ELSA LANCOM™ Business

Manual

No. 20857/0999

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.

ELSA AG
Sonnenweg 11
52070 Aachen
Germany

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

www.elsa.com

Aachen, September 1999

Preface

Thank you for placing your trust in this ELSA product.

By selecting the *ELSA LANCOM Business* you have chosen a router which you can use to connect local area networks or single workstations with other networks via ISDN lines.

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
  Extended description of the router functions and operating modes
- CD containing electronic documentation
  Reference manual, complete description of the menu

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

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

Content

Introduction

The current use of modern communication is making Internet and Intranet applications more and more important for companies in various industries. Online 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. ISDN routers from ELSA 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.

The routers also connect local networks with other LANs (Local Area Networks) and provide access to company data via their remote access function.

What does a router do?

A router connects local 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 over which data can be exchanged between the computers. This path is available in the form of an ISDN connection.

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, all computers in the LAN will be able to access the services and sites on the World Wide Web.

But routers are capable of more. 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 router which then takes care of the data transmission. Equipping the individual workstations with their own data communications equipment—a costly, high-maintenance scenario—thus becomes superfluous.

The 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. It automatically determines whether or not the data needs to be transmitted to another network. If necessary, it establishes the connection to the destination network. Of course, a dedicated line does away with the process of establishing a connection.

When precisely should the 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 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 leased 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 *ELSA LANCOM* 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*.

  LANCAPI is a special form of the CAPI 2.0 interface that applications such as *ELSA-RVS-COM* or *ELSA-ZOC* can use to access the router.

- Dial-up nodes for Internet providers

  With its 4 available S_0 interfaces, i.e. 8 B channels, the *ELSA LANCOM Business* is also suitable as a dial-up unit for providers. The IP pooling function adds convenience to the administration of a large number of remote stations that dial up connections via the router.

What does the *ELSA LANCOM Business* offer?

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

Easy installation

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

LAN connection

ELSA's ISDN routers work on Ethernet networks. A *ELSA LANCOM Business* can be connected to a (Fast) Ethernet network using the 10/100Base-T port.

WAN connection

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

Channel bundling and Compression

The device supports static and dynamicchannel bundling via MLPPP and BACP on the ISDN line. The *ELSA LANCOM Business 4100* supports up to 8 bundled channels. Stac data compression (hi/fn) can be used to achieve increases in the data transfer rate of up to 400%.

Multiple-channel management

Four ISDN connections or a total of eight B channels are available when using the *ELSA LANCOM Business 4100*. It is possible to specify the order in which the channels will be used for each connection. For example, certain channels can be set aside for RAS access, or others enabled for Internet access.

Status displays

A display and LED indicators on the front and back 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 operating systems have another option. With the *LANmonitor* you have status information of the *ELSA LANCOM* 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 connected unit module (router, *LANCAPI*)
- 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.

Statistics

The comprehensive statistics function lets you keep track of your 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.

Charge monitoring

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

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

Least-cost routing

Even if there is a large selection of telecommunications service providers you can always use the cheapest lines using the least cost router. You only need to specify the providers that have the best rates for your requirements once, then the router will automatically

(regardless of whether the call is being placed by the router or the *LANCAPI*) select the provider with the best rates.

Automatic time check

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

Configuration with *ELSA LANconfig*

Setting up and configuring the router to your specific needs is made quick and easy in the Windows operating systems by the configuration tool supplied, *ELSA LANconfig*. Users of other operating systems can use any telnet or terminal program. This means that you can access the device 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 devices in just a few steps.

Intruder protection

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

Compatibility through PPP

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

Remote configuration using PPP

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

Software update

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

The current version is always available to you on our online media and can be loaded via the LAN, the 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 device device. If the new firmware version does not function as desired after the upload you can simply revert to the previous version.

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

ELSA LANCAPI and *ELSA CAPI Faxmodem*

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

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

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

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

DHCP

The *ELSA LANCOM Business* has the functions of a DHCP server available to it. Thus you can define a certain range of IP addresses which the DHCP server then independently assigns to the individual devices on the local network.

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

NetBIOS proxy

ELSA routers are set up especially for the interconnection of Microsoft peer-to-peer networks. With the integrated routing of IP NetBIOS packets, the linking of Windows networks becomes child's play. The remote stations relevant for the exchange of data

are entered in a list to ensure that not every NetBIOS packet results in the establishment of a connection.

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

DNS server

The *ELSA LANCOM Business* also has the functions of a DNS server available to it. You can thus create associations between IP addresses and the names of computers or networks in order to directly provide the correct route for requests for known computer names.

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

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

Dial-up via GSM

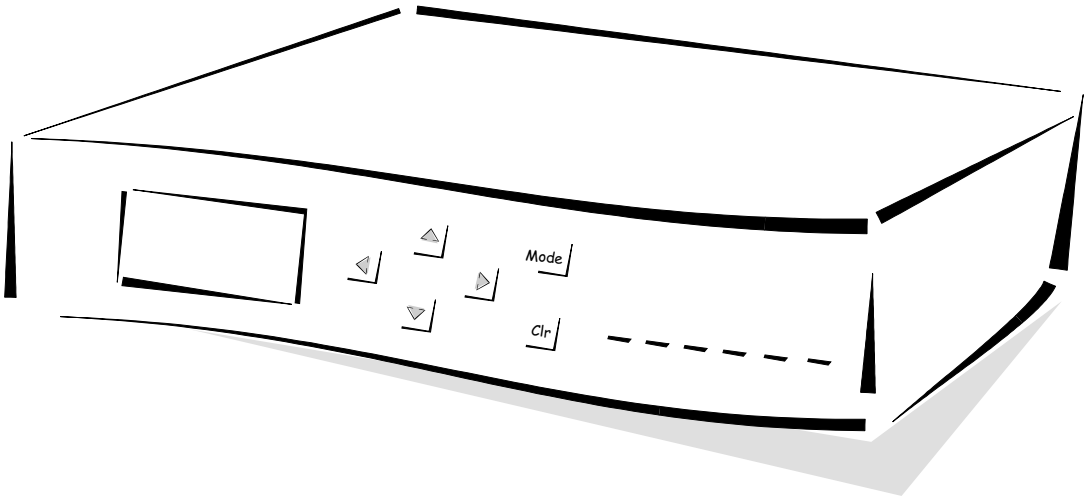
ELSA LANCOM Business also permits dial-up connections via GSM mobile telephones. The router recognizes the call using the V.110 protocol and automatically sets up the layer in use for this data transfer process. RAS access via GSM and ISDN can thus use the same layer.

The *ELSA LANCOM Business* takes the stage

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

What does the unit look like?

We would first like to familiarize you with the router. The display and operating elements can be found on the front: a display, several buttons and light-emitting diodes (LEDs).



The display indicates the various operating states and messages issued by the unit. Operating states and messages can be displayed in three different modes. Use the keys to select the display mode, confirm messages and scroll through the multi-line display. The precise function of each button for the *ELSA LANCOM*'s various operating modes is described in chapter 'Configuration modes'.

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

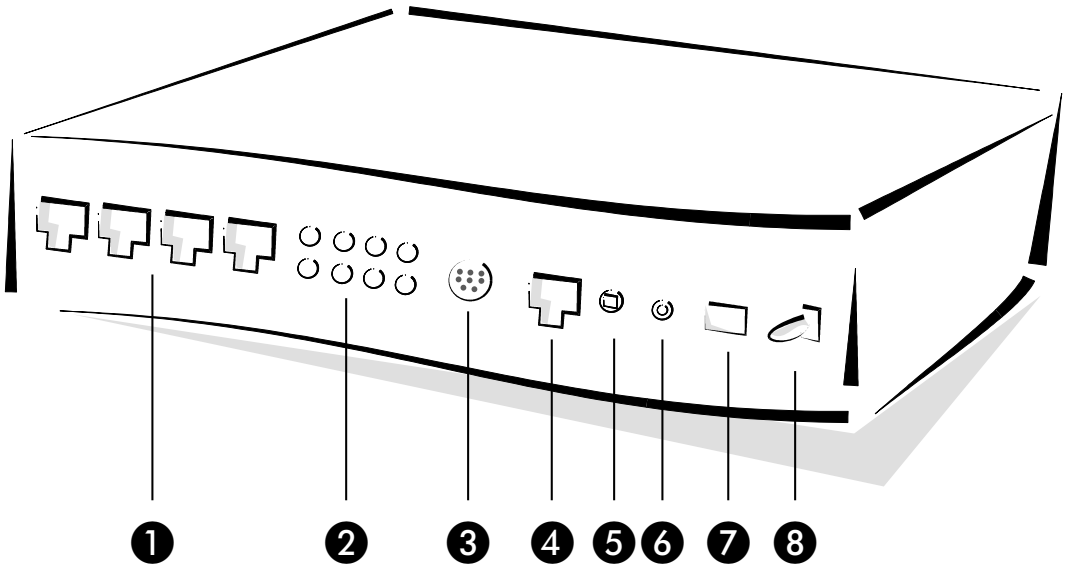
LAN-TX, -RX, LAN-Coll, -Link LAN-FDpx, -Fast

These LEDs show the corresponding network controller status:

LAN-RX/TX	yellow	Data packet sent from the device to the LAN or vice versa
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	green	*ELSA LANCOM* is operating at 100Mbit

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



1. four ISDN S_0 ports (*ELSA LANCOM Business 4100*)
2. Status LEDs for the four S_0 connections:

S_0 status	Off	Bus not activated
	flashing rapidly	Bus with D channel active, no TEI assigned
		D channel detected, bus not activated
	green	Bus with D channel active, TEI assigned
S_0 line	Off	No call, no connection
	flashing slowly (1x per sec., 2x or 3x in total)	Incoming call, but router is not responsible or the router is establishing a connection automatically
	flashing rapidly (3x per sec.)	Call has arrived, router is responsible but has not (yet) seized the line
	yellow	Connection (being) established

3. V.24/RS232 configuration interface
4. 10/100Base-TX for 10-Mbit or 100-Mbit networks
5. Node/hub selector switch
6. Reset button, resets the hardware or restores the unit's factory defaults (after holding for approx. 5 seconds).
7. Connection for power supply unit
8. On/Off switch

Node or hub?

Please check the position of the Node/Hub switch when connecting the unit to the LAN:

- As the factory default, the switch is set to 'Node'. In this setting, the device acts as a node on a network. It 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 device 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.

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 to 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.

Configuration modes

ELSA LANCOM Business 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 device and set it up.

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

Many paths lead to the *ELSA LANCOM*

In principle, there are different methods of accessing the router of ELSA:

- Through the configuration interface (config interface) on the rear of the 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?

On one hand, the availability of the units: Configuration via outband is always available. Inband configuration is not possible, however, in the event of a network fault. Remote configuration is also dependent on the transfer medium, such as the ISDN connection.

On the other hand, whether or not you will need additional software or hardware. The inband configuration requires one of the computers already available in the LAN or WAN, as well as suitable software. In addition to the software, the outband configuration also requires one of the computers (with a serial port) and a suitable configuration cable. Remote configuration requires a 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*.

The direct method: outband

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

You really only need to use the outband configuration method if you cannot access your device via TCP/IP.

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 router (the PCs 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 *ELSA LANCOM* devices in the local area network (but not on the serial ports). New devices can be found with **Device ▶ Find ▶ Search at all serial ports**. *ELSA LANconfig* displays new routers in the list by their devices types.

If your device 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 your *ELSA LANCOM* for the task selected.

Double-clicking on a device designation in the list of found devices opens the current configuration for editing.

Outband configuration using a terminal program

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 router. However, this is only possible if the 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 *ELSA LANconfig*. This means that the TCP/IP protocol must be installed on the computer being used and the router must be given an IP address which you will then use when addressing it. A device that has not been configured yet will respond to the IP address XXX.XXX.XXX.254, in which the Xs are placeholders for the network address in your LAN. If the computers on your network have addresses such as 192.110.130.1, then you will be able to address the 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 device using the outband configuration method before you install it on the LAN.

Alternatively: Address administration with the DHCP server

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

Beginning inband configuration using *ELSA LANconfig*

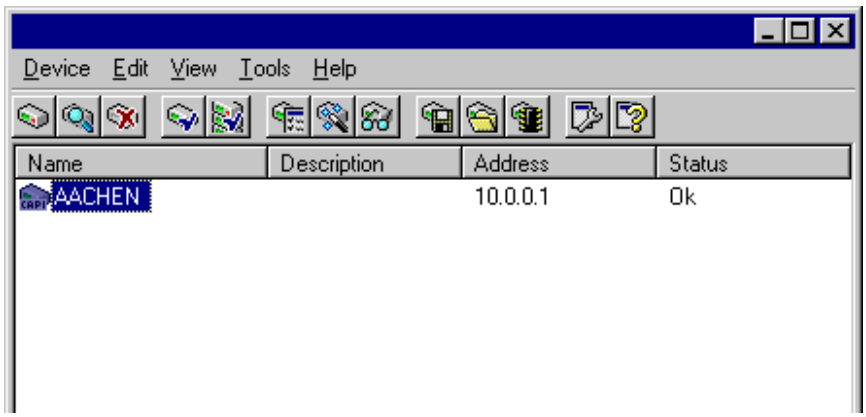
After the installation (double-click on 'autorun.exe') is complete, call up the *ELSA LANconfig* configuration tool, for example by clicking on **Start** ▶ **Programs** ▶ **ELSAlan** ▶ ***ELSA LANconfig*** in the Windows task bar. *ELSA LANconfig* searches the local area network for *ELSA LANCOM* devices. *ELSA LANconfig* will automatically start up the setup wizard if a device 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 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 device and then clicking the **Configure** button or the **Edit** ▶ **Edit Configuration File** option reads the device's current settings and displays the 'General' configuration selection.

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

Start up inband configuration using telnet

Start up inband configuration using telnet with the command:

```
telnet 10.1.80.125
```

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

Once you have entered the password, configuration can be carried out using any of the commands contained in 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 device 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 *ELSA LANCOM* with *ELSA LANCAPI*

This is how you prepare the 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 (*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 *ELSA LANCOM* 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 device 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 PPP client and telnet

① Establish a connection to the *ELSA LANCOM* with your PPP client using the following details:

- User name 'ADMIN'
- Password as set on the *ELSA LANCOM*, factory default setting is no password
- An IP address for the connection, only if required

② Open a telnet session to the *ELSA LANCOM*. 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 *ELSA LANCOM* 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 *ELSA LANCOM* 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 *ELSA LANCOM* remotely just like all other devices.

Limiting remote configuration

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

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

① 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.

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

```
set /Setup/Config-module/Wan-config [on][read][off]
```

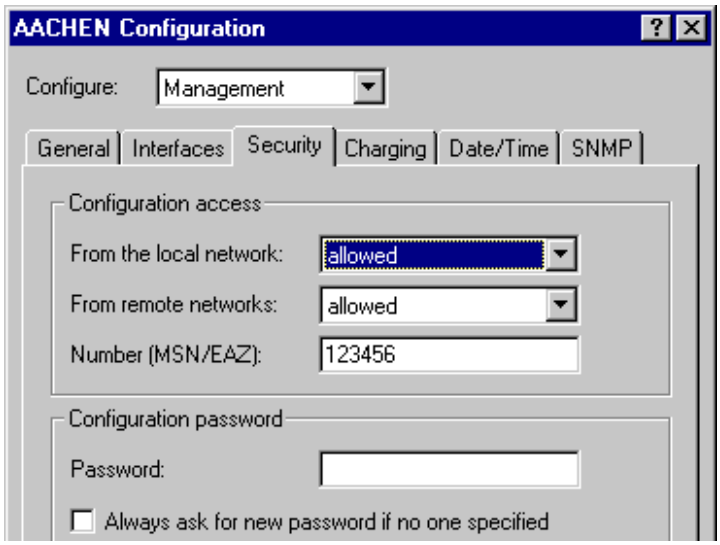
If you wish to block access to the router from the WAN entirely, set configuration access from remote networks to 'denied'.

③ As the calling number in the 'Configuration access' area, enter a MSN or EAZ of your ISDN connection which is not used by the router, the *LANCAPI* or the a/b ports.

