation of the specific settings you will need to enter in your *LANCOM Office* router (or a terminal adapter or ISDN card) to gain access the ELSA test network.

Each example is given based on the use of *ELSA LANconfig* for configuring. If using other tools such as Telnet for the configuration, you can make sense of the settings by analogy with the preceding configuration examples or with the aid of the extensive menu description in the Reference section of this Manual.

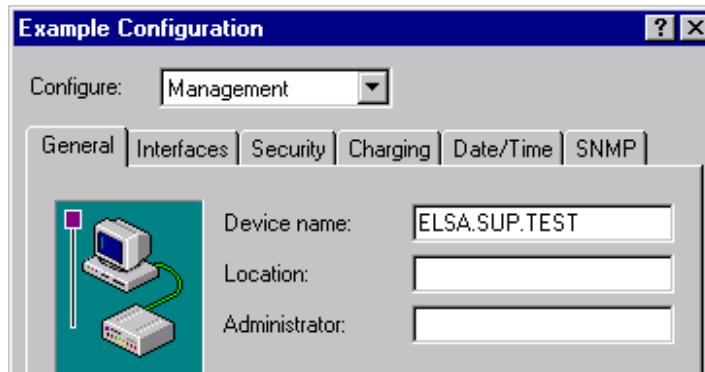
Router mode using PPP	3
Router mode using the ELSA protocol	8
Bridge mode	11



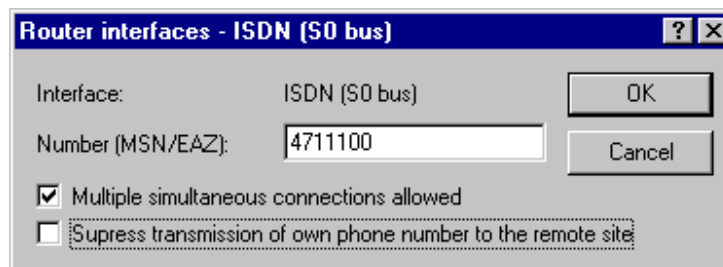
The examples are based on the LANCOM Office router in its factory settings. You should first save any settings you may have already entered and then carry out a system reset. You should also note that only those settings which are absolutely necessary to test the basic configuration and function of the devices are given here. Further settings to save on charges or improve performance in day-to-day use, for example, should be entered separately.

Router mode using PPP

- ① The *LANCOM Office* router must first be assigned a name which is recognized and accepted on the test network by the *LANCOM Office* router during protocol negotiation. This name **must** be entered as 'ELSA.SUP.TEST' exactly, otherwise access will be denied.



- ② Then, in the interface settings (configuration area 'Communication', 'General' tab) specify the call numbers for the ISDN connection you are using to run your *LANCOM Office* router:



- ③ In the name list, specify the device name of the *LANCOM Office* router on the test network and its associated call number. Modify the time-outs as shown here and select PPPHDLC as the layer:

Name list - New Entry

Name:

Phonenumber:

Short hold time: seconds

Short hold time (bundle): seconds

Layer name:

Automatic callback:
☒ No callback

OK Cancel

- ④ In the PPP list, select the newly created remote station and set PAP as the security procedure. The password 'test' will be replaced by several asterisks (*) when entered. The user name remains blank in this instance, which is why your *LANCOM*

Office router sends its device name to the *LANCOM Office* router on the test network during PPP negotiation.

PPP list - New Entry

Remote site: ELSA.SUP.3

Username:

Password: xxxx

Authentication of the remote site:

☐ No active authentication. However, the remote site (your Internet Service Provider for example) can do his own authentication.

☒ Authenticate the remote site via PAP.

☐ Authenticate the remote site via CHAP.

Time: 0

Retries: 5

Conf: 10

Fail: 5

Term: 2

OK Cancel

- ⑤ Only for IPX networks: Select the new remote station in the routing table (configuration area 'IPX/SPX', 'Routing' tab) supply a network number for the WAN and set the binding for the WAN to '802.3'.

Routing table - New Entry

Remote site: ELSA.SUP.3

Network: 0000FFFF

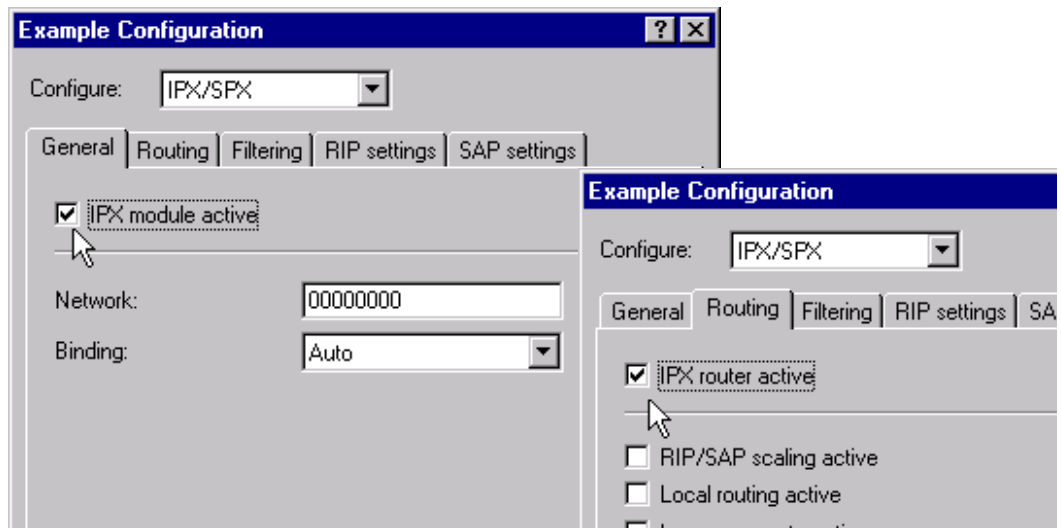
Binding: 802.3

Propagated: filter

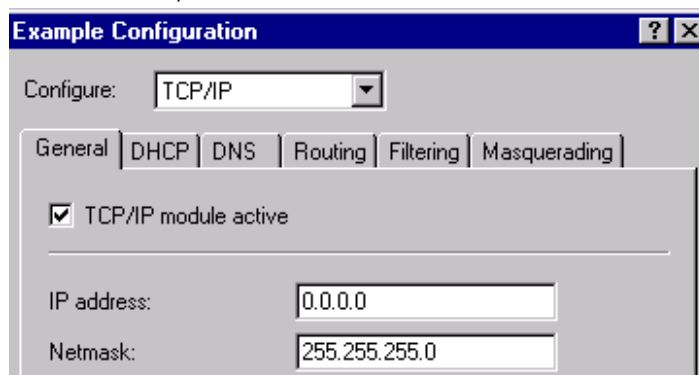
☒ Exponential backoff active

OK Cancel

- ⑥ Only for IPX networks: Setting the address of the LAN to '00000000' automatically selects the network with the highest occurrence of RIP and SAP packets. You should only switch on the IPX router once all the settings have been made.



- ⑦ Only for TCP/IP networks: Specify a free IP address from your LAN together with the associated network mask for the *LANCOM Office* router (configuration area 'TCP/IP', 'General' tab).



- ⑧ Only for TCP/IP networks: Now add a new entry to the routing table (configuration area 'TCP/IP', 'Routing' tab) specifying the addresses given below, the new remote station as the router and the distance as 2.

Routing table - New Entry

IP address: 223.254.245.0

Netmask: 255.255.255.0

Router: ELSA.SUP.3

Distance: 2

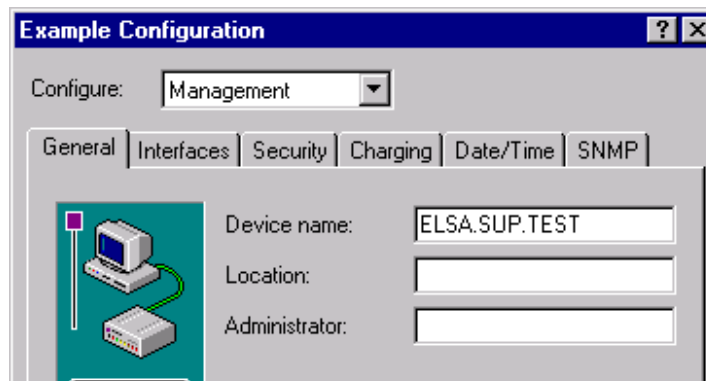
IP masquerading:
☒ IP Masquerading switched off

OK Cancel

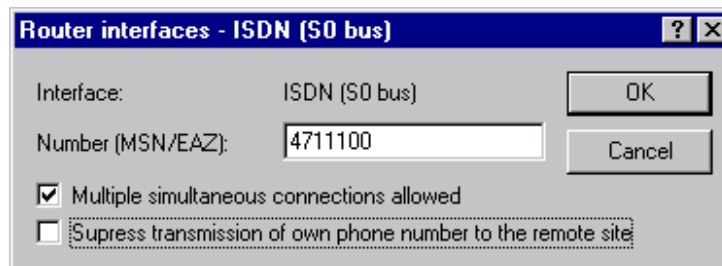
- ⑨ This concludes configuration for routing to the ELSA test network using PPP. You now have the means to access the server on the test network through appropriate settings on the workstation computers in your LAN. The user name should be 'Guest' and the password 'test'.

Router mode using the ELSA protocol

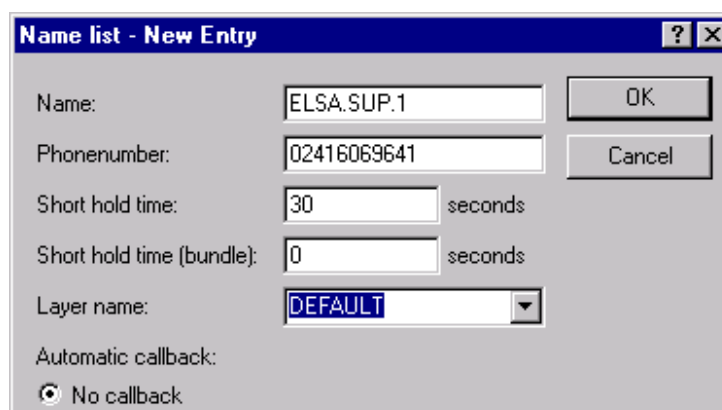
- ① The *LANCOM Office* router must first be assigned a name which is recognized and accepted on the test network by the *LANCOM Office* router during protocol negotiation. This name **must** be entered as 'ELSA.SUP.TEST' exactly, otherwise access will be denied.



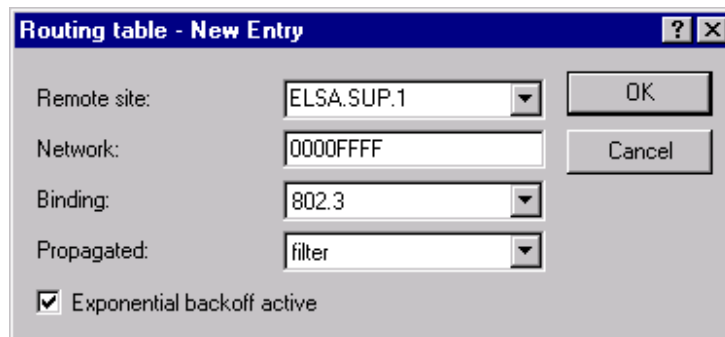
- ② Then, in the interface settings (configuration area 'Communication', 'General' tab) specify the call numbers for the ISDN connection you are using to run your *LANCOM Office* router:



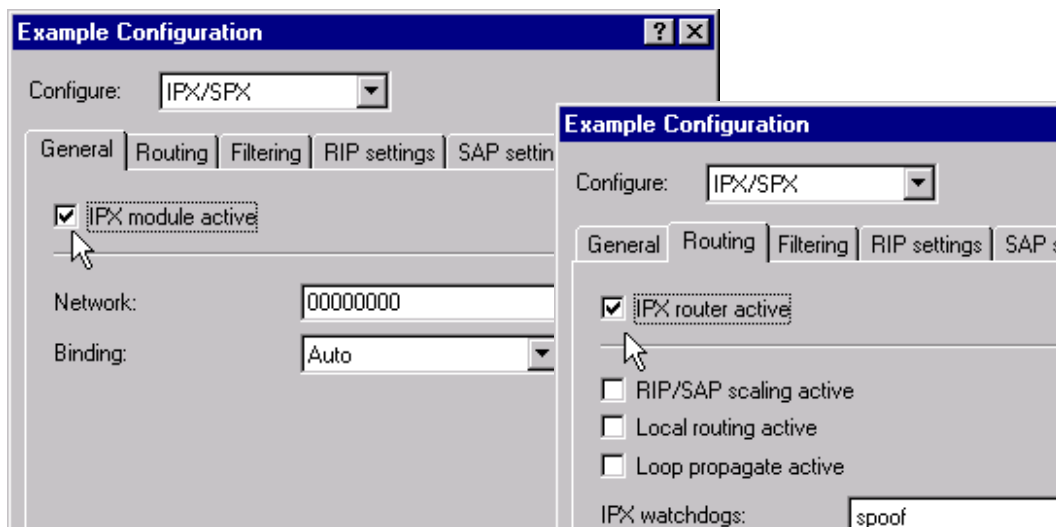
- ③ In the name list, specify the device name of the *LANCOM Office* router on the test network and its associated call number. Modify the time-outs as shown here and select DEFAULT as the layer:



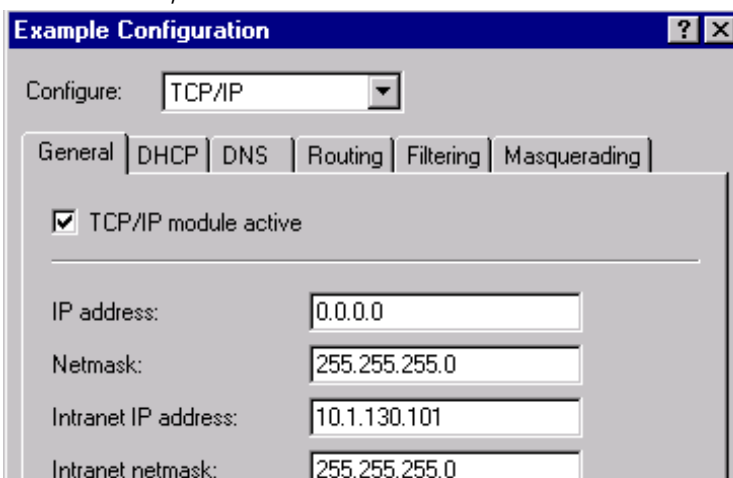
- ④ Only for IPX networks: Select the new remote station in the routing table (configuration area 'IPX/SPX', 'Routing' tab), assign a network number for the WAN (0000FFFF) and accept '802.3' as binding for the WAN.



- ⑤ Only for IPX networks: Setting the address of the LAN to '00000000' automatically selects the network with the highest occurrence of RIP and SAP packets. You should only switch on the IPX router once all the settings have been made if you are using Telnet or a serial connection for configuration.



- ⑥ Only for TCP/IP networks: Specify a free IP address from your LAN together with the associated network mask for the LANCOM Office router (configuration area 'TCP/IP', 'General' tab).



- ⑦ Only for TCP/IP networks: Now add a new entry to the routing table (configuration area 'TCP/IP', 'Routing' tab) specifying the addresses given below, the new remote station as the router and the distance as 2.

Routing table - New Entry

IP address: 223.254.245.0

Netmask: 255.255.255.0

Router: ELSA.SUP.1

Distance: 2

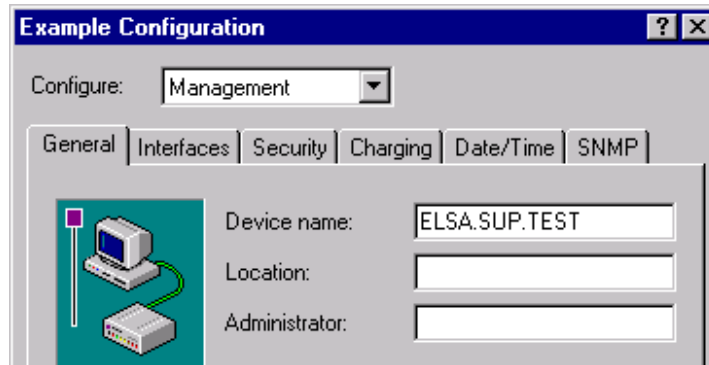
IP masquerading:
☒ IP Masquerading switched off

OK Cancel

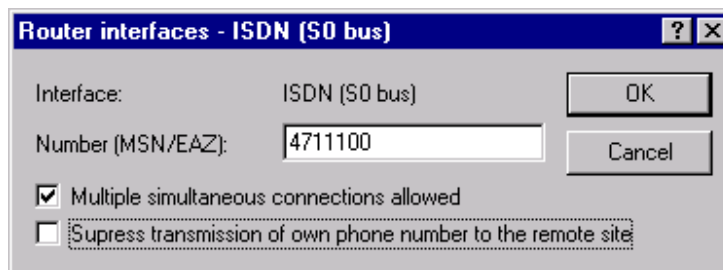
- ⑧ This concludes configuration for routing to the ELSA test network using the ELSA protocol. You now have the means to access the server on the test network through appropriate settings on the workstation computers in your LAN. The user name should be 'Guest' and the password 'test'.

Bridge mode

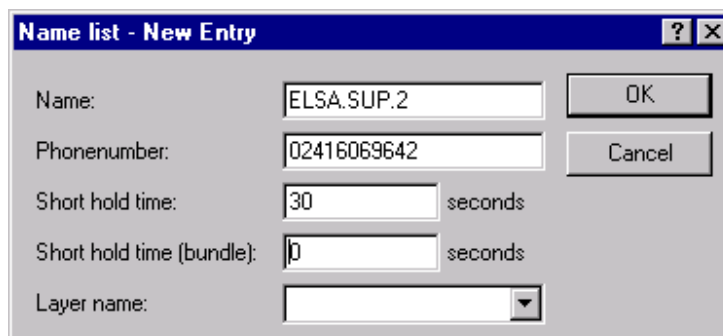
- ① The *LANCOM Office* router must first be assigned a name. A name is optional for bridge mode since it will not be sent to the *LANCOM Office* router on the test network.



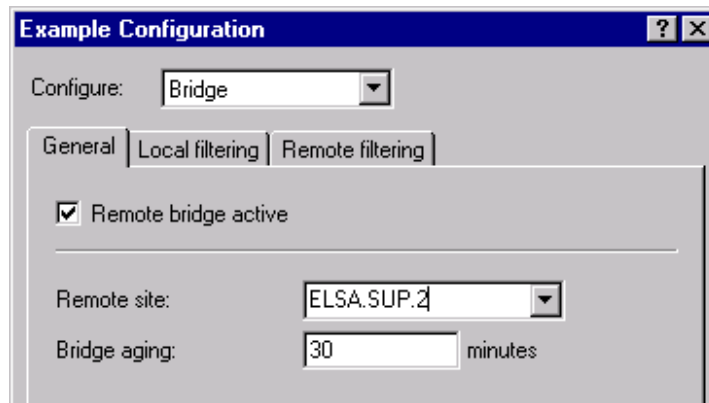
- ② Then, in the interface settings (configuration area 'Communication', 'General' tab) specify the call numbers for the ISDN connection you are using to run your *LANCOM Office* router:



- ③ In the name list, specify the device name of the *LANCOM Office* router on the test network and its associated call number. Modify the time-outs as shown here and select DEFAULT as the layer:



- ④ Disable the IP router (configuration area 'TCP/IP', 'Routing' tab)! Select the newly created remote station (configuration area 'Bridge', register 'General'), and activate the bridge:



Error Search

It is quite simple to set the configuration for many basic applications of the *LANCOM Office* router. *ELSA LAN-config* with its assistants also takes over some of the work for users of Windows 95 and Windows NT 4.0.

In spite of this, unwanted results can occur, particularly with more elaborate settings.

This chapter describes the systematic error search with the trace outputs and the statistics of the *LANCOM Office* router in somewhat more detail.

Three examples are used to show how the causes of failed attempts to establish a connection to the Internet provider, difficulties in contacting another network and undesired call origination can be found.

The Search Methods.....	2
No Connection to the Internet	3
Computer in the other Network Cannot Be Reached	4
Unwanted Call Origination	6

The Search Methods

The results of an erroneous configuration can usually be assigned to one of the three following groups:

- A connection to the network at the remote station is not established.
- A connection is established, but the expected computer or services in the network at the remote station are not visible or cannot be reached.
- The connection to the network at the remote station functions as expected, but connections are established far too often (resulting in high telephone charges).

The *LANCOM Office* router offers various possible ways of finding the causes of the unwanted behavior:

- The statistics can show everything that has occurred in your *LANCOM Office* router in the individual areas. For example, the connection statistics can show how many connections have been established on the B channels of your *LANCOM Office* router. Another example: The structure table in the router and bridge statistics shows information from what source addresses to what target addresses the last data packets (with IP data packets e.g. with details of the port numbers) were sent.
- To check what exactly is happening at the moment in the *LANCOM Office* router, use the trace outputs. In this way the actions during, for example, the PPP negotiation can be followed online. Or find with what remote station the *LANCOM Office* router wants to establish a connection permanently.



Continuing display of the trace outputs reduces the performance of the LANCOM Office router. Activate the traces only for specific diagnosis purposes for a limited time.

- For IP routing the command `ping` is also available. This enables a check of whether the corresponding remote station can even be reached with the current *LANCOM Office* router settings.

The prerequisite for error searching is a functioning connection to the local *LANCOM Office* router via telnet or a terminal program.

The *ELSA MicroLink LANCOM MPR* enables the statistics to be additionally queried on the display or a manual call origination to be started with the keypad.

No Connection to the Internet

The *LANCOM Office* router has been configured for access to the Internet. For this purpose a connection to the Internet service provider must be established and PPP used as protocol for the connection. The workstations are set appropriately. In spite of that the browser cannot access the WWW.

The following procedure can be used to find the error:

- ① First test whether the *LANCOM Office* router in the local network can be reached. For this purpose enter e.g. in the command line of a DOS window the following command:

```
ping 10.1.1.99
```

In this case, '10.1.1.99' is the IP or Intranet address of the *LANCOM Office* router.

- ② If the *LANCOM Office* router responds to this request, try to establish a connection to the ISP manually, e.g. with the command:

```
do /other/manual/establish internet
```

The name of the remote station (here e.g. 'internet') can be taken from the name list.

The device should then dial. Watch the display or activate the trace function for the display so all display outputs will also be shown on the terminal connection:

```
trace + display
```

If the connection was successful, the name of the remote station will appear on the display. Otherwise an error message will be output, which will already provide information on the error source, e.g.:

- 'ISDN layer 1' usually means that there is no connection to the ISDN terminal.
- 'CHAP Tx timeout' shows an error in the PPP negotiation.

In addition, the status menu also has information on the reason for the failure of the connection (e.g. `dir /status/info connection`).

- ③ If an error in the PPP negotiation is suspected, this command

```
trace + ppp
```

can activate the trace outputs during the negotiation. After a (manual) call origination the individual steps and phases of the point-to-point protocol can be followed. Ensure that the buffer storage of your terminal program is large enough to display all steps of the negotiation.

There is a description of the trace outputs in the Reference Manual of your *LANCOM Office* router.

Computer in the other Network Cannot Be Reached

The *LANCOM Office* router is configured for a network coupling via TCP/IP or IPX or for the access to the Internet.

The connection was correctly established, but addresses from the remote network cannot be reached.

Error Search in TCP/IP Networks

Go step by step to isolate the error. First test whether the *LANCOM Office* router in your LAN can be reached, then the establishment of a connection between the *LANCOM Office* router routers over the ISDN and finally the data transmission between two workstations in the remote networks.

- ① First test whether the *LANCOM Office* router in the local network can be reached. For this purpose enter e.g. in the command line of a DOS window the following command:

```
ping 10.100.1.99
```

Here '10.100.1.99' is the IP or Intranet address of the *LANCOM Office* router in the local network.

- ② If the *LANCOM Office* router in your own network responds to this request, you can check whether the *LANCOM Office* router in the remote network can be reached. For this purpose enter e.g. in the command line of a DOS window the following command:

```
ping 10.200.1.99
```

Here '10.200.1.99' is the IP address of the *LANCOM Office* router in the remote network.

- ③ If this test is successful, attempt to address a workstation in the network at the remote station:

```
ping 10.200.1.50
```

Here '10.200.1.50' is the IP address of the workstation in the remote network.

- ④ The ping commands in the first three steps enable the availability in the TCP/IP network to be checked. If one of these ping requests fails (the response is then 'request timed out'), the function of the IP router can be tested with the IP router trace in the *LANCOM Office* router. Start a telnet session to the *LANCOM Office* router and enter this command in the *LANCOM Office* router configuration menu

```
trace + ip-rt
```

- ⑤ Then repeat the ping commands and see how the data packets from the IP router in the *LANCOM Office* router are handled.

If the routing functions correctly, packets should be received from the LAN ('LAN-Rx') and sent via ISDN ('WAN-Tx') and vice versa.

Pings to the *LANCOM Office* router directly are flagged as 'internal Rx' or 'internal Tx' in the trace outputs.

- ⑥ If expected trace outputs are missing or are rejected with other details as 'route', check the entries in the IP routing table of the associated *LANCOM Office* router. Sometimes important routes are missing, or ZERO routes (router name 0.0.0.0) prevent correct routing.
- ⑦ A typical error is also erroneous configuration of the gateway address in the workstations. In the LAN every workstation needs to know that the *LANCOM Office* router is the standard gateway or there must be a (standard) route to the *LANCOM Office* router present.

Error Search in IPX Networks

If servers and services on the remote network are not visible, the RIP and SAP tables of the *LANCOM Office* router should be checked first. After the IPX router has been activated, it attempts to get the information from the remote side.

- ① Check the RIP tables in the status menu:

```
Dir Status/IPX-statistics/RIP-statistics/table-RIP
```

Here network numbers of the local and remote IPX networks should be listed.

- ② Check the SAP tables in the status menu:

```
Dir Status/IPX-statistics/SAP-statistics/table-SAP
```

Here services and servers in the local and remote IPX networks should be listed.

- ③ If the RIP and SAP information at the remote station is not found in the corresponding table, check the configuration of the IPX router in the *LANCOM Office* router.
- ④ The trace function

```
trace + IPX-Rt
```

can be used to check the correct operation of the IPX router.

Unwanted Call Origination

Your *LANCOM Office* router has been configured for the proposed application as desired. The router operates correctly now, but establishes too many connections. There are various possibilities for finding the cause of unwanted call origination in the *LANCOM Office* router.

- ① Check for an unwanted call origination in the corresponding structure table.

For TCP/IP this is found e.g. under

```
/Status/IP-router-stat./Establish-table.
```

The cause in the local network can easily be found with the addresses and port numbers.

For IPX the structure table can be found under

```
/Status/IP-router-stat./Establish-table
```

or by using the bridge under

```
/Status/Bridge-statistics/Establish-table.
```

- ② Activate the router trace

```
trace + IP-Rt or trace + IPX-Rt
```

to record the operation of the router.

Description of the menu options

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

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

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

Some of the features described in this Reference Manual apply only to specific models in the *ELSA LANCOM Office* router family. Restrictions with relation to the particular models are indicated by the symbols in the margin.







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

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




















































Status.....	3
Setup.....	34
Firmware	82
Other	84



Symbols

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

Overview of the menus






















	Setup			Status
	Name			Connection
	WAN-module			Current-time (<i>LANCOM Office</i> router only)
	Charges-module			Operating-time
	LAN-module			S ₀ -bus
	Bridge-module			WAN-statistics
	IPX-module			LAN-statistics
	TCP-IP-module			PPP-statistics
	IP-router-module			Bridge-statistics
	SNMP-module			IPX-statistics
	DHCP-module (<i>LANCOM Office</i> router only)			TCP-IP-statistics
	Config-module			IP-router-statistics
	Miscellaneous (<i>ELSA MicroLink LANCOM MPR</i> only)			Config-statistics
	AB-module (<i>LANCOM Office</i> router only)			Queue-statistics (<i>LANCOM Office</i> router only)
	LANCAPI-module (<i>LANCOM Office</i> router)			Connections-statistics
	LCR-module (<i>LANCOM Office</i> router only)			Info-connection
	Time-module (<i>LANCOM Office</i> router only)			Layer-connection
	Firmware			Call-info-table
	Version-table			Remote-statistics
	Firmware-upload			Channel-statistics (<i>LANCOM Office</i> router only)
	Table-firmsafe (<i>LANCOM Office</i> router only)			Time-statistics (<i>LANCOM Office</i> router only)
	Mode-firmsafe (<i>LANCOM Office</i> router only)			Delete-values
	Timeout-firmsafe (<i>LANCOM Office</i> router only)			Other
	Test-firmware (<i>LANCOM Office</i> router only)			Manual-dialing
				Reset-system
				Boot-system
				System-upload

Status

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

Most status displays on the display (*ELSA MicroLink LANCOM MPR* only) or in the configuration status menu of all *ELSA LANCOM Office* routers are continually updated and can be deleted with a **value** or set to 0 in the current menu.


The menu has the following layout:

Status		Running status displays
Connection-state		Status of the WAN route
Current-time		Current time in device
Operating-time		Period of time the device has operated since it was last switched on
S ₀ -bus		Status of the S ₀ interface
WAN-statistics		Displays WAN statistics
LAN-statistics		Displays LAN statistics
PPP-statistics		Displays LAN statistics
Bridge-statistics		Bridge area statistics
IPX-statistics		Statistics from the IPX and IPX router area
TCP-IP-statistics		Statistics from the TCP/IP area
IP-router-statistics		Statistics from the IP router
Config-statistics		Remote configuration statistics
Queue-statistics		Statistics relating to the packets in the queues of the individual modules (<i>LANCOM Office</i> routers only)
Conn.-statistics		Connection information for each interface
Info-connection		Information on the last connection for each interface
Layer-connection		Information on the B-channel protocol used for each interface
Call-info-table		Information on the last 10 calls received
Remote-stat.		Statistics on the last 10 connections
Channel-statistics		Information of the status of the individual B channels. Also information on the a/b ports with <i>LANCOM 2000 Office</i> .
Time-statistics		Time module information
Delete-values		Deletes all values except tables with substatistics.