Alternatively, enter the following command:

```
set /Setup/Config-module/Farconfig (EAZ-MSN) 123456
```

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



Alternatively, enter the following command:

`passwd`

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

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 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 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 /setup/name GLASGOW assigns the name 'GLASGOW' to the device.
set <VALUE> ?	shows you which values can be specified here.	
del <VALUE>	deletes a a table row.	del /se/wan/nam/GLASGOW Deletes the entry for the remote station GLASGOW.
do <ACTION> (parameters)	executes the ACTION according to any parameters specified.	do /firmware/firmware-upload starts the upload of new firmware.
passwd	allows a new password to be specified. The old password, if there is one, must be entered first. The new password must then be entered twice in a row and confirmed each time with ↵.	
repeat <sec> <ACTION>	repeats the action at an interval of the number of seconds specified. Any key can be used to terminate the repetition.	repeat 3 dir/status/wan-statistics displays the current WAN statistics every 3 seconds
time	sets the system time and date.	time 24.12.1998 18:00:00
language	sets the language for the current configuration session.	Languages currently supported: English (language English) German (language German)
exit, quit, x	configuration is terminated.	

Text entries with spaces are only accepted if they are placed in quotation marks, i.e. `set/se/snmp/admin "The Administrator"`.

Text entries (individual and table values) can be deleted as follows:

```
set /se/snmp/admin ""
```

New firmware with FirmSafe

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

This is how FirmSafe works

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

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

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

How to load new software

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

- Configurations tool *ELSA LANconfig* (recommended)
- 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 router will add the missing values using the default settings.

ELSA LANconfig

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

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

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

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 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

With TFTP you can use the **writeflash** command to install new firmware. To transmit a new firmware version which, for example, is in the 'LC_1000U.130' file, to a 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 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 device 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, other configuration commands can be performed too. The syntax is best demonstrated with the following examples:

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

Configuration using SNMP

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.

The firmware of ELSA routers includes an implementation for an SNMP V.1 agent (in accordance with RFC 1157). 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 router completely using SNMP. All menus and parameters of the 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-devices/isdn-router/...
or 1.3.6.1.4.1.2356.400.1...

Accessing tables and parameters using SNMP

Any of the 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 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 device'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 router's password is not entered.

The settings in 'Setup/Config-module' are evaluated as follows if using SNMP to access the 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-config	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

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 the 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. They are only displayed in the menu for information purposes.

The Management Information Base (MIB)

A textual representation of the configuration structure (the so-called private MIB) must be supplied with the *ELSA LANCOM* 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 CD and in the ELSA online media.

What's happening on the line?

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

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

Trace outputs

Trace outputs may be used to monitor the internal processes in the 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 *ELSA LANCOM* 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

This parameter ...	... brings up the following display for the trace:
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
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	Displays the status of the PPP
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 manual.

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 operating systems. Many of the internal messages generated by the device are converted to plain text, thereby helping you to troubleshoot.

Installing *ELSA LANmonitor*

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

If *ELSA LANmonitor* is not yet installed on your computer, place the *ELSA LANCOM* 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 CD *ELSA LANCOM* and follow the instructions in the install program.

During the installation you should activate the 'ELSA LANmonitor' 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 router connected to the serial interface.

Checking your Internet connection with *ELSA LANmonitor*

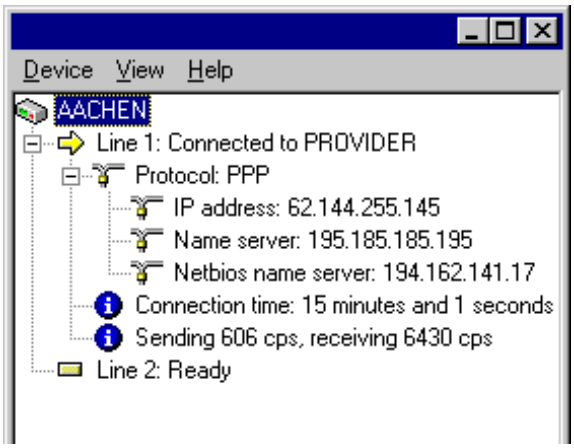
To demonstrate the functions of *ELSA LANmonitor* we will first show you the types of information *ELSA LANmonitor* provides about connections being established to your Internet provider.

① Setup the router to connect to your provider, e.g. with the *ELSA LANconfig* setup wizard.

② Start up *ELSA LANmonitor* by clicking **Start** ▶ **Programs** ▶ **ELSAlan** ▶ **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 the *ELSA LANconfig* and monitor it using **Tools** ▶ **Monitor Device**.

③ *ELSA LANmonitor* automatically creates a new entry in the device list and initially displays the status of the 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 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 LC 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 a log of the *LANmonitor* output in file form, select 'Options' from the 'View' menu and go to the 'Log' tab. Enable logging and specify whether *LANmonitor* should create a log file daily, monthly, or on an ongoing basis.

Operating modes and functions

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

- Security for your configuration
- Security for your LAN
- Call charge management
- ISDN connections
- Leased lines and backup procedures
- Dial-up via GSM
- Point-to-point protocol
- IPX routing
- IP routing
- Automatic address administration with DHCP
- DNS-server
- NetBIOS proxy
- IP pooling for dial-up access
- *ELSA LANCAPI*
- Time check
- The least-cost router

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

Detailed sample configurations can be found in the Workshop.

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

Security for your configuration

A number of important parameters for the exchange of data are established in the configuration of the device. These include the security of your network, monitoring of costs and the authorizations for the individual network users.

Needless to say, the parameters that you have set should not be modified by unauthorized persons. The *ELSA LANCOM Business* thus offers a variety of options to protect die configuration.

Password protection

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

The password input field can be found in the *ELSA LANconfig* in the 'Management' configuration section on the 'Security' tab. The password prompt can be activated in a terminal or telnet session in the `/Setup/Config-module/password-required` menu. In this case, the password itself is set with the command `passwd`.

Login barring

The configuration in the *ELSA LANCOM Business* 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 menu:

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

Access control via TCP/IP

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

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

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

Security for your LAN

You certainly would not like any outsider to have easy access to or to be able to modify the data on your company's servers. The *ELSA LANCOM Business* offers you various ways of restricting access from outside:

- Access protection using name, password and call number
- Callback to defined call numbers
- Data packet filtering
- IP masquerading (also known as NAT or PAT)

Security check

The identifier to be used to recognize callers can be set in the 'Communication' configuration section of the 'Call Accepting' tab or using the `/Setup/WAN-module/Protect` 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 corresponding information is also sent by the caller.

Verification of name

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

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

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

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

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

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

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

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

Checking the number

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

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

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

Callback

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

The callback characteristics of your router can be controlled using the settings in the name and number lists and the selection of the (PPP) protocol:

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

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

If the router is requested to call back, the Fast 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 routers 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 while connected with the Internet. Only the router module of the unit and its IP address are visible on the Internet. The IP address can be fixed or assigned dynamically by the provider. The computers in the LAN then use the router as a gateway so that they themselves cannot be detected. To do this, the router separates Internet and intranet, as if by a wall. Therefore, IP masquerading is also called a "firewall function".

The use of IP masquerading is set individually for each route in the routing table. The routing table can be found in the *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Routing' tab, or in the `/Setup/IP-router-module/IP-routing-table` menu.

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

Call charge management

The capability of the router to automatically establish connections to all required remote stations and close them again when no longer required provides users with extremely convenient access to the Internet, remote networks and individual computers. However, incorrect configuration of the router (such as badly configured filters) for data transfer via ISDN dial-up connections or excessive use of the features provided (continual Internet surfing, for example) can result in high telephone charges.

Charge-based connection limits

In order to limit these charges, the software has long offered the option of specifying a ceiling on the charges incurred during a specified period. For example, in its default state, a maximum of 830 charge units may be used per week. The router will not permit the establishment of any further connections once this limit has been reached.

*The best way to use the 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 telecommunications 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!

Time-dependent connection control

However, this mechanism will not work if the ISDN connection does not provide charge information. That may be the case, for example, if the provision of charge information was not requested for the connection, or if the telecommunications provider generally does not supply this information.

The telephone charges can still be controlled by limiting the maximum connection time. This requires setting up a time budget—similar to the charge budget—for a specified period. In the router's default state, for example, connections may only be established for a maximum of 210 minutes per week.

When either of these limits are reached, all open connections that were initiated by the router itself will be shut down automatically. The budgets will not be reset to permit the establishment of connections until the current period has elapsed. Needless to say, the administrator can reset the budgets at any time if required!

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

Only the router functions are protected by the charge and time monitoring functions! Connections via LANCAPI are not affected.

Settings in the charge module

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

In the charge module, the online time and registered charges can be set, monitored and used to control call establishment.

- Day(s)/Period
  The duration of the monitoring period in days can be specified here.
- Budget-units, Minutes-budget
  The maximum number of units or online minutes in a monitoring period
- Spare-units, Spare-minutes
  Available units or online minutes remaining in the current period
- Router-units, Router-minutes
  Units or online minutes over all periods

- Router-units

  All charges incurred through the unit

- Table-budget, Time-table

  Tables with charges or times for the respective modules

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

ISDN connections

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

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

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

Name list

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

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

- Name

  This name is used to identify the remote station in the router modules.

- Phone number

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

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

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

- Short hold

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

  – the last data has been exchanged across static connections for the holding time B1.

  – the data throughput has dropped below a specified level for the holding time B2 in dynamic connections.

- Layer-name

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

- Callback

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

  – Normal callback

  – Callback using the fast ELSA process

  – Callback after name verification

  – Await the callback from the remote station using the fast ELSA process

Interface settings

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

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

- The D channel protocol used on the S_0 port

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

- Leased line option

  B channel to be used for the leased line

- Dial prefix

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

Router interface settings

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

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

- Phone numbers (MSN/terminal device selection numbers)

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

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

- Option for multiple simultaneous connections

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

- Suppression of own phone number

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

This function must be supported by the network operator.

LANCAPI interface settings

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

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

- Phone numbers (MSN/terminal device selection numbers)

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

- Access to *LANCAPI*

  Here you can completely disable the *LANCAPI* functions for the interface, or enable

it only for incoming or outgoing calls.

- Transfer of own subscriber number

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

Layer list

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

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

- Layer-name

  The protocol settings will be saved under this name. In the name list, select the settings with the layer name for the appropriate connection.

- Encapsulation

  Specify here whether an Ethernet header should be added to the data packets. Normally the setting 'Transparent' will be sufficient; this setting may only be required for HDLC connections to third-party devices.

- Layer-3

  Layer-3 protocol for the connection. Recognized automatically in the case of some incoming connections.

  An additional entry is required in the PPP list when using PPP.

  An additional entry is required in the scripts list when using scripts.

- Layer-2

  Layer-2 protocol for the connection.

- Options

  Enables data compression and channel bundling. This option is only effective when supported by the protocols of Layer 2 and Layer 3.

- Layer-1

  Layer-1 protocol for the connection. Recognized automatically in the case of some incoming connections.

Round-robin list

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

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

- Remote site

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

- Round-robin

  Additional numbers for this remote station. Multiple numbers are separated by hyphens.

- Begin with:

  Indicate whether a new call establishment should start with the last successfully used number, or always with the first number of the list.

Channel list

The channel list in the *ELSA LANconfig* can be found in the 'Communication' configuration section on the 'Remote Sites' tab, or under `/Setup/WAN-module/Channel-list` during telnet or terminal sessions.

Use the channel list to determine the minimum and maximum number of B channels to be used for the connection, which channels are to be connected in which sequence, and the number of channels to be used as a dial-up backup for a fixed connection if required.

- Remote site

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

- Min

  Minimum number of channels to be used to establish a connection.

  If more than one channel is specified, static channel bundling will be used for this connection. The layer to be used must be set up for bundling in the Layer-2 options.

- Max

  Maximum number of channels to be used to establish a connection.

  If a larger maximum number of channels is stated than the minimum, dynamic channel bundling will be used for this connection. The layer to be used must be set up for bundling in the Layer-2 options.

- Order

  The sequence in which connections for the individual channels are established;

stated with the syntax [Interface]-[Channel];[Interface]-[Channel] etc.

- Back-up channels

  Number of channels to be opened over dial-up lines when a leased line is down.

PPP list

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

Use the PPP list to establish additional parameters for connections that use PPP in the communications layer on layer 3.

- Remote site

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

- Username

  User name to be used when establishing a connection with the remote station.

- Password

  Password to be used when establishing a connection with the remote station.

- IP, NetBIOS, IPX

  Protocols that may be used over this connection.

- Auth.

  Authentication process that the router should request from the remote station.

- Time, Ret., Conf., Fail., Term.

  Parameters pertaining to connection characteristics that will not be described in greater detail here.

Script

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

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

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

- Remote site

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

- Script

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

Call acceptance

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

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

- all

  Every call is accepted.

- by name

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

- by number

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

- by name or number

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

Number list

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

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

- Phone number

  subscriber number transmitted by the remote station (incl. country and long distance codes if available).

- Remote site

  Name of the remote station as specified in the name list. The remote station will be called back if so specified in the name list.

Leased lines and backup procedures

If your ISDN connection is in permanent use, or you need to establish dial-up connections repeatedly at short intervals, a fixed ISDN connection may prove more economical for your purposes. As the D channel is not required for data communications via fixed

connections, yet the provision of a D channel is generally billed, fixed connections without a D channel offer the best value for money.

If one channel is sufficient in the long term, select D64S. If the data throughput of a single channel is not satisfactory, consider the deployment of the D64S2. Two D64S connections may be used for connections to two different remote stations. This combination is also referred to as D64SY:

Leased-line connection	Type
D64S	One B channel, no D channel to remote station
D64S2	Two B channels, no D channel to remote station
D64SY	Two B channels, no D channel to two different remote stations

All three types are set as Group 0 fixed connections in the interface table. The versions are distinguished by the YV. flag in the interface table, the layer-2 options in the layer list and the entries in the channel list.

Setting up fixed connections

The following settings are required to prepare the router for use with the various fixed connection types.

Settings in the Interface table

- Specify the **Grp0** protocol in the interface table.
- The **YV. flag** must be set to **Off** for connections to a single remote station, or to **On** for multiple remote stations.
- For connections with one B channel, the layer-2 option **compr.** can be specified in the layer used.

  For connections with two B channels to a single remote station, enter **bundle** as well as **compr.** as required.

  When connecting to two remote stations via 2 B channels, **compr.** can be specified.

Settings in the channel list

Use the channel list to specify the channels to be used for the fixed connection. The same settings must be used for the channels and their sequence on both sides of the connection. If applicable, the number of channels to be used for a backup connection should be entered here (also the same on both sides of the connection).

Remote site	Min	Max	Order	Back-up channels
FVG0	2	2	1-1;1-2	0

Settings in the name list

With a Group 0 fixed connection, the units automatically go online when switched on and establish a connection with the default layer.

The remote station must be specified in the name list in the event that a different layer, the dial-up backup mechanism or dynamic bundling via dial-up lines are to be used.

Name	Phone number	Short hold	Short hold 2	Layer-name	Callback
FVG0	1234	20	0	PPPHDLC	Off

The subscriber number is used to establish further dial-up connections to be dynamically bundled to the leased line. If required, additional numbers can be entered in the round-robin list.

The numbers entered are used to establish backup connections if the leased line is not available due to a malfunction and the dynamically bundled dial-up connections have been terminated due to a reduction in data throughput.

Settings in the layer list

A Group 0 fixed connection is initially always established with the default remote station, i.e. with the layer entered for the default remote station. If no default remote station is available or no layer entry is available for the remote station, the connection will be established with the layer entered as the DEFAULT in the layer list. If no DEFAULT entry has been specified, the connection will be established with the following layer settings:

Layer-name	Encapsulation	Layer-3	Layer-2	Options	Layer-1
DEFAULT	TRANS	PPP	TRANS	none	HDLC64K

For example: D64S2, dynamic bundling (one channel), no backup

Assign the layer 'MLHDLC' to the fixed connection in the name list and specify the subscriber number for the dynamic dial-up line:

Name	Phone number	Short hold	Short hold 2	Layer-name	Callback
FVG0	123456	20	20	MLHDLC	Off

Enter the required number of channels in the channel list and specify the channels to be used. No backup channel is specified.