Status/Connection-state

The **Status/Connection-state** menu option displays the status messages for the individual channels, which also appear in the *ELSA MicroLink LANCOM MPR* display

/Connection-state	Running status displays
Connection-state	 CH01: Ready; CH02: Ready

The system distinguishes among the following states (shown in the *ELSA MicroLink LANCOM MPR* display):

Ch01: Ready Ch02: Ready	No data is being transmitted.
Ch01: xxxxxx-> Ch02: Ready	The call number xxxxxx... is being dialed via the first B channel.
Ch01: Incoming call Ch02: Ready	A call is pending on the first B channel.
Ch01: Protocol Ch02: Ready	The connection protocol is being exchanged on the first B channel.
Ch01: Remote station name Ch02: Ready	An active connection exists to the remote station "remote station name" on the first B channel.
Ch01: Remote stn. name/2 Ch02: Bundle-connect	An active connection exists to the remote station "remote station name" with channel bundling.
Ch01: Disconnecting Ch02: Ready	The connection on the first B channel is being disconnected.
Ch01: Callback Ch02: Ready	The remote terminal is being called back.
Ch01: Establ. D64S Ch02: Reserved	A group 0 dedicated line is being connected.
Ch01: Establ. S01/02 Ch02: Bundle-connect	A group 2 dedicated line is being connected.

This option also allows you to display errors that can occur during a connection attempt. So far, the following displays have been defined:

Ch01: Protocol error Ch02: Ready	Protocol negotiation could not be performed.
Ch01: Error message Ch02: Ready	An error has occurred in the ISDN network and, if possible, will be displayed in plain text.



Sometimes an error message is issued in the form of two three-digit numbers (e.g. generated by your PBX) which, as internal system error codes, cannot be translated into plain text by the LANCOM Office router.



Status/Current-time

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

Status/Operating-time

This option allows you to display the router's operating time since it was last switched on as a number of years, months, days, hours, minutes and seconds.

Status/S₀-bus

This option allows you to display the current status of the S₀ interface. The statistics have the following layout:



/S ₀ -bus	Running status displays	
Power		S ₀ bus power ('Yes' or 'No')
S ₀ -activation		Displays activation status ('Yes' or 'No')
TEI		TEI assigned ('Yes' or 'No')
Layer-2		Activation of layer 2 of the D channel ('Yes' or 'No')
Protocol		D-channel protocol. Either the protocol fixed in the interface table or the protocol detected in the 'Auto' settings at the ISDN terminal.
D2-statistics		Breakdown of the D-channel information for the B channels.



D2-statistics










The D2 statistics provide more detailed information on the B channels:

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

Status/WAN-statistics

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

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

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



Byte-transport-statistics

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

Ifc	CRx-bytes	Rx-bytes	Tx-bytes	CTx-bytes
Ch01	0	0	0	0
Ch02	0	0	0	0
Ser1	0	0	0	0



The serial interface entry applies to the ELSA MicroLink LANCOM MPR only!

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

Ifc	(Abbrev. for interface) designates the associated B channel. The possible values are: Ch01 (1st B channel), Ch02 (2nd B channel) and Ser1 (connection via the serial WAN interface on the ELSA MicroLink LANCOM MPR).
CRx-bytes	Number of bytes received (compressed)
Rx-bytes	Number of bytes received (uncompressed)
Tx-bytes	Number of bytes sent (uncompressed)
CTx-bytes	Number of bytes sent (compressed)

Packet-transport-statistics

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

lfc	Rx	Tx-total	Tx-normal	Tx-reliable	Tx-urgent
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0
Ser1	0	0	0	0	0



The serial interface entry applies to the ELSA MicroLink LANCOM MPR only!

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

lfc	(Abbrev. for interface) designates the associated B channel. The possible values are: Ch01 (1st B channel), Ch02 (2nd B channel) and Ser1 (connection over the serial WAN interface on the <i>ELSA MicroLink LANCOM MPR</i>).
Rx	Number of packets received
Tx-total	Number of packets sent (data and protocol packets)
Tx-normal	Number of normal data packets sent
Tx-reliable	Number of data packets transferred with secured handling
Tx-urgent	Number of data packets transferred with priority handling (urgent queue)

Error-statistics

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

lfc	Rx-l3-error	Rx-l2-error	Rx-l1-error	Tx-error	Stack-error
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0
Ser1	0	0	0	0	0



The serial interface entry applies to the ELSA MicroLink LANCOM MPR only!

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

lfc	Designates the associated B channel (also see Status/WAN-statistics).
Rx-l3-error	Number of layer-3 errors in data received (i.e., the protocol header of layer-3 is incorrect)
Rx-l2-error	Number of layer-2 errors in data received (i.e., similar to the layer-3 errors, e.g. defective PPP, X75UI or X75BUI header)
Rx-l1-error	Number of layer-1 errors in data received (i.e., similar to layer-3 errors, an error in the HDLC header)
Tx-error	Number of transmission errors that occurred while sending
Stack-error	Number of stack errors for data received. Stack errors are caused when frames are received that cannot be assigned to an internal processing procedure (IP/IPX router or bridge). (Examples might be AppleTalk, DECNet or NetBEUI frames.)

*Throughput-
statistics*

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












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

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

Ifc	(Abbrev. for interface) designates the associated B channel. The possible values are: Ch01 (1st B channel) and Ch02 (2nd B channel).
Rx/s current	Throughput on the channel in the last second in the receiving direction
Tx/s current	Throughput on the channel in the last second in the transmission direction
Rx/s average	Average throughput on the channel in the receiving direction
Tx/s average	Average throughput on the channel in the transmission direction

Status/LAN-statistics













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

/LAN-statistics	Running status displays	
LAN-rx-packets		Number of data packets received
LAN-tx-packets		Number of data packets sent
LAN-rx-errors		Number of data packets incorrectly received
LAN-tx-errors		Number of data packets incorrectly sent
LAN-stack-errors		Number of packets without a suitable receive module (bridge/router)
LAN-NIC-errors		Number of data packets discarded by the NIC
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
LAN-queue-errors		Number of packets discarded due to a lack of buffers
LAN-collisions		Number of collisions during a send procedure
Delete-values		Deletes LAN statistics

Status/PPP-statistics

Within the PPP statistics, the states of individual subprotocols of the PPP are managed separately for each interface. However, statistics relating to the frames transmitted for

individual subprotocols are maintained only in joint statistics. Consequently, the **Status/PPP-statistics** menu has the following layout:

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



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

PPP-phases

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

lfc	Phase to	LCP	IPXCP	IPCP	CCP (LANCOM Office router only)
Ch01	DEAD	Initial	Initial	Initial	Initial
Ch02	DEAD	Initial	Initial	Initial	Initial
Ser1	DEAD	Initial	Initial	Initial	



The serial interface entry applies to the ELSA MicroLink LANCOM MPR only!

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

lfc	Designates the associated B channel (also see Status/WAN-statistics).
Phase to	Indicates the current phase of the PPP. The possible values are DEAD , ESTABLISH , TERMINATE , AUTHENTIC and NETWORK .
LCP	Status of the 'Link Control Protocol' subprotocol. The possible values are: Initial , Starting , Stopping , Stopped , Closing , Closed , ReqSent , AckRcvd , AckSent and Opened .



IPCP	Similarly to 'LCP', displays the status of the 'IP Control Protocol' subprotocol.
IPXCP	Similarly to 'LCP', displays the status of the 'IPX Control Protocol' subprotocol.
CCP	Similarly to 'LCP', displays the status of the 'Compression Control Protocol' subprotocol.

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

Status/PPP-statistics/LCP-statistics

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

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

Status/PPP-statistics/PAP-statistics

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

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

Status/PPP-statistics/CHAP-statistics

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

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

Status/PPP-statistics/IPXCP-statistics

When IPX is used, the **IPXCP** (Internet Exchange Protocol Control Protocol) indicates the status of the protocol and the packets exchanged in the negotiation. Below is a detailed description of the meanings of the parameters for these statistics:

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

Status/PPP-statistics/IPCP-statistics

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

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

Tx-terminate-ack.	Number of terminate acknowledge packets sent for IPCP
Tx-code-reject	Number of code reject packets sent for IPCP
Delete-values	Deletes IPCP statistics.

Status/PPP-statistics/CBCP-statistics

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

Rx-request	Number of CBCP request packets received
Rx-discarded	Number of CBCP packets discarded
Rx-acknowledge	Number of CBCP acknowledge packets received
Tx-request	Number of CBCP request packets sent
Tx-response	Number of CBCP response packets sent
TX-acknowledge	Number of CBCP acknowledge packets sent
Request-discarded	Number of CBCP request packets discarded
Response-discarded	Number of CBCP response packets discarded
Ack.-discarded	Number of CBCP acknowledge packets discarded
Delete-values	Deletes IPCP statistics



Status/PPP-statistics/CCP-statistics

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

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

Tx-code-reject	Number of CCP queries rejected because the <i>LANCOM Office</i> router does not wish to use compression (by layer list settings).
Tx-reset-request	Number of CCP queries sent after synchronizing the compression (e.g. after transfer errors)
Tx-reset-ack.	Number of CCP confirmations sent for synchronizing the compression
Delete-values	Deletes CCP statistics.

Status/PPP-statistics/ML-statistics

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

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




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

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

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

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

The two submenus have the same layout:

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



The LCP table has separate listings for every channel:

MRU	M aximum R ecieve U nit designates the maximum packet size that the remote station can receive
ACCM	A synchronous C ontrol C haracter M ap designates the character in the asynchronous data flow that is interpreted as the control character
Auth.	Authentication procedure used (PAP/CHAP)
Call-back	Callback negotiation type

The IPXCP table shows the negotiated IPX option separately for every channel:

Network	Network number of the WAN network
Node-ID	The Rx options show the node ID assigned to the <i>LANCOM Office</i> router (generally 000000000000 or the MAC address of the router). The Tx options show the node ID of the remote station (also 000000000000 or the MAC address of the remote station)
Routing-method	The routing protocol in use is given here (RIP/SAP or nothing), in the Rx what the remote station has assigned to us and in the Tx the one that the <i>LANCOM Office</i> router assigns to the remote station.

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

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

Status/Bridge-statistics

This option allows you to display statistical information relating to the bridge. The bridge statistics contain the following parameters:

/Bridge-statistics	Running status displays	
Brg-LAN-rx	0	Number of data packets received from the LAN
Brg-LAN-tx	0	Number of data packets sent to the LAN
Brg-LAN-filters	0	Number of filtered data packets from the LAN
Brg-LAN-broadcasts	0	Number of broadcasts received from the LAN
Brg-LAN-multicasts	0	Number of multicasts received from the LAN
Brg-WAN-rx	0	Number of data packets received from the WAN
Brg-WAN-tx	0	Number of data packets sent to the WAN
Brg-WAN-filters	0	Number of filtered data packets from the WAN
Brg-WAN-broadcasts	0	Number of broadcasts received from the WAN
Brg-WAN-multicasts	0	Number of multicasts received from the WAN
Brg-addresses	0	Number of addresses currently known




/Bridge-statistics	Running status displays	
Table-bridge		Displays bridge filter table.
Establish-table		Table of the last 20 packets that required a connection
Delete-values		Deletes bridge statistics.

Table-bridge

The **bridge table** provides information on the MAC addresses known to the bridge, the time when the last packet was received from this device (specified in tics), and whether the relevant device is local or remote. This table is for internal bridge module use only and cannot be modified manually.

Node ID	Last-access	Forward-Flag
00a0570308e1	396442 tics	local
00a0570308e2	29442 tics	remote

Establish-table

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








A bridge establish table might have the following appearance:

Time	Dest	Source
1T; 16:45:01	ffffffffffff	0000c0057891
1T; 10:45:10	080000785734	0000c0057891

The 'Time' is displayed as either the device operating time or the system time of the ISDN (if provided by the ISDN terminal). The destination address 'ffffffffffff' might refer, for example, to a broadcast packet.

Status/IPX-statistics

The statistics from the IPX area are grouped here and classified by type, socket and router information. The IPX statistics contain the following parameters:

/IPX-statistics	Statistics from the IPX and IPX router area	
MAC-statistics		Statistics from the IPX packet media access control
Watchdog-statistics		Statistics for watchdog packets
Propagate-statistics		Statistics for IPX propagated packets (IPX type 20)
RIP-statistics		Statistics for NetWare RIP
SAP-statistics		Statistics for NetWare SAP
IPX-router-statistics		Statistics on the remote IPX router
Delete-values		Deletes IPX statistics

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

Status/IPX-statistics/MAC-statistics

These statistics include the following values:

IPX-LAN-rx	Number of IPX packets received from the LAN
IPX-LAN-rx-broadcasts	Number of broadcast IPX packets received from the LAN
IPX-LAN-rx-multicasts	Number of multicast IPX packets received from the LAN
IPX-LAN-rx-unicasts	Number of directly addressed IPX packets received from the LAN
IPX-LAN-tx	Number of IPX packets sent to the LAN
IPX-WAN-rx	Number of IPX packets received from the WAN
IPX-WAN-rx-broadcasts	Number of broadcasts received from the WAN
IPX-WAN-rx-multicasts	Number of multicasts received from the WAN
IPX-WAN-rx-unicasts	Number of directly addressed IPX packets received from the WAN
IPX-WAN-tx	Number of IPX packets sent to the WAN
Delete-values	Deletes MAC statistics

Status/IPX-statistics/Watchdog-statistics

These statistics include the following values:

IPX-watchdog-LAN-rx	Number of IPX watchdog packets received from the LAN
IPX-watchdog-LAN-tx	Number of IPX watchdog packets sent to the LAN
IPX-watchdog-WAN-rx	Number of IPX watchdog packets received from the WAN
IPX-watchdog-WAN-tx	Number of IPX watchdog packets sent to the WAN
SPX-watchdog-LAN-rx	Number of SPX watchdog packets received from the LAN
SPX-watchdog-LAN-tx	Number of SPX watchdog packets sent to the LAN
SPX-watchdog-WAN-rx	Number of SPX watchdog packets received from the WAN
SPX-watchdog-WAN-tx	Number of SPX watchdog packets sent to the WAN
Delete-values	Deletes watchdog statistics

Status/IPX-statistics/Propagate-statistics

These statistics include the following values:

Propagate-LAN-rx	Number of IPX propagated packets received from the LAN
Propagate-LAN-filters	Number of IPX propagated packets from the LAN that were received/filtered
Propagate-LAN-tx	Number of IPX propagated packets sent to the LAN
Propagate-LAN-socket-errors	Number of IPX propagated packets from the LAN filtered by socket filter
Propagate-LAN-hop-errors	Number of IPX propagated packet filtered from the LAN by hop count
Propagate-LAN-backroute-errors	Number of IPX propagated packets to be backrouted from the LAN
Propagate-LAN-contention	Number of packets to be routed from the LAN during a defective connection

Propagate-WAN-rx	Number of IPX propagated packets received from the WAN
Propagate-WAN-filters	Number of IPX propagated packets from the WAN that were received/filtered
Propagate-WAN-tx	Number of IPX watchdog packets sent to the WAN
Propagate-WAN-socket-errors	Number of IPX propagated packets filtered from the WAN by socket filter
Delete-values	Deletes IPX propagated packet statistics

Status/IPX-statistics/RIP-statistics

These statistics include the following values:

RIP-LAN-rx	Number of RIP packets received from the LAN
RIP-LAN-errors	Number of RIP packets with defective content received from the LAN
RIP-LAN-tx	Number of RIP packets sent to the LAN
RIP-WAN-rx	Number of RIP packets received from the WAN
RIP-WAN-errors	Number of RIP packets with defective content received from the WAN
RIP-WAN-tx	Number of RIP packets sent to the WAN
Delete-values	Deletes RIP statistics
Table-RIP	Displays RIP table

Table-RIP

There are 256 entries with RIP information in the **RIP table**. It has the following layout:

Network	Hops	Tics	Node-ID	Time	Flags
Network address	Number of routers to be passed on the path to the other network	Time required for this route in tics	MAC address of the server	Number of table updates until the entry is deleted	local, remote, loop or down

Status/IPX-statistics/SAP-statistics

These statistics include the following values:

SAP-LAN-rx	Number of SAP packets received from the LAN
SAP-LAN-errors	Number of SAP packets with defective content received from the LAN
SAP-LAN-tx	Number of SAP packets sent to the LAN
SAP-WAN-rx	Number of SAP packets received from the WAN
SAP-WAN-errors	Number of SAP packets with defective content received from the WAN
SAP-WAN-tx	Number of SAP packets sent to the WAN
Delete-values	Deletes SAP statistics
Table-SAP	Number of SAP packets received from the LAN

Table-SAP There are 512 entries with SAP information in the **SAP table**. It has the following layout:

Type	Server-name	Network	Node-ID	Socket	Hops	Time	Flags
Service SAP no.	Server com- puter name	Network address	Server MAC address	Socket for the ser- vice	Number of routers to the destination network	Number of table updates until the entry is deleted	local, remote, loop or down

Status/IPX-statistics/IPX-router-statistics

These statistics include the following values:

IPXr-LAN-rx	Number of IPX packets to be routed from the LAN
IPXr-LAN-tx	Number of IPX packets routed to the LAN
IPXr-LAN-hop-errors	Number of IPX packets filtered by hop count to be routed from the LAN
IPXr-LAN-socket-errors	Number of IPX packets filtered by socket filter to be routed from the LAN
IPXr-LAN-net-errors	Number of packets from the LAN to be routed to incorrect networks
IPXr-LAN-backroute-errors	Number of IPX packets to be backrouted from the LAN
IPXr-LAN-contention	Number of packets to be routed from the LAN during a defective connection
IPXr-LAN-down-errors	Number of IPX packets to be routed from the LAN to logged-off networks
IPXr-WAN-rx	Number of IPX packets to be routed from the WAN
IPXr-WAN-tx	Number of IPX packets routed to the WAN
IPXr-WAN-hop-errors	Number of IPX packets filtered by hop count to be routed from the WAN
IPXr-WAN-socket-errors	Number of IPX packets filtered by socket filter to be routed from the WAN
IPXr-WAN-net-errors	Number of packets from the WAN to be routed to incorrect networks
IPXr-WAN-backroute-errors	Number of IPX packets to be backrouted from the WAN
IPXr-WAN-down-errors	Number of IPX packets to be routed from the WAN to logged-off networks
IPXr-intern-rx	Number of packets from internal modules to the IPX router
Networks	Table of networks in the IPX routing table with node IDs
Delete-values	Deletes IPX router statistics
Establish-table	Table of the last 20 packets that required a connection

Establish-table The **establish table** is a further submenu option within router statistics. It contains the last 20 entries, which provide information on the system time, the IPX destination address, and the IPX source address of the data packets that should have caused a connection to be established.

An IPX establish table might have the following appearance:

Time	Destination	Source
1T; 16:45:01	00000081 ffffffff 0453	00000001 00a05702000a 0453
1T; 10:45:10	00000081 ffffffff 0452	00000001 00a05702000a 0452

The 'Time' is displayed as the device operating time or the ISDN real time (if this is available from the ISDN terminal). The destination address 'fffffff' might refer, for example, to a broadcast packet. The destination and source addresses both consist of the network number, MAC address and the socket number (all hexadecimal values).

Networks

The **network statistics** are also a submenu option within the IPX router statistics. This table provides more extensive information on a static route (remote station) It has the following layout:








Remote-ID	Network	Binding	Propagate	Backoff	Time	Node-ID
Logical remote station	Network address	Binding	Route/Filter	Connection counter	Time remaining until next connection	Node-ID of remote station

The different entries have the following meaning:

Remote-ID	Logical name of the remote station as it is entered in the routing table. An entry for the LAN link is also present; it is located in the first position in the table and has the name "LAN".
Network	Address of the network in which the remote station is located. For remote WAN stations, this corresponds to the entry in the routing table. If the autodetect function is configured in the IPX routing table (/SETUP/IPX-MODULE/LAN-CONFIGURATION/NETWORK), the network that was detected is displayed here.
Binding	Ethernet binding to which the remote station is linked. For remote WAN stations, this corresponds to the entry in the routing table. If the autodetect function is configured in the IPX routing table (/SETUP/IPX-MODULE/LAN-CONFIGURATION/NETWORK), the binding that was detected is displayed here.
Propagate	Filter flag for IPX type 20 (propagated) frames. For remote WAN stations, this corresponds to the entry in the routing table. For the LAN, a route is always entered here.
Backoff	Connection counter for the exponential backoff algorithm. When the connection counter reaches a value of 16, no more attempts are made, meaning that the route is deactivated (also possible for the LAN).
Time	Time remaining (specified in seconds) until the next connection attempt is made by the exponential backoff algorithm. When a connection has been successfully established, the remaining time is set to zero, thus activating the route.
Node-ID	Node ID of the responsible router in the WAN network. The node ID of the router is entered here for the LAN entry.

Status/TCP-IP-statistics

This menu allows you to display the statistics from the TCP/IP area, classified by ARP, IP, ICMP, TCP and TFTP packet types. The TCP-IP statistics contain the following parameters:

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



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

Status/TCP-IP-statistics/ARP-statistics

These statistics include the following values:

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

Table-ARP

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

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

Status/TCP-IP-statistics/IP-statistics

These statistics include the following values:

IP-LAN-rx	Number of IP packets received from the LAN
IP-LAN-tx	Number of IP packets sent to the LAN
IP-LAN-checksum-errors	Number of IP packets incorrectly received from the LAN
IP-LAN-service-errors	Number of IP packets received from the LAN for an incorrect service

IP-WAN-rx	Number of IP packets received from the WAN
IP-WAN-tx	Number of IP packets sent to the WAN
IP-WAN-checksum-errors	Number of IP packets incorrectly received from the WAN
IP-WAN-service-errors	Number of IP packets received from the WAN for an incorrect service
IP-WAN-rx-disconnect	Number of packets from the WAN discarded by timeout
Delete-values	Deletes IP statistics

Status/TCP-IP-statistics/ICMP-statistics

These statistics include the following values:

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

Status/TCP-IP-statistics/TCP-statistics

These statistics include the following values:

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

Status/TCP-IP-statistics/TFTP-statistics

These statistics include the following values:

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

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

These statistics include the following values:

DHCP-LAN-rx	Number of DHCP packets received from the LAN
DHCP-LAN-tx	Number of DHCP packets sent to the LAN
DHCP-WAN-rx	Number of DHCP packets received from the LAN
DHCP-discard	Number of DHCP packets discarded
DHCP-rx-discover	Number of discover messages received

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














Table-DHCP








There are 16 entries with DHCP information in the **DHCP table**. It has the following layout:

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

Status/IP-router-statistics

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

/IP-router-statistics	Statistics from the IP router area	
IPr-LAN-rx		Number of data packets to be routed from the LAN
IPr-LAN-tx		Number of data packets routed to the LAN
IPr-LAN-local-routings		Number of packets received from the LAN and routed to the LAN
IPr-LAN-network-errors		Number of LAN packets that were not routed
IPr-LAN-routing-errors		Number of LAN packets that must be sent to another router
IPr-LAN-ttl-errors		Number of LAN packets with an expired time-to-live value
IPr-LAN-filters		Number of LAN packets filtered by the filter table
IPr-LAN-discards		Number of LAN packets discarded
IPr-WAN-rx		Number of data packets to be routed from the WAN
IPr-WAN-tx		Number of data packets routed to the WAN
IPr-WAN-network-errors		Number of WAN packets that were not routed
IPr-WAN-ttl-errors		Number of WAN packets with an expired time-to-live value
IPr-WAN-filters		Number of WAN packets filtered by the filter table

/IP-router-statistics	Statistics from the IP router area	
IPr-WAN-discards		Number of WAN packets discarded
IPr-WAN-type-errors		Number of packets from the WAN without an IP router ID
IPr-ARP-errors		Number of unsuccessful accesses to the ARP cache
Delete-values		Deletes IP router statistics
Establish-table		Table of the last 20 packets that required a connection
Protocol-table		Table of routed packets arranged by protocol
RIP-statistics		Statistics from the IP/RIP area

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

An IP router establish table might have the following appearance:

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

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

Protocol-table

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

A protocol table might have the following appearance:

Prot.	LAN-Tx	WAN-Tx
tcp	14	30
udp	15	50
icmp	60	40

Status/IP-router-statistics/RIP-statistics

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

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

Table-IP-RIP









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




An IP-RIP table might have the following appearance:

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

Status/Config-statistics

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


























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




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



Status/Queue-statistics

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

/Queue-statistics		Statistics on the queue
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
WAN-heap-packets		Number of buffers available
WAN-queue-packets		Number of buffers in use
Bridge-internal-queue-packets		Number of bridge packets from the LAN
Bridge-external-queue-packets		Number of bridge packets from the WAN
ARP-query-queue-packets		Number of ARP packets in the query queue
ARP-queue-packets		Number of ARP packets in the normal queue
IP-queue-packets		Number of IP packets in the normal queue
IP-urgent-queue-packets		Number of IP packets in the secured queue
ICMP-queue-packets		Number of ICMP packets
TCP-queue-packets		Number of TCP packets
TFTP-queue-packets		Number of TFTP packets
SNMP-queue-packets		Number of SNMP packets
IPX-queue-packets		Number of IPX packets
RIP-queue-packets		Number of RIP packets
SAP-queue-packets		Number of SAP packets
IPX-watchdog-queue-packets		Number of watchdog-packets
SPX-watchdog-queue-packets		Number of SPX watchdog packets
IPX-router-queue-packets		Number of IPX router packets
Prot-heap-packets		Number of prot heap packets
IPr-queue-packets		Number of packets remaining to be processed by the IP router.
DHCP-server-queue-packets		Number of packets in the receive queue of the DHCP server.
IPr-RIP-queue-packets		Number of packets in the receive queue of the IP-RIP module (for RIP queries, RIP propagations ...).
DNS-Tx-queue-packets		Number of packets to be forwarded to DNS or NBNS servers.

/Queue-statistics	Statistics on the queue	
DNS-Rx-queue-packets		Number of packets that come from DNS or NBNS servers and are to be forwarded to the host.
IP-Masq.-Tx-queue-packets		Number of packets to be sent masked (to the Internet).
IP-Masq.-Rx-queue-packets		Number of packets received from the Internet and have to be demasked.

Status/Connection-statistics

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

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

lfc	Connections	Active	Passive	Errors	Con.-Time	Charge
Ch01	0	0	0	0	No connection	0
Ch02	0	0	0	0	No connection	0
Ser1	0	0	0	0	No connection	0



The serial interface entry applies to the ELSA MicroLink LANCOM MPR only!

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

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

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

Status/Info-connection

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

lfc	Status	Mode	Dialup-remote	Device-name	B1-DT	B2-DT
Ch01	Ready				0	0
Ch02	Ready				0	0
Ser1	Ready				0	0



The serial interface entry applies to the ELSA MicroLink LANCOM MPR only!

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

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

Status/Layer-connection

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

lfc	WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
Ch01	DEFAULT	ETHER	ELSA	X.75ELSA	compr.	HDLC64K
Ch02	PPPHDLC	TRANS	TRANS	PPP	none	HDLC64K
Ser1	V.24_DEF	ETHER	ELSA	X.75ELSA	compr.	HDLC64K



The serial interface entry applies to the ELSA MicroLink LANCOM MPR only!

Status/Call-info-table

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

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

System-time	Ifc	CLIP-Caller	Dial-Caller	Capab.	B-chan.
OT; 00:20:57	S0	5678	1234	HDLC64K	2
OT; 00:20:46	S0	4321	1234	HDLC64K	1
OT; 00:19:47	S0	4321	1234	HDLC64K	1
OT; 00:11:33	S0	5678	1234	HDLC64K	1
OT; 00:01:13	S0	4321	1234	HDLC64K	2
OT; 00:01:02	S0	4321	1234	HDLC64K	1
OT; 00:00:06	S0	5678	1234	HDLC64K	1

The different entries have the following meaning:

System-time	Time when the call came. Either the device operating time or the system time of the ISDN is displayed (if made available from the ISDN terminal).
Ifc	Interface at which the call was received. Possible values are S ₀ for the internal S ₀ bus and Ser1 for the external interface.
CLIP-Caller	Call number (CLIP) of the caller
Dial-Caller	The MSN/EAZ dialed by the caller
Capab.	The service requested by the caller. Possible values are HDLC64K, HDLC56K and unknown. An analog call is displayed as unknown here. <i>LANCOM Office</i> router can also display the values A-3 kHz (analog 3 kHz), language (for normal speech transmission) and fax G2/3 (for analog fax transmission as per group 2 or 3).
B-chan.	The B channel used. A value of 0 means that both channels have already been seized, i.e. call waiting is activated.



The serial interface entry applies to the ELSA MicroLink LANCOM MPR only!



A tip for those using a LANCOM Office router in a PBX: Following a call to any ISDN device under the number of the ISDN bus, the MSN/EAZ displayed under 'Dial-Caller' is exactly the entry that must be entered in the LANCOM Office router at /SETUP/WAN-MODULE/S0-INTERFACE/MSN-IN in order for a call to be correctly answered from an external station.

Status/Remote-statistics

This table shows the last ten connections of the *LANCOM Office* routers with information on the remote station.

The table has the following layout:

Conn.-start	Remote-ID	Mode	lfc	Conn.-time	Charge
OT; 00:20:57	BERLIN	Active	Ch01	50	5
OT; 00:20:46	Chemnitz	Passive	Ch02	230	10
OT; 00:19:47	Dresden	Callback	Ser1	25	3

The different entries have the following meaning:

Conn.-start	Time at which the connection was established. Either the device operating time or the system time of the ISDN is displayed (if available from the ISDN terminal).
Remote-ID	Logical remote station name.
Mode	Type of connection establishment: Active – the connection was actively established from the <i>LANCOM Office</i> router Passive – <i>LANCOM Office</i> router was called Callback – <i>LANCOM Office</i> router called the remote station back
lfc	The channel over which the connection is made (Ch01, Ch02, Ser1).
Conn.-time	Duration of connection.
Charge	Charges for this connection in units.

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



Status/Channel-statistics

This table shows information on the current status of the two B channels. With the *LANCOM 2000 Office* information on the a/b ports is also shown. The information from this table is primarily used for output via *ELSA LANmonitor*. Therefore, some values are shown simply as bits with no further explanation.