Remote site	Min	Max	Order	Back-up channels
FVG0	2	3	1-1;1-2;2-1	0

For example: D64S2, dynamic bundling (one channel), backup (one channel)

The entry in the name list remains the same. Specify a backup channel in the channel list.

Remote site	Min	Max	Order	Back-up channels
FVG0	2	3	1-1;1-2;2-1	1

For example: D64S2, no bundling, backup (two channels)

The entry in the name list remains the same. Specify a backup channel in the channel list.

Remote site	Min	Max	Order	Back-up channels
FVG0	2	3	1-1;1-2	2

Dial-up via GSM

With a greater number of available B channels, *ELSA LANCOM Business* is an ideal remote-access server for small and mid-size businesses. The router also supports the V.110 protocol to permit field staff to connect to the company network using notebooks via GSM mobile phones.

GSM access is set up in the same way as any other remote access, using the convenient wizard in *ELSA LANconfig*, for example. The layer used must then be adapted to the appropriate protocol.

Layer name	Encapsulation	Layer-3	Layer-2	Options	Layer-1
DEFAULT	TRANS	APPP	TRANS	none or comp.	V.110 9600

Not all providers offer data services via GSM telephones as a standard part of their service agreements. In some cases these must be enabled separately and are subject to additional charges. Some providers also distinguish between outgoing and incoming data calls.

Point-to-point protocol

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

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

The protocol

What is PPP?

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

- Password protection according to PAP or CHAP
- 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 (IP Control Protocol and IPX Control Protocol).
- Verification of the connection through the LCP (Link Control Protocol)
- 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 *ELSA LANCOM* 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 state.

- Authenticate phase

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

  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 *ELSA LANCOM*.

  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 *ELSA LANCOM*

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

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

```
trace + ppp
```

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

The PPP list

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

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

In this column of the PPP list...	...enter the following values:
Remote site	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.
Password	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.
Retries	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 *ELSA LANconfig* 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.
Rights	Network protocols to be routed over this connection: IP, IPX, NTB (NetBIOS). NetBIOS always requires one of the other two protocols.

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. This may be found in the form of a backup line, for example.

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 'Retries' 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 *ELSA LANCOM* 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, on the other hand, is used only within the LAN.

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

- For 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' field. In this case the router name is the name

the remote station uses to identify itself to the *ELSA LANCOM*.

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 *ELSA LANCOM*. 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.

- For example: Internet access

  The assignment of IP addresses can take place the other way round if the *ELSA LANCOM* is used to provide access to the Internet for a local area network. In this case it is possible to configure the *ELSA LANCOM* 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 *ELSA LANCOM* also receives information on DNS servers at the provider in addition to the IP address during PPP negotiation.

  The *ELSA LANCOM* 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 *ELSA LANCOM* 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 *ELSA LANCOM*:

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. 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 *ELSA LANCOM* 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.*

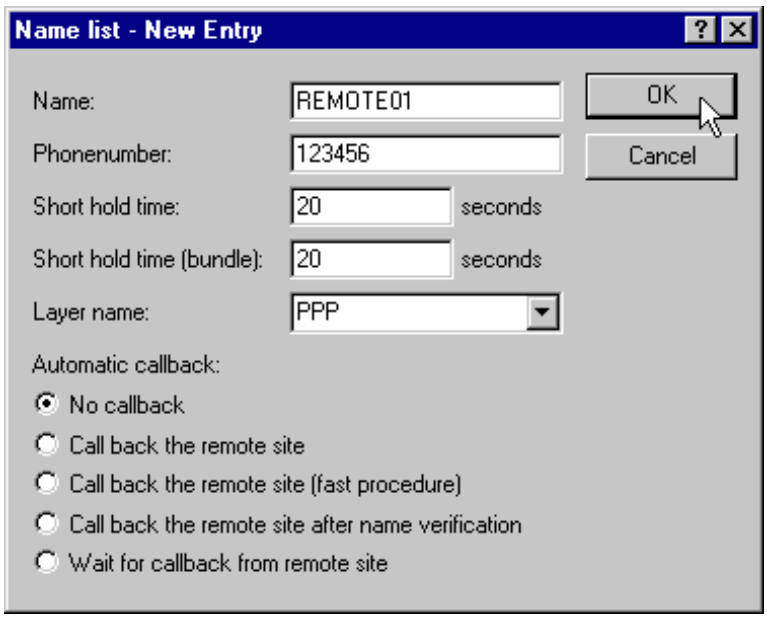
Microsoft CBCP callback

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 *ELSA LANCOM* 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.



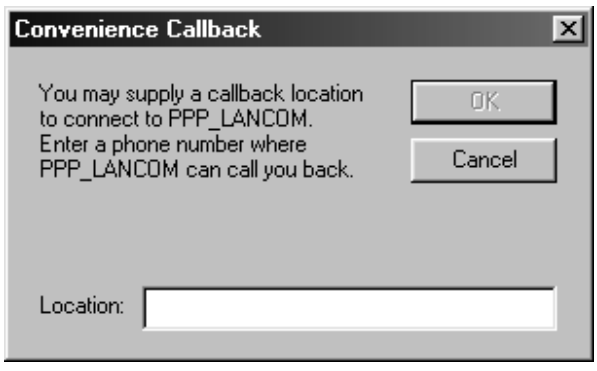
No callback

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.

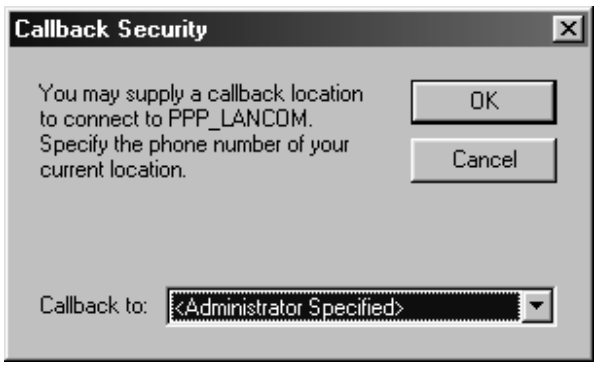
Following the authentication process, the dialog box below will appear in Windows 95 in which the user can specify his call number:



Callback number specified by the *ELSA LANCOM*

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 is delay is specified by Windows and cannot be shortened.

Fast ELSA callback

This fast, ELSA-specific process is ideal if two *ELSA LANCOM* 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 *ELSA LANCOM*. All versions will be processed in the same way, however:

The *ELSA LANCOM* 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 several B channels for the transfer (channel bundling).

Connections using channel bundling differ from ”normal“ connections inasmuch as they use not only one, but several 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 router tries to establish the number of B channels specified as 'Minimum' in the channel list. Either the channels specified in the channel list or random free channels are used.

- Dynamic channel bundling

  In the case of dynamic channel bundling, the router initially establishes the number of B channels specified as 'Minimum' in the channel list and starts the data transfer. If the router determines that the throughput stays above a certain threshold for a given period of time, it will attempt to add further channels until the number specified as 'Maximum' in the channel list has been reached. Either the channels specified in the channel list or random free channels are also used in this case.

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

How to configure channel bundling

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

⑦ 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 several 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, the setting for the Y connection in the interface table and the setting for the channel table.

– **bnd+compr** uses both compression and channel bundling and therefore provides maximum possible transmission performance.

⑧ 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 hold time determines the delay time after which the dynamic channels are terminated once the data throughput drops below the threshold value.

⑨ Use the channel list to determine the number of channels to be used for the connection. You may also specify the channels to be used, thus keeping certain channels free for dial-up connections via RAS, for example.

The channel list entry determines whether static or dynamic channel bundling will be used (see above). More than one minimum channel results in static bundling, whereas a difference between the minimum and maximum number of channels permits dynamic channel bundling.

⑩ Use the entry for the Y connection in the interface list to determine what should happen if an additional connection to a different remote station is requested during an existing connection using channel bundling, but no further B channels are available.

– Y connection **On**: The router interrupts the bundled connection on this interface to establish a connection to the other remote station. When the 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 holds the existing bundled connection on this interface, the other connection must try a different interface or wait if none of the interfaces with active channel bundling permit a channel to be terminated.

IPX routing

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 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 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 determine 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
BRANCH01	00000245	802.3	Route	On
BRANCH02	00000320	SNAP	Filt.	On
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 ≠ WAN address 1 = WAN address 2 ≠ LAN address 2 ≠ 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).

  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 and is ready for operation, it 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 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 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 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 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, 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 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 device addressed.

Redundant routes

A 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. Therefore, it 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-Config/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 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 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-module/IPX-router/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 router has derived from other routers. It gets its information for this purpose from routers on both local and remote networks. The 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 router incorporates the information on the services available in its internal SAP table and registers which service is available on which network at which MAC address. At the same time it 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 (`setup/IPX-module/RIP-config` *or* `SAP-config`*) of the 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 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, 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:

  - IPX watchdogs receive no response. 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 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' in the reference manual.

IP routing

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

The IP routing table

Use the IP routing table to tell the router which remote station (which other router or computer) it should send the data for particular IP addresses or IP address ranges to. This type of entry is also known as a "route" since it is used to describe the path of the data

packet. This procedure is also called ”static routing“ since you make these entries yourself and they remain unchanged until you either change or delete them yourself. Naturally, there is ”dynamic routing“, too. The routers use the routes in this way to exchange data between themselves and continually update it automatically. The static routing table can hold up to 64 entries, the dynamic table can hold 128. The IP router looks at both tables when the IP RIP is activated.

You also use the IP routing table to tell the 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 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 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.

The routing table can be found in the *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Routing' tab, or in the `/Setup/IP-router-module/IP-routing-table` menu. This, then, is how an IP routing table might look:

IP address	Netmask	Router	Dis-tance	Mask.
192.168.120.0	255.255.255.0	GLASGOW	2	On
192.168.125.0	255.255.255.0	LONDON	3	Off
192.168.130.0	255.255.255.0	191.168.140.123	0	Static

What do the various entries on the list mean?

- IP addresses and Network

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

- Router

  The 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 router on the network cannot address the remote station itself.

- Distance

  Number of routers between your own and the destination router. This value is often equated with the cost of the transmission and used to distinguish between inexpensive and expensive call paths for wide-area connections. The distance

values entered are propagated as follows:

- All networks which can be reached while a 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 transmitting 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. These ”Proxy hosts“ are not propagated at all.

- Mask.

  Use the 'Masquerade' option in the routing table to inform the router which IP addresses to use when transferring the packets.

  - 'Off': No masquerading.
  - 'On': This entry requests a random IP address valid in the Internet from your provider which is then used for the connection and masquerading.
  - 'stat.': Use this entry to request the assignment of a specific IP address from your provider as entered in the 'TCP/IP' configuration section on the 'General' tab or in the `/Setup/TCP-IP-module` menu. This address will be used for the connection and masquerading.

  For further information see the 'IP Masquerading' section.

- 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 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. 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	Netmask	Router	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.

IP address	Netmask	Router	Dist.	This is what happens:
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	HEAD OFFICE	2	All data packets which cannot be allocated to the entries listed above are transmitted to the HEAD OFFICE remote station.

The sequence of the entries is important here: They are processed from top to bottom. The router sorts entries automatically: Firstly by network masks, in descending order. Then by the IP addresses, in ascending order. This places the 'HEAD OFFICE' entry at the very end of the list. If this entry were at the top of the list, the router would send all (!) data packets not belonging to the local network to the network of the head office.

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' 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' in the reference manual). The source ports, on the other hand, may be selected freely within certain ranges.

The router can check the source and destination ports of data packets using the TCP or UDP protocols. It can then deduce the purpose of the data from these ports. For example, FTP accesses or Telnet sessions can be identified. 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 IP router has two separate filter tables, for packets coming from the LAN and from the WAN. These filter tables can be found in the *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Filtering' tab, or in the `/Setup/IP-router-table/WAN-filter-table` or `LAN-filter-table` menus.

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 a router. This is the case when individual workstation computers (teleworkers) are networked via TCP/IP to the company network. The teleworker then has an IP address which is located in the same local network as all the other computers in the LAN. A data packet from LAN to the teleworker would usually only search for a receiver locally, but would not be able to find one.

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

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

IP address	Netmask	Router	Dis-tance	Mask
192.168.110.123	255.255.255.255	Teleworker01	0	off

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

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

Local routing

You know the following behavior of a workstation within a local network: The computer searches for a router to assist with transmitting a data packet to an IP address which is not on its own 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 can you assist the workstation computer now?

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

Certain computers, however, do not know how to handle ICMP redirects. To ensure that the data packets reach their destination anyway, use local routing (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Routing' tab or in the `/Setup/IP-router-module/Local-routing` menu). This is how you tell the 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 ELSA routers also have a dynamic routing table containing up to 128 entries. Unlike the static table, you do not fill this out yourself, but leave it to be dealt with by the router itself. It uses the routing information protocol (RIP) for this purpose. 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 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 running on other routers in the local network.
- Routes linking individual computers to the LAN by proxy ARP.

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

- If the 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 router which they can use. The establishment of additional connections by routers with dial-up connections can be prevented, thus reducing connection costs.

- If this router cannot establish a further connection to another remote station, all other routes are propagated with the distance '16' in the RIPs. The '16' stands for "This route is not available at the moment". If a router cannot establish a connection, in addition to the present one, this may be due to one of the following causes:
  - Another connection has already been established on all the other channels (also via the *LANCAPI* or a/b ports).
  - The existing connection is using all B channels (channel bundling).

To take advantage of this function, enable the 'IP RIP' option (in ELSA 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 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 the router receives such IP RIP packets, it incorporates them in its dynamic routing table, which looks something like this:

IP address	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 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), the 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 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.

IP masquerading (NAT, PAT)

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

This particular solution is called IP masquerading. This is a procedure whereby only one LAN router appears on the Internet with an IP address. This IP address is allocated to the router either permanently by the NIC or temporarily by an Internet provider. All the other computers on the network then ”conceal“ themselves behind this one IP address. Aside

from the welcome savings, IP masquerading has the added benefit of guarding very effectively against attacks on the local network from the Internet.

Two addresses for the router

Masquerading pits two opposing requirements of the 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 router is therefore assigned an **Inter**net address and an **intra**net address, each with its own fitting network mask. Use the 'Masquerade' option in the routing table to inform the router which of the two addresses to use when transferring the packets. If a specific address is requested from the provider, two options are available for the actual address assignment:

- The provider assigns the desired address to the router. The network mask now decides how many computers are masked behind the 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 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 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 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 router receives a data packet for transfer it now notes the IP address and the sender's port in an internal table. It 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 router with the new sender port number. The entry in the internal table allows the router to assign this response to the original sender again.

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

Simple and inverse masquerading

This masking operates in both directions: The local network behind the IP address of the 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 router appears to be the FTP server. The router knows the intranet address of the server from the entry in the service table (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Masq.' tab or in the `Setup/IP-router-module/Masquerading/Service-table` menu). 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 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 router itself makes the entry in the port and IP address information table.

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

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

Which protocols can be transmitted using IP masquerading?

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

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

- FTP
- TCP
- UDP
- ICMP

DNS forwarding

Names rather than IP addresses are generally used to access a server over the Internet. Who knows which address is behind 'www.domain.com'? The DNS server, of course.

DNS stands for Domain Name Service and refers to the assignment of domain names (such as domain.com) to the corresponding IP addresses. This information must be

constantly updated and be accessible all over the world at any time. DNS servers holding long tables containing IP addresses and domain names exist for this purpose.

If a computer calls up a home page from the intranet, it first sends out a DNS request: "Which IP address belongs to www.domain.com?" If the router has been specified as the DNS server in the workstations, the request is handled as follows:

- Initially the router checks whether a DNS server has been entered in its own settings (in *ELSA LANconfig* in the 'TCP/IP' configuration section on the 'Addresses' tab or in the `/Setup/TCP-IP-module` menu). If it finds one it connects to this server and retrieves the information required.
- If no DNS server is entered in the router, it 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 router during PPP negotiation.
- If no connection exists, the default route is established and a search is then carried out there for the DNS server.

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 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.

Policy-based routing

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

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

Automatic address administration with DHCP

In order to operate smoothly in a TCP/IP network, all the devices in a local network must have unique IP addresses. They also need the addresses of DNS-servers and NBNS-servers 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 router as DHCP server

As a DHCP server, the 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 DHCP server 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 router of ELSA 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 router to a network without other DHCP servers and switch it on. The 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 routers of ELSA 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 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 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 device then disables its own DHCP server if any other DHCP servers are found. This prevents the unconfigured router from assigning addresses not in the local network when switched on.

– The device then enables its own DHCP server if no other DHCP servers are found.

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

The default state is 'auto'.

How are the addresses assigned?

IP address assignment

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

- The IP address 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 DHCP server 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 DHCP server determines the first and last possible IP address in the local network as a start or end address for the address pool.
- If the router has neither an IP address of its own nor an intranet address, the device has gone into a special operating mode. It then uses the IP address '10.0.0.254' for itself and the address pool '10.x.x.x' for the assignment of IP addresses in the network. In this state, the DHCP server only assigns IP addresses and their validity to the computers in the network, but not the other information.

If only one computer in the network is started up that is requesting an IP address via DHCP with its network settings, a 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 previous stage, it requests this same address and the DHCP server attempts to reassign it this address if it has not already been assigned to another computer.

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

Network mask assignment

The network mask is assigned in the same way as the address. If a network mask is entered in the DHCP module, this mask is used for the assignment. Otherwise, the network mask from the TCP/IP module is used (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 router passes its own IP address as a DNS address. This address is determined as described under 'IP address assignment'. The router then uses DNS-forwarding (also see 'DNS-forwarding'), to resolve DNS or NBNS requests from the host.

Default gateway assignment

The 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 DHCP server assigns a host.

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

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

- Default lease time in minutes

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

Priority for the DHCP server—Request assignment

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

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

Under the 'WINS configuration' tab, the 'Enable 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 DHCP server 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 'Setup/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 DHCP server verifies the uniqueness

of the address that is to be assigned to the computer.

- unknown

  While verifying uniqueness, it was determined that the address has already been assigned to another computer. Unfortunately, the DHCP server has no means of obtaining additional information on this computer.

- status

  A computer has informed the DHCP server that it has a fixed IP address. This address can no longer be used.

- dynamic

  The DHCP server assigned an address to the computer.

Configuring the router as a DHCP server

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

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

Configuration using *ELSA LANconfig* and the wizards

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

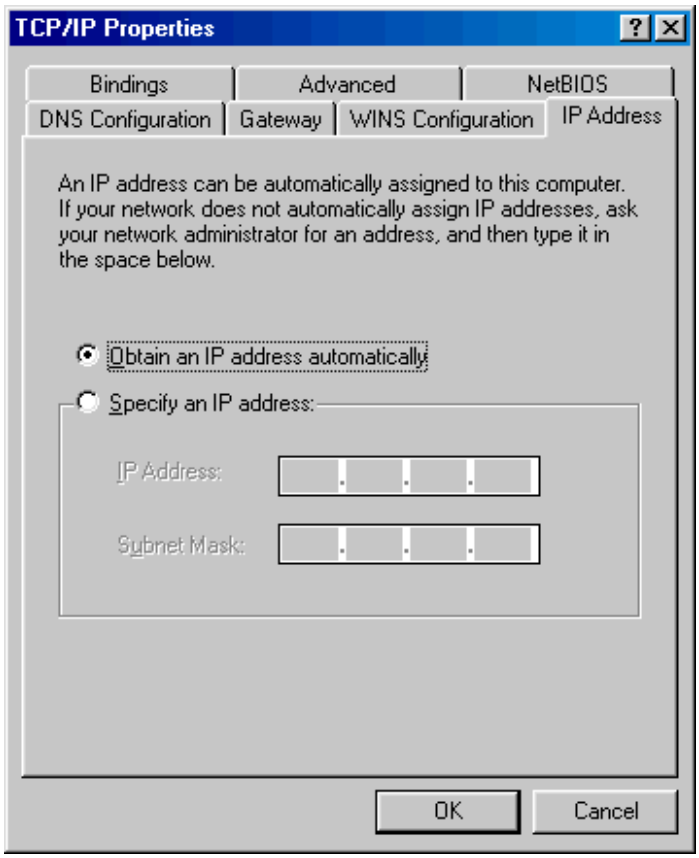
① Connect the unconfigured router to your local network using a network cable. If you are connecting the device to a hub, the node/hub switch must be set to 'Node'. If you are connecting the router directly to the network adapter of a computer in your network, set the switch to the 'Hub' position.

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

③ If you have not done so already, install the TCP/IP protocol on all computers in the LAN.

  – Usually when the protocol is installed, the default configuration is such that the computers are automatically ready to obtain the IP address from a DHCP server. After rebooting at the end of the protocol installation, the computers automatically request an IP address from the DHCP server.
  – If the protocol is already installed, enable the DHCP function on all of the computers in the local network. Under Windows 95, for example, this is done by selecting **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network** to open the window

for configuring network properties. Double-click the entry for the 'TCP/IP' protocol.
Enable the 'Obtain an IP address automatically' option. Switch over to the 'DNS Configuration' tab and delete all of the existing DNS addresses. Next, delete any entries under the 'Gateway' tab and click **OK** to close all the windows. This change will require a reboot, after which the computer will automatically request an IP address from the router's address pool.



You will learn how to install a network protocol under, for example, Windows 95 or Windows NT in the Workshop chapter. 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 'ELSAlan' program group. When loading, the *ELSA LANconfig*, will detect an unconfigured router in the network and will launch the wizard for the basic settings.

– If you have not previously used any IP addresses in your network, select the option 'Make all settings automatically' in this wizard and confirm your selection with **Finish** in the next window.
The wizard assigns the IP address '10.0.0.1' with the netmask '255.255.255.0' to the router and enables the DHCP server. On the basis of this IP address, the device then determines the valid address pool for the DHCP assignment.

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

Manual configuration

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

DNS server

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

What does a DNS server do?

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

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

- An *ELSA LANCOM Business* can automatically distribute IP addresses for the computers in the local network when in DHCP server mode. In other words, the DHCP server already knows the names and IP addresses of all of the computers in its own network that were assigned IP addresses via DHCP. With the dynamic address assignments of a DHCP server, an external DNS server might have

difficulties in keeping the associations between the names and IP addresses current.

- When routing Microsoft Networks via NetBIOS, the *ELSA LANCOM Business* also knows the computer names and IP addresses in the other connected NetBIOS networks. In addition, computers with fixed IP addresses can also enter themselves in the NetBIOS table and thus be known by their names and addresses.
- The DNS server in the *ELSA LANCOM Business* can also be used as an extremely convenient filter mechanism. Requests for domains can be prohibited throughout the LAN, for subnetworks, or even for individual computers—simply by specifying the domain name.

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

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

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

Setting up the DNS server

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

① Switch the DNS server on.

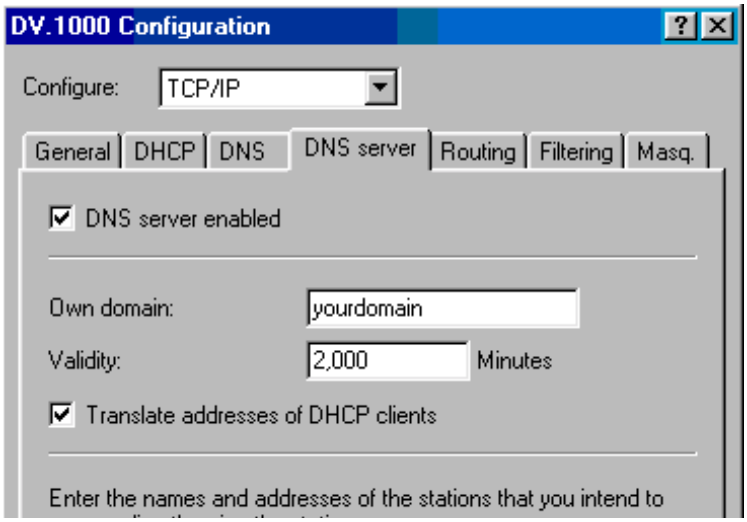
```
set setup/DNS-module/operating on
```

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

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

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

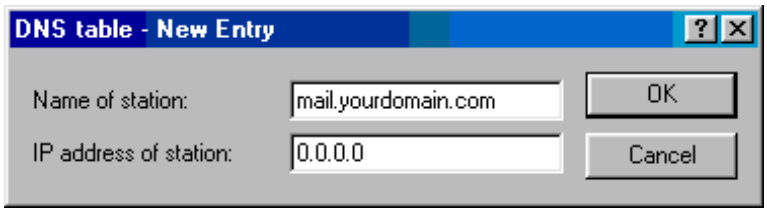
```
set setup/DNS-module/dhcp-usage yes
set setup/DNS-module/NetBIOS-usage  yes
```



④ The main task of the DNS server is to distinguish requests for names in the Internet from those for other remote stations. Therefore, enter all computers into the DNS table

- for which you know the name and IP address,
- that are not located in your own LAN,
- that are not on the Internet and
- that are accessible via the router.

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

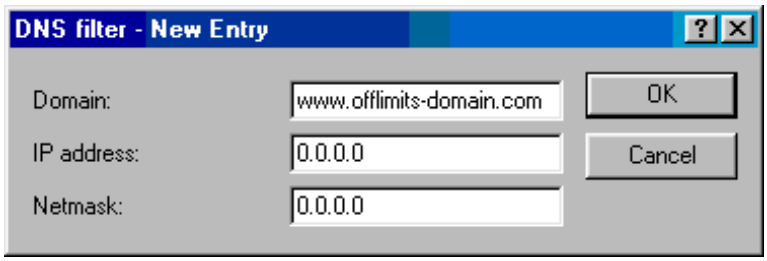



```
cd setup/DNS-module/DNS-table
set mail.yourdomain.com 10.0.0.99
```

Stating the domain is optional but recommended.

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

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




```
cd setup/DNS-module/Filter-list
set 001 www.offlimits-domain.com 0.0.0.0 0.0.0.0
```

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

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

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

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

NetBIOS proxy

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

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

To the point: What is NetBIOS?

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

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

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

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

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

Handling of NetBIOS packets

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

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

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

exchange of information, no new connections are established as a result of queries to workstations in the local network, or to known workstations in the remote network.

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

Which preconditions must be fulfilled?

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

Installed components

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

- Network protocol

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

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

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

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

- Client

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

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

- Capab.

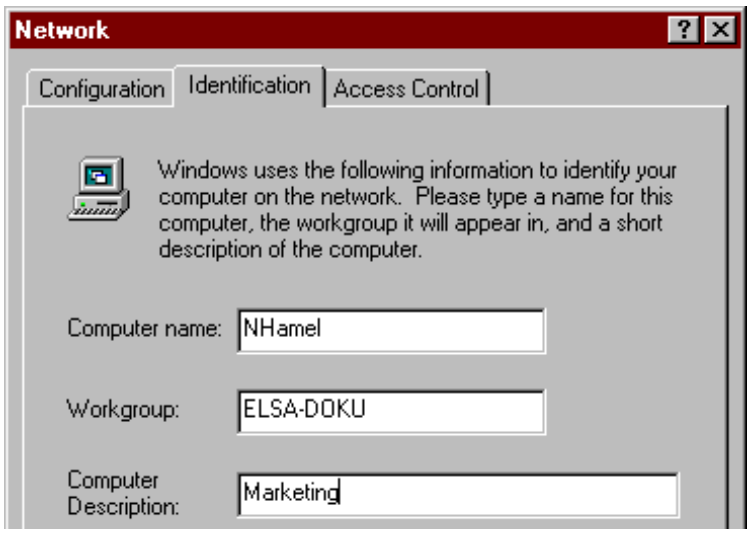
File and printer sharing permits drives and printers to be shared with other users in the Microsoft Network.

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

Microsoft Network settings

- Name and group designation

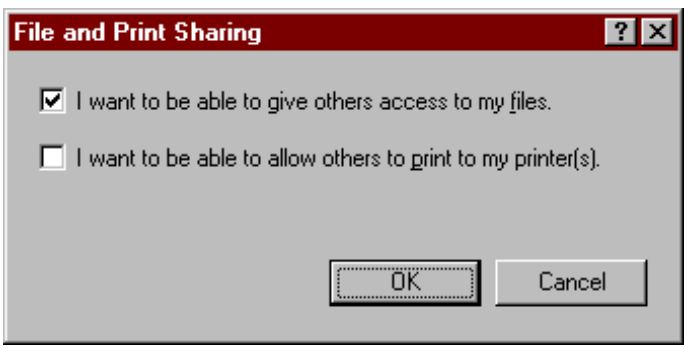
  Click **Start** ▶ **Settings** ▶ **Control Panel** ▶ **Network** and switch to the **Identification** tab.



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

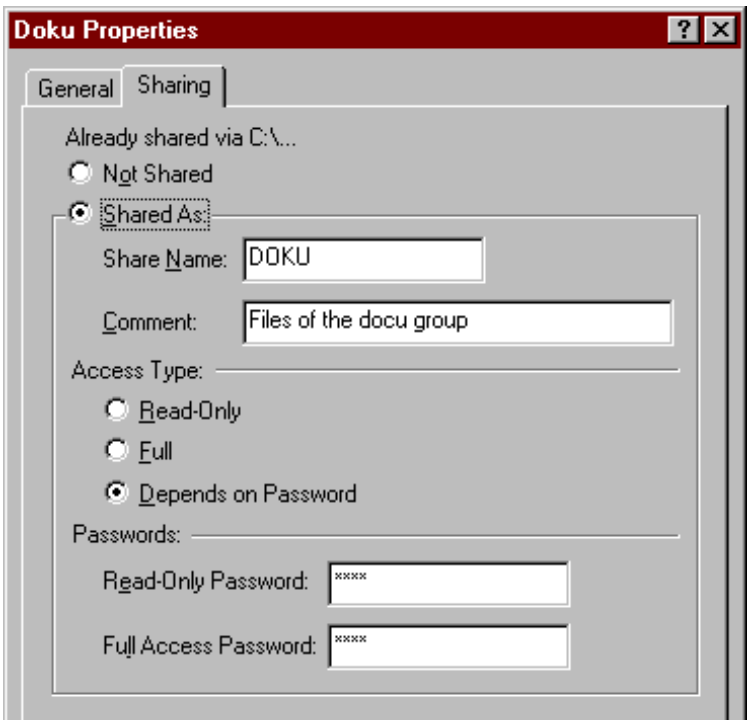
- File and printer sharing

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



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

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



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

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

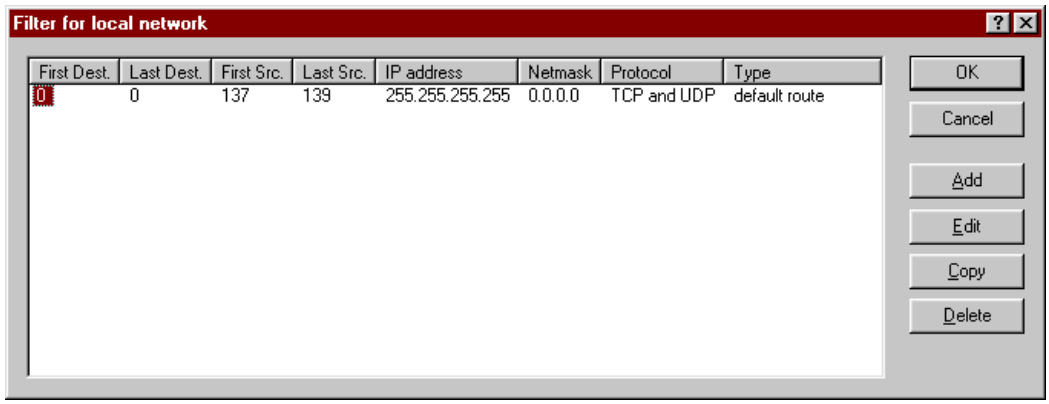
Linking two Microsoft Networks via ISDN

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

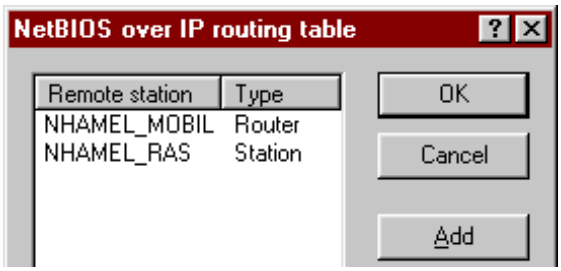
① Set up both networks for a LAN-LAN interconnection via TCP/IP as described in the Workshop. We recommend using the convenient *ELSA LANconfig* wizard.