The table has the following layout:

Chan.	State	App	Mode	Cause	Number	Sub-address	Charg	Conn.-time	Extra	ISDN-display
S0-ERR	00000000	Router	active	0000	0241123456	00000000	3	0		
S0-B1	00000000	a/b	active	0000	0241123457	00000000	2	20		
S0-B2	00000000	LAN-CAPI	passive	0000	0241123458	00000000	4	180		
AB-ERR	00000000	none	unknown	0000		00000000				
AB-1	00000000	none	unknown	0000		00000000				

Chan.	State	App	Mode	Cause	Number	Sub-address	Charg	Conn.-time	Extra	ISDN-display
AB-2	00000000	none	unknown	0000		00000000				
AB-3	00000000	none	unknown	0000		00000000				
AB-4	00000000	none	unknown	0000		00000000				

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

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



Status/Time-statistics

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

The menu has the following layout:

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

Status/Time-statistics/ISDN

These statistics include the following values:

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














Status/Delete-values

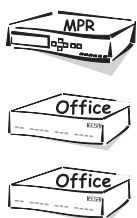
With the exception of the tables, this option allows you to delete all the values in the substatistics. To do so, enter the following command:

```
do delete-values
```

Setup

This menu allows you to query and modify all the system parameters that are necessary to the functioning of the *LANCOM Office* router.

/Setup		System configuration
Name		Entering the device name
WAN-module		WAN settings
Charges-module		Charge management settings
LAN-module		LAN settings
Bridge-module		Remote bridge settings
IPX-module		IPX module (IPX router) settings
TCP-IP-module		TCP/IP module settings
IP-router-module		IP router module settings
SNMP-module		Settings for configuration via SNMP
Config-module		Configuration module settings
Other (<i>ELSA MicroLink LANCOM MPR</i> only)		Display and keyboard settings
LCR-module		Least-cost router settings
Time-module		Time module settings



Name

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

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

In the default configuration, no name is entered.

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

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

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

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

Setup/WAN-module

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



Interface-list



/WAN-module		WAN settings
Interface-list		S ₀ interface settings
Router-interface-list		Router module settings
Name-list		Remote station settings
RoundRobin-list		Settings for different remote station numbers
Layer-list		Settings for the layer combinations used
PPP-list		Parameter settings for PPP connections
Number-list		Settings for call numbers with access authorization
Script-list		Dial script settings
Dial-prefix		Initial numbers for active connection establishment via the serial interface
Manual-dialing		Settings for manual connection control
Protect		Protection for answering incoming calls
CB-attempts		Number of callback attempts when the remote station is busy
V.24-max-bitrate		Maximum transmission rate via the serial interface
Backup-delay-seconds		Delay in establishing backup connections in the event of disturbances on the line

This table contains the interface settings, which apply to all operating modes (modules) of the *LANCOM Office* routers.

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

Additional, special interface settings are also available for the various modules, e.g. the call numbers to which a module should react (see also `setup/wan module/router interface list`, `setup/lancapi-module` and `setup/ab-module/port list`).

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

Ifc	Designates the associated D channel. The possible values are: S0 (internal interface setting) and Ser1 (serial port). <i>ELSA MicroLink LANCOM MPR only</i>
Protocol	D-channel protocol setting. The possible values are: Auto : automatic detection of the D-channel protocol DSS1 : Euro-ISDN 1TR6 : National ISDN GRP0 : Leased-line connection group 0 GRP2 : Leased-line connection group 2 (<i>ELSA MicroLink LANCOM MPR only</i>) P2P-DSS1 : Point-to-point connection (<i>LANCOM Office routers only</i>)
FV-B-chan.	B-channel settings for a leased-line connection. The possible values are: none : Leased-line connection not assigned to a specific channel. 1 or 2 : Leased-line connection operates over the assigned B channel. Please refer to the information on setting these parameters in the fixed connection description. The fixed connection function is not a standard component of the <i>LANCOM Office</i> routers.
Dial-prefix	Global dialing prefix for all modules of the <i>LANCOM Office</i> router. The digits entered here (maximum 8) are automatically prefixed to the selected call number in every call. Use this prefix when, for example, the router is connected to a PBX.

Router-interface-list



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

Ifc	MSN/EAZ	YC.	CLIR
S0	123456	Off	Yes

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

Ifc	Designates the associated interface. The possible values are: S0 (internal interface setting) and Ser1 (serial port). <i>ELSA MicroLink LANCOM MPR only</i>
-----	---

MSN-EAZ	<p>If your <i>LANCOM Office</i> router is connected to an ISDN port with 1TR6, enter the EAZ to which the a/b port is to respond.</p> <p>If your <i>LANCOM Office</i> router is connected to an ISDN port with DSS1, enter the MSN to which the port is to respond. If you wish the port to respond to several different MSNs, enter them here separated by semicolons. A '#' in the list enables any number of incoming MSNs.</p> <p>For outgoing calls, the first MSN in this list will be reported to the remote station. If no MSN is entered, the switching center sends the main MSN of the terminal.</p>
YC.	<p>This entry can be used to control the interface's ability to establish Y connections. Possible settings are:</p> <p>On: Y connection is supported; a number of connections can be established simultaneously (default). A channel bundling connection is broken off when a second connection to another remote station has to be established. Refer also to the settings for the availability of the <i>LANCAPI</i> and the telephone system with the <i>LANCOM 2000 Office</i>.</p> <p>Off: Y connection not supported; only one connection can be established. The second connection is blocked. If a connection to an additional remote station is to be established, this establishment is rejected. A channel bundling connection is not affected.</p>
CLIR	<p>Calling Line Identification Restriction: Suppresses the outgoing MSN.</p> <p>Possible values:</p> <p>Yes: Activate CLIR, do not send MSN.</p> <p>No: Deactivate CLIR, send MSN to remote station.</p> <p>Please note: The "selective suppression of call number transmission" may be a service feature that will have to be obtained from the telephone company.</p>

Name-list

The *LANCOM Office* router needs the device names entered in the name list in order to determine the numbers to be called and the B channel protocol (Layername) to be set. The name list is also used for the callback function.

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

Device-name	Dialup-remote	B1-DT	B2-DT	WAN-layer	Callback
AACHEN	875463	180	0	X75COMPR	On
BERLIN	040785647	20	20	RAWHDLC	Off

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

Device-name	In the Device Name column, you can enter an original remote station name, which you must then assign to the relevant remote station via the Name option in the Setup menu (default: Default).
Dialup-remote	In this column, you can store the number to be called and, if applicable, supplement it with special dialing characters (see above, default: None).
B1-DT	<p>In this column, you can define appropriate connection timeouts (in seconds) for the first B channel.</p> <p>If no data is being transmitted when this time expires, the connection on this channel is released (default: 20).</p> <p>If charging information is transmitted over the ISDN network during the connection, the <i>LANCOM Office</i> router will make full use of every charging unit and will only terminate the connection just before the beginning of the next unit. This function is also referred to as dynamic short-hold.</p>

B2-DT	In this column, you can define appropriate connection timeouts for the second B channel (same as B1-DT, default: 20). The B2 hold time controls the bundling behavior during a channel bundling. Values of 0 or 9999 identify static bundling, values between them dynamic bundling.
WAN-layer	In this column, a name is stored that must also be entered in the layer list. This serves to define the B channel protocol setting required for this connection in accordance with a specific ISDN layer combination (default: no layer, ELSA default).
Callback	In this column, you can define whether a callback is to be made for the relevant remote station (Off/Name/Auto/Looser; default: Off).

■ Callback options

Off	No callback is made.
Looser	The <i>LANCOM Office</i> router stops attempting to establish a connection when there is a call from this remote station (reciprocal call establishment). This setting must be used when a callback from the remote station is expected.
Auto (not applicable to Windows 95 or Windows NT)	The connection will be rejected and a direct callback will be initiated if the remote station is specified in the number list. This means that the caller is not charged. If the remote station is not specified in the number list, a callback will be negotiated in a protocol negotiation (ELSA or PPP). A charge of one unit is incurred for this.
Name	This setting forces a protocol negotiation. This enables call number protection to be set in the number list and also a callback to be started using the protocol negotiation. A charge of one unit is incurred for this.

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

#		Trunk seizure (only with some PBXs).
S		The semipermanent connection (SPV) is used for connections via the first B channel.
S2		The semipermanent connection (SPV) is used for connections via both B channels (channel bundling).
I	Internal S ₀ bus (ISDN)	The remote station can be reached via the internal S ₀ bus only.



E	External interface	The remote station can be reached via the external interface only.
B	Backup for dial-up connection	The remote station can be reached via the external interface only. If a connection is already established via the external interface, this connection is in any case released.
F	Backup for leased-line connection	The remote station can be reached via the leased-line connection only. This can be entered only in the name list! If the F is followed by a call number, it is identified as the backup call number. This call number is composed of the elements described in the Round Robin section.

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

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

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

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

Device name	RoundRobin	Head
AACHEN	4321-5555-6666	Last

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

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

Layer-list

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



The following table below is provided as an example and also shows the default settings for the *ELSA MicroLink LANCOM MPR*:

WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	ETHER	ELSA	X.75ELSA	compr.	HDLC64K
V.24_DEF	ETHER	ELSA	X.75ELSA	none	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	none	HDLC64K
RAWHDLC	TRANS	TRANS	TRANS	none	HDLC64K
X75	TRANS	TRANS	X.75LAPB	none	HDLC64K
X75COMPR	TRANS	TRANS	X.75LAPB	compr.	HDLC64K
X75BUNDLE	TRANS	TRANS	X.75LAPB	bundle	HDLC64K
X75B._C.	TRANS	TRANS	X.75LAPB	bnd+cmpr	HDLC64K
BRIDGE_BC	ETHER	TRANS	X.75LAPB	bnd+cmpr	HDLC64K
BRIDGE_B	ETHER	TRANS	X.75LAPB	bundle	HDLC64K



The following standard settings are valid for *LANCOM Office* router:

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

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

Layer-name	In this column, you can enter an original name designating the layer combination that you use. These names can then be used in the name list 'layer name' column depending on their spelling to set the B channel protocol. If an entry with the name DEFAULT is defined in this column, the settings stored there are always used when no layer name can be assigned or a caller does not transmit his or her call number. This entry is also used when a group 0 leased-line connection is established. If the DEFAULT entry is not present, a B channel protocol developed by ELSA is used as the default. The user may delete or change any of the layers predefined here.	
Encaps.	Additional information regarding the data to be transmitted may be specified in the Encaps column. The following entries are possible:	
	ETHER	The data is provided with an Ethernet header. This setting is required for communication with older <i>LANCOM Office</i> router devices, the workstation drivers or in bridge operation.
	TRANS	No Ethernet header is sent in this setting. Only “pure” IPX or IP data packets are transferred. This setting provides the greatest possible effective data throughput.
Lay-3	In the lay-3 column, you can define additional headers for data transmission in ISDN. You can select from among the following settings:	



	TRANS	No additional header is inserted (higher data throughput). Always select this setting if the remote station sends the data transparently via ISDN layer 3 (e.g. transparent HDLC, transparent X.75LAPB).
	CISCO	This setting inserts a header as per the Cisco standard.
	CONWARE	This setting inserts a header as per the CONWARE standard.
	ELSA	The data is provided with an ELSA header. In addition, when a connection is established, a protocol negotiation is performed in which the remote stations exchange names. Incoming-call protection by name is possible only if this setting is selected. Without an ELSA setting, incoming-call protection is possible by call number only. This setting is required for communication with older <i>LANCOM Office</i> router devices or the workstation drivers.
	PPP	A negotiation is performed according to the point-to-point protocol. Data compression and channel bundling are not possible with this setting with the <i>ELSA MicroLink LANCOM MPR</i> .
	APPP	A negotiation is performed as per the asynchronous PPP. APPP is then used when PPP is not possible because the connection does not permit synchronization (e.g. for analog modem operation).
	SCPPP	Following completion of script processing, a synchronous PPP negotiation is initiated.
	SCAPPP	Following completion of script processing, an asynchronous APPP negotiation is initiated.
	SCTrans	Following completion of script processing, a connection exists to the remote station. No further protocol negotiation is performed.
Lay-2	In this column, you can select the protocol for ISDN layer 2:	
	TRANS	The data is packed directly in HDLC packets. Always select this setting if communication is to take place via transparent HDLC. Data compression and channel bundling are not possible with this setting.
	X.75UI	The data is prefixed with an X.75UI header (Unnumbered Information Header). Data compression and channel bundling are not possible with this setting.
	X.75BUI	The data is prefixed with an X.75BUI header (Broadcast Unnumbered Information Header). Data compression and channel bundling are not possible with this setting.
	X.75ELSA	The data is exchanged in X.75 ELSA format. This format permits data compression. This setting is required for communication with older <i>LANCOM Office</i> router devices or the workstation drivers. It does not allow communication with devices from other manufacturers.
	X.75LAPB	The data is exchanged in X.75 secured format. Always select this setting if the remote station is to work with X.75 data protection. This format permits data compression.
L2-Opt.	The L2-opt. enables the setting of an option for the data transfer setting under Lay-2 with an additional <i>LANCOM Office</i> router.	
	none	No data compression or channel bundling is performed.



	compr.	Data compression as per V.42bis is performed (<i>ELSA MicroLink LANCOM MPR</i>) or Stac (<i>LANCOM Office</i> router). Data compression as per V.42bis is possible only in connection with X.75ELSA or X.75LAPB. Compression as per Stac (Hi/fn) must be used in connection with PPP or multilink PPP. Stac compression may also be used in connection with Windows remote stations.
	bundle	Channel bundling is performed via two B channels. Channel bundling with <i>ELSA MicroLink LANCOM MPR</i> is only possible for the Lay-2 settings of X.75ELSA or X.75LAPB. <i>LANCOM 1100 Office</i> uses PPP for channel bundling (multilink PPP). Static or dynamic channel bundling depends on the B2 connection time-out. A B2 hold time of '0' or '9999' will set a static channel bundling in which both channels are always used. In the event of dynamic channel bundling with other B2 hold times, the second channel is only activated when the data throughput exceeds a specified threshold.
	bnd+cmpr	Channel bundling and data compression takes place over two B channels.
Lay-1		The lay-1 column allows you to define the speed at which the data is sent in ISDN.
	HDLC64K	The data is transmitted at 64,000 bps.
	HDLC56K	The data is transmitted at 56,000 bps. This setting is especially important for connections in the USA.

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

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

For Internet and remote access, PPP is generally specified.

PPP-list

The *LANCOM Office* router needs the device names contained in the PPP list in order to determine the security procedure settings suitable for the connection and to determine the PPP parameters. It has the following layout:

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

Not all parameters can be reached via the telnet configuration. Use *ELSA LANconfig*.

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

Device-name	In the Device-name column, you can enter the name with which the remote station logs onto the <i>LANCOM Office</i> router. In the case of connections via the data transmission network, this is the name entered as "Username". For remote access via the data transmission network, the 'Username' field (see above) is not evaluated! Entries are not case-sensitive!	
Auth.	In this column, you can enter the security procedure to be used for verification of the remote station. Default: PAP	
	none	The <i>LANCOM Office</i> router does not negotiate authentication with the remote station when establishing a connection. However, the remote station can itself require authentication from the <i>LANCOM Office</i> router (e.g. dialing to an ISP).
	PAP	The remote station is checked as per the Password Authentication Protocol.
	CHAP	The remote station is checked as per the Challenge Handshake Authentication Protocol.
Key	A password may be entered in this column. Its presence is indicated by the symbol * and it is used to check the remote station. It may consist of 95 characters (7-bit ASCII, including spaces). Default: None The <code>set ?</code> command shows a list of the allowable characters.	
Time	In this column, you can enter the period of time between two remote station verifications specified in minutes. The CHAP protocol must be set here. Default: 0	
Try	In this column, you can specify the number of times the verification attempt is to be repeated. If verification fails, the connection is immediately terminated. Default: 5	
Conf, Fail and Term	These parameters may be used to influence the operation of the PPP. They are defined and described in RFC 1661. The default values are sufficient for most remote stations. If nothing is entered here, the values 0,0,0 appear in the display but the default values 10, 5, 2 are still used. These parameters can only be changed via SNMP or TFTP (using the <i>ELSA LANconfig</i> configuration program)!	
Username	The user name (max. 64 characters) transmitted to the remote station during PPP negotiation. The <i>LANCOM Office</i> router identifies itself to the remote station with it. If no user name is entered, the device name serves as the user name. Entries are case-sensitive here.	

A maximum of 64 entries can be managed in the PPP list.

Number-list

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

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

Dialup-remote	Device-name
875463	AACHEN
040785647	BERLIN

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

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

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

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

If the name of the remote station (and the layer to be used) cannot be sent using the number list, the call will be received with the DEFAULT layer and verified as per the protocol negotiation (ELSA protocol with *ELSA MicroLink LANCOM MPR* or PPP with *LANCOM Office* router) for a corresponding entry in the name list.



This procedure cannot be used with analog modems on the serial interface of the ELSA MicroLink LANCOM MPR, because CLIP transfer is normally not possible with analog lines.

Script-list

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

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

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

The entries in the script list have the following meaning:

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

Ext. Dial-prefix

The 'ext. Dial-prefix' menu item may be used to define a dial prefix for all outgoing calls over the serial V.24 interface (*ELSA MicroLink LANCOM MPR* only).

Protect

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

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

CB-attempts

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

V.24-max-bitrate

The 'V.24-max-bitrate' option allows you to set the maximum transmission rate for the external interface. The following settings are possible:

- 115200 Maximum transmission rate of 115,200 bps
- 230400 Maximum transmission rate of 230,400 bps

This setting is necessary because there are specific combinations of *ELSA MicroLink LANCOM MPR* and external terminal devices with which only the lower transfer rate can be used. The default setting is 115200 and operates with any hardware combination.




Backup-delay-seconds

The 'Backup-delay-seconds' option allows you to select the period of time after which a backup connection via the external interface should be established when the leased-line connection fails. The possible values are from 10 to 999 seconds. The default setting is 15 seconds.

If a time of zero seconds in input, the active part of the backup mechanism is deactivated, i.e., a backup connection is no longer actively established.

Setup/WAN-module/Manual-dialing

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

/Manual-dialing	Settings for manual connection control	
Connect		Establishes a connection.
Disconnect		Releases the current connection.
State		Displays the current connection status.

Connect

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

You can use the command

Do /Setup/WAN-module/Manual-dialing/Connect to remote station

serves to initiate the manual establishment of a connection via remote configuration. The remote station's device name specified as a parameter must also be entered in the name list with a call number.

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

Disconnect

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






Setup/Charges-module

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



Charge protection is only valid for the router modules of the LANCOM Office routers, not for the LANCAPI or the a/b ports with the LANCOM 2000 Office.

The default setting for charge protection is 830 units per week. This means that no more than approx. DM 100 can be accrued within a period of seven days. The menu has the following layout:

/Charges-module		Charge management settings
Budget-units		Units available for each monitoring period
Day(s)/Period		Length of one period in days
Spare-budget		Number of units still available
Router-units		Units used by the router modules
Table-budget		Local budget settings for the individual interfaces

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



Efficient use of charge monitoring is possible only if the charge information is sent during the connection (AOCD). Please keep this in mind when subscribing to your ISDN connection.

Charge protection may not function in other European countries, because there is no European standard yet.

Budget-units

This option allows you to define the number of charge monitoring units that are to be available as a global budget for all interfaces. These units can only be entered in increments of ten, with a maximum total of 2550 units. The default setting is 830 units (approx. DM 100). The charge units transmitted in the charge information are added up during operation.

If you enter a value of 0, only the local budget is taken into account (see below). Once the charges budget has been exceeded, active connection establishment is no longer possible. The following message appears on the display *ELSA MicroLink LANCOM MPR*:

```
Charge locked
Ch02: Ready
```

The power LED flashes on the *LANCOM Office* router.

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

Day(s)/Period

This menu option allows you to define a period of time in days (0 to 255) during which the charge information is to be added up and compared to the budget. The default setting is seven days. When this period has expired, the adding up of charges starts over again.

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

Table-budget

In addition to the global charges budget, you can define separate local budgets for each interface. When a local budget has been exhausted but the global budget has not, only the interface associated with the local budget is locked until the charge period has expired. All the other interfaces can continue active connection establishment until either their own local budget or the global budget has been exhausted. This allows you to distribute the charges to the individual interfaces as desired.

The table for setting the local charges budget has the following structure in the *ELSA MicroLink LANCOM MPR*:

lfc	Budget-units	Spare-Budget	Router-units
S0	0	0	0
Ser1	0	0	0

The table appears as follows for the *LANCOM Office* router:

lfc	Budget-units	Spare-Budget	Router-units
Router	830	830	0
LANCAPI	0	0	0
AB-1	0	0	0
AB-2	0	0	0
AB-3	0	0	0
AB-4	0	0	0



The entries for the a/b ports are only valid for LANCOM 2000 Office.

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




Entering zero budget units deactivates charge monitoring for the particular interface. If you enter zero for all budgets, no charges are monitored.

If no charge information or charge information that cannot be evaluated for the *LANCOM Office* router is not transferred, the router will report 'No charge info' after every connection.

These functions require that you subscribe to the telecommunication service's "Advice of charge during connection" feature for the ISDN port. If the "advice of charge" is transferred only after connection, monitoring during connection cannot be guaranteed. In this case, charge monitoring applies only until the next connection is established. Connections that extend over an excessively long period of time cannot be monitored and thus are not subject to charge monitoring.

Setup/LAN-module

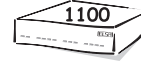
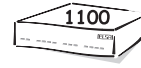
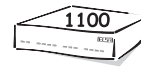
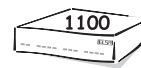
This menu allows you to select the settings needed for the local network. The menu has the following layout:

/LAN-module	LAN settings	
Connector		Selection of the network connection
Node-ID		MAC layer address of the <i>LANCOM Office</i> router
Spare-heap		Buffers that receive data packets from the local network

Connector

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

Connector	Meaning
Auto	Default setting, only from hardware release F with the <i>ELSA MicroLink LANCOM MPR</i> , activates the autosense function of the network chips for the 10BASE-2 and 10BASE-T ports. This automatically sets the <i>LANCOM Office</i> router to the port in use without requiring manual configuration of this item. This does not apply to the 10BASE-5 port, which must always be configured manually.
10B-T	10BASE-T
10B-2	10BASE-2
10B-5	10BASE-5
10BTX	10BASE-T in half-duplex mode
FD10BTX	10BASE-T in full-duplex mode
100BTX	100BASE-T in half-duplex mode
FD100BTX	100BASE-T in full-duplex mode



When making settings for LANCOM 1100 Office, please note that the selected transfer mode must also support the additional terminals.

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

Node-ID

This option allows you to display the router's own Ethernet address. The value displayed here was set at the factory and cannot be changed. The Ethernet address is displayed as a 12-position hexadecimal number in which the first six positions remain constant.

Node-ID
00A057xxxxxx







Displays the Ethernet address.

Spare-heap

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

Setup/Bridge-module

This menu allows you to select the settings necessary for bridge mode. The menu has the following layout:

/Bridge-module		Remote bridge settings
Operating		Remote bridge active or inactive
Remote-ID		Remote station name for local connection establishment
Table-bridge		Displays bridge table.
Aging-minute(s)		Dwell time of MAC addresses in the bridge table
LAN-config		Settings for the LAN side
WAN-config		Settings for the WAN side

Operating

This option allows you to activate or deactivate the remote bridge. In the default configuration, the remote bridge is deactivated.

If the device is used just as an IP router or IPX router connection, the remote bridge should be deactivated.

Remote-ID

The name of the remote station to be called is stored here (as a string of max. 16 characters). For active dialing, the name list must contain a matching entry.

Table-bridge

This option allows you to display the entries in the current bridge table. The table is automatically created and managed by means of a hash procedure. It comprises max. 512 entries.

Entries in the bridge table may appear as shown below when the bridge has acquired local and remote MAC addresses over time:

Node-ID	Last-access	Forward-Flag
00a05702000a	4 tics	local
0800096483d4	105073354 tics	local
00001b157de0	105079059 tics	remote





The last access time to occur since the system was switched on is stored as a multiple of 9 ms (tics). The forward flag reflects the location of the MAC address. An entry in the form 00a057XXXXXX is the unique MAC address of the *LANCOM Office* router.

The forward flag column is output for remote configuration only. This column is not included in the display.

Aging-minute(s) This option allows you to enter a time (from 1 to 60 minutes), after which the bridge table is automatically updated, i.e. all MAC addresses that have not been accessed since the last automatic update are removed. The default setting is 30 minutes.

Setup/Bridge-module/LAN-configuration

This option allows you to set the transmission profiles needed for the LAN data packets. The menu has the following layout:

/LAN-configuration		Settings for the LAN side
Broadcast		Filter behavior of broadcast data packets
Multicast		Filter behavior of multicast data packets
Dest.-address		Destination address filtering
Src.-address		Source address filtering



Broadcast This option allows you to specify whether broadcast data packets are to be transmitted always (**pos** = default), never (**neg**), or only when a connection is established (**sem**).

Multicast This option allows you to specify whether multicast data packets are to be transmitted always (**pos** = default), never (**neg**), or only when a connection is established (**sem**).

The setting 'pos' with multicast or broadcast may result in excessive charges, because connections are established very frequently.

Setup/Bridge-module/LAN-configuration/Destination-addresses

This menu item enables all settings required to filter destination addresses.

/Dest.-address	Destination address filtering	
Filter-type		Positive or negative filter
Filter-table		Processing of address filter table

Filter-type

The filter type to be used for the destination address list may be specified here. The settings (**pos**) are possible, so only data packets whose destination address is included in the destination address filter table will be transferred. The setting (**neg**) default value transfers all frames whose destination address is not included in the destination address filter table.

Filter-table

The destination addresses can be administered in this table. Entries simply comprise the **MAC-address** field.

Dest. address

0000c051d266

Setup/Bridge-module/LAN-configuration/Source-addresses







The settings for source addresses are made analogously to the settings for the destination addresses.

Setup/Bridge-module/WAN-configuration

This option allows you to select the settings for WAN data packets. The settings in this menu are exactly the same as the settings in the **LAN-configuration** menu except that they serve to filter the data packets received from the WAN.

Setup/IPX-module

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

/IPX-module	IPX module (IPX router) settings	
Operating		Activates or deactivates the IPX module.
IPX-router		Activates or deactivates the IPX router.
LAN-config		Settings for the LAN side
WAN-config		Settings for the WAN side
RIP-config		RIP settings
SAP-config		SAP settings

Operating

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

Remote configuration via DOS/IPX and the IPX router can be used only if the IPX module is activated. For local configuration via a LAN, the router does not have to be activated.










IPX-router

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

When the IPX router module is activated, the IPX module is also activated. The IPX router can be activated only if different, permissible network addresses are entered under LAN-configuration and WAN-configuration.

Setup/IPX module/LAN-configuration

Settings for the LAN data packets may be made here. The menu has the following layout:

/LAN-configuration		Settings for the LAN side
Network		Logical IPX network number of the LAN port
Binding		Ethernet frame type setting for the LAN port
IPX-watch		Settings for IPX watchdog management
SPX-watch		Settings for SPX watchdog management
NetBIOS-watch		Settings for NetBIOS watchdog management
Socket-filter		Filter table for destination socket filtering
Loc.-routing		Activates or deactivates local routing.
RIP-SAP-scal.		Activates or deactivates RIP-SAP scaling.
LOOP-prop.		Activates or deactivates propagation of redundant routes.

Network

The NetWare network number of the network (8-digits, hexadecimal) that is connected to the LAN port under the binding (see below) may be entered here. If there is a NetWare server in the local network, the *LANCOM Office* router can automatically detect the network number and the binding.

The default value is '00000000' and means that the *LANCOM Office* router should automatically detect the network number.

Binding

This option allows you to select the Ethernet packet format (Auto, II, 802.3, 802.2, SNAP) for the LAN port. This format must match the Ethernet format used in the local network under the above-mentioned network number.

The default is 'auto' and means that the *LANCOM Office* router should automatically detect the binding (only if there is a NetWare server in the local network).

IPX-watch

This option allows you to define the type of management used for IPX watchdog packets.

- **Filter** means that the IPX watchdog packets are neither answered nor transferred locally. Users are always logged off after the period of time set in the NetWare server.

- **Route** causes the watchdog packets to be transferred and, consequently, also causes a regular establishment of connections by means of the server's watchdog packets.
- **Spoof** (default) ensures that IPX watchdog packets are answered locally by the router and therefore that users are no longer automatically logged off. This setting is especially economical but steps must be taken in the server to ensure that users are logged off at specific times in order to prevent the usage of too many user licenses.

SPX-watch

This option allows you to define the type of management used for SPX watchdog packets.

- **Route** causes the SPX watchdog packets to be transferred and, consequently, also causes a regular establishment of connections by means of the server's SPX watchdog packets.
- **Spoof** (default) causes SPX watchdog packets to be answered locally. This setting is especially economical.

NetBIOS-watch

This item specifies how NetBIOS watchdog packets should be treated. NetBIOS watchdog packets occur, e.g., if Windows networks are connected by IPX. The same options are available as with IPX or SPX watchdog packets (filter, route, spoof).

Socket-filter

The socket filter table permits the selective filtering of LAN packets to specific ranges of destination sockets. Filtering is performed for both single IPX packets and propagated IPX packets. The following sockets (which are periodically sent in the network and, therefore, would result in connections being established too frequently) are already entered in the LAN filter table as default values (for details, also see FAQs on the 'IPX router').

Start-socket	End-socket
0455	0457
0550	0555
1401	1402
1480	1481
83ba	83ba
900f	9010

Loc.-routing

This setting supports the scaling of multiple routers in a local network. When all the channels for one router are already seized and packets for other remote stations are still being received at this router, other routers in the LAN may still have free channels.

If the 'Loc.-routing' option is activated, the router forwards the packets in the local network to a router that has propagated a route to the remote station desired. The *LANCOM Office* router has saved this route, although it is less efficient than its own, and marked it with the 'reserve' flag in the RIP table.

The default setting for this option is 'Off' since an IPX client sends a RIP request for the relevant route after a timeout, thus automatically finding a different router through which it can access the destination network.

RIP-SAP-scal.

Another option for supporting scaling is to propagate every route to which there is an active connection with a somewhat better tic count than the actual one. This will ensure that all clients will send their packets for these routes to the *LANCOM Office* router that has the connection. In addition, in the event that all channels are busy, the routes that are no longer available will be propagated as 'DOWN'. Because one or more broadcasts are sent on the LAN by this procedure every time a connection is established and released (which may require other routers for additional broadcasts and may result in a high network load), this feature can be activated and deactivated. The default setting is 'Off'.



LOOP-prop.