② Check the settings of the IP filter. This filter must capture all NetBIOS packets to be sent over the DEFAULT route to ensure that they do not lead the establishment of a

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



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



Alternatively, enter the following when configuring via telnet:

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

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

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

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

⑤ Once all remote stations have been entered, activate the NetBIOS function.

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

After switching the module on, a connection is established after an unspecified waiting time to all remote stations not identified as dial-up nodes. The required

information regarding the other computers in the networks is then exchanged during this initial connection. Computers on the remote side cannot be accessed until this operation is complete.

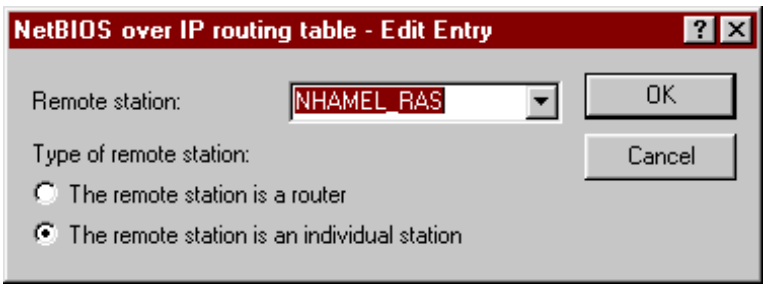
Dial-up procedure for a remote access station

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

① The *ELSA LANCOM Business* and the remote access computer must be prepared for network access as described in the Workshop. In this case as well, check the IP filters in the *ELSA LANCOM Business* (See 'Connecting two Windows networks via ISDN').

② A route must also be entered in the IP routing table if the assignment of the IP address for the remote station is realized from the IP pool.

③ Also create an entry for the remote stations in the NetBIOS IP routing table.




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

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

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

Search and Find: the Network Neighborhood

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

NetBIOS routing via LAN-LAN interconnections

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

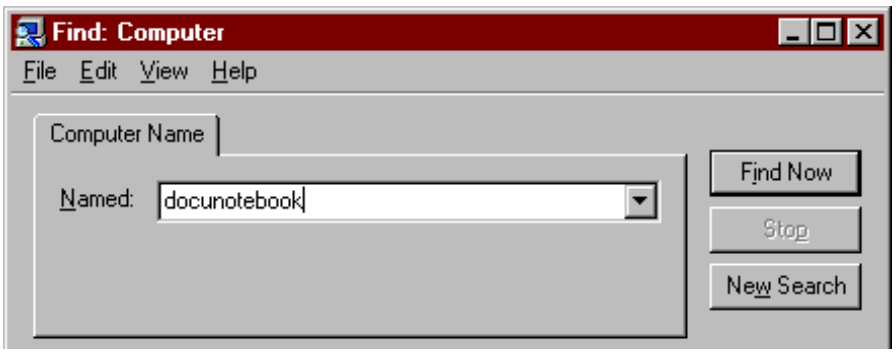
```
dir /Setup/NetBIOS-module/Host-list
```

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

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

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

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



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

NetBIOS routing via RAS

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

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

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

IP pooling for dial-up access

With a greater number of available B channels, *ELSA LANCOM Business* is an ideal remote-access server for small and mid-size businesses. The router has a pool of IP addresses from which an IP address is assigned to the LAN for the duration of the connection so that a separate route does not have to be set for every dial-up access.

The settings for the IP address pool in *ELSA LANconfig* in the 'TCP-IP' configuration section on the 'Addresses' tab or under `/Setup/IP-router-module` for telnet or terminal connections.

Office communications and *LANCAPI*

LANCAPI from ELSA is a special version of the popular CAPI interface. CAPI (Common ISDN Application Programming Interface) establishes the connection between ISDN adapters and communications programs. For their part, these programs provide the computers with office communications functions such as a fax machine or 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 a *ELSA LANCOM Business*, 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 *ELSA LANCOM Business* is simply installed in the network. All devices present in the local network then share the pending tasks.

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

Installing the *LANCAPI* client

The *LANCAPI* is made up of two components, a server (in the *ELSA LANCOM Business*) 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

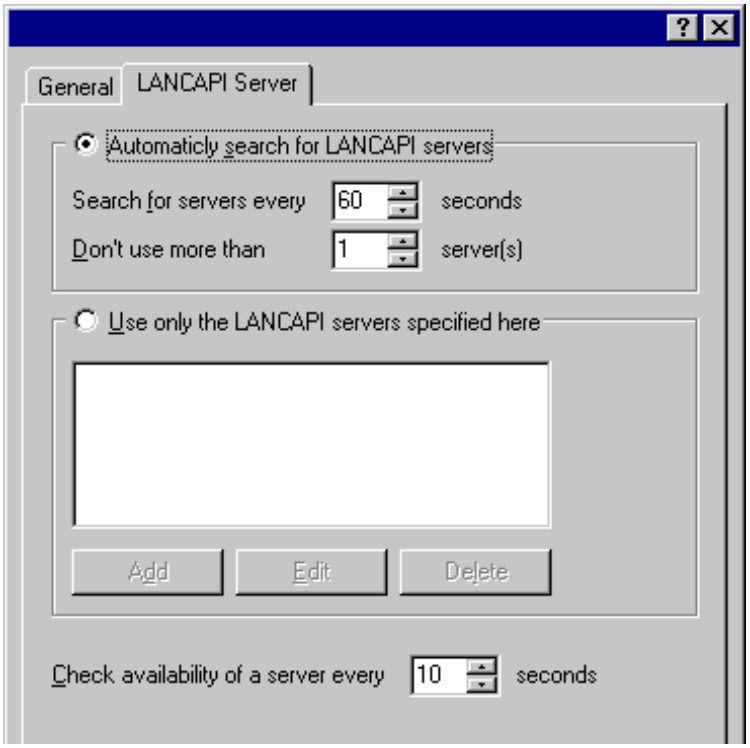
The configuration of the *LANCAPI* client is used to determine which *LANCAPI* servers will be used and how these will be checked. All parameters can remain at their default settings if you are using only one *ELSA LANCOM Business* in your LAN as a *LANCAPI* server.

① Start the *LANCAPI* client in the 'ELSAlan' program group. Information regarding the drivers for the available service can be found on the 'General' tab.

② Switch to the 'LANCAPI Server' tab. First, select whether the PC should find its own *LANCAPI* server, or specify the use of a particular server.

- For the former, determine the interval at which the client should search for a server. It will continue searching until it has found the number of servers specified in the next field. Once the required number of servers has been found, it will stop searching.
- In the event that the client should not automatically search for servers, list the IP addresses of the servers to be used by the client. This can be useful if you are operating several *ELSA LANCOM Business* in your LAN as *LANCAPI* servers and you would like to specify a server for a group of PCs, for example.

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



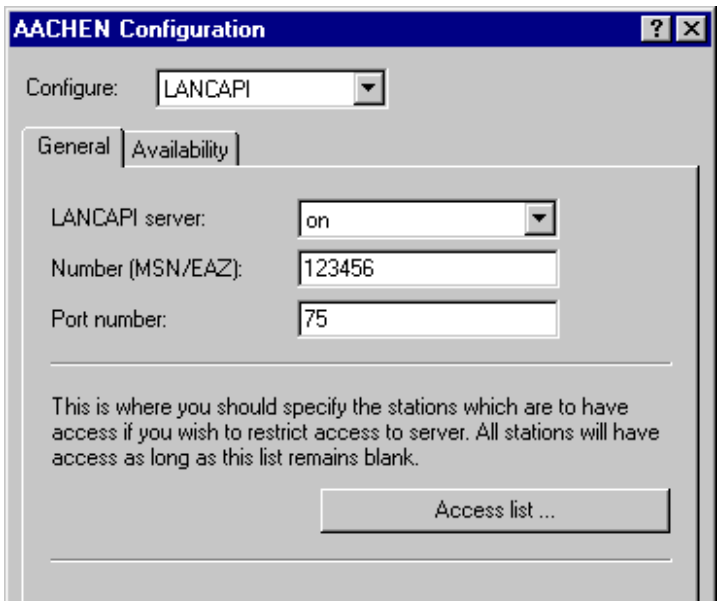
Configuring the *LANCAPI* server

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

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

Set the relevant parameters as follows:

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



② Activate the *LANCAPI* server, or set it to permit outgoing calls only. In the latter case, the *LANCAPI* will not respond to incoming calls—to receive faxes, for example. Permitting outgoing calls only is useful if you do not have a specific call number available for the *LANCAPI*.

③ When the *LANCAPI* server is activated, enter the call numbers to which the *LANCAPI* should respond in the 'Number' field. You can enter several call numbers separated by semicolons. If you do not enter a call number here, all incoming calls are reported to *LANCAPI*.

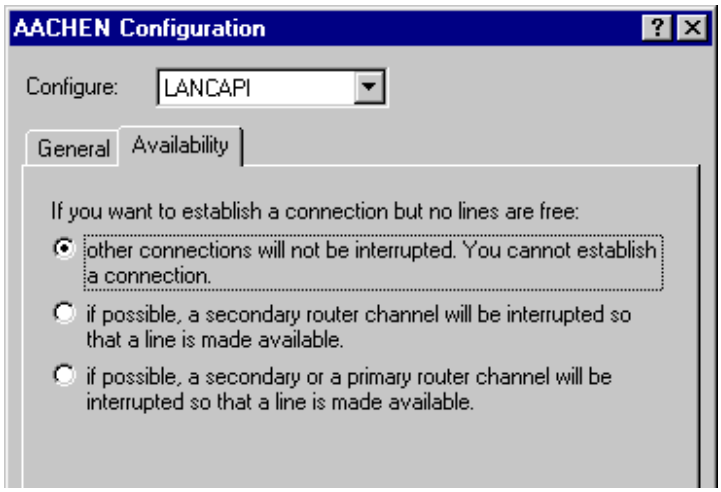
④ *LANCAPI* is preset to use port '75' (any private telephony service). Do not change this setting unless this port is already in use by a different service in your LAN.

⑤ If you do not wish all the computers in the local network to be able to access the *LANCAPI* functions, you can define all the authorized users (by means of their IP addresses) by entering them in the access list.

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

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

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



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

Using the *LANCAPI*

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

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

ELSA CAPI Faxmodem

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

Installation

The *ELSA CAPI Faxmodem* can be installed from the CD setup. Always install the *ELSA CAPI Faxmodem* together with the current version of *ELSA LANCAPI*. After restarting, the *ELSA CAPI Faxmodem* will be available to your system. Under Windows 95 or Windows 98, it can be found under **Start settings** ▶ **Control Panel** ▶ **Modems**.

Faxing with the *ELSA CAPI Faxmodem*

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

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

The least-cost router

The liberalization of telecommunications markets in European 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 dial-around basis without a contract with a specific provider. The prefix of the provider must be dialed to access the desired network on a call-by-call basis. The normal telephone number is dialed after the network identification prefix.

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

Function of the *ELSA LANCOM* least-cost router

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

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

the network identification prefix for the connection will be prepended to the prefix. The number is not sent out to the exchange until it has been completed in this manner.

The LCR also requires the following information:

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

Initial tests

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

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

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

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

For advanced users: Systematic use of the LCR

- The first example has shown how connect charges can be reduced with only a few entries. If you would like to put the least-cost router to optimal use, detailed information is required with regard to the connect-charge structure of the dial-around providers. Next, decide how these rates and rate zones can be best organized in the *ELSA LANCOM Business* LCR table. A variety of approaches are possible:
- Obvious options for saving telephone charges can be entered directly:
  - '00' for international connections

- Entering a single '0' will initially reroute all numbers starting with a zero. However, as neighboring local exchanges may also start with a '0' and yet be billed as local calls, their prefixes should be listed separately to prevent these calls from being rerouted. This strategy should also be applied to special prefixes such as '0800' etc.
- Another strategy aims to achieve the highest possible level of control over the routing activities. Start with the prefixes of the local area and then define the next larger zones. The closer, and thus less expensive, tariff zones are set with longer prefixes, the remaining more distant prefixes with a smaller number of digits.

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

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

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

Setting up the least-cost router

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

- Which operating modes of the *ELSA LANCOM Business* 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

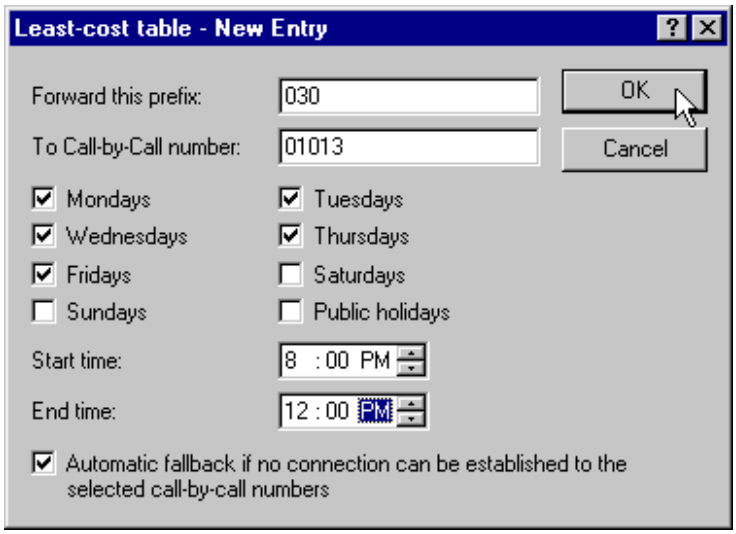
from the ISDN network itself (see also 'Time for the Selection' further below). Activate the following operating modes for the least-cost router as required:

– The router
– The *LANCAPI*

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

③ Change over to the 'Time periods and public holidays' tab. Open the **Least-cost table**, create a new entry and enter the following data:

– Which prefix should be rerouted?
– Which provider should be used for this prefix? If you have entered several network prefixes separated by semicolons, the LCR will automatically try the next prefix if the current one is busy.
– On which days and what times should the routing be active? Please note that time blocks cannot extend from one date to another (i.e. 6:00 p.m. to 6:00 a.m.).
– Should the call be handled by the default telephone provider if all dial-around providers are busy? If 'Fallback' is disabled, the LCR will start at the beginning after unsuccessfully trying the last network prefix.



④ If you have also made entries in the LCR table for holidays, open the **Public holidays** list. Enter each holiday with its full date (DD.MM.YYYY).

⑤ Check the internal clock of the unit (incl. the date), to ensure that the LCR activates the routing at the correct time (see also 'Time for the Selection' further below).

Build the LCR table one step at a time and check your results. Open the ELSA LANmonitor, for example, and establish connections to the remote stations to be

*rerouted according to the table using the ELSA LANCAPI. Use the dialed number to verify whether the LCR settings suit your requirements. For router connections, check the log file for the number dialed (LANmonitor: **View** ▶ **Options** ▶ **Protocol** ▶ **Display**).*

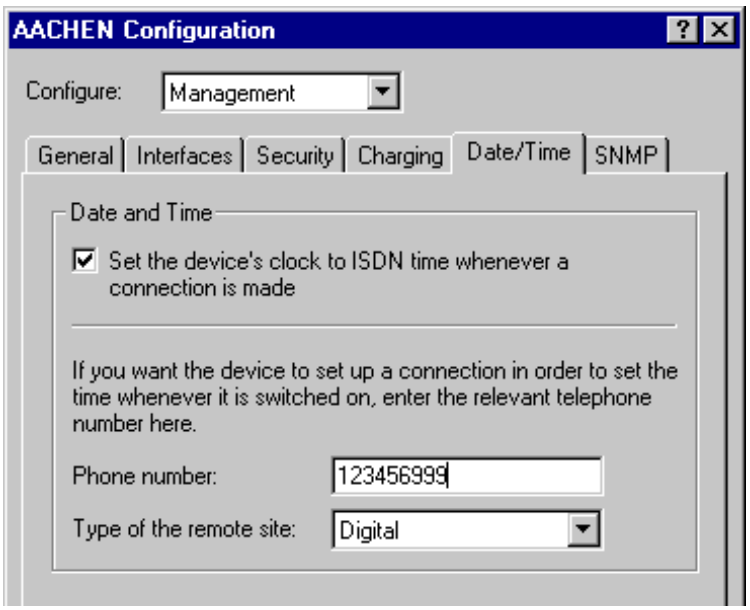
Time for the selection

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

① In *ELSA LANconfig*, switch to the 'Date/Time' tab in the 'Management' configuration section.