Redundant routes, i.e. routes with the same tic and hop count, are only sent to the remote station by which they were not received (split horizon). When the 'LOOP-prop.' function is activated, these routes can still be propagated. Redundant routes are identified in the RIP table by means of the LOOP flag.

Although the propagation of redundant routes is not prohibited by the Novell specification, it should still be avoided as much as possible. Therefore, the default setting is 'Off'.

Setup/IPX-module/WAN-configuration

This option allows you to maintain the data packet settings for the WAN port. The menu has the following layout:

/WAN-configuration	Settings for the WAN side	
Routing-table		Routing table for IPX network and remote station assignment
Socket-filter		Filter table for destination socket filtering

Routing-table

The routing table can hold up to 16 remote stations and destination networks. It contains the following entries:

Remote-ID	Network	Binding	Propagate	Backoff
Name of the IPX remote station	Network address	802.3, II, 802.2, SNAP	Route / Filter	On / Off

The columns have the following meanings:

- **Remote-ID:** Name of the logical remote station (as specified in /Setup/WAN-module/Name-list).
- **Network:** Address of the network on the WAN side. A standalone network must be used, but it must be same for both of the participating routers!

- **Binding:** The Ethernet binding to be used on the ISDN route. This setting is taken into account only if Ethernet encapsulation is set in the layer used. If no binding is specified, a value of 802.3 is assumed.
- **Propagate:** This entry indicates how IPX type-20 packets (NetBIOS propagated frames) are to be handled. The possible settings are Route and Filter. With **Filter**, no propagated frames are routed to the remote station. If the entry has the value **Route**, the packets are forwarded to all currently available remote stations, i.e., there must be a connection to the remote station, or there must be at least one channel available for establishing a connection the remote station.

If no connection or channel is available, the packet is discarded. For this reason, propagated frames can be received by no more than two or, if the external interface is used as a third dial-up line, by no more than three remote stations. This applies particularly to a WAN configuration by LC_CONF.EXE, (*ELSA MicroLink LANCOM MPR* only) because this uses "propagated frames". The default setting is 'Filter'.

- **Backoff:** The IPX router uses a special algorithm (exponential backoff) to keep the connection charges as low as possible in the event of erroneous configurations (see below).

If there is no server in the remote network (e.g. with remote access from a workstation), the router cannot detect this and the corresponding remote station will be deactivated after a day at the latest. In order to prevent this from happening, the exponential backoff algorithm can be deactivated for these remote stations.

The default setting is 'On'.

Socket-filter

The socket filter table permits the selective filtering of WAN packets to specific ranges of destination sockets. Filtering is performed for both single IPX packets and propagated IPX packets.

Setup/IPX-module/RIP-configuration

This option allows you to store settings for RIP data packets (router information). The menu has the following layout:








/RIP-configuration		RIP settings
Table-RIP		Displays the RIP table.
LAN-filter-table		Filter ranges for IPX network addresses (LAN)
WAN-filter-table		Filter ranges for IPX network addresses (WAN)
Routes/Frm		Max. no. of RIP entries per RIP frame sent
Aging-minute(s)		Aging period in update units
Spoofing		Sets RIP spoofing procedure
WAN-update-min.		RIP update period; effectiveness depends on spoofing

Table-RIP

This option allows you to display the entries in the current RIP table. The table contains a maximum of 64 entries.

The entries in the RIP table might, for example, look like the entries shown below with the networks 00000001, 00000002, 00000010, 00000081, where these networks can be accessed via different routers. The flags can be used to determine where these networks are located with relation to the particular router (**local** or **remote**). The entry **direct** indicates whether this network is directly the local or remote network. **DOWN** indicates a network that is known but is not currently available. The table is sorted by the network numbers.

Network	Hops	Tics	Node-Id	Time	Flags
00000001	0	1	00a05702000a	0	local, direct
00000002	1	2	00608c70ab56	1	local
00000010	2	7	00a057020014	1	local, DOWN
00000081	1	6	00a05702000b	0	remote, direct

LAN-filter-table

The LAN filter table permits the selective filtering of routes that are 'learned' via the local network. Filtered routes do not appear in the IPX-RIP table.

A LAN filter table for filtering routes in the range from 00001000 to 00001fff might, for example, have the following appearance:

Start-net	End-net
00001000	00001fff

WAN-filter-table

The WAN filter table permits the selective filtering of routes that are 'learned' via the wide-area network. Filtered routes do not appear in the IPX-RIP table.

A WAN filter table for filtering routes in the range from 00002000 to 00002fff might, for example, have the following appearance:

Start-net	End-net
00002000	00002fff

Routes/FRM

This parameter sets the maximum number of routes that can be included in a RIP frame. The specified value originally defined by Novell is 50. Today, however, it is common practice to pack a higher number of routes in each frame in order to reduce network utilization. If all participating devices in the network support a higher number, this value can be raised as high as 182.

Aging-minute(s)

This option allows you to set the number of times the RIP table will be updated until an entry in the RIP table ages, i.e. until the route recorded there is marked as 'not reachable (down)'. You can enter a value from 1 to 60; the default value is 3.

Spoofing

This option allows you to determine how the router will handle RIP packets.

- If you select **Off**, RIP packets are handled in the WAN in precisely the same manner as in local networks. RIP data are sent to the remote side in the event of new information and at intervals of one minute, i.e. a connection is established.
- With the **Trig** setting, the RIP data is sent to the remote end any time changes are detected.
- With the **Time** setting, the RIP data is sent to the remote end at selectable intervals (see below) but only when a connection exists.
- **pBack** (default) is the most economical setting. In this case, the RIP data is sent to the remote end only when a connection is activated.

*When spoofing is set to **pBack**, entries in the RIP table age only when a new connection is established and an entry has been explicitly marked as 'not reachable'.*

WAN-update-min.

The periodic transfer interval for a spoofing time control in which RIP data can be transferred to the remote side is given here. You can enter a value from 1 to 60 minutes; the default value is 5.

Setup/IPX-module/SAP-configuration

This option allows you to store settings for SAP data packets (server information).








/SAP-configuration		SAP settings
Table-SAP		Displays the SAP table.
LAN-filter-table		Filter ranges for IPX service addresses (LAN)
WAN-filter-table		Filter ranges for IPX service addresses (WAN)
Server/Frm		Max. no. of SAP entries per SAP frame sent
Aging-minute(s)		Aging period in update units
Spoofing		Sets SAP spoofing method.
WAN-update-min.		SAP update period; effectiveness depends on spoofing.

Table-SAP

This option allows you to display the entries in the current SAP table. The table contains a maximum of 128 entries. It is sorted first by service type and then by server name. A SAP table might, for example, have the following appearance:

Type	Server-name	Network	Node-Id	Socket	Hops	Time	Flags
0004	Y	000000c1	000000000001	0451	1	1	local
0047	X	00000001	0000c0123456	8060	1	0	local
0107	Z	000000c1	000000000001	8104	2	1	local

Different SAP types are stored in the table. The server name, the applicable network, the server MAC address (000000000001 for internal server networks), the socket number and information on the location of the server must be read.

LAN-filter-table Entries in the LAN filter table make it possible to exclude specific service information ranges of a Novell network from being included in the SAP table and therefore to make better use of the resources of the IPX router. This also prevents unwanted connections from being established by these SAPs (services).

None of the service information located within a range of filters entered in the LAN filter table is transferred by the local network to the IPX router's SAP table. They are also not transferred to the remote station of the IPX router and therefore are also not available there.

For example, the service information for the printer server is often unnecessary for the remote station of the IPX router. If this information is to be excluded from the SAP table by means of the LAN filter table, the following entry is required:

Start-service	End-service
030c	030c

For a list and description of SAP services, please refer to the section entitled 'Novell SAP Numbers'.

WAN-filter-table

As with the LAN filter table, you can use the WAN filter table to prevent ranges of service information from being transferred from the WAN to the SAP table.

Therefore, the blocked services have resulted in the establishment of a connection to the remote station before the destination router could filter them on the WAN side.

The layout and function of the WAN filter table are exactly the same as that of the LAN filter table. A WAN filter table for filtering file services might, for example, have the following appearance:

Start-service	End-service
0004	0004

Server/FRM

This parameter sets the maximum number of services that can be included in a SAP frame. The specified value originally defined by Novell is 7. Today, however, it is common practice to pack a higher number of services in each frame in order to reduce network utilization. If all participating devices in the network support a higher number, this value can be raised as high as 22.

Aging-minute(s) This option allows you to set the number of times the SAP table will be updated until an entry in the SAP table ages, i.e. until the service recorded there is marked as “not reachable (down)”. You can enter a value from 1 to 60; the default value is 3.

Spoofing This option allows you to determine how the router will handle SAP packets.












- If you select **Off**, SAP packets are handled in the WAN in precisely the same manner as in local networks. SAP data are sent to the remote side in the event of new information and at intervals of one minute, i.e. a connection is established.
- With the **Trig** setting, the SAP data is sent to the remote end any time changes are detected.
- With the **Time** setting, the SAP data is sent to the remote end at selectable intervals (see below) but only when a connection exists.
- **pBack** (default) is the most economical setting. In this case, the SAP data is sent to the remote end only when a connection is activated.




*When spoofing is set to **pBack**, entries in the RIP table age only when a new connection is established and an entry has been explicitly marked as 'not reachable'.*

WAN-update-min. The periodic transfer interval for a spoofing time control in which SAP data can be transferred to the remote side is given here. You can enter a value from 1 to 60 minutes; the default value is 5.

Setup/TCP-IP-module

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

/TCP-IP-module		TCP/IP module settings
Operating		Activates or deactivates the TCP/IP module.
IP-address		Local IP address
IP-netmask		Local network's matching IP network mask
Intranet addr.		Local Intranet address
Intranetmask		Local network's matching Intranet network mask
Access-list		Restricts access to internal functions via TCP/IP.
DNS-default		Domain name server
DNS-backup		Backup domain name server
NBNS-default		NetBIOS name server
NBNS-backup		Backup NetBIOS name server
Table-ARP		ARP table for mapping an IP address onto a MAC address

/TCP-IP-module		TCP/IP module settings
ARP-aging-min.		Dwell time for entries in the ARP table
TCP-aging-min.		Time limit for configuration connections that are inactive
TCP-max.-conn.		Max. number of simultaneous configuration connections to the <i>LANCOM Office</i> router

Operating

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

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

IP address

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

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

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

IP-netmask

The network mask belonging to the IP address must be entered here. The default setting is 255.255.255.0 (class C network). A network mask of 255.255.255.255 means that there is only one computer in this network (the *LANCOM Office* router itself). This setting (an IP address registered in the Internet with a fully assigned network mask) can be used for masquerading via a raw IP access, such as that offered by the provider of the individual network. With such an access an IP address is not assigned to the *LANCOM Office* router by a PPP negotiation, but it must have a fixed IP address registered in the Internet.

Intranet-address

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

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

The default address on delivery is '0.0.0.0'.

Intranet-mask

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



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

If there is already such an IP address in the network, the keyboard (ELSA MicroLink LANCOM MPR only) or the outband configuration (terminal program) must be used to enter another address.



Access-list

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

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



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

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

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

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

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

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

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

IP-address	IP netmask
192.234.222.0	255.255.255.0

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

DNS-default

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

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

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

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

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

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

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

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

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

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

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










TCP-max.-conn. In the *ELSA MicroLink LANCOM MPR*, this option allows you to display the number of TCP connections that can exist simultaneously. In the default configuration, four connec-

tions to the router can exist at one time. You cannot modify this value. It is relevant for configuration sessions only. The number of TCP connections via the router is not limited.

In the *LANCOM Office* router the maximum number of allowable connections can be set here. DEFAULT setting is '0', meaning the same as "any number".

Setup/IP-router-module

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

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

Operating

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

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

IP-routing-table

A maximum of 64 (*ELSA MicroLink LANCOM MPR*) or 128 (*LANCOM Office* router) entries of destination network addresses or direct IP addresses with their associated network mask and names of the remote stations or IP addresses of other local routers can be included in the router table. Alternatively, you can enter a setting by means of which packets to specific destination IP addresses are discarded and are not answered by proxy ARP. This is done by entering 0.0.0.0 for the name of the responsible router.

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

- **On:** IP masquerading is switched on and functions with dynamic assignment of the IP address by the remote station. In this procedure the *LANCOM Office* router queries the IP address '0.0.0.0' at the remote station and is assigned a random IP address by the remote station, which is then used for further processing.
- **Off:** Masquerading is switched off.

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

The IP routing table is generally sorted as shown below:

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

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

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

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

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

- Example
 - The local network address is 192.120.130.0.
 - Three terminal units must be available via proxy ARP with the IP addresses 192.120.130.10, 192.120.130.11 and 192.120.130.12 via a *LANCOM Office* router 'Dresden'.
 - Two destination networks 192.120.131.0 and 192.120.132.0 can be accessed by the remote stations 'AACHEN' and 'BERLIN'.
 - Data packets for the destination network 193.140.300.0 are to be sent to another local router with the IP address 192.120.130.200.
 - Absolutely nothing is to be transmitted to the destination network 193.140.200.0.

- All other non-local data packets must be sent to the router 'PROVIDER' at the Internet service provider.

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

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

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

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

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

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

The table fields have the following meaning:

- Idx.
Unique index. This entry is required to enable the filters to be distinguished. The index may be four characters long and selected as desired.
- D-st., D-end
Destination port range that is to be filtered. A range of 0 to 0 means that no destination port is affected by this filter.
- S-st., S-end

Source port range that is to be filtered. A range of 0 to 0 means that no source port is affected by this filter.

■ Src-address, Src-netmask

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

■ Prot

Protocol that is to be filtered. Possible entries are **TCP**, **UDP**, **ICMP** and all.

The setting **all** filters out every packet from the specified source network or to the destination network

■ Type

Filter type. The possible values are Always-filt., Connect-filt. and Internet-filt.

- **Always** filter: The packet is discarded.
- **Connect** filter: The packet is discarded if there is no connection to the remote station.
- **Internet** filter: The packet is discarded if its destination can be accessed only via the default route.

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

WAN-filter-table

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

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

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

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

■ Dst-address, Dst-netmask

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

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

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

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

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

Proxy-ARP

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



Loc.-routing

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

Setup/IP-router-module/Routing-method

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

The menu has the following layout:

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

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

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




ICMP-routing-method

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

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

Setup/IP-router-module/RIP-configuration

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

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

RIP-type

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

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

R1-mask

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

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

Table-RIP






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

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

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

Setup/IP-router-module/Masquerading

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

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

Service-table

The use of inverse masquerading makes 'services' (e.g. a file server) selectively visible in the Internet by entering specified ports in the service table in the IP network, while all other services and computers remain invisible from the local network (see also 'IP Masquerading (NAT, PAT)' on page 1.4.15). The service table (also called the static masquerading table) can contain up to 16 entries and has the following layout:

D-port	Intranet-addr.
20	10.1.1.10
21	10.1.1.10

The different columns have the following meaning:

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

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

You can use the command

```
telnet 192.38.50.100:27
```

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

Table-masquerading

With IP masquerading, the IP addresses of computers in the local network are rendered invisible to external devices by means of a conversion of addresses and ports in the *LANCOM Office* router. The dynamic masquerading table displays the IP addresses from the local network that the *LANCOM Office* router is currently masking. The dynamic masquerading table has a maximum of 512 (*ELSA MicroLink LANCOM MPR*) or 2048 (*LANCOM Office* router) entries with the following structure:








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

The different columns have the following meaning:

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

Setup/SNMP-module

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

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

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

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

Administrator Administrator's name

Location Device location

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

Register-monitor

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

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

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

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

Delete-monitor

This command removes the entries from the monitor table.

Monitor-table

The monitor table has the following structure:

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

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



Setup/DHCP-module

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

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

Operating

On: The *LANCOM Office* router operates as a DHCP server

Off: The *LANCOM Office* router operates as a non-DHCP server

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



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

Start-address-
pool
End-address-
pool

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

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

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

A valid address is then taken from the pool for the IP address. If the computer has previously been assigned an IP address, it will request this address again, and the LANCOM Office router will attempt to assign it this address again, unless it has already been assigned to another computer.

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

Netmask

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

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

Broadcast-
address

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

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

Max.-lease-
time-minute(s)

The maximum validity period that the LANCOM Office router assigns to a host can be entered here.

The DEFAULT value of 6000 minutes equals approximately 4 days.

Default-lease-
time-minute(s)

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

The DEFAULT value of 500 minutes equals approximately 8 hours.

Table-DHCP

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

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








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

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

- **new**: The computer has made its initial request. The *LANCOM Office* router checks that the address to be assigned to the computer is unique.
- **unkn.**: While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the *LANCOM Office* router cannot obtain additional information on this computer.
- **stat.**: A computer has informed the *LANCOM Office* router that it has a fixed IP address. This address can no longer be used.
- **dyn.**: The *LANCOM Office* router has assigned an address to the computer.

Setup/Config-module

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

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



The configuration language can only be set with the LANCOM Office router.

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

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

If your router must be configured from the WAN side first, this option must be set to 'On'.

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

Maximum connections This option allows you to display the maximum number of remote configuration sessions that can occur simultaneously for the device. There can be four simultaneous configuration connections to a router. You cannot modify this value.

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

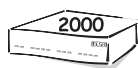
Login-errors This entry specifies the number of failed attempts allowed before the log-in block is activated. An empty password (simply pressing <ENTER> at the password prompt) is not considered an attempt and therefore does not activate the block.



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

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







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



Setup/ab-module

Please refer also to the description in the corresponding chapter in the User Manual for the functions of the telephone system in the *LANCOM Office* router.

The settings for the analog ports (a/b ports) are entered in the AB module. The menu has the following layout:

/ab-module		Configuration module settings
Port-list		Base settings for the various devices
Public-exchange-list		Trunk seizure settings
Class-of-service-list		Authorization settings
Priority-list		Priority settings for router connections
Ringing-sequence		Ringing sequence settings for several connected devices
Country		Country setting where the device is operated

Port-list

The port list has the following layout:

Port	Device	EAZ/MSN(s)	Capab.	Mode	CLIP
1	Telephone	0	A-3,1kHz	0	YES
2	Answering machines	0	A-3,1kHz	8	YES
3	Fax	0	A-3,1 kHz	8	YES
4	Telephone	0	A-3,1kHz	8	YES

To set these options use *ELSA LANconfig* so far as possible.

You can enter the following values for the 4 available a/b ports:

- **Device:** Description of the connected device with no effect on the functions.
- **EAZ/MSN(s):** If your *LANCOM Office* router is connected to an ISDN port with 1TR6, enter the EAZ to which the a/b port is to respond.
If your *LANCOM Office* router is connected to an ISDN port with DSS1, enter the MSN to which the port is to respond. If you wish the port to respond to several different MSNs, enter them here separated by semicolons. For outgoing calls, the first MSN in this list will be reported to the remote station.
- **Capab.:** Select the service with which the a/b port is to work. Possible settings are:
 - 'A-3,1kHz': Analog 3.1 kHz (default setting)
 - 'Speech'
 - 'Fax Grp2/3': Fax Group 2/3
- **Mode:** Select the way in which the a/b ports are to announce incoming calls. This table displays it in the form of a number, which represents an 8-bit mask. The bits have the following meaning:

Bit no.	Meaning
Bit 7	Reserved
Bit 6	Reserved

Bit no.	Meaning
Bit 5	Switches two external connections on hang-up (service feature: ECT)
Bit 4	Autom. call answering from other ports (answering machine mode)
Bit 3	Deactivate port (telephone idle)
Bit 2	Reserved
Bit 1	Charging pulse
Bit 0	Call Waiting

Examples:

- If you wish to activate a service such as call waiting with further calls on this port and generate a charging pulse for a telephone, set bits no. 0 and no. 1 to '1'. The bit display '00000011' is converted to a decimal display and receives the '3'. Enter this '3' as mode into the table.
- It is normally not desirable to activate any of the above functions for a fax and the '0' is entered into the table.
- In the case of an answering machine, as an example only the automatic answer is activated, so you can answer the call when the answering machine has already answered it. Bit no. 4 is switched on for this and the decimal display '16' is entered into the table.

- **CLIP:** You can either activate or deactivate this option (with 'Yes' or 'No'), depending on whether you wish the remote station to know who is currently calling it.

Public-exchange-list

In this list specify for every port whether you are connected with the router internal telephone system (internal) or with the external ISDN bus (private) when you lift the receiver or press the flash key.

Class-of-service-list

Here set whether all calls, national long-distance and local calls only or local calls only can be conducted from this port. Enter additional call numbers that may not be called from this port.

To set these options use *ELSA LANconfig* so far as possible.

- **Class-o:** This table displays it in the form of a number, which represents an 8-bit mask. The bits have the following meanings:

Bit no.	Meaning
Bit 7	External calls not permitted
Bit 6	free
Bit 5	Allow local calls and national long-distance calls without authorization number
Bit 4	Allow local calls only without authorization number
Bit 3	free
Bit 2	free
Bit 1	Allow local calls and national long-distance calls with authorization number
Bit 0	Allow local calls only with authorization number

As with 'mode' in the port list, the individual bits are set to activate a function, the bit display is then converted to decimal display and entered into the table.

Examples:

- All numbers greater than '127' block the port for all outgoing calls.
- '00110011' is converted to '51' and allows all calls, even foreign calls.

Priority-list

The priority for a port controls the option for breaking connections via this a/b port router connections. Option '1' does not break router connections, the setting '2' breaks only auxiliary connections of a router connection with channel bundling, the selection '3' also breaks main channels of a router connection.

Ringling-se- quence

This sets how incoming calls are reported to the a/b ports when more than one port is to ring. The possible values are:

- **single:** All ports ring in succession.
- **paired:** Two ports always ringing alternately.
- **all:** All ports ring simultaneously.

Country

This sets the country where the device is operated. The country setting sets the following values:

- Length of the flash pulse
- Length of the charging pulse
- Frequency of the charging pulse
- Frequency of the ringing signal








Setup/LANCAPI-module

Configuring *LANCAPI* basically involves answering two questions:

- What call numbers from the telephone network should *LANCAPI* respond to?
- Which of the computers in the local network should be able to access the telephone network via *LANCAPI*?
- Via which UDP port do the *LANCAPI* server and *LANCAPI* clients communicate?

The *LANCAPI* module has the following layout:

/LANCAPI-module		LANCAPI settings
Operating		<i>LANCAPI status</i>
Access-list		List of computers allowed to use the <i>LANCAPI</i>
UDP-port		UDP port for communication between the <i>LANCAPI</i> server and clients
EAZ-MSN(s)		EAZ or MSN to which the <i>LANCAPI</i> should respond
Prio-out		Priority for the <i>LANCAPI</i> versus router connections

- **Operating:** 'on', 'off' or 'outgoing'. Under the last setting the *LANCAPi* will not accept incoming calls.
- **Access-list:** This option allows you to limit the circle of computers permitted to use the *LANCAPi*. This table can have a maximum of 16 entries. If the table is empty, all computers can access the *LANCAPi*.
- **UDP-port:** This port is set to '75' as the default setting. Change this port only if other devices on your network already use this port.

When you change the port, all active connections via the LANCAPi are lost!

- **EAZ/MSN(s):** This option allows you to enter the call numbers to which the *LANCAPi* is to respond. If you wish to enter more than one number, place a semicolon between the individual numbers.
- **Prio-out:** The priority for a port controls the option for breaking outgoing connections via the *LANCAPi* router connections. Option '1' does not break router connections, the setting '2' breaks only auxiliary connections of a router connection with channel bundling, the selection '3' also breaks main channels of a router connection.








Setup/LCR-module

Enter the following information when setting the least-cost router:

- For which modules in the *LANCOM Office* router should the LCR functions be active?
- Which area codes should be diverted when via which call-by-call provider?

When setting the least-cost router please also note the explanation in the 'The least-cost router' section in the chapter 'Operating Modes'.

The LCR module has the following layout:

/LCR module		Least-cost router settings
Router-usage		Activate LCR for the router modules, On or Off
Lancapi-usage		Activate LCR for the <i>LANCAPi</i> , On or Off
ab-port-usage		Activate LCR for the a/b ports, On or Off
Timetable		List of computers allowed to use the <i>LANCAPi</i>
Celebration-day-table		UDP port for communication between the <i>LANCAPi</i> server and clients

The timetable has the following layout:

Index	Prefix	Days	Start	Stop	Number-list	Fallback
1	0171	192	0:00	23:59	01013;01070	YES

The individual entries have the following meaning:

Index	Continuing index of entries in the table.
Prefix	Area code to be diverted.
Days	Validity of the entry for week days and holidays shown in an 8-bit mask: Bit 0 represents Monday, bit 7 holidays. The entry '31' therefore designates all business days, '192' Sundays and holidays.
Start	Beginning time for the validity of the entry on the defined days.
Stop	Termination time for the validity of the entry on the defined days.
Number-list	Network identification number of the call-by-call providers.
Fallback	Automatic fallback to your own telephone company if all call-by-call numbers are busy.

Example:

set 1 02 31 1:00 11:59 01030;01090;01070 to On diverts all long-distance calls to region '02' between one and twelve o'clock to the provider with the network identification number '01030'. If this number is busy, the network identification numbers '01090' and '01070' will be attempted. If they are also not available, the connection will be made via the normal telephone company.

The Celebration day table has the following layout:

Index	Date
1	01010000
2	01050000
3	03100000
4	25120000
5	26120000
6	02041999
7	13051999

The individual entries have the following meaning:

Index	Continuing index of entries in the table.
Date	Dates of holidays. Enter the index and the date in full without separators, e.g. 'set 8 13041999' for April 13, 1999 as the eighth entry in the list. Enter '0000' as the year for annually occurring holidays.







Setup/Time-module

The least-cost router in the *LANCOM Office* router requires correct time information to calculate the call number diversions via call-by-call provider. Precise time information is also desirable for some statistics.

The time in the *LANCOM Office* router may be set manually (with the 'time' command) or automatically read from the ISDN network.

For automatic time comparison when the module is switched on, a previously specified remote station is called directly and the time information is taken from the ISDN network. So long as the time module is switched on, the time will be taken from the ISDN every time the *LANCOM Office* router establishes a connection.




The time module has the following layout:

/Time-module		Time module settings
Operating		Activating the module: On, Off
Current-Time		Displays the current time in the device.
Time-EAZ-MSN		Call number to which a connection must be established to receive time information from the ISDN.
Service		Service detection for the called remote station: Digital for BBS systems, providers, etc. Analog for telephone announcements or other speech services



Setup/Other

This menu allows you to select the options for the display and keyboard. The menu has the following layout:

/Other		Display and keyboard settings
LCD-brightness		Sets the LCD contrast.
Key-password		Issues keyboard password
Key-lock active		Locks the keyboard.

LCD-brightness This option allows you to enter the LCD contrast: Valid values are 1 to 8. The default value of 3 is set after a restart.

Key-password This option allows you to enter the keyboard password. This password must not exceed 8 characters. The key password can only be entered from the keyboard.

Key-lock active This option allows you to lock the keyboard. When the keyboard is locked, the password is requested as soon as a key is pressed. The keyboard is unlocked when the correct password is entered. If an incorrect password is entered, the keyboard remains locked.







The keyboard can only be locked when a password is set.

The keyboard lock can be set and canceled by means of remote configuration (also see the section entitled 'Frequently Asked Questions and Answers').

If both the keyboard password and the password for protecting the configuration are forgotten, it will no longer be possible to configure the router without losing all settings!

Firmware

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

/Firmware		Display and keyboard settings
Version-table		Displays hardware releases and serial numbers for the <i>LANCOM Office</i> router and the device connected to the serial interface.
Firmware-upload		Initiates a firmware upload via the serial interface using X-modem.
Table-firmsafe		Information on the two firmware versions stored in the device and on the bootloader.
Mode-firmsafe		Firmware activation mode
Timeout-firmsafe		Time in minutes required to test new firmware
Test-firmware		Tests the inactive firmware

Version table

The version table displays the version both of the device itself and of the device connected to the serial interface.

lfc	Module	Version	Serial number	Online-Bps
S0	ELSA MicroLink LAN-COM MPR	v1.39C 28.03.97	0317.000.005	
Ser1	ELSA ISDN/TLV.34	v1.57J 08.05.96	0326.003.908	230400

lfc	Module	Version	Serial number
S0	LANCOM 2000 Office	v1.39C 28.03.97	0317.000.005

The Online-Bps entry indicates the transmission rate used by the *LANCOM Office* router when transmitting data to external modules. The maximum rate possible is determined when the external module is initialized.

Table firmsafe



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

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

Mode firmsafe







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

- 'immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
 - The new firmware is successfully loaded and then operates as desired. Everything is then in order.
 - However, if the new firmware does not operate correctly, it may not be possible to communicate with the device after the restart. If an error occurs during the upload, the *LANCOM Office* router will automatically reactivate the previous firmware and will restart the device with it.
- 'login': To prevent problems caused by defective firmware, the second option will load the firmware and start it immediately.
 - In contrast to the first option, the *LANCOM Office* router will wait until it has successfully logged on to the device over outband or inband (by telnet). The new firmware will only be permanently activated when the login occurs successfully within the time set under 'Timeout firmsafe'.
 - If it is not possible to communicate with the device and it is not possible to log on to it, the *LANCOM Office* router will automatically activate the previous firmware version and restart the device with it.
- 'manual': The third option allows you to set a period (Timeout firmsafe) beforehand for testing the new firmware. The *LANCOM Office* router will start with the new firmware and wait for the preset period until the loaded firmware is manually activated and therefore becomes permanently effective.

Other

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

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

Other/Manual Dialing

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

Boot-system This option allows you to reboot the device.

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

Reset-system This option resets all the settings that have been entered. The device is reset to the delivery version and the following display briefly appears on the *LANCOM Office* router:

System reset
please wait ...

A reset is being performed.

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

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

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

LANCOM Office router Internal

This chapter provides information on the internal functions of the *LANCOM Office* router. It is not always necessary in day-to-day work with the ISDN routers but can be very useful to specialists in specific situations.

Script Processing	2
Online Trace Outputs	5
Policy Based Routing	18

Script Processing

General

Some Internet service providers (e.g. CompuServe) run a script-controlled logon procedure before a PPP negotiation. To enable the establishment of such a connection, a simple script process is implemented in the *LANCOM Office* router.

A script can include the following elements:

Element	Description
<>	Send the included text with a carriage return at the end.
[]	Wait until the included text has been received. The text may be upper or lower case. It is sufficient to enter an unambiguous subtext.
\$U	Send the user name (from the PPP table) with a carriage return at the end.
\$P	Send the password (from the PPP table) with a carriage return at the end.
\$C	End of the script

As previously noted in the overview, the user name and password are taken from the PPP table if there is an appropriate entry there. If there is no user name in the PPP table, the device name of the *LANCOM Office* router is forwarded as the user name.

Once the script is complete, a PPP negotiation is started or the login procedure is concluded.

The layer 3 entry in the layer list is used to define whether a PPP negotiation is started after the script has been processed. There are three possible entries:

SCPPP	A synchronous PPP negotiation is started once the script has been processed.
SCAPPP	An asynchronous PPP negotiation is started once the script has been processed.
SCTTRANS	The logical connection to the remote station exists once the script has been processed. There is no more protocol negotiation.

The Script List

Scripts are entered in a script list table provided for that purpose. This table is in the /Setup/WAN module and has the following structure:

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

The entries in the script list have the following meaning:

Device name:	Name of the logical remote station.
--------------	-------------------------------------

Script: All commands to be executed—a maximum of 58 characters per line is available. If the required command sequence is longer, another entry similar to the Round-Robin list for the logical remote station may be added. The syntax for this is: Device name followed by '#' and a number. The entries are processed from top to bottom.

Example:

Device name	Script
CSERVE#1	<>[Host]<CIS>[User]
CSERVE#2	\$U[Password]\$P[PPP]\$C

In the *LANconfig* the script list is on the 'Communication' tab.

CompuServe Select

The settings required for selection on the CompuServe network via X.75, asynchronous PPP and script control with an example.

Layer list:

Layer-name	Encaps.	Lay-1	Lay-2	L2-Opt.	Lay-3
CSERVE	TRANS	SCAPPP	X.75LAPB	none	HDLC64K

Name list:

Device-name	Call-number	B1-HZ	B2-HZ	Layer-name	Callback
CSERVE	0021194260	60	60	CSERVE	Off

PPP list:

Device-name	Authent.	Password	Time	Rep.	User-name
CSERVE	none	*	0	0	xxxxxx,xxxx/PPP:CISPPP

The CompuServe account is to be entered for xxxxxx,xxxx.

Script list:

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

The script elements have the following meaning:

Element	Meaning
<>	Start script on the remote station by sending a carriage return.

Element	Meaning
[Host]	Wait for the answer from the CompuServe node. At some point the 'Host Name' will appear in the answer.
<CIS>	Send 'CIS' followed by a carriage return.
[User]	Wait for the answer. CompuServe requests the 'User ID'.
\$U	Send the user name. For CompuServe this consists of the CompuServe User ID with attached '/PPP:CISPPP'. The user name is taken from the PPP table and sent to the remote station with a final carriage return.
[Password]	Wait for the password query.
\$P	Send the password followed by a carriage return. The password will be taken from the PPP table.
[PPP]	Wait for the connect message from the remote station.
\$C	The script is fully processed. The asynchronous PPP negotiation (SCPPP) in the layer list is started.

Online Trace Outputs

General

With so-called 'online trace outputs' (control outputs) the user can receive information on internal processes of a working *LANCOM Office* router. Such information can aid in finding erroneous configurations easily and securely, both from *LANCOM Office* router also from other devices with a *LANCOM Office* router.

The online trace outputs can be flexibly administered for individual protocols and functions in the firmware and individual configuration sessions. With session-based 'Trace Profiles' only the trace information activated within a session is displayed.

The online trace outputs are controlled by a newly implemented command in the remote configuration, which is evaluated by the command interpreter and gives a direct acknowledgment of the settings that have been made to the user. Changes to these settings are effective immediately and generate or suppress the corresponding outputs directly.

The online trace outputs are displayed by the remote configuration with a time delay with respect to the actual event. The time stamp that is optionally displayed reflects the time of the output, but not the time of the actual event. There is usually not a substantial difference between these times; however, this point should always be considered when analyzing the outputs.

All displays within the online trace outputs are shown in plain text so far as possible. Because analysis of network protocols cannot completely avoid showing numerical parameters and a trace system only makes sense when the information displayed is also understood, exact descriptions of the trace information will be given below for all protocols and functions.

If displays are activated for a protocol, the next output will overwrite the current system prompt; every additional output will be preceded by a <Return> <LineFeed>. If the user presses a key, the entire buffered input will be shown again with the current system prompt. The user therefore receives visual feedback and inputs need not to be entered 'blind.'

Control of Trace Outputs

Trace outputs are controlled by command line in the usual way. For this purpose, the remote configuration has the command `trace` added; this has the following command syntax

`trace [key] [parameter] ...[parameter]`

Shows or influences the status of the trace outputs of individual protocols or functions.

Key	'?' display a help page '+' activate the trace outputs '-' deactivate the trace outputs '#' toggle the trace outputs (toggle) (no) status display
Parameter	Symbolic protocol or function name.

Keys and parameters must be separated by spaces. The keys are recognized by the command interpreter only if they are unambiguous, ie they consist of one of the characters listed above with no prefix or suffix. For the input of the symbolic protocol or function name the input of an unambiguous prefix is sufficient, as usual.

Any number of keys and parameters may be entered in a command line, limited only by the size of the line input buffer. The parameters are processed corresponding to the last preceding key. If a key is not entered prior to the parameters, the status of that trace function (ON or OFF) is output.

It should also be noted that the command line is processed from left to right. Therefore, the trace output of a parameter can be activated and deactivated several times in one line, because it is toggled from the input buffer while the token is being read (see also examples).

In addition to activating online trace outputs, the preset output of the system time and the protocol names may be activated or deactivated via the key words 'Time' and 'Source.' Without these two displays every trace output is shortened to 21 characters.

Examples for Control of Trace Outputs

The table below is intended to show some practical examples of how the command for the trace outputs can be used:

Input	Effect
trace	Output of all protocols that can be generated in the trace outputs configuration session, and the status of the outputs (ON, OFF).
trace + all	Activates all trace outputs in the current session.
trace + protocol display	Activates all connection structural protocols and the display outputs.
trace + all - icmp	Activates all trace outputs, but deactivates outputs from the ICMP protocol.
trace ppp elsa	Shows the status of the PPP and ELSA trace outputs.
trace # ipx-rt display	Toggles the trace outputs of the IPX router and the display outputs.
trace - time	Deactivates the operating time display before the actual output.

Supported Protocols and Functions

The following symbolic names for protocol stacks are supported:

Status	Display status messages via connections
Error	Display error messages via connections
ELSA	Display ELSA protocol negotiation (only <i>ELSA MicroLink LANCOM MPR</i>)
PPP	Display PPP protocol negotiation
SCRPT	Display scrip negotiation
IPX-Rt.	Display IPX routing
RIP	Display IPX routing information protocol
SAP	Display IPX service advertising protocol
IPX-Wd.	Display IPX watchdog spoofing
SPX-Wd.	Display SPX watchdog spoofing
NetBIOS	Display IPX NetBIOS administration
IP-Rt.	Display IP routing
IP-RIP	Display IP routing information protocol
ICMP	Display Internet control message protocol
IP-MASQ	Display procedures in masquerading module
ARP	Display address resolution protocol
DHCP	Display Dynamic Host Configuration Protocols (only <i>LANCOM 1000 Office</i> and <i>LANCOM 2000 Office</i>)
Packet dump	Display of the 64 bytes of a packets in hexadecimal format (only <i>LANCOM 1000 Office</i> and <i>LANCOM 2000 Office</i>)

In addition to these parameters there are also the following 'group parameters' (parameters for a specific type of protocol), with whose aid the online trace outputs for a complete, logically connected protocol family can be activated or deactivated:

All	Display all online trace outputs
Display	Display 'status' and 'error'
Protocol	Display 'ELSA', 'PPP' and 'SCRPT'
TCP-IP	Display 'IP-Rt.', 'IP-RIP', 'ICMP', 'ARP' and 'IP-MASQ'
IPX-SPX	Display 'IPX-Rt.', 'RIP', 'SAP', 'IPX-Wd.', 'SPX-Wd.' and 'NetBIOS'

Finally, still more parameters are recognized with which the display format of the trace outputs can be influenced

Time	Display the system time as a prefix
Source	Display the generating protocol as a prefix

Every trace output is shortened to 21 characters by switching off the prefix outputs 'time' and 'source'. The output of the prefixes is activated by default.

Prefix Output 'Time'

By activating the prefix output 'time' every trace output has the system time (at the time the output is generated) in the following form as a prefix

- Format: [days]d; _[hours]:[Minutes]:[Seconds]_
- Example:

12t; 07:23:15

corresponds to the system time of twelve days, seven hours, twenty-three minutes and fifteen seconds.

Prefix Output 'Source'

Activation of the prefix output 'source' shows a trace output of the symbolic name of the protocol that caused this trace output. The display is always 9 characters (if necessary by filling spaces).

- Example: ICMP

ie the following trace output was caused by the ICMP protocol.

Online Trace 'Status'

The output under 'status' describe status changes on a WAN interface (at present only the internal S₀ terminal). They are displayed in the following format:

- Format: [Interface] [Status]
- Example:
Ch01: Dial 8700

On the first B channel of the internal S₀ terminal the call number 8700 is dialed.

Online Trace 'Error'

The outputs under 'error' describe errors that have occurred on a WAN interface. They are displayed in the following format:

- Format: [Interface] [Error]
- Example:
Ch01: No response

The remote station dialed did not react to the call.



Online Trace 'ELSA'

The outputs under 'ELSA' describe the sequence of a protocol negotiation in the ELSA format by displaying protocol frames received and sent, their content and the resulting actions. They are displayed as shown below

- Format: [Interface] [Direction] [Frame type] [Parameter] [Action]
- Example: (Passive establishment of a connection without CLIP evaluation)
Ch01: Rx protocol request ELSA.SUP.TEST Accept
Ch01: Tx protocol response ELSA.SUP.1
Ch01: Rx protocol response ELSA.SUP.TEST Connect

A protocol request with device ID 'ELSA.SUP.TEST' is received on the first B channel. Because this is an authorized peer (remote station or partner), the ID is accepted and a protocol response with its own ID 'ELSA.SUP.1' is returned. With another protocol response 'ELSA.SUP.TEST' displays the receipt of the protocol response, the three-way handshake is complete and the logical connection is established.

Online Trace 'PPP'

The point-to-point protocol consists of a collection of subprotocols, of which *LANCOM Office* router detects and manages the following

LCP	The link control protocol
PAP	The password authentication protocol
CHAP	The challenge-handshake protocol
IPXCP	The IPX control protocol
IPCP	The IP protocol

These PPP subprotocols are addressed directly in specific phases during a protocol negotiation. The link control protocol is negotiated within the ESTABLISH phase; at this time only LCP packets are permitted within the PPP. If an authentication is negotiated by the LCP, PPP switches into the AUTHENTICATE phase; LCP, PAP and CHAP packets may be transmitted from this point. After the end of the (optional) authentication PPP switches to the NETWORK phase; LCP, authentication and network control protocol packets (such as IPXCP and IPCP) may be transmitted immediately in any combination. To terminate a PPP connection it switches into the TERMINATE phase where once again only LCP packets are permitted. Once the connection has been terminated, PPP is in the DEAD phase. It will switch into the ESTABLISH phase only when a new connection is established. Every PPP phase change is displayed in the form

Change Phase to [New phase]

approximately as below

Change Phase to AUTHENTICAT

Received and sent packets, important parameters and options with completed actions are displayed for all PPP subprotocols listed above. A received frame is always displayed in the following format:

■ Format: [Interface] Rx [Protocol] [Packet type] [Packet type] [Length of packet]

■ Example:

Ch01: Rx IPXCP ConfReq ID=00 Length=22

In the above example a configure request for the IPX control protocol with the ID 00 and a length of 22 bytes has been received on the first B channel. If a packet cannot be assigned to any of the five subprotocols, this message appears

■ Format: [Interface] Rx Unknown Protocol [Protocol ID]

■ Example:

Ch01: Rx Unknown Protocol 8029

A Packet with the protocol ID 8029 (= Appletalk control protocol) has been received.

Online Trace 'IPX-Rt.'

The outputs under 'IPX-Rt.' describe the processing of IPX frames by the IPX router. They are displayed in the following format:

- Format: [Source interface] [IPX target address] [IPX source address] [Target / Action]

- Example:

Internal Rx

DstAddr: 00000002 ffffffff 0453

SrcAddr: 00000002 00a057123456 0453

WAN-Tx Peer: ELSA.SUP.TEST

The IPX router has received a frame from an internal process (in this case from the entity of the routing information protocol) whose target address is assigned to a logical remote station (ELSA.SUP.TEST) and therefore is sent to a WAN interface.

LAN RX

DstAddr: 00000001 ffffffff 0455

SrcAddr: 00000001 0123456789ab 0455

Filter

The IPX router has received a NetBIOS frame (IPX-socket 455) from the local network, which is to be forwarded as broadcast ffffffff to all stations in network 00000001. Because a filter has been set on the socket, the frame is rejected by the router.

Online Trace 'RIP'

The outputs under 'RIP' describe the processing of IPX routing information protocol frames by the RIP process of the IPX router. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit/Action] [Source node address] [Frame type] [Para.] [Network address] [Hops] [Tics] [Action] ... [Network address] [Hops] [Tics] [Action]

- Example:

LAN-Rx node: 0000c0123456 Req: 00000002

An RIP request for the IPX network 00000002 is received from the local network. The RIP request was sent from the IPX node 0000c0123456.

- Example:

LAN-Rx node: 00a057123456 Resp

Route: 00000002 Hops: 0001 Tics: 0002 Up

An RIP response (routing information protocol response) was received from the local network (generated by the IPX node 00a057123456). With this response route 00000002, with a hop distance (number of interim stations) of 1 and a tic distance of 2, is entered as available again in the RIP table.

LAN update

The RIP process sends all required routing information to the local network.

Online Trace 'SAP'

The outputs under 'SAP' describe the processing of IPX service advertising protocol frames by the SAP process of the IPX router. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit/Action] [Source node address] [Frame type] [Para.] [Service type] [Server name] [Action] ... [Service type] [Server name] [Action]
- Example:

LAN-Rx node: 00a057123456 response

0004 FS_development up

0107 FS_development up

023f FS_development up

0511 FS_development up change

030c 08000912345678CGNP-development filtered

An SAP response was received (sent by the IPX node 00a057123456) by the local network. With this response the servers 'FS_development' (file server), 'FS_development' (NetWare 386 server), 'FS_development' (DNS server) and 'FS_development' (time sync server) are recorded as available again in the SAP table. In this case the status of the time sync server 'FS_development' has changed in the SAP table (ie the server was previously not available). The last displayed server is a print server; because this server type is set with a SAP filter, it is not recorded in the SAP table but is rejected.

LAN trigger

Because of a received SAP response a status change in the SAP table has occurred, which is immediately reported in the local network by the SAP process; the change can therefore only have occurred because of the WAN's evaluation of a SAP response.

LAN age

The SAP process of the router "ages" all server/services forwarded from the local network minute by minute. After a period that can be adjusted a SAP entry is deleted (Setup/IPX-module/SAP-configuration/Aging-minutes)

Online Trace 'IPX watchdogs'

The outputs under 'IPX-Wd.' describe the processing of so-called 'IPX watchdog' packets. These are packets that are sent at regular intervals from a Novell server to a workstation to verify the connection to this workstation. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit] [Source address] [Target address] [Action]

- Example:

LAN RX

DstAddr: 12345678 00a057654321 0451

SrcAddr: 00000002 00a057123456 0451

Spoof

The *LANCOM Office* router has received an IPX watchdog from the node 00a057123456, which was intended for checking a remote workstation. Because the remote network with the workstation is active, the IPX watchdog is answered locally by *LANCOM Office* router to avoid establishing a connection unnecessarily. Alternatively the following displays for actions will appear:

- **Route:** The IPX watchdog is forwarded (establishes a connection)
- **Filter:** The IPX watchdog is rejected and not answered
- **Dst Net DOWN Error:** The IPX watchdog target network is not available

Online Trace 'SPX watchdogs'

The processing of 'SPX watchdog' packets by the outputs under SPX-Wd. is described analogous to the trace outputs for IPX watchdogs. These are packets sent by a Novell server at regular intervals to the workstation to check an SPX connection (e.g. R console). The trace outputs are displayed as follows:

- Format: [Source interface] [Receive/Transmit] [Source address] [Target address] [Action]

therefore completely analogous to the displays of the IPX watchdog packets.

Online Trace 'IPX-NetBIOS'

The outputs under NetBIOS describe the processing of IPX NetBIOS and IPX propagated packets. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit] [Source address] [Target address] [Action]
- Example:
LAN RX

DstAddr: 12345678 00a057654321 0455

SrcAddr: 00000002 00a057123456 0455

Route

Online Trace 'IP-Rt.'

The outputs under 'IP-Rt.' describe the processing of IP frames by the IP router. They are displayed in the following format:

- Format: [Source interface] [IP target address] [IP source address] [Protocol] [Target port] [Source port] [Type of service] [Action] [Target]
- Example:
LAN RX

```
DstIP: 195.162.38.161, SrcIP: 194.162.38.162
Prot.: TCP, DstPort: 23, SrcPort: 1197, TOS: ----
Route: WAN-Tx peer: R1
```

The IP router has received a TCP packet from the computer with the IP address 194.162.38.162, which is to be sent to the computer 195.162.38.161.

The source port is 1197, the target port 23 (telnet), a bit is not set in the TOS. The field TOS may accept the following values (or a combination of them):

D---	Low delay
-T--	High throughput
--R-	High reliability
---C	Low costs

The packet is routed and the target computer can be reached under the logical remote station **R1**. Therefore, the packet is sent on a WAN interface.

LAN RX

```
DstIP: 195.162.38.161, SrcIP: 194.162.38.162
Prot.: ICMP, DstPort: ---, SrcPort: ---, TOS: --R-
Route: WAN-Tx peer: R1
```

The IP router has received an ICMP packet from the computer with the IP address 194.162.38.162, which is to be sent to the computer 195.162.38.161.

Because ICMP does not know any ports, --- is output as target or source port. The field **High Reliability** is set in the TOS.

Online Trace 'IP-RIP'

The outputs under 'IP-RIP' describe the processing of IP routing information protocol frames by the RIP process of the IP router. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/transmit/Action] [Source address] [RIP version] [Routing domain] [Network address] [Network mask] [Best route] [Distance] [Action] ... [Network address] [Network mask] [Best route] [Distance] [Action]

- Example:

```
LAN-Rx Src: 194.162.38.252
```

```
Vers.: RIP-1      Routg.Dom.: 0000
```

```
190.254.0.0      255.255.0.0    194.162.38.1623 Store
```

```
195.126.38.0     255.255.255.0  194.162.38.1623 update
```

```
255.255.255.255 0.0.0.0        194.162.38.1622 Discard
```

```
194.162.38.0     255.255.255.0  194.162.38.1622 Discard
```

An RIP-1 frame has been received from the local network. This frame contains the route to the networks 190.254.0.0, 195.126.38.0, 255.255.255.255 (DEFAULT route) and 194.162.38.0. The procedure with these routes was as follows:

Route 190.254.0.0 is saved because it is either better than the prior one or is still unknown.

Route 195.126.38.0 is processed, ie the route is unchanged, only the distance may have changed. In every case the aging timer is reset.

The DEFAULT route has been rejected because a better route is known.

The route to network 194.162.38.0 is rejected because it is a route to the local network (split horizon).

The trace outputs of received RIP frames are always done after they have been evaluated by the RIP process and network masks (RIP-1) and best route have been determined. With RIP frames that have been sent the packets are displayed as they were sent. For example, with RIP-1 frames this means that the network masks are always output as 0.0.0.0.

Online Trace 'ARP'

The outputs under 'ARP' describe the processing of address resolution protocol frames by the TCP-IP module. The trace outputs are displayed in the following format:

- Format: [Source interface] [Receive/Transmit/Action] [Source address] [Target address] [Target/Action]

- Example:

LAN-Rx request

SrcIP: 194.162.38.162, DstIP: 194.162.38.171

Cache update: 194.162.38.162 : 0000c0717860

Response LAN-Tx

An ARP request for the IP address 194.162.38.171 has been received from computer 194.162.38.162. The MAC address of the source computer is saved in the ARP table. In addition, the queried computer is the *LANCOM Office* router. Then an ARP response is sent back on the LAN interface.

Online Trace 'ICMP'

The outputs under 'ICMP' describe the processing of Internet control message protocol frames by the TCP-IP module. The trace outputs are displayed in the following format:

- Format [Source/Target interface] [Receive/Transmit] [Source/Target address] [Message] [Action]

- Example:

LAN RX

SrcIP: 194.162.38.162: Echo request

LAN TX

DstIP: 194.162.38.162: Echo reply

An ICMP echo request (**ping**) from computer 194.162.38.162 has been received on the LAN interface. The *LANCOM Office* router answers this with an ICMP echo reply.

Online Trace 'IP-MASQ'

The outputs under 'IP-MASQ' describe the procedures in the masquerading module. The opening and the closing of a masked connection is output. The display is in the following format:

- Format: [Open/close]: [Protocol] [IP source address] [Source port] [Mapped port] [Reason]

TCP, UDP or ICMP are possible protocols. If the protocol is ICMP, the source port gives the identifier of the request packet. The mapped port field shows how the source port has been set. The cause of a close is given in the reason field. Possible reasons are:

Timeout	The set protocol timeout is expired
TCP finish	A TCP connection was terminated normally
TCP reset	A TCP connection was interrupted because of an error in one of the machines involved
Port assigned	A 'passive' TCP connection was assigned to source port. Example: FTP in passive mode

■ Examples:

```
Open: TCP SrcIP: 10.0.0.44, 1121 -> 64107
```

```
Open: TCP SrcIP: 10.0.0.44, 1122 -> 64104
```

```
Open: TCP SrcIP: 10.0.0.44, 1123 -> 64105
```

```
Close: TCP SrcIP: 10.0.0.44, 1121 -> 64107 TCP reset
```

Online Trace 'SCRPT'

The outputs under 'SCRPT' describe the progress of a script negotiation. The display is in the following format:

■ Format: [Source interface] [Receive/transmit/Error] [Text] [Action]

■ Example:

```
CH01: Rx: Password -> Tx: * \r
```

In the above example, the password is requested by the remote station. It is returned to the remote station (hidden under a '*').

Online Trace 'DHCP'

The outputs under 'DHCP' describe the procedures in the Dynamic Host Configuration Protocol. The queries from DHCP clients and the answer from the DHCP servers are then displayed in the *LANCOM Office* router. The display is in the following format:

■ Format: [DHCP Client Message] [DHCP Server Message]

Online Trace 'Packet dump'

The 'packet dump' online trace supplements the trace outputs, which are generated by the IP router. The first 64 bytes of a packet is output in hexadecimal format.

Policy Based Routing

General

The term 'policy based routing' describes the option of using additional routing methods to the standard routing procedure for IP packets (these 'policies').

To make the in-band configuration easier on wide-area networks with heavy data traffic and to improve the cooperation of *LANCOM Office* router with 'ping' and 'traceroute' mechanisms, two methods for the IP routing have been introduced. Both methods are based on the evaluation of the 'Type of Service' field in the IP header.

The 'Type of Service' field (for short TOS) describes how IP packets should preferably be treated (but need not be), i.e. it reflects the preferred processing procedure intended by the generator of this IP packet. TOS has the following structure in this context

Bit 7, 6	Bit 5	Bit 4	Bit 3	Bit 2, 1, 0
Unused	R eliable transmission	High T hroughput	Low d elay	Precedence

The **R** and the **D** bit are evaluated and the behavior adapted to its circumstances by the routing methods.

A set **R** bit requires secured transmission of the associated IP packet. Packets identified as such are always transmitted over a 'secured' queue corresponding to their reception sequence. In an extreme case this can result in a 'normal' packet that is already in a transmission queue being removed and placed back into the heap to make room for the packet to be sent. This occurs if the maximum number of buffers for the associated connection has already been used. However, the transmission sequence between packets with a set **R** bit and 'normal' bits is not changed by this mechanism.

The secured transmission can be activated for all ICMP packets independently of the entry in the 'Type of Service' field. Because an ICMP packet identified as such is sent without changing the transmission sequence, the throughput delays of a *LANCOM Office* router can be determined by 'ping' or 'traceroute'.

With a set **D** bit the generator requests the fastest possible forwarding of an IP packet. IP packets identified as such are transmitted over an 'urgent' queue before the send queue packets corresponding to their reception sequence. On one hand, this results in changes in the transmission sequence, because an IP packet identified as last received is sent first. On the other hand, there is the possibility that a packet already in the send queue will be removed from it again to make room for the IP packet that is to be sent (see above).

Packets that are already in the secured or urgent queue are not rejected. If there is no longer a packet in the normal send, secured or urgent queue, no more packets can be sent. Received IP packets are therefore rejected even with the **D** or **R** bit set.

Examples

With the setting

Setup/IP router module/Routing method/IP TOS

the 'Type of Service' field of the IP header of a received packet is evaluated as described above, ie IP packets with set **D** bit are placed in the urgent queue and packets with set **R** bit in the secured queue. All other packets are placed in the normal send queue.

This means simultaneously that any 'normal' IP packets from 'secured' or 'urgent' packets can be removed (with maximum filling of the send queue of this connection) or changes in the packet sequence can be made.

In the 'normal' setting all IP packets are treated equally, in accordance with the routing regulations of the Internet protocol.

With the setting

Setup/IP router module/Routing method/ICMP secured

all received ICMP packets are transmitted as if they had the **R** bit in the 'Type of Service' field of the IP header (see above).

This means that the secured transmission of ICMP packet may result in errors in other data flows. The latency period of the router is however not influenced, because the ICMP packet is taken into the send queue as the last in spite of this.

With the 'normal' setting ICMP packets are treated like all other IP packets in accordance with the routing regulations of the Internet protocol.

Messages, Numbers, Ports

This section contains the error messages you may see when using a *LANCOM Office* router, plus extensive lists of Novell SAP numbers and TCP/IP ports.

We have not listed the IPX/SPX sockets, as such a list would be beyond the scope of the present documentation.

You can obtain a current list, for example, from Novell or Microsoft on the Internet or in the relevant documentation for your network operating system.

Error Messages.....	2
Novell SAP Numbers	9
TCP/IP Ports	13

Error Messages

LANCOM Office router Error Messages

Error message	Cause	Remedy
No number	No call number has been specified for the remote station.	Enter a call number for the remote station connected under SETUP/WAN/NAMelist, if you wish.
No remote	A remote station name given in the IP or IPX router was not found in the name list.	Check the routing tables and compare the names listed there with those in the name list.
Charge locked	The charges preset in the SETUP/CHARGES-MODULE have been consumed.	Try to prevent the <i>LANCOM Office</i> router establishing unnecessary connections by filtering, modify the number of charge units or reduce the period.
Remote doubled	The router has attempted to dial the same remote station on several channels.	Dial again
Remote locked	Another packet needing to be routed has tried to call a remote station whose callback is already awaited.	This generally presents no problem. Check the remote station for the outstanding callbacks if the message persists for a lengthy period.
Invalid module	An unsupported device has been connected to the serial port.	Make sure the device connected is listed in the compatibility list and is working correctly.
No Data-Device	No modem/terminal adapter was detected at the serial port.	Check the cable and that the equipment connected is functioning.
MLP block error	The remote station is not ELSA-MLP compliant.	A connection is only possible without channel bundling.
MLP conn. disc.	Channel bundling was terminated by a parallel connection.	Possible remote station error.



ISDN Error Messages

Error message	Cause	Remedy
Error conn. D 1	No connection or only a faulty connection could be established to the ISDN network.	Check the cable and connectors from the terminal device to the ISDN S ₀ port. Also remove other devices from the bus to exclude these as a source of the error.
Error conn. D 2	See error conn. D1	See error conn. D1
Error conn. B 1	The wrong B channel protocol has been set.	Correct the setting in SETUP/WAN-MODULE/INTERFACE
Error conn. B 2	See error conn. B1	See error conn. B1
Fail. D-chan. 2	See error conn. D1	See error conn. D1
Fail. D-chan. 3	The wrong B channel protocol has been set.	Correct the setting in SETUP/WAN-MODULE/INTERFACE
Fail. B-chan. 2	Connection aborted by the remote station	Initiate another dialing attempt.

Error message	Cause	Remedy
Serv. not avail.	The 'Digital data transmission' service is not available.	Check the destination call number and that the 'Digital data transmission' service is enabled. This also applies to PABXs.
Local busy	Other devices are already occupying the available B channels.	Drop existing connections if necessary.
FAC not supp.	The 'semi-permanent connection' operating mode selected is not supported by the current connection.	Check whether this service has been enabled for your S ₀ bus.
FAC not avail.	The 'semi-permanent connection' operating mode selected is not supported by the current connection.	Check whether this service has been enabled for your S ₀ bus.
Local line lock	The busses connected to the <i>LANCOM Office</i> router are already occupied elsewhere or blocked for incoming calls.	Dial again later and check whether outgoing calls are permitted on the bus connected to the <i>LANCOM Office</i> router.
Remote line busy	The remote station line is busy.	Dial again later.
FAC not permit.	The 'semi-permanent connection' operating mode selected is not supported by the current connection.	Check whether this service has been enabled for your S ₀ bus.
Wrong number	The telephone number is incomplete or invalid.	Check the telephone number assignment in Setup/Wan/Numberlist.
Number changed	The remote station call number has changed.	Check the telephone number assignment in Setup/Wan/Numberlist.
Remote not ready	The remote station is not operational.	Check the remote station.
No response	The call was not answered.	Check the remote station.
Remote busy	The remote station is busy.	The remote station should have its own bus, if necessary, since other devices installed on the same remote station bus can seize its bus.
Remote barred	The remote station was blocked to incoming calls.	Check the remote station and the settings of an intervening PABX if necessary.
Conn. rejected	The remote station has rejected the incoming call.	This is normal if the remote station has been programmed to call back, but check the remote station if not.
ISDN congestion	An intervening PABX has no more lines available to access the remote station.	Try dialing again later.
Local error	A protocol error has occurred.	Dial again.
Remote error	A protocol error has occurred.	Dial again.

PPP Error Messages

Error message	Cause	Remedy
LCP rejected	The remote station has rejected the PPP link control protocol.	Check the remote station's PPP settings.
Auth. error	The remote station does not support the authentication protocol selected.	Compare the settings of the <i>LANCOM Office</i> router with those of the remote station or do without authentication.