② Activate the option for automatic synchronization at each call establishment. If you would rather enter the time manually, disable this option.

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



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

Workshop

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

All the configurations assume the device has the factory settings. You should therefore reset your 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 software and to make the use of *ELSA 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 *ELSA LANconfig* and its wizards to set up configurations in Windows operating systems 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 *ELSA LANconfig* or via a terminal or telnet connection.

	Setup/WAN-module	
	Interface	S0 DSS1 0 123456 123456

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

```
cd setup/WAN-module/Interface-list
```

```
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 device are you using?

You can work through the tasks in Workshop described using a number of models from the *ELSA LANCOM* family. Any restrictions with regard to specific models are indicated by the corresponding symbols shown next to the text.

All descriptions apply to routers with a single S_0 interface, i.e. with 2 B channels. For units with several S_0 interfaces (such as *ELSA LANCOM Business 4100*), the settings may need to be transferred to the other interfaces and channels.

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 device.

Internet applications

This first section on the practical uses of the devices will introduce you to applications involving the Internet.

The first example shows a company seeking to use a 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 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

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

The router is the only machine on the LAN to have a valid IP address on the Internet. 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 router.

This process has even more benefits:

- IP masquerading makes Internet access simple.

  Only one device needs to be configured. 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 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 router manages the ISDN line automatically and only establishes a link to the service provider when there is actually a need to transfer data.

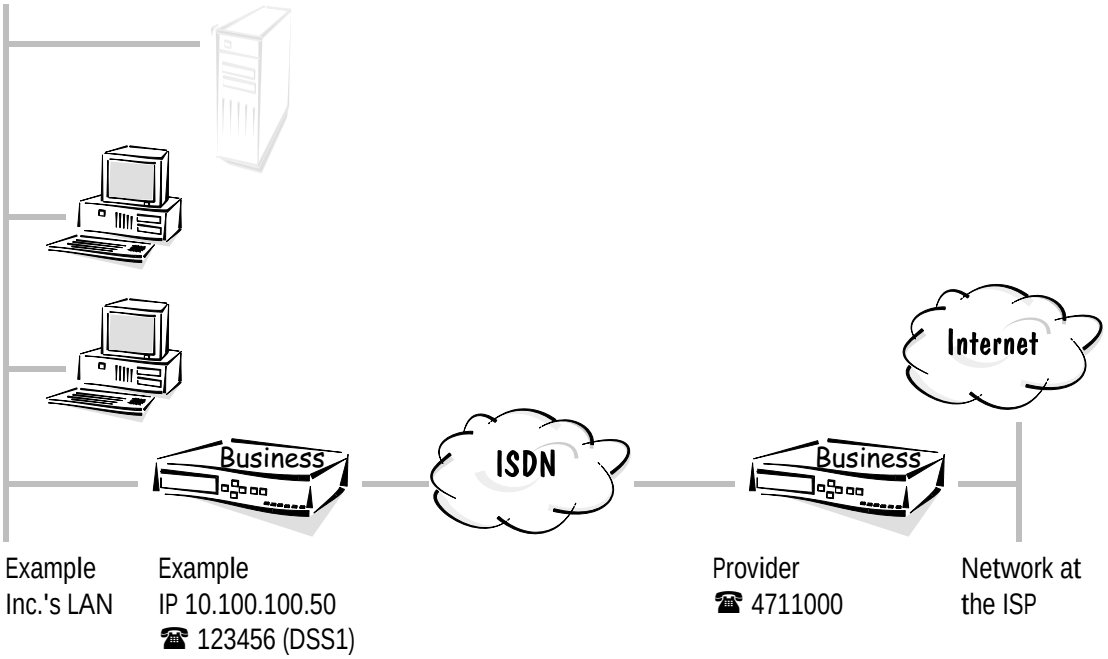
- IP masquerading makes Internet access secure.

  The computers in the local area network become invisible from outside. Only the IP address of the 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 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 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-up node needs to be addressed with PPP and requires 'CHAP security'. The required access data is the user name 'WEB_USER' and the password 'surfing'.



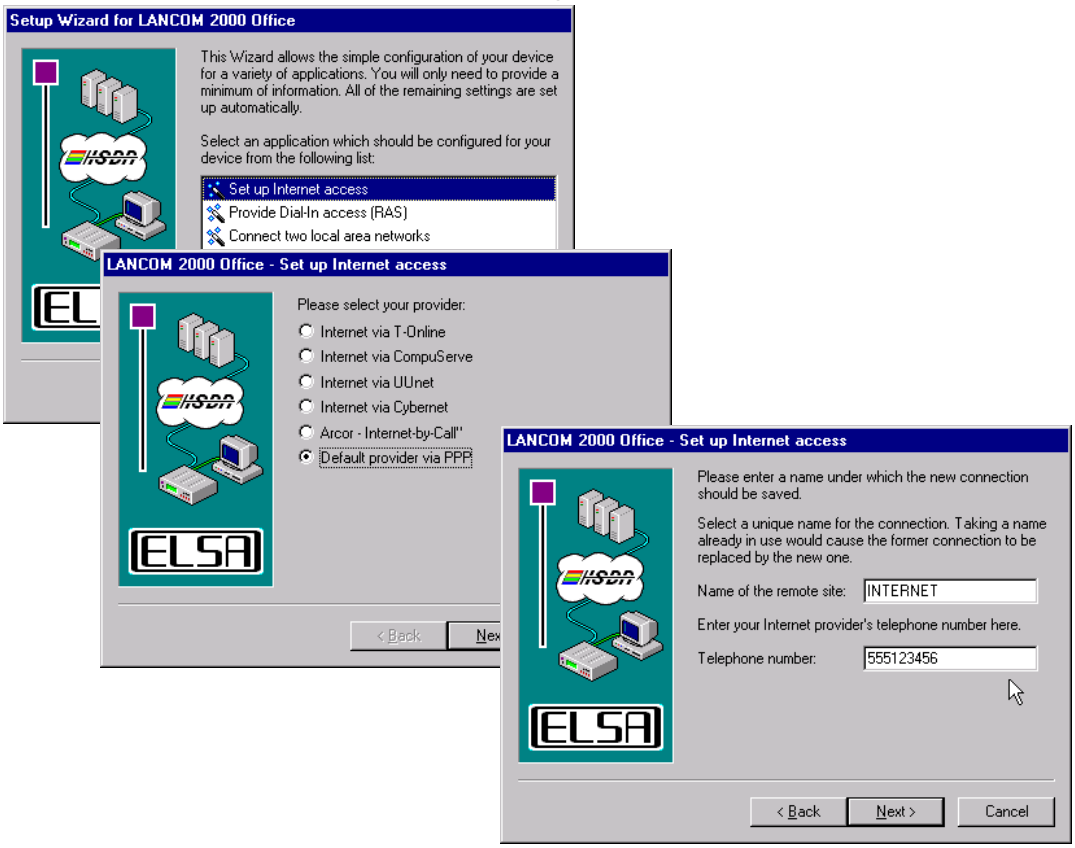
The table below shows how all the important data are assigned as used in the example. We recommend that you create a table such as this for each application. It will assist you in your work of configuring, troubleshooting and when requesting support information.

	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 router	10.100.100.50	
IP netmask	255.255.255.0	
Device-name	Example Inc.	Service provider
Dialup-remote	123456	4711000

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

Various wizards have been put together in the *ELSA LANconfig* which make all the settings in the *ELSA LANCOM* software required to configure the *ELSA LANCOM* 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: which settings do you configure on the 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:

```
cd /Setup/WAN-module/Router-interface-list
S0-1 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.

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 router in the central office to call the routers at the ISP:

```
cd Setup/WAN-module/Name-list
```

```
set Provider 4711000 * * PPPHDLC 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.

```
cd Setup/WAN-module/PPP-list/Default
set Provider no surfing * *  WEB_USER IP
```

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. To enable the router 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 netmask (configuration area 'TCP/IP', 'General' tab).

```
cd Setup/TCP-IP-module
set Intranet IP address 10.100.100.50
set Intranet netmask 255.255.255.0
set operating on
```

The entries for the IP address and the IP netmask are empty because in this example the 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 netmask (see also 'Intranet with its own Web server on the Internet').

⑤ The settings thus far have practically integrated the 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).

```
cd Setup/IP-router-module
set 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 netmask '0.0.0.0' intercepts all packets which cannot be assigned locally. 'Router' identifies the remote station to which the relevant data is to be sent. The remote station can be accessed directly from your 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 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 router is ready for the WWW.

```
cd Setup/IP-router-module
set operating on
```

⑦ What's left to do? Obviously the computers in the LAN will also need to know that the *ELSA LANCOM* is the gateway to the Internet. This will require the router's Intranet address being specified as the default gateway and DNS server for the workstation computers.

These settings can be assigned automatically when using the router as a DHCP server (see 'DHCP Server').

The result

When an employee starts up a browser on a workstation computer and enters a Web address (ELSA, for instance), then the DNS server specified in the operating system (in this case the router) will try to determine the associated IP address. The 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 router. The 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

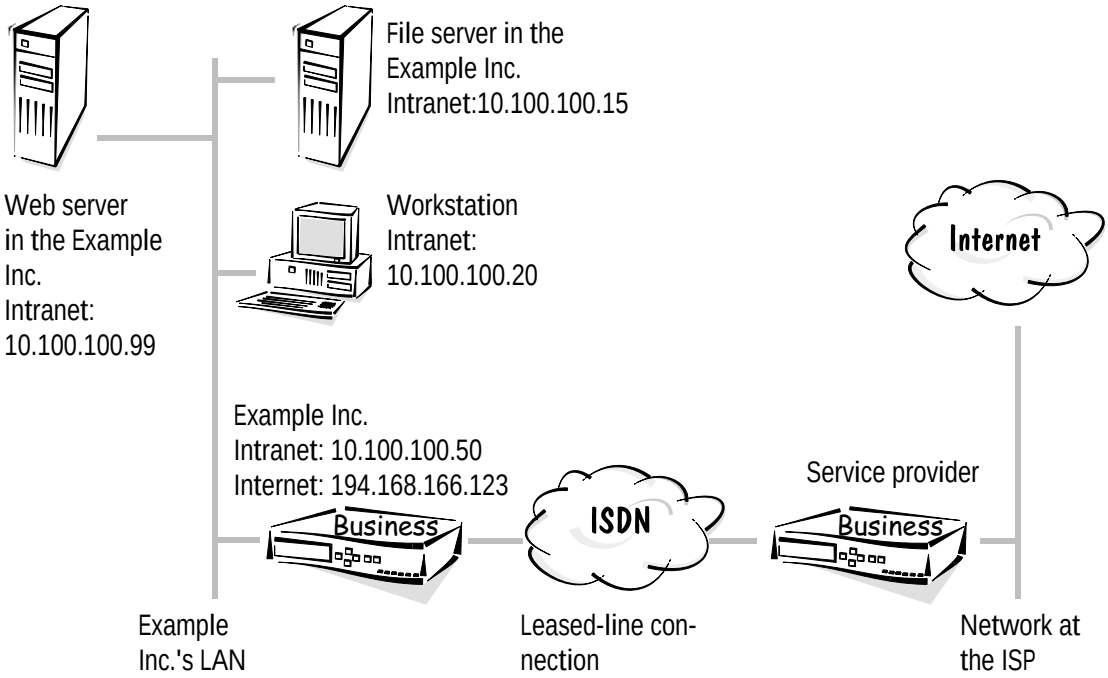
The motivation

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 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 router. The 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 network in the Example Inc. company which has several workstation computers and a 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 router at your ISP and configure both devices for the leased-line connection used.
- A single router in your local area network will be sufficient if a leased-line connection is not required. Set your 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).

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 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 router	194.168.166.123	
Netmask for the router	255.255.255.255	
Intranet address of the LAN	10.100.100.0	
Intranet address for the router	10.100.100.50	
Intranet address for the Web server	10.100.100.99	
Intranet-mask	255.255.255.0	
Device-name	Example Inc.	Service provider

Leased-line connection: which settings do you configure on the router?

The settings for the two devices are very similar. We will use the settings for the router at the Example Inc. as our basis and indicate any differences for the router at the service provider.

① First set the router in the interface table for a leased-line connection using D64S (configuration area 'Management', 'Interfaces' tab):

```
cd Setup/WAN-module/Interface-list
set S0-1 GRP0 1
```

The the B channel used in the router must be the same, i.e. this must also be a '1'.

② These settings alone allow the two 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.

To ensure that the leased-line connection uses another layer, create a new layer in the layer list and set it up according to your requirements in the layer lists of both units ('Communication' configuration section, 'General' tab), e.g. with the PPP protocol and compression.

```
cd Setup/WAN-module/Layer-list
set FVG0 TRANS PPP TRANS compr.  HDLC64K
```

③ A new entry in the name list ('Communication' configuration section, 'Remote sites' tab) with identification of the remote station and the layers to be used enables the router to establish a leased-line connection with the correct settings. It is not necessary to enter a subscriber number.

```
cd Setup/WAN-module/Name-list
set remote connection* 0 0 FVG0 Off
```

The time-outs will be set to '0' since the establishment of unnecessary connections could cause delays.

④ Use the channel list to specify the channels to be used for the fixed connection. The same settings must be used for the channels and their sequence on both sides of the connection. If applicable, the number of channels to be used for a backup connection should be entered here, ensuring that these are the same for both sides of the connection ('Communication' configuration section, 'Remote sites' tab).

```
cd Setup/WAN-module/Channel-list
set remote connection 1 1 1-1 0
```

⑤ Name the device appropriately so that the router can also send and recognize the names from the namelist (configuration area 'Communication', register 'General'):

```
cd Setup
set Name Example Inc.
```

⑥ Now all that is needed is to clarify the IP addresses. The 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. It receives this as part of the entry for the Intranet address together with the associated netmask (configuration area 'TCP/IP', 'General' tab). It will also receive the registered IP address, including the netmask as negotiated. For these entries to become effective, activate the TCP-IP module.

```
cd /Setup/TCP-IP-module
set IP-address 194.168.166.123
set IP-netmask 255.255.255.255
set Intranet address 10.100.100.50
set Intranet netmask 255.255.255.0
set operating on
```

By analogy, the other router is assigned a permanent IP address and (if using IP masquerading) an Intranet address from the address range at the ISP.

⑦ Setting the IP address practically integrates the Example's 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.

```
cd Setup/IP-router-module
set IP-routing-table 255.255.255.255 0.0.0.0 leased-
line connection 2 ON
```

The route to the IP address '255.255.255.255' with the netmask '0.0.0.0' intercepts all packets which cannot be assigned locally. 'Router' identifies the remote station to which the relevant data is to be sent. The remote station can be accessed directly from your 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 router's address so that they will not appear on the Internet.

⑧ The router at the ISP must have the same entry in the routing table. This route contains the registered IP address of the 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.

```
cd /Setup/IP-router-module
set IP-routing-table 194.168.166.123 255.255.255.255
Example 2 Off
```

The 'Proxy-ARP' function must be enabled since this IP address falls within the service provider's own address range:

```
cd /Setup/IP-router-module
set Proxy-ARP ON
```

⑨ The web server is made visible on the Internet by an entry in the service list for the Example Inc.'s device (configuration area 'TCP/IP', 'Masq.' tab):

```
cd /Setup/IP-router-module/Masquerading/Service-table
set 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'.

⑩ Now activate the IP router only (configuration area 'TCP/IP', 'Routing' tab), and the router is ready for the WWW.