Error message	Cause	Remedy
Auth. rejected	The remote station has rejected any sort of authentication.	Disable authentication in the <i>LANCOM Office</i> router. Setup/WAN/PPP/Security none
PAP rejected	The remote station has rejected the Password Authentication Protocol despite it being accepted in the LCP negotiation.	Check the remote station's PPP stack and change to Challenge Handshake Authentication Protocol (CHAP) if necessary.
PAP Rx timeout	The remote station has not started to send PAP requests within the time set.	This problem can generally be solved by increasing the timeout in the <i>LANCOM Office</i> router.
PAP Tx timeout	The remote station has not reacted to a PAP request from the <i>LANCOM Office</i> router within the time set.	Increase the number of repetitions in the <i>LANCOM Office</i> router PPP setup.
Wrong PAP req	The password used by the remote station was rejected as incorrect by the <i>LANCOM Office</i> router.	Check the passwords. Overwrite the password in the <i>LANCOM Office</i> router PPP list if necessary.
PAP NAK received	The PAP request from the <i>LANCOM Office</i> router was rejected by the remote station because the combination of peer ID (name) and password used for both sides did not match.	Check the name and coded entry combination in the <i>LANCOM Office</i> router.
CHAP rejected	The remote station has rejected the CHAP despite it being accepted in LCP negotiation.	Check the remote station's PPP stack and change to PPP if necessary.
CHAP Rx timeout	The remote station has not responded to a CHAP challenge with a CHAP response within the time set.	This problem can generally be solved by increasing the timeout in the <i>LANCOM Office</i> router.
CHAP Tx timeout	The remote station has not reacted to a CHAP response from the <i>LANCOM Office</i> router within the time set.	Increase the number of repetitions in the <i>LANCOM Office</i> router PPP setup.
Wrong CHAP resp	The response sent by the remote station does not match the expected value.	Check the remote station's name and password combination in the <i>LANCOM Office</i> router configuration.
CHAP fail recvd	The remote station has rejected the CHAP response from the <i>LANCOM Office</i> router.	Check the name and password combination for the remote station in the <i>LANCOM Office</i> router.
Unkn. CHAP Peer	A peer ID has been specified in the CHAP request by the remote station which the <i>LANCOM Office</i> router cannot resolve in the PPP table.	Add the name and password required to the PPP table if necessary.
IPXCP rejected	The remote station has rejected IPX control protocol used for IPX parameter negotiation.	Check whether IPX routing on the remote station was authorized for this connection or whether it is possible at all.
Wrong IPXCP net	The IPX network addresses used by both sides for ISDN do not match.	The IPX router is incorrectly configured either in the <i>LANCOM Office</i> router or in the remote station.

Error message	Cause	Remedy
IPXCP net reject	The remote station has rejected the negotiation of an IPX address for ISDN.	Either the remote station must be reconfigured or it does not support this function.
IPXCP route unkn.	The remote station is using a routing protocol for IPX other than RIP/SAP.	Check the remote station's settings.
IPCP rejected	The remote station has rejected IP control protocol used for IP parameter negotiation.	Check whether IP routing has been authorized on the remote station for this connection or whether it is possible at all.
No NCP available	Neither IPXCP nor IPCP could be activated for this connection.	Compare the names of the remote station provided by <i>LANCOM Office</i> router under Status/Info-connection/Code rem. st. with the remote station names of the IPX router and/or the entries in the IP router table.



Modem Error Messages

Error message	Cause	Remedy
Dial failure	An unforeseen error has occurred.	Please contact ELSA Support.
Failure S37	The bit rate set cannot be used for the external serial device.	Check the device connected.
ATA/O no call	Either the remote station has already hung up or another device on the same bus has already seized the line.	Check whether another device on the same bus is listening to the same MSN.
Failure ATZ	A character was send to the connected modem during the establishment of a connection.	
Carrier lost	The connected modem has lost contact with the remote station.	Check the telephone line and establish connections to other remote stations if necessary to check the function of the modem and your telephone installation.
No error corr.	Error correction could not be negotiated with the remote station.	Check the remote station for LAPB compatibility
Prot. ans. lost	A protocol could not be negotiated with the remote station.	Check the remote station for compatibility.
Remote is sync	The remote station is attempting to establish a synchronous connection.	Check the remote station configuration.
No framing	A protocol could not be negotiated with the remote station.	Check the remote station configuration.
No protocol	An agreement on a V.42, MNP or LAPB protocol could not be negotiated.	Check the remote station configuration.
V42bis error	An error occurred during V.42bis data compression.	Check the remote station configuration.
Inactiv. timer	The line was dropped because inactivity timer elapsed.	Check the remote station configuration.
Line disconnect	Another device is presently using the telephone line or the connector is incorrectly wired.	Ensure that no terminal devices, such as a fax or phone, are currently using your line.



Error message	Cause	Remedy
Remote busy	The remote station is already being called and so is busy.	Dial again later.
No dialtone	No dialing tone detected. PABX (have their own dial tone) or line faulty.	Modify the settings in the Setup/WAN module to use a modem on a PABX or check the telephone connection.
No answertone	The call has not been answered by a modem on the remote side.	Check the call number of the remote station.
Timeout	An agreement on a common protocol could not be reached within the time set.	Check the remote station configuration.
No fallback L2	The modems could not agree on a common data signaling rate.	Check the remote station configuration.
No remote modem	No modem is answering on the remote station number.	Check the call number and the remote station configuration if necessary.

Status Displays

Message	Cause	Remedy
Init	The <i>LANCOM Office</i> router is initializing and carrying out a self-test. This message will not usually appear.	Please contact ELSA Support if this message persists for some time.
Setup WAN	The <i>LANCOM Office</i> router is initializing and testing the ISDN and serial modules. This message will not usually appear.	The self-test has detected a malfunction of the corresponding interface if this message remains displayed for a lengthy period. Try installing a firmware update and/or contact ELSA Support.
Ready	The <i>LANCOM Office</i> router is inactive.	
Dial	The <i>LANCOM Office</i> router is dialing a remote station	The display will only show the last digits of longer numbers.
Incoming call	A call is waiting on the bus allocated to the <i>LANCOM Office</i> router.	
Protocol	The <i>LANCOM Office</i> router is attempting to negotiate a protocol with the remote station.	
Connection	The router is connected to the remote station displayed. The window may also be blank if the remote station has not been assigned a name.	
Disconnecting	The <i>LANCOM Office</i> router is attempting to establish a dial-up connection.	
Call-back	The <i>LANCOM Office</i> router is attempting to call back a remote station.	
Reserved	The Y-connectability has been deactivated. The 2nd B channel can now only be used for the bundling.	
Bundle	The 2nd B is being used for the bundling.	

Message	Cause	Remedy
Establ. D64S	The <i>LANCOM Office</i> router is attempting to establish a D64S (Grp0) dedicated line connection.	
Establ. S ₀ 1/S ₀ 2	The <i>LANCOM Office</i> router is attempting to establish a TS ₀ 1/TS ₀ 2 (Grp2) dedicated line connection.	
Not available	The 2nd channel is no longer available for leased line operation with only one B channel.	
No device	There is no device attached to the serial port or it is not functioning.	Check that any device connected is functioning correctly.

Novell SAP Numbers

Decimal	Hexa-decimal	SAP description
1	0001	User
2	0002	User Group
3	0003	Print Queue or Print Group
4	0004	File Server (SLIST source)
5	0005	Job Server
6	0006	Gateway
7	0007	Print Server or Silent Print Server
8	0008	Archive Queue
9	0009	Archive Server
10	000a	Job Queue
11	000b	Administration
15	F000	Novell TI-RPC
23	0017	Diagnostics
32	0020	NetBIOS
33	0021	NAS SNA Gateway
35	0023	NACS Async Gateway or Asynchronous Gateway
36	0024	Remote Bridge or Routing Service
38	0026	Bridge Server or Asynchronous Bridge Server
39	0027	TCP/IP Gateway Server
40	0028	Point to Point (Eicon) X.25 Bridge Server
41	0029	Eicon 3270 Gateway
42	002a	CHI Corp
44	002c	PC Chalkboard
45	002d	Time Synchronization Server or Asynchronous Timer
46	002e	ARCserve 5.0 / Palindrome Backup Director 4.x (PDB4)
69	0045	DI3270 Gateway
71	0047	Advertising Print Server
74	004a	NetBlazer Modems
75	004b	Btrieve VAP/NLM 5.0
76	004c	Netware SQL VAP/NLM Server
77	004d	Xtree Network Version Netware XTree
80	0050	Btrieve VAP 4.11
82	0052	QuickLink (Cubix)

Decimal	Hexa-decimal	SAP description
83	0053	Print Queue User
88	0058	Multipoint X.25 Eicon Router
96	0060	STLB/NLM
100	0064	ARCserve
102	0066	ARCserve 3.0
114	0072	WAN Copy Utility
122	007a	TES-Netware for VMS
146	0092	WATCOM Debugger or Emerald Tape Backup Server
149	0095	DDA OBGYN
152	0098	Netware Access Server (Asynchronous gateway)
154	009a	Netware for VMS II or Named Pipe Server
155	009b	Netware Access Server
158	009e	Portable Netware Server or SunLink NVT161
161	00a1	Powerchute APC UPS NLM
170	00aa	LAWserve
172	00ac	Compaq IDA Status Monitor
256	0100	PIPE STAIL
258	0102	LAN Protect Bindery
259	0103	Oracle DataBase Server
263	0107	Netware 386 or RSPX Remote Console
271	010f	Novell SNA Gateway
273	0111	Test Server
274	0112	Print Server (HP)
276	0114	CSA MUX (f/Communications Executive)
277	0115	CSA LCA (f/Communications Executive)
278	0116	CSA CM (f/Communications Executive)
279	0117	CSA SMA (f/Communications Executive)
280	0118	CSA DBA (f/Communications Executive)
281	0119	CSA NMA (f/Communications Executive)
282	011a	CSA SSA (f/Communications Executive)
283	011b	CSA STATUS (f/Communications Executive)

Decimal	Hexa-decimal	SAP description
286	011e	CSA APPC (f/Communications Executive)
294	0126	SNA TEST SSA Profile
298	012a	CSA TRACE(f/Communications Executive)
299	012b	Netware for SAA
301	012e	IKARUS virus scan utility
304	0130	Communications Executive
307	0133	NNS Domain Server or Netware Naming Services Do
309	0135	Netware Naming Services file
311	0137	Netware 386 Print Queue or NNS Print Queue
321	0141	LAN Spool Server (Vap, Int)
338	0152	IRMALAN Gateway
340	0154	Named Pipe Server
358	0166	NetWare Management
360	0168	Intel PICKIT Comm Server or Intel CAS Talk Server
371	0173	Compaq
372	0174	Compaq SNMP Agent
373	0175	Compaq
384	0180	XTree Server or XTree Tool
394	018A	NASL services broadcast se (Novell)
432	01b0	GARP Gateway (net resear)
433	01b1	Binview (Lan Support Gro)
447	01bf	Intel LanDesk Manager
458	01ca	AXTEC
459	01cb	Shiva NetModem/E
460	01cc	Shiva LanRover/E
461	01cd	Shiva LanRover/T
462	01ce	Shiva Universal
472	01d8	Castelle FAXPress Server
474	01da	Castelle LANPress Print S
476	01dc	Castille FAX/Xerox 7033 F Server/Excel Lan Fax
496	01f0	LEGATO
501	01f5	LEGATO
563	0233	NMS Agent or Netware M gement Agent
567	0237	NMS IPX Discovery or LAN Read/Write Channel

Decimal	Hexa-decimal	SAP description
568	0238	NMS IP Discovery or LANtern Trap/Alarm Channel
570	023a	LABtern
572	023c	MAVERICK
575	023f	Used by eleven various Novell Servers / Novell SMDR
590	024e	Netware Connect
591	024f	NASI server broadcast (Cisco)
618	026a	Network Management (NMS) Service Console
619	026b	Time Synchronization Server (Netware 4.x)
632	0278	Directory Server (Netware 4.x)
640	0280	Novell File and Printer Sharing Service for PC
989	03dd	Banyan ENS for Netware Client NLM
772	0304	Novell SAA Gateway
776	0308	COM or VERMED 1
778	030a	Galacticomm's Worldgroup Server
780	030c	Intel Netport 2 or HP JetDirect or HP Quicksilver
800	0320	Attachmate Gateway
807	0327	Microsoft Diagnostiocs
808	0328	WATCOM SQL server
821	0335	MultiTech Systems Multisynch Comm Server
835	0343	Xylogics Remote Access Server or LAN Modem
853	0355	Arcada Backup Exec
858	0358	MSLCD1
865	0361	NETINELO
894	037e	Twelve Novell file servers in the PC3M family
895	037f	VirusSafe Notify
902	0386	HP Bridge
903	0387	HP Hub
916	0394	NetWare SAA Gateway
923	039b	Lotus Notes
951	03b7	Certus Anti Virus NLM
964	03c4	ARCserve 4.0 (Cheyenne)
967	03c7	LANspool 3.5 (Intel)

Decimal	Hexa-decimal	SAP description
983	03d7	lexmark printer server (type 4033-011)
984	03d8	lexmark XLE printer server (type 4033-301)
990	03de	Gupta Sequel Base Server NetWare SQL
993	03e1	Univel Unixware
996	03e4	Univel Unixware
1020	03fc	Intel Netport
1021	03fd	Print SErver Queue
1196	04ac	On-Time Scheduler NLM
1034	040A	ipnServer Running on a Novell Server
1037	040D	LVERRMAN Running on a Novell Server
1038	040E	LVLIC Running on a Novell Server
1044	0414	Kyocera
1065	0429	Site Lock Virus (Brightwork)
1074	0432	UFHELP R
1075	0433	Synoptics 281x Advanced SNMP Agent
1092	0444	Microsoft NT SNA Server
1096	0448	Oracle
1100	044c	ARCserve 5.01
1111	0457	Canon GP55 Running on a Canon GP55 network printer
1114	045a	QMS Printers
1115	045b	Dell SCSI Array (DSA) Monitor
1169	0491	NetBlazer Modems
1200	04b0	CD-Net (Meridian)
1299	0513	Emulux NQA Something from Emulux
1312	0520	Site Lock Checks
1321	0529	Site Lock Checks (Brightwork)
1325	052d	Citrix OS/2 App Server
1343	0535	Tektronix
1344	0536	Milan
1387	056b	IBM 8235 modem server
1388	056c	Shiva LanRover/E PLUS
1389	056d	Shiva LanRover/T PLUS
1408	0580	McAfee's NetShield anti-virus
1466	05BA	Compatible Systems Router

Decimal	Hexa-decimal	SAP description
	05B8	NLM to workstation communication (Revelation Software)
	0606	JCWatermark Imaging
1569	0621	IBM AntiVirus NLM
1600	0640	Microsoft Gateway Services for NetWare
1614	064e	Microsoft Internet Information Server
1900	076C	Xerox
1947	079b	Shiva LanRover/E 115
1958	079c	Shiva LanRover/T 115
1972	07B4	Cubix WorldDesk
	07c2	Quarterdeck IWare Connect V2.x NLM
	07c1	Quarterdeck IWare Connect V3.x NLM
2084	0824	Shiva LanRover Access Switch/E
2154	086a	ISSC collector NLMs
2175	087f	ISSC DAS agent for AIX
2857	0b29	Site Lock
3113	0c29	Site Lock Applications
3116	0c2c	Licensing Server
9088	2380	LAI Site Lock
9100	238c	Meeting Maker
18440	4808	Site Lock Server or Site Lock Metering VAP/NLM
21845	5555	Site Lock User
25362	6312	Tapeware
28416	6f00	Rabbit Gateway (3270)
30467	7703	MODEM??
32770	8002	NetPort Printers (Intel) or LAN-port
32776	8008	WordPerfect Network Version
34238	85BE	Cisco Enhanced Interior Routing Protocol (EIGRP)
34952	8888	WordPerfect Network Version or Quick Network Management
36864	9000	McAfee's NetShield anti-virus
38404	9604	?? CSA-NT_MON
46760	b6a8	Ocean Isle Reachout Remote Control
61727	f11f	Site Lock Metering VAP/NLM

Decimal	Hexa-decimal	SAP description
61951	f1ff	Site Lock
62723	f503	Microsoft SQL Serve
63749	f905	IBM Time and Place/ tion
64507	fbfb	TopCall III fax server
65535	ffff	Any Service or Wildcard

TCP/IP Ports

Service	Port no.	Protocol
echo	7	tcp
echo	7	udp
discard	9	tcp
discard	9	udp
systat	11	tcp
systat	11	tcp
daytime	13	tcp
daytime	13	udp
netstat	15	tcp
qotd	17	tcp
qotd	17	udp
chargen	19	tcp
chargen	19	udp
ftp-data	20	tcp
ftp	21	tcp
telnet	23	tcp
smtp	25	tcp
time	37	tcp
time	37	udp
rlp	39	udp
name	42	tcp
name	42	udp
whois	43	tcp
domain	53	tcp
domain	53	udp
nameserver	53	tcp
nameserver	53	udp
mtp	57	tcp
bootp	67	udp
tftp	69	udp
rje	77	tcp
finger	79	tcp
www	80	tcp
www	80	udp
link	87	tcp
supdup	95	tcp
hostnames	101	tcp
iso-tsap	102	tcp
dictionary	103	tcp

Service	Port no.	Protocol
x400	103	tcp
x400-snd	104	tcp
csnet-ns	105	tcp
pop	109	tcp
pop2	109	tcp
pop3	110	tcp
portmap	111	tcp
portmap	111	udp
sunrpc	111	tcp
sunrpc	111	udp
auth	113	tcp
sftp	115	tcp
path	117	tcp
uucp-path	117	tcp
nntp	119	tcp
ntp	123	udp
nbname	137	udp
nbdatagram	138	udp
nbssession	139	tcp
NeWS	144	tcp
sgmp	153	udp
tcprepo	158	tcp
snmp	161	udp
snmp-trap	162	udp
print-srv	170	tcp
vmnet	175	tcp
load	315	udp
vmnet0	400	tcp
sytek	500	udp
biff	512	udp
exec	512	tcp
login	513	tcp
who	513	udp
shell	514	tcp
syslog	514	udp
printer	515	tcp
talk	517	udp
ntalk	518	udp
efs	520	tcp
route	520	udp
timed	525	udp

Service	Port no.	Protocol
tempo	526	tcp
courier	530	tcp
conference	531	tcp
rxd-control	531	udp
netnews	532	tcp
netwall	533	udp
uucp	540	tcp
klogin	543	tcp
kshell	544	tcp
new-rwho	550	udp
remotefs	556	tcp
rmonitor	560	udp
monitor	561	udp
garcon	600	tcp
maitrd	601	tcp
busboy	602	tcp
acctmaster	700	udp
acctlave	701	udp
acct	702	udp
acctlogin	703	udp
acctprinter	704	udp
elcsd	704	udp
acctinfo	705	udp
acctlave2	706	udp
acctdisk	707	udp
kerberos	750	tcp
kerberos	750	udp
kerberos_master	751	tcp
kerberos_master	751	udp
passwd_server	752	udp
userreg_server	753	udp
krb_prop	754	tcp
erlogin	888	tcp
kpop	1109	tcp
phone	1167	udp
ingreslock	1524	tcp
maze	1666	udp
nfs	2049	udp
knetd	2053	tcp
eklogin	2105	tcp
rmt	5555	tcp

Service	Port no.	Protocol
mtb	5556	tcp
man	9535	tcp
w	9536	tcp
mantst	9537	tcp
bnews	10000	tcp
rscs0	10000	udp
queue	10001	tcp
rscs1	10001	udp
poker	10002	tcp
rscs2	10002	udp
gateway	10003	tcp
rscs3	10003	udp
remp	10004	tcp
rscs4	10004	udp
rscs5	10005	udp
rscs6	10006	udp
rscs7	10007	udp
rscs8	10008	udp
rscs9	10009	udp
rscsa	10010	udp
rscsb	10011	udp
qmaster	10012	tcp
qmaster	10012	udp

Appendix

This glossary is intended mainly to offer assistance with any problems you may encounter when using your new ELSA product and includes the technical data.

The general warranty terms, a glossary and the Index can be found at the end of the chapter.

Technical Data	2
Frequently Asked Questions and Answers	5
Warranty conditions	22
Glossary	24

Technical Data

Hardware Specifications

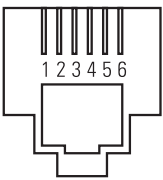
Dimensions:	158 x 40 x 125 mm (W x H x D)
Style:	Stable metal housing
CPU/memory:	Hitachi RISC SH3 60Mhz, 2 MB Flash ROM, 4MB EDO RAM
LAN interface:	Ethernet, automatic detection 10BASE-T (Twisted Pair, RJ 45), Node/Hub changeover, <i>LANCOM 1000</i> and <i>LANCOM 2000</i> Ethernet, automatic changeover 10/100Mbit 100Base-TX (Twisted Pair, RJ 45), Node/Hub changeover, <i>LANCOM 1100 Office</i> 10BASE-2 (Cheapernet, BNC)
WAN interface:	ISDN/S ₀ (BRI)
Configuration interface:	V.24/V.28 Mini-DIN (8-pin) with adapter cable
a/b interface:	4 x RJ11, including terminal adapter (<i>ELSA LANCOM 2000 Office</i> only)
Displays:	<i>LANCOM 1000</i> 9 LEDs <i>LANCOM 2000</i> 13 LEDs <i>LANCOM 1100 Office</i> 10 LEDs
Controls:	On/Off switch
Software upgrade:	Integral Flash ROM, remote upgrade
Power supply:	24V AC with AC adapter for 230 V, 20 VA
Operating environment:	Temperature: 5-40 °C, humidity: 0-80%, non-condensing
EC conformity:	EN 50082 (part 1), EN 55022 (class B), EN 60950, NET 3
Approvals:	
Warranty:	6 years
Service & Support:	via the hotline, ELSA LocalWeb and Internet; access to test networks, free software updates advance exchange

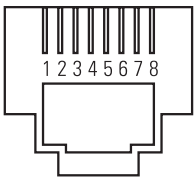
Standards:

RFC 768	UDP: User Datagram Protocol	RFC 1332	IP Control protocol (IPCP)
RFC 791	IP: Internet Protocol	RFC 1334	Authentication protocols (PAP, CHAP (MD5))
RFC 792	ICMP: Internet Control Message Protocol	RFC 1350	TFTP: TFTP Protocol Rev. 2
RFC 792	ICMP: Internet Control Message Protocol	RFC 1388	RIP2: Routing Information Protocol version 2.0
RFC 793	TCP: Transmission Control Protocol	RFC 1552	IPX Control protocol (IPXCP)
RFC 826	ARP: Address Resolution Protocol	RFC 1570	PPP LCP Extensions (also CBCP, Microsoft)

RFC 854	Telnet: Telnet Protocol specification	RFC 1618	PPP over ISDN
RFC 855	Telnet option specifications	RFC 1661	Point-to-Point Protocol
RFC 894	IP datagrams over Ethernet networks	RFC 1662	PPP in HDLC-like framing (async & sync PPP)
RFC 919	Broadcasting Internet datagrams	RFC 1717	The PPP Multilink Protocol (MP)
RFC 922	Broadcasting Internet datagrams in the presence of subnets	RFC 1782	TFTP: Option Extension
RFC 950	Internet standard subnetting procedure	RFC 1783	TFTP: Blocksize Option
RFC 1058	RIP1: Routing Information Protocol	RFC 1784	TFTP: Timeout Interval and Transfer Size Option
RFC 1157	SNMPv.1	RFC 1785	TFTP: Option Negotiation Analysis
RFC 1321	MD5-Message digest algorithm	RFC 1877	IPCP Extension for name server addresses

Connector Pinouts:

Connection	RJ11 pin	Line
 a/b-Ports – RJ11	1	free
	2	free
	3	a
	4	b
	5	free
	6	free

Connection	RJ45 pin	Line	IAE
 ISDN – RJ45	1	free	free
	2	free	free
	3	T+	2a
	4	R+	1a
	5	R-	1b
	6	T-	2b
	7	free	free
	8	free	free

Frequently Asked Questions and Answers

This chapter contains help with problems encountered while running a *LANCOM*, which other users have previously solved with our support.

So if you have difficulty configuring a *LANCOM* or suspect a malfunction, please check this section first to see if the solution has already been documented.

To make searching easier, the questions have been arranged by subject.

In addition, the index at the end of this section can be used to find answers...

General



Why does it take longer to start programs?

The throughput over an ISDN line compared to a local network connection is low (approx. 20 to 1000 times less). For this reason it does not make sense to send programs from a network over the router to the workstation. Instead all frequently used programs should be stored on a local hard disk and only the user data processed by these programs sent over the router.

Possible data throughput with connections over two routers are between 4.5 kbytes (with one B channel without data compression and without PBURST.NLM) and 40 kbytes (with two B channels, data compression and PBURST.NLM) for IPX. With TCP/IP connections throughput rates of 6 kbytes (with one B channel without data compression) to 32.5 kbytes (with two B channels and data compression) are possible.



The use of databases in remote mode is not really feasible over ISDN except with SQL databases. If it is absolutely necessary to use a non-SQL database for specific reasons, using network-capable remote control software (e.g. PC Anywhere) to reach acceptable answer times in remote-control operation will often help.



What can be done if *LANCOM* after successfully dialing returns the message 'Failure D-channel'?

- Check the ISDN terminal to exclude the possibility of a line malfunction.
- Check whether the correct D channel protocol is set in menu setup/WAN module/D channel. When using the national protocol select the 1TR6 setting and with Euro-ISDN the DSS1 setting.



Why does the *LANCOM* return 'No response'?

- The called station is not operating.
- The wrong number was entered.



Why is the status message (Display with *ELSA MicroLink LANCOM MPR*) often 'Remote locked'?

- If a connection is actively rejected by *LANCOM* the other station, for example to initiate a return call, the calling *LANCOM* must wait for this return call. If additional data are sent for the same remote station in this time to *LANCOM*, another connection will not be established but the message 'Remote locked' will be output.
- If the authentication is rejected by the remote station during a PPP negotiation or another error occurs in the PPP negotiation, an additional call will also be delayed with output of the message 'Remote locked'.

After a random waiting period of 20-40 seconds the remote station lock will be released and the same remote station can be dialed again.



Why does the *LANCOM* return 'Protocol error' ?

- The calling *LANCOM* used the layer ELSA-DEFAULT and the called uses, for example, RAWHDLC. Then the calling *LANCOM* attempts a protocol negotiation according to the ELSA standard, to which the called device does not respond. Using the same layers on both sides will help here.
- The called device breaks the connection in the case of call-back by name during the protocol negotiation directly after transmission of the name. The caller cannot distinguish this action from that described above. Therefore, the same error message appears until the called device is called back.



In spite of being entered in the number list, the erroneous layer and/or the wrong remote station is detected.

- The area code is forwarded even within the local calling area. Please add the corresponding area code before the number in every case.
- In Germany Telekom uses two types of exchanges. One forwards the area code with and the other without the leading '0'.

Example:

Aachen: 0241...

Munich: 89...

Solution 1: Enter both variations in the number list.

Solution 2: Check in /Status/Info-connection./Number to see which CLIP is forwarded. Then add it to the number list.

- Exchanges tend to add extra characters before the CLIP. For example, cases are known in which 0241... became an 00241... or an #0241... Note this in the method described in solution 2 and correct the number list appropriately.
- Situation: Two *LANCOM* in one exchange are used and encounter the above problem.

Solution: Exchanges often do not identify their terminals with the complete number but only with the internal extension number.

Example: *LANCOM 1* dials #705

LANCOM 2 receives 705 as CLIP



Why does the *LANCOM* terminate the ISDN connection immediately after the CONNECT?

The access protection is activated in the menu Setup/WAN-module/Protect, but the entry is either not in the number or name list or is wrong.



What can cause high charges?

The device configuration is not optimum. Check the settings of the bridge module or the router modules.



Some servers in your network send data to the remote network. With the establishment tables of the bridge or router modules the MAC addresses of the devices involved in establishing a connection can easily be found (see Chapter 'Status/Connection-statistics' on page 3.1.28).



How can excessive connection charges be avoided?

Erroneous configuration of the router or frequent usage of the WAN connection can result in high charges. The *LANCOM* offers effective protection against unwanted high connection charges. All settings required for charge protection can be made in Setup/Charges module. The default setting for charge protection is 830 units per week. With this setting a maximum of approximately DM 100 in charges can occur (see also 'Setup/Charges-module' on page 3.1.46).

The menu item 'Budget-units' specifies the number of units available as budget in charge monitoring. These units can only be entered in sets of ten to a maximum 2550 units (default value 830 = approx. DM 100). This function can be used to set the connection costs as desired and in case of error will warn of unnecessary establishment of a connection. After the budget has been used up the *LANCOM* prevents further use.



Even though local programs are available, why are there always unexplained waiting periods during which the workstation does not seem to be operating?

It may be that programs on a network drive are started during a logon procedure. Check all path statements and change them to local settings. Naturally, the desired programs should be copied to the appropriate local environment.



What can cause the connection not to be cleared?

- The hold period assigned to this connection (possibly in the name list) is set to the value 0 (0 = hold the connection indefinitely).

- Continuous transmissions prevent call clearing. The connection can be manually cleared and wait for the connection to be automatically established again. The cause of the reestablishment can be found in the establishment tables (see 'Status/Connection-statistics' on page 3.1.28'). The problem can be solved by adapting the workstation/server configuration or improved use of the filter on *LANCOM*.
- Data packets that are periodically sent in Novell networks may prevent call clearing. If frames of this type are present in your network, they should be included in your socket filter table (see 'Socket-filter' on page 3.1.54).



What is the reason for no data being exchanged after a passive call origination?

Check whether the number list includes a reference to the remote station. In addition, the name list must have a reference to the desired WAN layer by the calling station.



What should be done if the passwords protecting the system are not known?

If the passwords assigned for the keyboard and the remote configuration have been forgotten, the device can be reset with the out-band interface. The procedure is as follows:

- ① First establish an out-band configurations connection (see 'The Direct Method: Out-band' on page 1.3.3).
- ② As soon as the password is requested, enter the serial number of the *LANCOM*. The serial number is on the bottom of the device. This automatically starts a firmware upload.
- ③ Run the firmware upload as described in Chapter 'How to Load New Software' on page 1.3.11. Then the passwords for the remote configuration and the keyboard are deleted. The keyboard is then released.



If I try to install new firmware into the *MicroLink LANCOM* with Telix for DOS from a DOS window under Windows 95, the FlashROM upload is interrupted every time with the message 'FlashROM defective'. Does the device require repair?

If a FlashROM update with Telix for DOS is run from a DOS window under Windows 95, it must be ensured that the update is not interrupted by other programs starting (e.g. Windows 95 screen savers). The device does not need to be repaired but the upload may be run again.

IP-RIP



I set the *LANCOM*-devices with and without IP-RIP support in the same network. If IP-RIP has been activated, the devices establish connections continuously without IP-RIP. How can this be prevented?

RIP datagrams are sent as IP broadcast or RIP-2 multicast. Because the *LANCOM* cannot detect these datagrams without RIP support, there is the danger that the RIP packets will be sent to the WAN if the standard route entered in this *LANCOM* is a remote device. To avoid unnecessarily establishing a connection (and the associated charges), IP-RIP for this *LANCOM* should be entered in the LAN and also in the WAN filter table:

LAN filter table for suppressing RIP:

Initial port	Final port	Protocol	Type
520	520	UDP	Always filter

WAN filter table to suppress IP-RIP:

Initial port	Final port	Protocol
520	520	UDP

With an established connection, why are (non-standard route) IP packets that are intended for transmission over the standard route not acknowledged with error messages such as 'Destination Network unreachable' but with 'Connection timed out' or 'Time to live exceeded'?

- There is another router (no *LANCOM*) in the network that sends RIP packets. The *LANCOM* is entered as the standard route in the (static) routing table of this router. In this case the IP packets are continuously sent back and forth between router and *LANCOM*. Removal of the static entry of the standard route will help.
- The 'routing daemon routed' is incorrectly installed on one or more workstations on your network. These workstations behave as if they were routers and release their standard route (*LANCOM*, see above). Install the 'routing daemon' on the next system start (reboot) as below:

```
routed -q
```

Because of the IP-RIP support by *LANCOM*, the standard route has been removed from all workstations and instead the 'routing daemon routed' started. Why can an Internet connection no longer be established?

- The RIP support of the *LANCOM* is not activated (menu: Setup/IP-router-module/RIP-configuration/Operating is set to Off)
- The 'routing daemon routed' on your UNIX systems understands only RIP-1, but in the *LANCOM* R1 comp. or RIP-2 is set (menu Setup/IP-router-module/RIP-configuration/Type).

I have several *LANCOM* devices 'parallel switched', i.e., they have the same routing table and should establish connections over the currently 'free' *LANCOM*. The call origination in the ISDN functions properly, but a TCP/IP connection is established only if a specified *LANCOM* establishes the connection.

- The ELSA protocol for the remote stations has been entered under the menu Setup/WAN module/Layer list as a layer 3 protocol. In this case all parallel switched devices must have the same names.
- For the remote stations this common name must be entered as router name in the routing table (menu: Setup/IP router module/IP routing tab.) for the associated routes

- A different layer 3 protocol is set. In this case any name assignment of the parallel switched *LANCOM* may be used.

In the remote stations the call numbers of each parallel switched *LANCOM* must be labelled with the same names in the number list (menu: Setup/WAN module/number list). This name must correspond to the name list (Menu: Setup/WAN module/name list) over which the remote station establishes a connection to one of the parallel switched *LANCOM*.



I have several *LANCOM* devices 'parallel switched', i.e., they have the same routing table and should establish connections over the current 'free' *LANCOM*. In the case of an incoming call on one of the *LANCOM*, another *LANCOM* attempts to establish a connection to the caller.

In this case the *LANCOM* that attempts to establish the connection is entered as standard router for the receiver of the incoming IP packet. In addition, the RIP support with this *LANCOM* is either not switched or wrongly configured. Set the same values for the entries 'type' and 'R1-mask' in the menu 'Setup/IP router module/RIP setting' in each parallel switched *LANCOM*.

PPP



A PPP connection to a PPP capable remote station cannot be established. At every attempt the protocol negotiation is interrupted. What can be done to correct the error?

In most cases the cause of the failure of the PPP negotiation can be determined by evaluating the error messages. The error messages displayed by the *LANCOM* may have the following causes:

Error	Possible cause
LCP rejected	The remote station has rejected the link control protocol of the PPP. There is a serious function fault in the PPP stacks of the remote station.
Auth. error	The remote station does not support the set checking protocol. The settings must be equalized between the <i>LANCOM</i> and the remote station. A connection may possibly only be established if the check is deactivated.
Auth. rejected	The remote station has rejected any check. A connection may only be established after deactivating the check in the PPP list.
PAP rejected	Although accepted in the LCP negotiation, the remote station has rejected the password authentication protocol in checking. There is a serious fault in the PPP stacks of the remote station. The connection may possibly be established by activating the challenge handshake authentication protocol (CHAP) in the PPP list, but secured.
PAP Rx timeout	The remote station has not begun sending PAP requests to the <i>LANCOM</i> within the set time. Increasing the repeat number can solve this problem in most cases.

Error	Possible cause
PAP Tx timeout	The remote station has not responded to a PAP request from the <i>LANCOM</i> within the set time. Increasing the repeat number can solve this in most cases.
Wrong PAP req	The password used by the remote station does not match the password in the PPP list.
PAP NAK received	The PAP request from the <i>LANCOM</i> has been rejected by the remote station. The combination of peer ID (device name) and password used for both sides does not match. In the <i>LANCOM</i> either the device name or the key entry must be adapted in the PPP list.
CHAP rejected	Although accepted in the LCP negotiation, the remote station has rejected the challenge handshake authentication protocol for checking. There is a serious fault in the PPP stacks of the remote station. However, the connection may be established secured by activating the password authentication protocol (PAP) in the PPP list.
CHAP Rx timeout	The remote station has not reacted to a CHAP challenge with a CHAP response within the set time. Increasing the repeat number can solve this problem in most cases.
CHAP Tx timeout	The remote station has not reacted to a CHAP response from the <i>LANCOM</i> within the set time. Increasing the repeat number can solve this in most cases.
Wrong CHAP resp	The response value received from the remote station does not conform to the value expected. The combination of name and password used for both sides does not conform. In the <i>LANCOM</i> either the device name or the key entry must be adapted in the PPP list.
CHAP fail recvd	The remote station has rejected the CHAP response from <i>LANCOM</i> . This is the same error as the wrong CHAP resp error.
Unkn. CHAP Peer	A peer ID has been entered in the CHAP request by the remote station that cannot be deleted in the PPP table by the <i>LANCOM</i> . This is possibly the same error as the wrong CHAP resp error.
IPXCP rejected	The remote station has rejected the IPX control protocol for negotiating the IPX parameter. Either the remote station does not support IPX routing under PPP or IPX is not activated in the remote station for this connection. The configuration of the remote station must be checked.
Wrong IPXCP net	The IPX network addresses used by both sides for the ISDN do not conform. Either the IPX router of the <i>LANCOM</i> or the IPX router on the remote station is erroneously configured.
IPXCP net reject	The remote station has rejected the negotiation of the IPX network address for the ISDN. The configuration of the remote station must be checked.
IPXCP route unkn.	The remote station uses a different routing protocol for IPX from RIP/SAP. The configuration of the remote station must be checked.
IPCP rejected	The remote station has rejected the IP control protocol in the negotiation of the IP parameter. Either the remote station does not support IP routing under PPP or IP is not activated in the remote station for this connection. The configuration of the remote station must be adapted.

Error	Possible cause
No NCP available	Neither the IPXCP nor the IPCP could be activated for the connection. Neither the IPX router nor the IP router have a reference to the remote station in their configuration. Compare the remote station names (in the menu: Status/Info-connection/Remote-id) determined by the <i>LANCOM</i> for the connection with the remote station names of the IPX router (under the menu: Setup/IPX-module/WAN-configuration/Dialup-remote) or the entries in the routing table of the IP router (under the menu: Setup/IP-router/IP-routing-table) and make sure they are identical.



My provider has assigned me a user name, a password and the authentication protocol PAP for the Internet connection. Although user name, a password and the authentication as in PAP have been correctly entered in the PPP list, the connection is immediately broken and the *LANCOM* reports 'Auth. rejected'.

Because an Internet provider usually has a number of customers on the same dial-up line, the provider often does not run the authentication procedure with the customer and only requests the customer router for authentication under PAP or CHAP. However, with a set authentication protocol the *LANCOM* actively requests an authentication of the remote station with name and password. If this request is not answered the connection is immediately broken. Therefore, in Setup/WAN module/PPP list under security select 'none'. Then the *LANCOM* will automatically answer the PAP or CHAP request of the provider but the other side will not actively request authentication. Then the PPP negotiation can be successfully run.

Bridge



The connection is established but the bridge does not work. Why is this?

- Because a remote bridge works on ETHERNET addresses, only protocols that have an ETHERNET prefix may be used on the B channel. Ensure that only entries that have the setting ETHER in the Encaps column are sent from the layer list. The current setting may be checked in the menu item Miscellaneous/Info-connection/Encapsulation.
- Check the filter settings of the bridge, particularly the WAN filter settings in the menu 'Setup/Bridge-module/WAN-configuration'.



Why is a connection established?

This occurs very often in connection with a network link over a bridge. A bridge must establish a connection because of the regular transmission of broadcast data packets by some servers, which in most cases need to be transmitted to the remote side. In specific cases broadcasts can be prevented from transmission to the remote side (configure Setup/Bridge-module/LAN-configuration/broadcast to negative).

For example, in the ARP problem under TCP/IP the conversion of an IP address to the MAC layer address of the associated network card by ARP. The address resolution protocol works with broadcast data packets that force the bridge to establish a connection.

This unwanted establishment of a connection can be avoided by setting up a local ARP server. A static ARP table is set up on the server for this purpose in which as a minimum the assignment of IP address and MAC layer address for all remote workstations is entered. All broadcasts can then be filtered by the LAN on the local *LANCOM*. Analogous to this procedure a RARP server can also be set up.



Why is a NetWare workstation logged off by the server after a specified time?

A NetWare server expects acknowledgments from linked workstations. If these acknowledgments are not received, the logical connection will be deemed invalid after an adjustable period and the message 'Connection no longer valid' sent, if the workstation attempts to exchange data with the server.

When a bridge is in use, this status only occurs if the WAN connection to the server has been broken for a longer period by the short hold mode and the *LANCOM* has not selected a call number on the server side, therefore itself cannot establish the connection. The time setting required by the server to establish a logical connection should be increased. The following server parameter, which can be influenced by the SET command on the server console or in the STARTUP.NCF, can be used:

NUMBER OF WATCHDOG PACKETS:	<number>
DELAY BETWEEN WATCHDOG PACKETS:	<time setting>
DELAY BEFORE FIRST WATCHDOG PACKET:	<time setting>

IPX Router



Why can the IPX router in Setup/IPX-module not be activated?

There was no logical IPX network number entered yet for the LAN or WAN link in the menu Setup/IPX-module/Network. The assignment of both network numbers is absolutely essential for the function of an IPX router. Only then is IPX routing possible and the module can be activated.



Why is a NetWare workstation logged off from the server after a specific time?

A NetWare server expects acknowledgments from linked workstations. If these acknowledgments are not received, the logical connection will be deemed invalid after an adjustable period and the message 'Connection no longer valid' sent, if the workstation attempts to exchange data with the server.

Filter is selected in 'Setup/IPX-module/LAN-configuration/IPX-watchdog'. IPX watchdog packets are not answered. Use the Spoof setting (economy) or route (watchdog packets are routed).

**Why does the *LANCOM* not establish a connection to the remote station?**

- The values set in the parameters 'Setup/IPX-module/LAN-configuration/Binding' or 'Setup/IPX-module/LAN-configuration/Network' do not agree with the values of the local network. Check these settings with the NetWare server configuration.
- The name of the remote station is not entered.
- The remote station is not found.
- Your workstation NetWare requester has set a false frame, and a connection by the *LANCOM* cannot be established.

Check whether the type set in the *LANCOM* in 'Setup/IPX-module/LAN-configuration/Binding' (e.g. 802.2) conforms with the NET.CFG used by the NetWare requester.

**Why does the router establish a connection to the remote station, but does not send any data packets?**

The name set in the parameter Setup/IPX-module/WAN-configuration/Dialup-remote does not conform with the name of the selected *LANCOM* device on the remote side.

**Why does the router establish a connection to the remote station and send data that are not received by the IPX router of the remote side?**

- The value set in the parameter Setup/IPX-module/WAN-configuration is not the same in both *LANCOM* devices.
- The IPX router on the remote side is not activated.



When the *LANCOM* is started, why is the error message *Router configuration ERROR detected, Router at node xxx claims Network xxx should be xxx* output on the file server?

The network number set in the parameters 'Setup/IPX-module/LAN-configuration/Network' or 'Setup/IPX-module/WAN-configuration/Network' has already been assigned to another station or does not fit in the network string in use.



Why does the router seem to establish connections for no obvious reason?

The following circumstances result in the establishment of a connection:

- Spoofing for RIP and/or SAP in progress:
 - Without, therefore Novell compatible
 - Period in connection with a short WAN update time.
- 'Setup/IPX-module/LAN-configuration/IPX-watchdog' is set to route, better to set it to Spoof.
- 'Setup/IPX-module/LAN-configuration/IPX-watchdog' is set to route, better to set it to Spoof.

The settings 'trig' (only changes are transmitted) or 'pBack' (RIP/SAP information is updated only when there is a connection) are economical in this case.

- Servers in the local network send data packets to remote servers.
If a remotely connected workstation stops received messages by NetWare command CASTOFF ALL, in the older requester there will be a permanent communication between server and remote server/remote workstation over the ISDN link (the server will attempt to send the message again every 2 seconds). This problem can be corrected by a Novell VLM shell from Version 1.20a, with which this special case is managed differently.
- Information on the last 20 data packets that resulted in the establishment of a connection can be found in the statistics in Status/IPX-statistics/Router-statistics/Establish-table. Conclusions regarding causes can be deduced and if applicable corrective action taken. One possible solution is targeted filtering of specific sockets for the LAN filter (Setup/IPX-module/LAN-configuration/Socket-filter) of the router. However, you should first try to suppress transmission with the local servers. Sockets that often result in problems are not displayed by default:

Socket	Meaning
0455h:	Novell NetWare, NetBIOS packets
0456h:	Novell NetWare, diagnostics packets (every 8 minutes)
0457h:	Novell NetWare, serialization packets (every minute or every 5 minutes)
0550h - 0555h:	Microsoft-NetBIOS packets (Win95/NT)
1401h - 1402h:	Periphery File Services (CD-ROM clients)

1480h - 1481h:	HP-Keep alive packets (print server)
83BAh:	Ferrari fax server client query
900fh - 9010h:	SNMP via IPX, protocol and traps

Other applications may show similar behavior.



What settings can optimize the router operation under Novell NetWare?

■ SHELL.CFG

This file has parameters for operating the drivers IPX.COM and NETX.COM. By changing these parameters (e.g. with an editor program) specific functions can be influenced directly in Novell operation. For workstations that work over the routers the following parameters are significant:

– IPX RETRY COUNT

The operation of the driver IPX.COM can be influenced with this parameter. It defines how often a data packet should be repeated before the driver reports a network error. The standard value for this counter is 20. In addition, the following setting is recommended for ISDN connections:

```
IPX RETRY COUNT=100
```

– SPX ABORT TIMEOUT

The operation of the driver IPX.COM can be influenced with this parameter as well. It defines how long (measured in 1/18 second) SPX waits for the answer to a data packet, before SPX terminates the associated session. The standard value is 540 (approx. 30 seconds). In addition, the following setting is recommended for ISDN connections:

```
SPX ABORT TIMEOUT=1100 (approx. 1 minute)
```

■ NET.CFG

The file NET.CFG contains parameters for operating the DOS requester, comprising LSL, a card-specific driver, IPXODI and the VLMs. With changes to these parameters various functions for operating with the router can be optimized.

– AUTO RECONNECT

If this parameter is set to **ON**, the DOS requester attempts to reestablish an expired connection ('Connection no longer valid'). This setting is particularly applicable for linking a workstation to a network if the connection can be interrupted by the router line management.

As well as this setting, the **AUTO.VLM** must be loaded. This is done by the parameter:

```
vlm auto.vlm
```

or by entering this module in NET.CFG

– BIND RECONNECT

The DOS requester initiates the re-establishment of lost bindery connections, disk drive mappings and printer connections with this parameter. The parameter is effective only in combination with the parameter **AUTO RECONNECT**.

– BROADCAST RETRIES

This parameter specifies how often the requester repeats a request by broadcast. If this value is increased (standard setting = 3), the period before the requester reports a network error is increased. During this time the *LANCOM* can, if necessary, reestablish the connection.

– BROADCAST SEND DELAY

This parameter sets the time (in Tics) for which the DOS requester waits between sending the broadcast and processing the corresponding request. This parameter may be used to equalize run times with slow connections.

– BROADCAST TIMEOUT

This parameter can be used to set the time for which the DOS requester waits between sending two broadcast requests.

– MINIMUM TIME TO NET

In networks connected by remote bridges or satellite links the TIME TO NET default of the local router can be set to short. Because the router “knows” nothing of the interim bridge, it would not be possible to establish a connection with a remote workstation with the router.

Errors may be corrected with this parameter under the following conditions:

- The remote workstation is a NetWare 3.x type or older.
- The data throughput rate on one of the WAN links is less than 2400 bit/s.



What must be considered for the burst mode?

This is a special mode for managing data transmissions with which the number of network data packets can be significantly reduced. If the burst mode on the server and on the workstation is activated, large files are transmitted in consecutive network data packets. A confirmation from the remote side is not required after every data packet.

The burst mode can be activated on the server by loading the module *PBURST.NLM* and on the workstation by using the driver *BNETX.COM*.

To install the *PBURST.NLM* module on the file server Version 2.02 dated 10.7.93 at least should be used. This module can be used under Novell NetWare 3.11; there are corresponding patches for later versions of Novell NetWare.

As well as installing the *PBURST.NLM* module, the files *LOGIN.EXE* and *ATTACH.EXE* may need to be replaced by an adapted version.

The following entry is required when using the VLM shell in the NET.CFG:

```
PB BUFFERS = xx (2-255, e.g. 10)
```

IP Router



Why do error messages of the type 'Destination network unreachable' occur on TCP/IP servers?

- It was forgotten on this server to report the *LANCOM* router with a suitable entry (on many UNIX systems, e.g. with entries in /etc or by the command route add...).
- The *LANCOM* has no entry for the target IP address in the router table.
- Communication has been halted by appearance of 'timeout bays', because the remote station could not be reached, there was a simultaneous connection to another remote station or the TCP/IP target server did not answer.



Why doesn't the router establish a connection to the desired remote station?

- The required entries in the router table in 'Setup/IP-router-module/IP-routing-table' are not there or are false (IP address, network mask or router name false).
- The router name is not in the name list in 'Setup/WAN-module/Name-list' or has no or the false call number.



Why does the router establish a connection to the remote station, but does not send any data packets?

The router name set in the table 'Setup/IP-router-module/IP-routing-table' does not conform to the names of the selected *LANCOM* device on the remote side.



Why does the router establish a connection to the remote station and transmit data that however are not received by the IP router of the remote side?

The IP router of the remote side is not activated or not correctly installed. Check whether the IP router is activated ('Setup/IP-router-module/Status/On').



How can individual stations on a local network be linked without assigning a logical IP network address and thereby having to set up several IP networks?

Proxy-ARP may be used for this. All complete IP addresses of the devices to be set up remotely with completely assigned IP network mask (255.255.255.255) and associated remote side names (*LANCOM2*) must be occupied on the network side (*LANCOM1*) in the router table. These IP addresses must be addresses on the local network. Also on both devices 'SETUP/IP router module/Proxy-ARP' must be activated.

The router table could appear as follows on the network side on linking two IP machines:

IP-address

IP-network-mask

Router-name

193.41.22.17	255.255.255.255	LANCOM 2
193.41.22.18	255.255.255.255	LANCOM 2

The actual IP network address with appropriate network mask (255.255.255.0) and the *LANCOM* names on the network side are entered in the router table of the remote device. If the individual remote servers also intercommunicate, to avoid problems their complete IP addresses, network masks and a router name 0.0.0.0 must be entered again. In this way ARP broadcasts for such addresses are not answered.

IP-address	IP-network-mask	Router-name
193.41.22.17	255.255.255.255	0.0.0.0
193.41.22.18	255.255.255.255	0.0.0.0
193.41.22.0	255.255.255.0	LANCOM 1

It is not necessary in the Proxy ARP technology to identify the *LANCOM* to the individual servers as routers, because the communication functions automatically by the ARP resolution.



Why do ARP caches on local machines have the MAC address of the *LANCOM* several times?

With the Proxy ARP mechanism the *LANCOM* answers with its own MAC address on all ARP broadcasts if the requested IP address is entered in the routing table. If the Proxy ARP mechanism is not required, deactivate it in the menu Setup/IP-router-module/Proxy-ARP. This can always be done during a classical IP router connection.



Why is the info that only four connections are permitted in 'Setup/TCP-IP-module/TCP-maximum-connections'. Can only four users use the router at the same time?

This info is exclusively based on solely TCP/IP configuration sessions for *LANCOM*. This means that a maximum of four users can establish one configuration session for *LANCOM*, of whom only the first is authorized to write to the system.

There is no limit to the maximum number of logical TCP/IP connections that can be established over the *LANCOM*.



Why can problems occur in reaching various IP addresses with connections to third-party devices (e.g. netGW from NetCS)?

Many third-party devices define their own IP network for the ISDN and assign their own IP addresses to the ISDN terminals from the network. To reach these IP addresses, the ISDN-IP network must also be entered into the routing table of the *LANCOM*. This applies particularly with access from a UNIX machine in which a NetGW router is

installed on a remote network. The UNIX machine leaves an address from the ISDN-IP network as the sender IP address.



Why is there no spoofing with IP routing?

Communication via the IP protocol is not based on periodically sent packets. It is therefore possible to configure the IP machines in a local network so that only straight user data are sent to a WAN over a router.

Warranty conditions

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

1 Warranty coverage

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

2 Warranty period

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

3 Warranty procedure

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

4 Suspension of the warranty

All warranty claims will be deemed invalid

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

5 Operating mistakes

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

6 Additional regulations

- a) The above conditions define the complete scope of ELSA's legal liability.
- b) The warranty gives no entitlement to additional claims, such as any refund in full or in part. Compensation claims, regardless of the legal basis, are excluded. This does not apply if e.g. injury to persons or damage to private property are specifically covered by the product liability law, or in cases of intentional act or culpable negligence.
- c) Claims for compensation of lost profits, indirect or consequential detriments, are excluded.
- d) ELSA is not liable for lost data or retrieval of lost data in cases of slight and ordinary negligence.
- e) In the case that the intentional or culpable negligence of ELSA employees has caused a loss of data, ELSA will be liable for those costs typical to the recovery of data where periodic security data backups 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.

Glossary

- **ARP** – Address Resolution Protocol is a protocol of the →TCP/IP family. ARP assigns IP addresses to MAC addresses.
- **Asynchronos transmission** – In serial data transmission a method is needed to synchronize transmitter and receiver in order to enable the receiver to detect the beginning and end of a transmitted character. In asynchronous transmission this structuring is achieved by marking each byte to be sent with one start bit and one or two stop bits. Especially in the microcomputer sector, this start/stop method is one of the most commonly used transmission methods, since, unlike synchronous transmission, it is comparatively easy to perform.
- **AUI** – Attachment Unit Interface = Interface for general network connections
- **B channel** – →Basic channel
- **Baseband** – With baseband signal transmission, unmodulated digital signals are fed directly into the cable. Thus the signal takes up all of the available bandwidth, which negates the need of a collision recognition →CSMA/CD. A typical example of a baseband LAN is Ethernet.
- **Basic channel** – ISDN transfer channel (also known as B channel) for the delivery of communications data with a capacity of 64,000 bps.
- **Basic Rate Interface** – ISDN subscriber connection with two →bearer channels (64,000 bps each) and a signal channel (16,000 bps). The →S₀ interface is the subscriber interface used by the Basic Rate Interface.
- **BNC** – Popular connection method for Cheapernet (Thin Ethernet), and also known as BASE2. The connection of devices with BNC connectors requires a T-piece connector.
- **bps** – Abbreviation of bits per second. This is the unit to measure the speed of a data transmission. Unlike the step rate measured in →Baud, the transmission rate indicates the actual amount of information transferred per second.
- **Bridge** – A bridge is a connection between two networks with the same layer 2 structure in the →OSI model. A bridge can consist of two devices connected via a data communications link, which is known as a remote bridge.
- **Broadcast** – Broadcasts are special data packets sent to all stations capable of receiving them. In Ethernet networks, these packages are addressed with FFh FFh FFh FFh FFh FFh (i.e. to all).
- **Burst Mode** – Burst mode is a special Novel Network data transport method which sends several data packets one after the other without any confirmation of receipt.
- **CEPT** – Confrence Europeenne des Postes = European body of experts which defines telecommunications standards.
- **Client** – Client = Workplace computer. A Client is a user of the services provided by a →Server.
- **CLIP** – Caller Line Identification Parameter = The caller's telephone number, which can be transmitted via ISDN.
- **CSMA/CD** – Carrier Sense Multiple Access with Collision Detection. With this process, the stations check to see if the channel is free to transmit data. If a collision caused by two stations simultaneously transmitting is detected, both stations stop sending. Transmis-

sion will be attempted again after a random time period.

- **CTS** – Clear To Send. This output is normally always active (ON).
- **D channel** – ➔ Signaling channel
- **Data packet** – A data packet contains a set number of characters (control commands) for transmitting data
- **DNS** – Domain Name Server. This server translates the alphabetic ➔ domain names into the digital IP addresses required by computers.
- **Domain** – A domain is an alphabetic description of a logically delimited network, such as a company network, or Internet provider.
- **DSS1** – A European standard developed by the ➔ ETSI for the ➔ D channel protocol (also known as Euro-ISDN). This standard has been in effect in Germany since the end of 1993 and will replace the FTZ standard ➔ 1TR6. ISDN connections will be available for a transitional period which support both standards.
- **Ethernet Network** – An Ethernet network is a ➔ bus system with ➔ CSMA/CD access and ➔ baseband transmission. Developed in 1979 by DEC, Intel and Xerox, this local network was one of the first ➔ LANs and became a de-facto standard. Ethernet was accepted by the IEEE (Institute of Electrical and Electronics Engineers) as a standard (Norm 802.3). Data transmission is via coax, twisted-pair or fiber-optic cable or other media with a speed of 10 mbps.
- **ETSI** – European Telecommunications Standards Institute. This is the standardization authority which developed the European ➔ D channel protocol (➔ DSS1).
- **Flash ROM** – Flash ROM (Read Only Memory) is a memory component which can be electronically overwritten. Flash ROM is often used for devices equipped with firmware which can be updated.
- **Gateway** – Gateway is a term describing the hardware and software which connect two ➔ LANs.
- **HDLC** – High-level Data Link Control – the format of a data packet being checked by a CRC check.
- **Hops** – The number of routers used to complete a network connection.
- **I.463** – ➔ V.110
- **I.465** – ➔ V.120
- **ICMP** – Internet Control Message Protocol = protocol from the TCP/IP world used to transfer status information and error messages.
- **Inband configuration** – Data is transferred to the device which is being configured via a direct network connection (➔ LAN or ➔ WAN). A disturbance to this network connection leads to a loss of the configuration connection.
- **Internet** – The Internet is a combination of all networks connected with the ➔ TCP/IP protocol.
- **Intranet** – Domains; network which, for example, is restricted for internal company use and allows only the controlled access to and from the outside
- **IP** – Internet Protocol is a collection of protocols developed by the DoD (Department of Defence) for connecting heterogeneous wide area networks (➔ WANs).
- **IPX** – Internet Packet eXchange = a transport protocol developed by Novell for transmitting

data over a network. On PCs this protocol is realized by the IPX.COM driver or the VLM shell.

- **IPX Watchdog** – Packets sent from a server to monitor a workstation at certain time intervals. If the workstation does not answer, it will automatically be logged off.
- **ISO** – International Organization for Standardization. ISO is an international organization coordinating the development of world-wide norms. Members include the national standards institutes like the BSI (Britain), DIN (Germany), ANSI (USA), or ANFOR (France).
- **ITU-T** – The Telecommunications Standardization Sector of the International Telecommunications Union (ITU) is working on the standardization of data and telephone services. The ITU-T standards of the V. series mainly deal with data transmission across telephone networks, while the I. and Q. series are standards for the ISDN. The ITU-T is the successor organization of the CCITT (Comit Consultatif International Tlgraphique et Tlphonique).
- **LAN** – Local Area Network; according to ➔ISO, a local area network is a "network located within property boundaries under the legal control of the user for the bit-serial transmission of information between its independent, connected elements." A local area network is therefore a very localized network, generally installed within a building or on a company site.
- **Leased line** – A leased line is a permanent connection between two subscribers which can only be used by these two subscribers.
- **Line on Demand** – A connection is made on demand. With the LANCOM, the content of received data packets from the LAN determine the establishment of a connection.
- **MAC** – Media Access Control. Sublayer of layer 2 of the ISO model defined by ➔ISO. In Ethernet networks, the source and target address and the protocol type belong to the MAC layer data in Ethernet networks.
- **MNP** – Due to the noise and distortion characteristics of a telephone network, conventional modems cannot guarantee a perfect, error-corrected transmission. The Microcom Networking Protocol (MNP) is an error correction method making 100% error-corrected transmission possible even on distorted telephone lines. This method is used world-wide in millions of modems. It may only be used by manufacturers licensed by Microcom, the developer of MNP. Besides the error correction protocol, MNP class 5 additionally provides a data compression method, thus increasing the effective transfer rate by a factor 1.3 to 2.0. Thus in a physical connection of 14,400 bps an ➔effective transfer rate of up to 28,800 bps can be achieved. To transmit data that have already been compressed (e.g. *.ZIP, *.ARC), MNP class 4 should be used, for no considerable further compression can be reached by MNP5 with these files, and the compression method might even slow down the transmission. ELSA MicroLink(r) modems featuring MNP support both classes of this error correction protocol, as well as the methods according to ➔V.42, V.42bis.
- **MSN** – Multiple Subscriber Number. With the ➔DSS1 protocol, the exchange can assign several subscriber numbers to one ISDN connection. Generally, three numbers are assigned; a maximum of eight are available. These dial numbers can be used, in a manner similar to that of the ➔1TR6 protocol and its ➔EAZ, to directly address individual terminal units attached to the ➔S₀ interface. Unlike the single-digit EAZ, which is actually a suffix

to the actual dial number, the MSN may have a maximum of eight digits.