```
cd /Setup/IP-router-module
set operating on
```

⑪ What's left to do? Obviously the computers in the LAN will also need to know that the router is the gateway to the Internet. This will require the 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.

These settings can be assigned automatically when using the router as a DHCP server (see 'DHCP 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 (ELSA, for instance), the DNS server specified in the operating system will try to determine the associated IP address. The 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 router. The 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 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 router. The 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. 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 leased lines and dial-up connections.

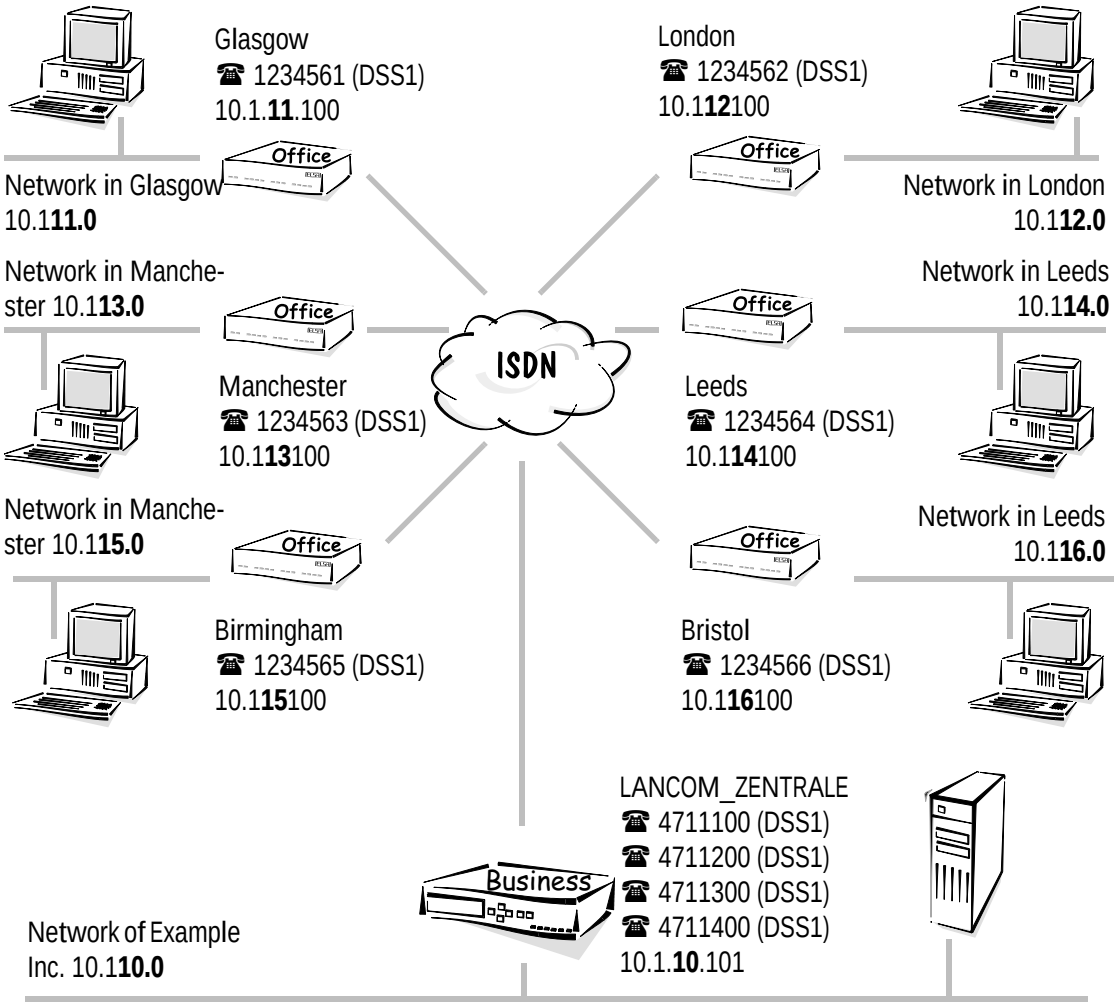
Networks connected with the IP router

The motivation

You 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'), 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 the central office has six branches. A "small" router that connects to the *ELSA LANCOM Business* in the central office via ISDN dial-up connections is located in each of the branch offices.



The following table shows the assignment of device names, addresses and telephone numbers as used in the example:

Network	Example Inc.	Glasgow	London	Manchester	Leeds	Birmingham	Bristol
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 addresses for the routers	10.1.10.101	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 netmask	255.255.255.0						
Device-name	Example_Inc.	Glasgow	London	Manchester	Leeds	Birmingham	Bristol
Call numbers	4711100 4711200 4711300 4711400	1234561	1234562	1234563	1234564	1234565	1234566

IP routing made simple with *ELSA LANconfig* and the wizards

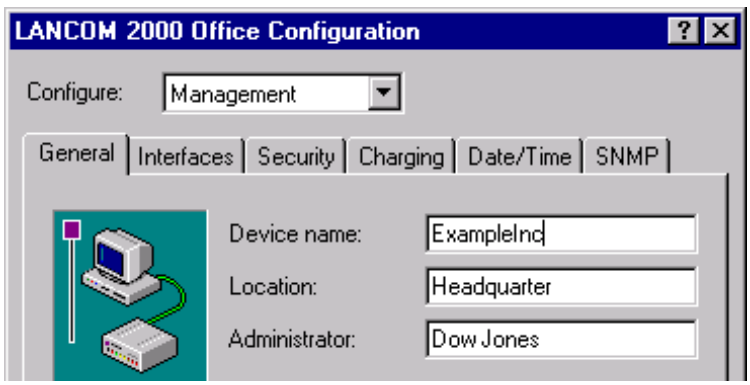
For the configuration on LAN to LAN coupling, there is a wizard in *ELSA LANconfig* which makes all required settings in the software for you and takes the peculiarities of TCP/IP networks into account. Once you have started up the wizard (automatically or by clicking **Tools** ▶ **Setup Wizard**) select 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.

As you would like to interconnect several networks in this example, run the wizard once on the router in the headquarters for each of the networks you would like to connect. The wizard is also used once for each of the branch office routers.

Step by Step: What settings are made in the routers?

In principle, the settings are the same for all routers. In the following configuration steps, beginning with the router in the central office, we show exactly what is set the same and provide information on the deviations in the other devices.

① For the names that are used in the name list to be also forwarded and detected by the routers, name the device appropriately (configuration area 'Management', 'General' tab):

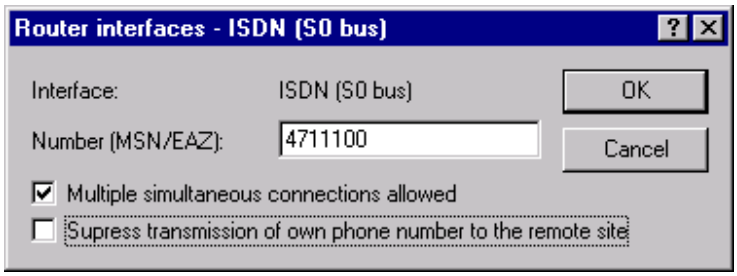


Enter the names of the devices directly in the 'Setup' menu with configurations with other aids:

```
set /Setup/Name Example_Inc.
```

The devices in the branches correspondingly acquire the names 'Glasgow' to 'Bristol'.

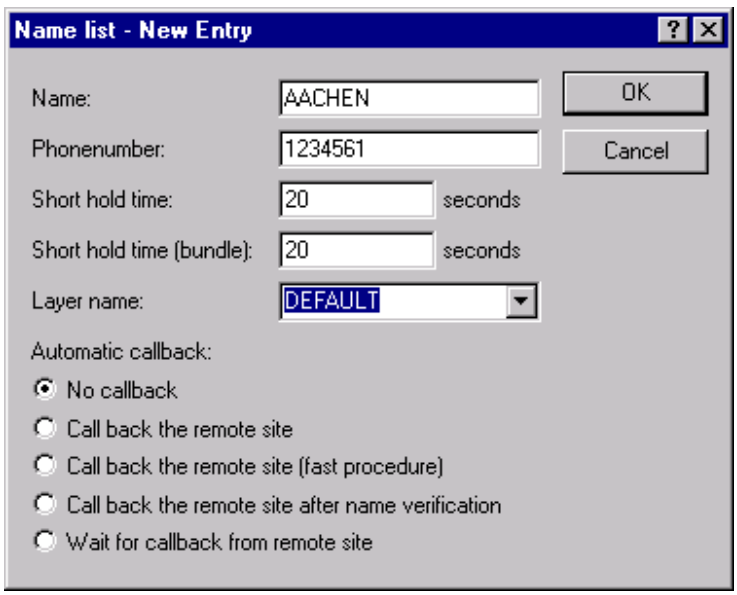
② Then enter the **specific** call numbers of the router in the central office (configuration area 'Communication', 'General' tab):




```
cd /Setup/WAN-module/Router-interface-list
set s0-1 4711100 On No
```

The other interfaces and devices correspondingly receive their own call numbers.

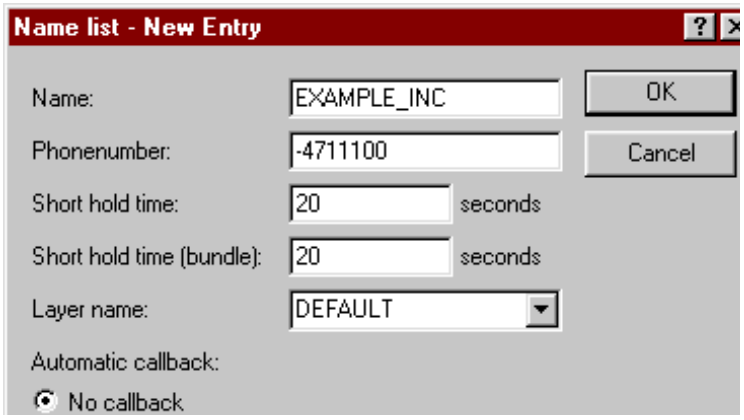
③ New entries in the name list (configuration area 'Communication', 'Remote Sites' tab) with identification of the remote stations and the call numbers with selection of a layer available on all routers (here for example the preset DEFAULT layer) enable the router in the central office to call the routers in the other networks. With the standard values for the B1 and B2 hold times, the 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:




```
cd /Setup/WAN-module/Name-list
```

```
set GLASGOW 1234561 * * DEFAULT OFF
```

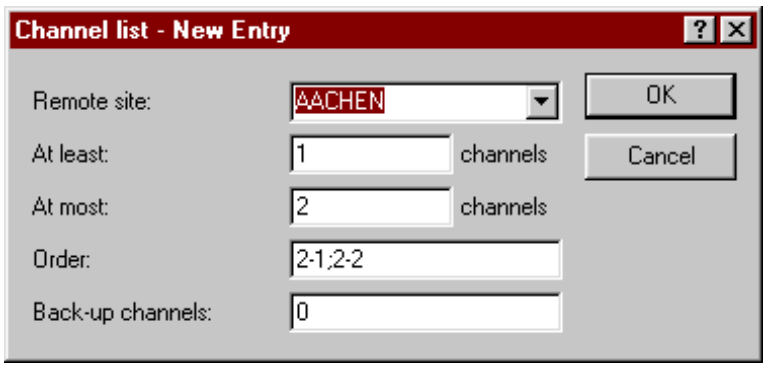
The other devices only enter the router 'Example_Inc.' and the subscriber numbers of the corresponding interfaces. The hyphen before the call number signals that there are still other call numbers for this network in the RoundRobin list.



④ The Round-robin list is given below. The call numbers of the other router interfaces in the central office, which have not previously been entered in the name list, are entered here in the routers of the branches.


```
cd /Setup/WAN-module/RoundRobin-list
set Example_Inc. 4711200 last
```

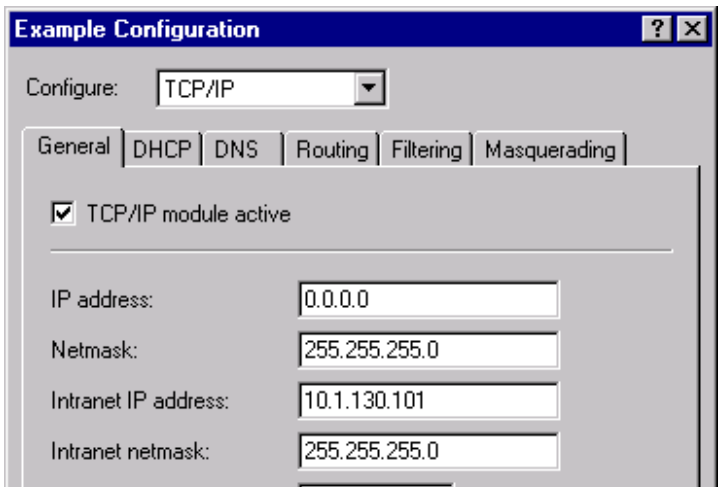
⑤ If the connections to the branch networks should use specific B channels, to keep other channels free for RAS access, for example, create an entry for each remote station defining the permissible channels in the channel list of the central router.




```
cd /Setup/WAN-module/Channel-list
```

```
set GLASGOW 1 2 2-1;2-2 0
```

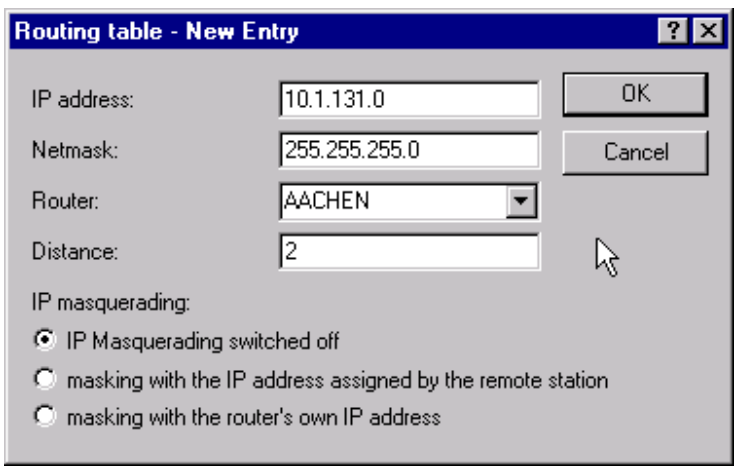
⑥ You must still clarify the addresses. So that the devices in the internal TCP/IP networks are found, one free IP address at least from the Intranet is required. They receive them with the entry of the Intranet address with the associated netmask (configuration area 'TCP/IP', register 'General'). For these entries to become effective, activate the TCP-IP module.




```
cd /Setup/TCP-IP-module/RoundRobin-list
set Intranet address 10.1.130.101
set Intranet netmask 255.255.255.0
```

The routers in the branch offices receive the IP addresses 10.131.1.100 to 10.136.1.100, all with the netmask 255.255.255.0, as illustrated and covered in the overview.

⑦ And what IP addresses should the routers route where? In the routing table of the router in the central office enter the IP addresses and netmasks of all branches with the remote station (without IP masquerading!):



Finally activate the IP router only, and the first *ELSA LANCOM* is ready for connection to the other networks.