- **Multicast** – Multicasts are special data packets sent to all stations in a group ready to accept them.
- **NBNS** – Net Bios Name Server identifies a server providing a name service for all the computers on a →domain. A machine which knows only the symbolic name of its target can find out the associated address by querying this server.
- **Network** – A network is a multiuser and multifunction system of a group of computer systems and terminals for the common use of data and resources connected together by communications lines.
- **NETX** – NETX = NetWare-Shell; this program represents the interface between application programs and the Novell NetWare operating system.
- **Node** – A node is a device connected to the network which receives or transmits data. This device may be a single LANCOM, a computer, server or printer which can be addressed by multiple network users.
- **Novell** – Producer of the Novell NetWare operating system.
- **OSI** – Open Systems Interconnection; reference model for networks developed by →ISO (International Organization for Standardization) to specify the interface standards between computer manufacturers in terms of hardware and software requirements.
- **Outband configuration** – In outband configuration, also known as out-of-band configuration, data exchange with the device to be configured takes place through a serial V.24 interface. The configuration connection is retained even in the event of interference with a network connection.
- **PPP** – Point-to-Point Protocol. This is a transmission protocol for carrying network packets (such as Internet etc.) to the end user.
- **Proxy-ARP** – Proxy-ARP makes it possible for stations which normally are connected directly to a local TCP/IP network and therefore have locally suitable IP address also to be reached over a WAN connection through a router. The router announces itself as the remote device to an ARP query in the local network, ie it returns its own MAC address. It can then receive the data packets and send them on to the remote side.
- **RARP** – Reverse Address Resolution Protocol is a protocol in the →TCP/IP family. This protocol maps MAC addresses to IP addresses.
- **RIP** – Routing Information Protocol is used in networks (Netware IPX in this case) for the distribution of information for routers.
- **Round robin** – A method for connecting to a logical remote station (e.g. a company head office) by way of multiple dial-up numbers on different devices. A call is passed to further free remote stations if the default remote station is busy.
- **Router** – A router is a device for the connection of two networks with the same layer 3 structure in the →OSI model. A router of this type can comprise two devices connected by a data transmission channel. This set-up is also known as a remote router.
- **RTS** – Request To Send
- **S₀ interface** – Subscriber interface of the →Basic Rate Interface. This interface is a bus permitting the connection of up to eight ISDN

terminal devices. Up to 12 sockets can be installed on this bus.

- **SAP** – Service Advertising Protocol is used in NetWare networks to propagate services.
- **Server** – A server is a device offering services that may be used by a ➔Client. Many network operating systems have a Client-Server architecture, ie a special, high-end computer operates as a server from which a large number of clients can draw data and programs.
- **Short hold mode** – A connection is dropped after a defined period if there are no data to be transmitted. This means that the connection can be retained until no data are being transmitted.
- **Signaling channel** – ISDN signaling channel (also ➔D channel), for the transfer of control information (e.g. the signaling of an incoming call, etc.) between the exchange and the ISDN network terminator, with a transfer capacity of 16,000 bps for ➔Basic Rate Connections or 64,000 bps for Primary Multiplex Connections.
- **SPC** – Semi-permanent Connection. A semi-permanent connection is currently available for the ➔1TR6 protocol and can be established between any two ISDN subscribers. The connection is effected separately for each B channel. The billing of communications charges is no longer based on connect time when a semi-permanent connection has been established, but on a flat monthly rate. This permits communications charges to be saved on individual connections.
- **Spoofing** – Spoofing is a method used to avoid unnecessarily incurred connection charges. Queries from the LAN side are answered directly by the router without a connection being established to send data to the remote side.
- **SPX** – Sequenced Packet eXchange, a protocol defined by Novell for the secure transmission of data in the network; this protocol is implemented on a PC by the driver NETX.COM (or similar).
- **SPX Watchdog** – Packets sent by the server at specified intervals to monitor an SPX connection.
- **Synchronous transfer** – Synchronous transfer is, like ➔asynchronous transfer, a process to achieve synchronism between the transmitter and receiver. In this data transfer format, synchronism is not achieved with start and stop bits for a whole character as with asynchronous transfer, but clock pulses for each individual bit. As no start or stop bits must be sent, synchronous transfer is faster, but also significantly more complex to realize.
- **TCP/IP** – Transmission Control Protocol/Internet Protocol is a comprehensive family of protocols developed at the start of the seventies by the US Department of Defense for the secure connection of heterogeneous Wide Area Networks. The two foundations of this family of protocols are IP, which implements layer 3 of the ➔OSI model and its analog, TCP, for the fourth layer.
- **Telnet** – Telnet is a protocol from the ➔TCP/IP family. It permits remote access by a workstation to another computer system located on the network. The telnet protocol uses ➔TCP for data transmission, as this requires a secure bidirectional communication. A virtual terminal to the telnet host is thus provided on the telnet client.
- **TICS** – LANCOM system time unit
- **Transceiver** – A device that converts an input signal format to a different output signal format.

- **UDP** – User Datagram Protocol: contributes to the transmission of data from certain services in IP networks, however, unlike TCP it does not provide for secure data transmission.
- **UNIX** – UNIX is an operating system for high-end microcomputers, minicomputers and mainframes developed by AT&T.
- **V.110** – V.110 (also referred to as I.463) is an →ITU-T standard for the adaptation of asynchronous or synchronous serial data streams to the ISDN line bit rate of 64,000 bps for the transmission over an ISDN →B channel.
- **V.42, V.42bis** – V.42 and V.42bis are error-correction and data compression processes standardized by the →ITU-T. V.42bis contains a data compression process which permits up to a fourfold increase in data throughput.
- **VLM** – Virtual Loadable Module, this program represents the interface between application programs and the Novell network operating system.
- **WAN** – Wide Area Network. Network extending beyond a single site such as connections using ISDN devices.
- **Workstation** – Desktop computer
- **X.75** – Similar to V.120. Recommendation by the →ITU-T for the secure transfer of data using the HDLC transfer process in the ISDN →B channel.
- **Xmodem** – Xmodem is a →transmission protocol featuring automatic error detection and error correction. Data are transmitted as data blocks of 128 bytes. If a transmission error has been detected, the defective block is transmitted again. Xmodem is one of the most common protocols and is supported by many standard terminal programs, but has mean-

while been surpassed by more efficient modern protocols like →ZModem.

- **Y connection** – Simultaneous connection to two different remote sites over one B channel each of the same ISDN S₀ connection.

Index

■ Numerics

10/100Base-TX	1.2.5
100Base-TX	1.2.5
100Mbit network	1.2.5
10Base-2	1.2.5
10Base-2 (BNC)	1.2.5
10Base-T	1.2.5
10Mbit network	1.2.5
1TR6	1.1.4, 1.2.6, 1.2.14
7 layer model	1.4.2

■ A

a/b 1	1.2.4
a/b ports	1.1.3, 1.1.7
Access list	1.3.2
Access protection	1.1.6, 1.2.7
name	1.2.7
name or number	1.2.7
none	1.2.7
number	1.2.7
Access Verification	1.4.18
Access-list	3.1.62
Adapter	1.3.3
Address filters	1.2.11
Address Resolution Protocol	1.4.10
Address Administration	1.3.4
Advice of charge	1.1.6
Aging-minute(s)	3.1.51, 3.1.57, 3.1.60
Analog connections	1.1.3
Analog terminals	1.2.5
Analogue terminal devices	1.1.7
Answering Machine	1.6.2
AOCD	1.1.6, 1.2.10, 1.2.12
Appendix	1.1.9
ARP request	1.4.10
ARP table	1.4.10
ARP-aging-minute(s)	3.1.63
Authentication	1.5.4, 1.5.10

■ B

B channel	1.2.14, 1.3.14
connection status	1.1.5
B channel protocol	1.2.8
B channel protocols	
Layer 1	
HDLC	1.2.15
Layer 3	
asynchronous PPP	1.2.15
synchronous PPP	1.2.15
Transparent	1.2.15
Baby monitoring	1.1.8
Backup-delay-seconds	3.1.45
Barring	1.2.8
BBS	1.6.7
B-channel protocol	1.2.7, 1.2.15
Binding	3.1.53
Boot loader	1.3.17
Boot system	3.1.84
Bridge	1.4.1, 1.4.2, 1.4.4
broadcast data packets	1.2.11
configuration	1.4.4
Filter tables	1.2.12
filtering data packets	1.4.5
Bridge Setup	2.3.37
Broadcast	3.1.51
Brokering	1.1.3, 1.1.8
Brute force	1.1.6, 1.2.7, 1.2.8, 1.3.2
Budget	1.2.12, 3.1.47
Budget-units	3.1.47

■ C

Call by call	1.2.13
Call charge	
information	1.1.5, 1.2.10, 1.2.12, 1.5.12
Call charge limit	1.2.12
Call charge management	1.2.12
Call charge metering	1.1.3, 1.1.8
Call charge unit	1.2.10
Call charge units	1.5.12
Call forwarding	1.1.8
Call pickup	1.1.3
Call redirection	1.1.3

Call switching	1.1.3	control outputs	3.2.5
Callback	1.2.7, 1.2.9	costs	1.2.10
fast call back	1.2.9		
Callback function	1.1.6	D	
Callback options	3.1.38	D channel	1.2.7, 1.2.14
Call-by-Call	1.2.10	D64S	1.2.6, 1.2.14
CAPI server	1.1.7	D64S2	1.2.6, 1.2.14
CBCP	1.5.8	D64SY	1.2.14
CE	1.1.10	Data	1.2.15
Challenge Handshake Authentication		Data Compression	1.2.12
Protocol	1.2.8	Data compression	1.2.10
Channel bundling .. 1.1.4, 1.2.12, 1.2.15, 1.5.12		Data compression procedure	
dynamic	1.5.12	LZS	1.5.12
static	1.5.12	Data transmission	1.5.12, 1.6.2, 1.6.5
CHAP	1.2.8	Data transmission in an IPX network	1.4.22
Charge monitoring	1.1.6	Data transmission in an TCP/IP network	1.4.10
Charge protection	3.1.46	Day(s)-per-period	3.1.47
Charges	1.2.10	dedicated	1.2.14
Charges budget	1.2.10	Dedicated lines	1.1.3, 1.2.14
CLI	1.2.7	Default layer	1.3.7
COM port	1.6.2	Delayed fax transmission	1.6.2
Communities	1.3.10	DHCP	1.1.7
Compatibility	1.1.4	DHCP server	1.1.7, 1.3.4
Compuserve	3.2.2	Dial prefix	3.1.45
Compuserve selectl	3.2.3	Dial-up	
Conditions of service	1.1.9	connection	1.1.3, 1.2.8, 1.2.14, 1.3.2, 1.3.6
Config-aging-minute(s)	3.1.75	Dial-up connections	1.2.14
Configuration	1.1.5	Disconnect	3.1.46
Commands	1.3.9	Display	3.1.3
methods	1.3.2	Display elements	1.2.1
SNMP	1.3.10	Distance of a route	1.4.8
Configuration access	1.3.7	DNS	1.4.18
Configuration block	1.3.2	DNS Forwarding	1.4.18
Configuration call number	1.3.2, 1.3.7	DNS-backup-IP-address	3.1.63
Configuration interface	1.3.2, 1.3.3	DNS-default-IP-address	3.1.62
Connect	3.1.46	Domain Name Service	1.4.18
Connection duration	1.1.5	DSS1	1.1.4, 1.2.6, 1.2.14
Connections	1.2.5	Dynamic channel bundling	1.5.12
Connectivity	1.2.1	Dynamic routing	1.4.7
Connector	3.1.49	Dynamic short hold	1.2.12
Consultation hold	1.1.3	dynamic short-hold	3.1.37
Contact addresses	1.1.9	E	
Control information	1.2.14	ELSA protocol	1.2.8

- ELSA test network 2.7.1
 - bridge mode 2.7.11
 - router mode using PPP 2.7.3
 - router mode using the ELSA protocol 2.7.8
 - ELSA-RVS-COM* 1.1.3, 1.6.2, 2.6.4, 2.6.6, 2.6.8
 - answering machine 2.6.4
 - installation Wizard 1.6.3
 - Setup 1.6.2
 - system requirements 1.6.3
 - telephone 2.6.4
 - ELSA-RVS-COM* Fax 1.6.2
 - ELSA-ZOC* 1.1.3, 1.6.7, 2.6.8
 - dialing 2.6.8
 - upgrade to ZOC/Pro 1.6.7
 - E-mail 1.1.2
 - Error search 2.8.1
 - Ethernet 1.1.4, 1.2.5, 1.2.15
 - 10/100Base-T 1.1.4
 - 10Base-2 1.1.4
 - 10Base-T 1.1.4
 - Fast Ethernet 1.1.4
 - Euro ISDN 1.2.14
 - EuroFileTransfer 1.1.7, 1.6.2, 2.6.6
 - setting up 2.6.6
 - transferring files 2.6.6
 - Euro-ISDN port 1.6.4
 - Exclusion routes 1.4.9
 - ext. dial prefix 3.1.45
 - Extra ISDN functions 1.1.8
- **F**
- FAQ
 - ARP cache A-20
 - Auth. rejected A-13
 - Break after CONNECT A-7
 - Break in PPP negotiation A-11
 - Bridge does not work A-13
 - Burst mode A-18
 - Call origination with the bridge A-13
 - Connection not cleared A-7
 - Connection timed out A-10
 - Continuous call origination with IP-RIP A-9
 - Destination Network unreachable A-10
 - Destination network unreachable A-19
 - Duration of program start A-5
 - Erroneous layer and/or erroneous remote station A-6
 - Establishing connection for no reason A-16
 - excessive connection charges A-7
 - Failure D-channel A-5
 - FlashROM defective A-9
 - Forgotten passwords A-9
 - high charges A-7
 - IPX router activate A-14
 - Max.number of connections A-20
 - NetWare computer logged off from server A-14
 - NetWare workstation logged off from the server A-14
 - no connection to desired remote station A-19
 - No connection to the remote station A-15
 - no data exchange after passive call origination A-9
 - no data transmission A-15, A-19
 - No response A-5
 - No spoofing with IP-Routing A-21
 - Optimize router operation under Novell NetWare A-17
 - Protocol error A-6
 - Remote Access A-19
 - Remote locked A-6
 - Remote side does not receive data A-19
 - Remote side not receiving data A-15
 - Router at node xxx claims Network xxx should be xxx A-16
 - Router configuration ERROR detected A-16
 - Routing daemon A-10
 - TCP/IP scaling A-10
 - TCP/IP-Skalierung A-11
 - Third-party devices A-20
 - Time to live exceeded A-10
 - Waiting times with locally available programs A-7
 - FAQs 1.1.9
 - Fast Call Back 1.2.9
 - Fast Ethernet 1.1.4, 1.2.5

Fast-Ethernet		Interface list	3.1.35
10/100Base-T	1.1.4	Interfaces	1.2.5
Fax	1.1.2, 1.1.3, 1.1.7, 1.2.13	Internal calls	1.1.3, 1.1.8
Fax polling	1.6.2	Internet	1.1.2, 1.2.9, 2.6.2
Fax via software	1.6.2	Internet access	1.5.6
File transfer	1.1.2	Internet account	2.2.1
Filter	1.2.7, 1.2.10	Internet address	1.4.16
Filter mechanisms	1.1.3	Internet applications	2.2.1, 2.5.1
Filter-table	3.1.52	Internet service provider	1.1.2
Filter-type	3.1.52	Intranet address	1.4.16
Firewall	2.2.1	IP	3.1.68
Firewall function	1.2.9	IP access list	1.3.4
FirmSafe	1.1.6, 1.3.17	IP address	1.2.9, 1.3.4, 1.3.14, 1.5.6
Firmware	1.1.6	IP addresses	1.1.7, 1.2.11
Firmware Upload		IP masquerading	
with LANconfig	1.3.18	1.1.2, 1.2.7, 1.2.9, 1.4.15, 2.2.2
Firmware upload	1.3.18	simple masquerading	1.4.17
using TFTP	1.3.19	supported protocols	1.4.17
with terminal program	1.3.18	IP network coupling	2.3.2
Firmware-upload	3.1.82	IP Router	1.4.6
Flash ROM	1.3.17	IP routing	
G		dynamic scaling	2.3.16
Gateway	1.2.9	Filter	1.4.11
Glossary	1.1.9	FTP	1.4.11
group work	2.6.2	static scaling	2.3.8
H		Telnet	1.4.11
Holding	1.1.8	IP routing table	1.4.7
Home office	1.1.3, 2.4.1	IP-routing-table	3.1.64
Hub	1.2.5, 1.2.6	IPX networks couple	2.3.25
Hyperterminal	1.3.3	IPX router	1.4.20
I		LAN and WAN filters	1.2.11
IANA	1.4.7	RIP/SAP tables	1.2.11
ICMP	3.1.68	scaling	2.3.31
Identifying the caller	1.2.7	Spoofing	1.2.11
Inband	1.3.2, 1.3.4	IPX routing	
Requirements	1.3.4	backoff	1.4.21
using Telnet	1.3.5	Binding	1.4.20
Inband configuration	1.3.2	binding	1.4.21
Install software	1.3.17	exponential backoff	1.4.23
Installation	1.1.4	Filter	1.4.24
Installing a Web server on the Internet	2.2.7	Hops	1.4.22
		network	1.4.21
		propagate	1.4.21

- Propagate loop function 1.4.23
- remote station 1.4.21
- RIP and SAP tables 1.4.22
- Tics 1.4.22
- IPX routing table 1.4.20
- IPX watchdogs 1.4.25
- IPX/SPX sockets 3.3.1
- IPX-router 3.1.53
- IPX-watchdog 3.1.53
- ISDN Basic Rate Interface 1.1.4
- ISDN Connection 1.2.6
- ISDN router
 - Sample applications 1.1.2
- ISDN time 1.1.7, 3.1.5
- ISDN-S0 port 1.2.5
- **K**
 - Kanalanzeige 1.3.14
 - Key 1.5.4
 - Key-lock-active 3.1.81
 - Key-password 3.1.81
- **L**
 - LAN connection 1.1.4
 - LAN to LAN coupling 1.1.2, 1.1.3
 - LANCAPI 1.1.2, 1.1.3, 1.1.7, 1.2.13, 1.3.6
 - LAN-Coll 1.2.3, 1.2.4
 - LANCOM
 - connect 1.2.5
 - LED indicators 1.1.4
 - LANCOM operating modes
 - IP router 1.4.1
 - IPX router 1.4.1
 - LANconfig 1.1.5, 1.2.15, 1.3.2, 1.3.4, 1.3.6, 1.3.13, 1.3.18
 - Wizards 1.3.4
 - LAN-configuration 3.1.75
 - LAN-Fast 1.2.3
 - LAN-FDpx 1.2.3
 - LAN-filter-table 3.1.57, 3.1.59, 3.1.66
 - LAN-Link 1.2.3, 1.2.4
 - LANmonitor 1.1.4, 1.3.12, 1.3.13
 - LAN-Rx 1.2.3, 1.2.4
 - LAN-Rx/Tx 1.2.3
 - LAN-Tx 1.2.2, 1.2.4
 - LapLink for Windows 1.6.5
 - LapLink license 1.6.5
 - Layer list 1.2.15
 - Layer-list 3.1.39
 - Layers 1.2.15
 - LCD-brightness 3.1.81
 - LCP echo reply 1.5.5
 - LCP echo request 1.5.5
 - LCR 1.1.6, 1.2.10, 1.2.12, 1.2.13
 - Leased lines 1.2.14
 - Leased-line connection 1.2.14, 2.2.7
 - Leased-line connections 1.2.6
 - Least-cost router 1.2.13
 - Least-cost routing 1.1.6, 1.2.10, 1.2.12
 - LED 1.2.2
 - LED display 1.3.14
 - LEDs
 - Meaning 1.2.2
 - Line establishment 1.1.5
 - Line management 1.1.3, 1.1.5, 1.2.10
 - Link Status LED 1.2.6
 - Local-routing 3.1.54, 3.1.68
 - Login 1.3.17
 - Login attempts 1.2.8
 - Login barring 1.2.7, 1.2.8
 - LOOP-propagate 3.1.55
 - LZS 1.2.15
 - LZS data compression 1.5.12
 - **M**
 - MAC addresses 1.4.2
 - MacOS 1.2.15
 - mailboxing 2.6.8
 - Management Information Base 1.3.12
 - Manager 1.3.12
 - Masquerading table 3.1.71
 - Maximum number of simultaneous
 - connections 3.1.75
 - Media Access Control 1.4.2
 - MIB 1.3.10
 - MLPPP 1.2.12, 1.5.12
 - Modem 1.1.7

Monitoring	1.3.13
Multicast	3.1.51
Multi-device terminal	1.1.4, 1.2.6
Multilink PPP	1.2.12, 1.5.2, 1.5.12

N

Name	3.1.34
Name list	1.2.7
Name-list	3.1.37
Naming IP Addresses	1.4.6, 1.4.20
NAT	1.2.7, 1.2.9, 1.4.15
national ISDN port	1.6.4
NBNS-backup-IP-address	3.1.63
NBNS-default-IP-address	3.1.63
NetBIOS	2.3.30
Network	3.1.53
IPX/SPX	1.2.15
TCP/IP	1.2.15
Network code	1.2.13
Network Connection	1.2.5
Network connection	1.1.2
Network Information Center	1.4.15
Network mask	1.4.6
Network protocols	1.4.2
NIC	1.4.15
Node	1.2.5
Node/hub selector switch	1.2.5
Node/Hub switch	1.2.5
Node-id	3.1.49
Number list	3.1.43

O

Objects	1.3.11
Office communications	1.1.7
Online banking	1.1.2
Online media	1.3.4
Online research	1.1.2
Operating	3.1.50, 3.1.52, 3.1.61, 3.1.64
Operating modes	1.1.7, 1.4.1
Operating status	1.2.3
Operating systems	1.2.15
OS	1.2.15
OS/2	1.2.15
OSI Reference Model	1.4.2

Other	3.1.84
Outband	1.3.2, 1.3.3
Requirements	1.3.3
using LANconfig	1.3.3
using Telix	1.3.3
Outband configuration	1.3.2

P

PABX	1.1.7
PAP	1.2.8
Password	1.2.7, 1.2.8, 1.3.2, 1.3.7, 1.3.13
password	1.2.8
Password Authentication Protocol	1.2.8
Password protection	1.1.6
Password-required	3.1.75
PAT	1.2.7, 1.2.9, 1.4.15
Point-to-multipoint configuration	1.1.4, 1.2.6
Point-to-point configuration	1.1.4, 1.2.6
Policy Based Routing	1.4.19, 3.2.19
Port 1	1.2.2
Port 2	1.2.2
Port 3	1.2.2
Port 4	1.2.2
Port filters	1.2.11
Port number	1.4.17
Power	1.2.2, 1.2.3
Power msg	1.2.2, 1.2.3
PPP	1.1.4, 1.1.5, 1.2.7, 1.2.8, 1.2.12, 1.3.14, 1.5.12
Assigning IP addresses	1.5.6
Callback functions	1.5.8
checking the line with LCP	1.5.5
PPP client	1.3.2, 1.3.6
PPP connection	1.3.2, 1.3.7
PPP LCP Extensions	1.5.11
PPP list	1.2.8, 3.1.42
PPP negotiation	1.3.7
PPP remote access	1.3.3
priority control	1.4.30, 1.4.49
Private Address Spaces	1.4.6, 1.4.7
Private automatic branch exchange	1.1.7
Propagated frames	1.4.24
Protect	3.1.45

Protocol	1.2.14
Provider	1.2.13
Proxy-ARP	3.1.68

R

R1-mask	3.1.69
recall	1.1.8
Reference Manual	1.1.9
Remote access	1.1.3, 1.3.6, 1.5.6, 2.4.2
Remote access for IPX	2.4.7
Remote access using TCP/IP	2.4.2
Remote configuration	1.1.5, 1.3.2
Remote connection	1.3.6
Remote control	1.6.5
Remote-id	3.1.50
Reset system	3.1.84
RIP	1.2.11, 1.4.22
RIP tables	1.4.22
RIP-SAP-scaling	3.1.55
RIP-type	3.1.69
Round robin list	3.1.39
Router	1.4.2
Router interface list	3.1.36
Router name	1.4.8
Routes/FRM	3.1.57
Routing Information Protocol	1.2.11, 1.4.22
Routing table	1.2.10
IP masquerading	1.4.9
special entries	1.4.9
Routing-table	3.1.55

S

S0 interface	1.1.4
S0 status	1.2.2, 1.2.3
SAP	1.2.11, 1.4.22
SAP numbers	3.3.8
SAP tables	1.4.22
Script List	3.2.2
Script list	3.1.44
Script processing	3.2.2
Search methods	2.8.2
Security	1.2.7, 1.2.9
Security features	1.1.2
Security procedures	1.2.8

Security settings	1.6.5
Serial interface	1.3.2
Serial port	1.3.19
Server/FRM	3.1.59
Service Advertising Protocol	1.2.11, 1.4.22
Service priority	1.5.13
Service table	3.1.70
Setting up Internet access	2.2.2
Setup	
Bridge-module	3.1.50
Charges-module	3.1.46
DHCP-module	3.1.72
IP-router-module	3.1.64
IPX-module	3.1.52
LAN-module	3.1.49
Miscellaneous	3.1.81
SNMP-module	3.1.71
TCP-IP-module	3.1.60
WAN-module	3.1.35
Setup Wizard	1.3.3
Short hold	1.2.12
Short-hold	3.1.37
Single user access	1.2.9
SNMP	1.3.10
Agents	1.3.10
Manager	1.3.10
MIB	1.3.10
Socket filter	1.4.24
Socket-Filter	3.1.54
Socket-filter	3.1.56
Software update	1.1.6
Spare-heap-blocks	3.1.50
special dialing characters	3.1.38
Split horizon	1.4.23
Spoofing	3.1.58, 3.1.60
Spoofing mechanisms	1.2.10
SPX watchdogs	1.4.25
SPX-watchdog	3.1.54
Stac	1.2.15, 1.5.12
Static channel bundling	1.5.12
Static routing	1.4.7
Statistics	1.1.6
Status	3.1.3

Bridge-statistics	3.1.15	Telnet	1.1.5, 1.3.6
Call-info-table	3.1.30, 3.1.32	Terminal program	1.1.5, 1.3.3, 1.6.7
Config-statistics	3.1.26	TFTP	1.3.4
Connection-state	3.1.4	Three-party conferencing	1.1.8
Connection-statistics	3.1.28	Throughput	1.5.12
Delete values	3.1.33	Time	3.1.5
Info-connection	3.1.29	Time check	1.1.7
IP-router-statistics	3.1.24	Time-out	1.2.14, 1.5.12
IPX-statistics	3.1.16	TOS	3.2.19
LAN-statistics	3.1.8	Trace	
Layer-connection	3.1.29	code and parameters	1.3.15
Operating-time	3.1.5	Examples	1.3.16
PPP-statistics	3.1.8	starting	1.3.15
Queue-statistics	3.1.27	Trace Outputs	3.2.5
SO-bus	3.1.5	Trace outputs	1.3.14
TCP-IP-statistics	3.1.21	ARP	3.2.16
WAN-statistics	3.1.5	control	3.2.5
Status Displays	1.1.4	DHCP	3.2.18
Subscriber numbers (Windows 95)	1.6.4	ELSA	3.2.9
Symbols	2.1.2	Error	3.2.9
Synchronizing folders	1.6.5	examples	3.2.7
System terminal	1.1.4, 1.2.6	ICMP	3.2.17
System-administrator	3.1.71	IP-MASQ	3.2.17
System-location	3.1.71	IP-RIP	3.2.16
T		IP-Rt.	3.2.14
Table-ARP	3.1.63	IPX watchdogs	3.2.13
Table-bridge	3.1.50	IPX-NetBIOS	3.2.13
Table-budget	3.1.48	IPX-Rt.	3.2.11
Table-RIP	3.1.57, 3.1.69	PPP	3.2.10
Table-SAP	3.1.58	RIP	3.2.11
TCP max. connections	3.1.63	SAP	3.2.12
TCP/IP	1.3.4, 1.4.6	SCRPT	3.2.18
TCP/IP ports	3.3.12	Source	3.2.8
TCP-aging-minute(s)	3.1.63	SPX watchdogs	3.2.13
Technical Data	A-2	Status	3.2.9
Technical data	1.4.4	Time	3.2.8
Telephone	1.1.3, 1.1.7, 1.2.13, 1.6.2	Trace-Ausgaben	
Telephone answering machine	1.1.2	SCRPT	3.2.18
Telephone directory	1.6.7	Transfer costs	1.1.5
Telephone functions	1.1.3	Transfer Master	2.6.6
Telework	2.4.2	Transfer protocols	1.2.14
Teleworking	1.1.3	B channel	1.2.15

D channel	1.2.14
Transmission costs	1.2.10
Transmission rates	1.1.5, 1.3.14
Transparent	1.2.15
Transport protocols	1.6.7
Trap	1.3.12
Trap-IP	3.1.71
Traps-active	3.1.71
Troubleshooting	1.3.13
Twisted pair cable	1.2.5
Type of Service	1.4.19
type of service	3.2.19

■ **U**

Unix	1.2.15
Upgrade	1.2.14
Upload	1.1.6, 1.3.17
Upload-system	3.1.84
User Guide	1.1.9
User name	1.2.8, 1.3.7, 1.5.4

■ **V**

V.24 configuration interface	1.2.5
V.24-max-bitrate	3.1.45
Version-table	3.1.82

Videoconferencing	1.6.2
Volume of data	1.2.14

■ **W**

WAN 1+2	1.2.4
WAN chan1	1.2.2, 1.2.4
WAN chan2	1.2.2, 1.2.4
WAN connection	1.1.4
WAN-1+2	1.2.2
WAN-configuration	3.1.75
WAN-filter-table	3.1.57, 3.1.59, 3.1.67
WAN-update-minute(s)	3.1.58, 3.1.60
Warranty conditions	1.1.9
Watchdogs	1.2.11, 1.4.25
Windows	1.2.15
Workshop	1.1.9
WWW	1.2.9

■ **X**

X.75LAPB	1.2.15
Xchange-Dienst	1.6.5
XModem	1.3.18

■ **Y**

Y connection	1.5.13
--------------------	--------