```
cd /Setup/IP-router-module/IP-routing-table
set 10.1.131.0 255.255.255.0 Glasgow 2 off
cd /Setup/IP-router-module
set operating on
```

The routers in the branch offices each receive one entry for the central office. All connections among the branch offices are thus routed via 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 router in the central office. In addition, the same entries are contained in the routing table as in the device in the central office, where the routing entry for the internal network is replaced by the entry for the central office network.

⑧ What's left to do? Naturally, the computers in the LAN also need to know that the router is the switching center for the other networks. For this purpose the Intranet address of the router is entered as default gateway for the workstations and servers.

These settings can be assigned automatically when using the router as a DHCP server (see 'DHCP Server').

The result

With the access from a computer in a branch to the central office network, it is now possible to deviate to another inferface via the entry in the RoundRobin list, if the first one dialed is busy.

Networks connected with the IPX router

The motivation

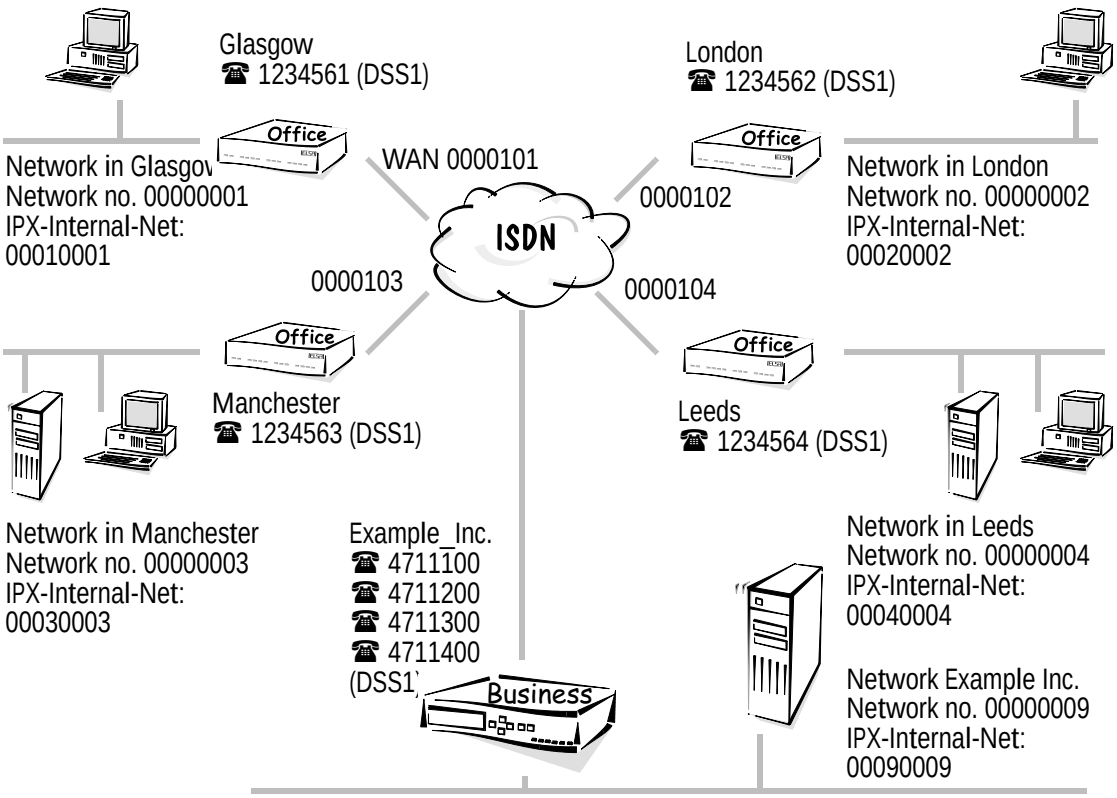
You can connect networks that use IPX/SPX as network protocol using the IPX router. For example, you can connect the network of the central office to those of several branch offices.

An example of the task

In this example the central office has four branches. A ”small“ router that connects to the *ELSA LANCOM Business* in the central office via ISDN dial-up connections is located in each of the branch offices.

The following table shows the assignment of device names, addresses and telephone numbers as used in the example:

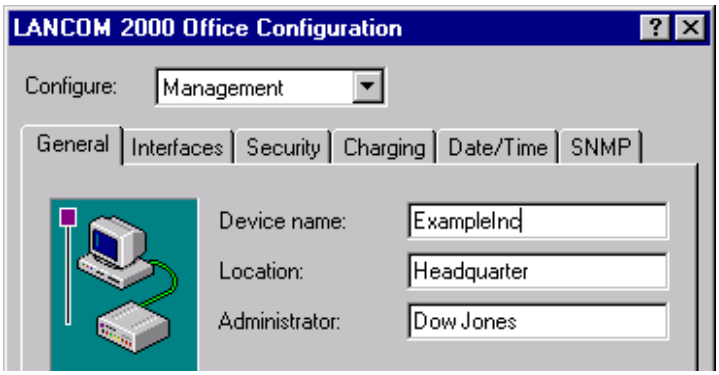
Network	LAN Example	LAN Glasgow	LAN London	LAN Manchester	LAN Leeds
Network address	00000009	00000001	00000002	00000003	00000004
IPX internal net	00090009	00010001	00020002	00030003	00040004
Binding	802.3	SNAP	SNAP	802.3	802.3
Device-name	Example_Inc.	Glasgow	London	Manchester	Leeds
Dialup-remote	4711100 4711200 4711300 4711400	1234561	1234562	1234563	1234564
WAN networks		00000101	00000102	00000103	00000104



Step by step: What settings are made in the routers?

In the following configuration steps, beginning with the router in the central office, we show exactly the settings and provide information on the deviations in the other devices.

① For the names that are used in the name list to be also forwarded and detected by the routers, name the device appropriately (configuration area 'Management', 'General' tab):

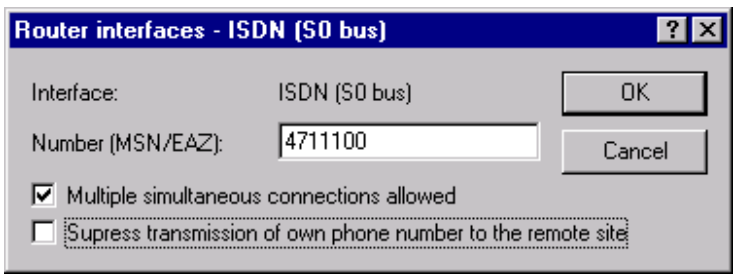


Enter the names of the devices directly in the 'Setup' menu with configurations with other aids:

```
cd Setup
set Name Example_Inc.
```

The routers in the branches receive the names 'Glasgow', 'London', 'Manchester' and 'Leeds'.

② Then enter the **specific** call number of the router in the central office (configuration area 'Communication', 'General' tab):

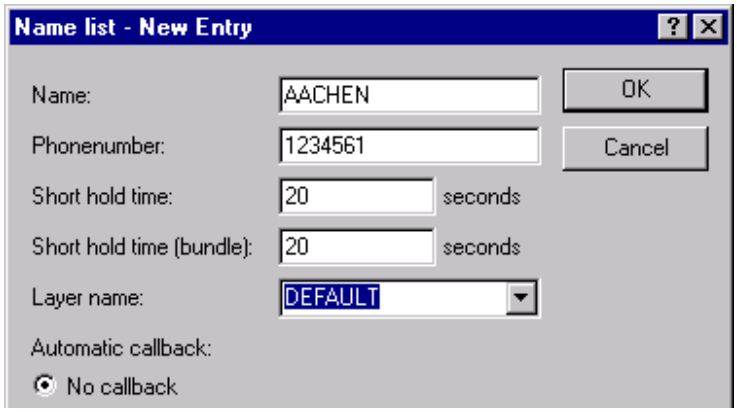



```
cd /Setup/WAN-module/Router-interface-list
S0-1 4711100
S0-2 4711200
S0-3 4711300
S0-4 4711400
```

The other devices correspondingly receive their own call numbers (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 router 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:




```
cd Setup/WAN-module/Name-list
set Glasgow 1234561 * * DEFAULT OFF
set London 1234562 * * DEFAULT OFF
set Manchester 1234563 * * DEFAULT OFF
set Leeds 1234564 * * DEFAULT OFF
```

The routers in the branch offices only enter the router 'Example_Inc.' and the subscriber number of one of the interfaces of the central office router.

④ You must still clarify the addresses. Specify the network address and the binding for the Example Inc.'s network so that the router can differentiate its own LAN from other LANs and the WAN: (configuration area 'IPX/SPX', 'General' tab):

```
Setup/IPX-module/LAN-config
set Network 00000009
set 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 router will always select the network on which the most RIP/SAP data is being exchanged.

Enter the appropriate network address with 'Auto' binding for the devices in the Manchester and Leeds branch offices.

```
cd /Setup/IPX-module/LAN-config
set network 00000003 and 00000004
set Binding auto
```

The bindings, e.g. 'SNAP', and network numbers must be explicitly stated for the branch office networks in Glasgow and London, as these networks do not have a server:

```
cd /Setup/IPX-module/LAN-config
set network 00000001 and 00000002
set Binding SNAP
```

⑤ And where should the devices 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 router in the network in the central office the table appears as below:

```
cd /Setup/IPX-module/WAN-config/Routing-table
set Glasgow 00000101 802.3 Route Off
set London 00000102 802.3 Route Off
set Manchester 00000103 802.3 Route on
set Leeds 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 Manchester and Leeds, the 'exponential backoff' mechanism is activated.

Further information on the function of the 'exponential backoff' mechanism is found in 'Exponential Backoff'.

The entry for the network in the Glasgow branch, for example, is as follows:

```
cd /Setup/IPX-module/WAN-config/Routing-table
set 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 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.

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 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 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 with TCP/IP

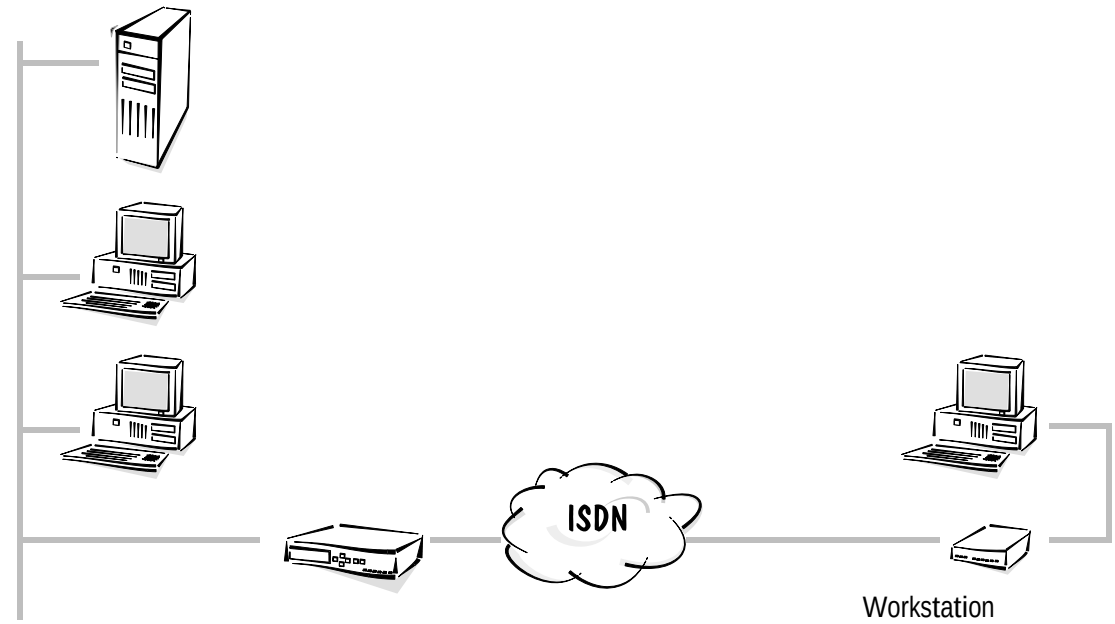
The motivation

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. The IP addresses are assigned from the IP pool to reduce the administrative requirements of the dial-up access points.

An example of the task

Staff using remote access will have a workstation computer with an ISDN terminal adapter or an ISDN card at home. Some field staff members also dial into the company network using notebooks and GSM mobile telephones.

A PPP client is installed on the remote computers, in this example Windows Dial-Up Networking using the TCP/IP protocol. The routing should also support NetBIOS packets to ensure that field staff members can also take advantage of Windows network file and printer sharing. A *ELSA LANCOM Business* is installed on the company's LAN to call back the workstation computers on demand.



Remote access made simple with *ELSA LANconfig* and its wizards

For the configuration of individual access accounts, there is a wizard in *ELSA LANconfig* which makes all required settings in the software for you and takes the peculiarities of TCP/IP networks into account. Once you have started the wizard (automatically or by clicking **Tools** ▶ **Setup Wizard**) select the entry 'Provide Dial-in access (RAS)'. The wizard will now prompt you for the required data, including the network protocol in use.

Step by step: which settings do you configure on the 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):

```
cd /Setup/WAN-module/Router-interface-list
set S0-1 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 Remote access should also be possible without verification of the incoming call number since field service employees at least sometimes 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. Check the values for the default layer and set them to the required values if required:

```
cd /Setup/WAN-module/Layer-list
set DEFAULT trans PPP trans none HDLC64K
```

This ensures that every caller that is not entered in the name list is immediately welcomed by PPP negotiation.

If the router determines that the remote station is calling via GSM, the `Trans APPP Trans no V.110 9600` protocol settings will be used automatically for the call establishment.

③ For callback to GSM mobile telephones, a layer will be needed later that is set up for connections using the V.110 protocol:

```
cd /Setup/WAN-module/Layer-list
set RAS_GSM Trans APPP Trans none or comp.  V.110 9600
```

④ The entry in the name list for each RAS remote station designating the remote station, layer ('DEFAULT' or 'RAS_GSM') and the callback option 'Name' allows the *ELSA LANCOM* to call back the 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. If a field staff

member calls in using both ISDN and GSM, two entries must be made in the name list for this employee.

```
cd /Setup/WAN-module/Name-list
set Tele_01_ISDN * * * DEFAULT Name
set Tele_01_GSM * * * RAS_GSM Name
set Tele_02 * * * DEFAULT Name
```

⑤ The channel list can be used to specify the number of channels to be used for dial-up access and to optionally determine the specific channels that may be used. The bundling of two channels should be permitted for access via ISDN. Only one channel on a different interface is available for GSM access:

```
cd /Setup/WAN-module/Channel-list
set Tele_01_ISDN 1 2 1-1;1-2 0
set Tele_01_GSM 1 1 2-1 0
set Tele_02 1 2 1-1;1-2 0
```

⑥ Since you are using PPP to access the remote computers, you can set the user names (e. g. Anybody) and password (e. g. Remote) in the PPP list for the 'Teleworker_01' remote station. Use PAP as your security process and enable the routing of IP and NetBIOS packets via this connection:

```
cd /Setup/WAN-module/PPP-list
Tele_01_ISDN PAP Remote 0 0 Tele_01 IP+NTB
Tele_01_GSM PAP Remote 0 0 Tele_01 IP+NTB
```

You may assign both entries for ISDN and GSM the same values for the user name. The staff member then can always use the same user name. The password ”Remote“ will be replaced by several asterisks (*) when entered.

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

⑦ An entry in the NetBIOS table is required for the routing of NetBIOS packets. This instructs the router that NetBIOS information may be exchanged, and that this is an individual workstation that may not be called up directly:

```
cd /Setup/NetBIOS-module/Remote-table
Tele_01_ISDN Workstation
Tele_01_GSM Workstation
```

⑧ You must still clarify the addresses. To enable the router router in its own TCP/IP network to be found, it needs a free IP address from the company network. It receives this when the Intranet address and associated netmask are entered:

```
cd /Setup/TCP-IP-module
set Intranet address 10.1.100.100
```

```
set Intranet netmask 255.255.255.0
```

⑨ What about the IP address for the computer making the call? They are dynamically assigned from a pool of IP addresses for the duration of the connection. Only the start and end of the address range is fixed. An entry in the IP routing table is thus superfluous:

```
cd /Setup/IP-router-module
set Start-WAN-pool 10.1.100.110
set End-WAN-pool 10.1.100.120
```

⑩ The proxy ARP must be enabled so that the router will be able to route data for a remote computer using an address from its own logical network.

```
cd /Setup/IP-router-module
set Proxy-ARP ON
```

⑪ Now switch the IP router on and the router is ready to receive calls from field staff.

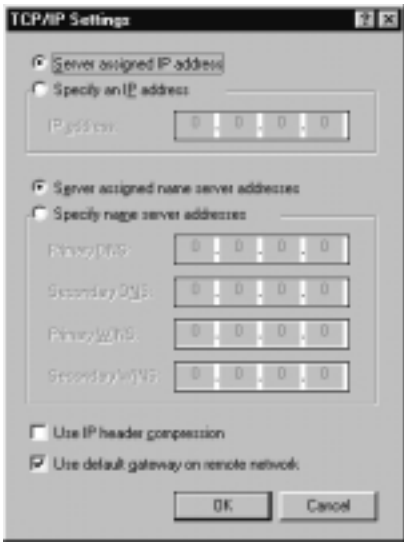
```
cd /Setup/IP-router-module
set operating on
```

⑫ 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 router
- Terminal adapter or ISDN card set to PPPHDLC
- PPP selected as the Dial-Up server type, 'Enable software compression' and 'Require data encryption' unchecked

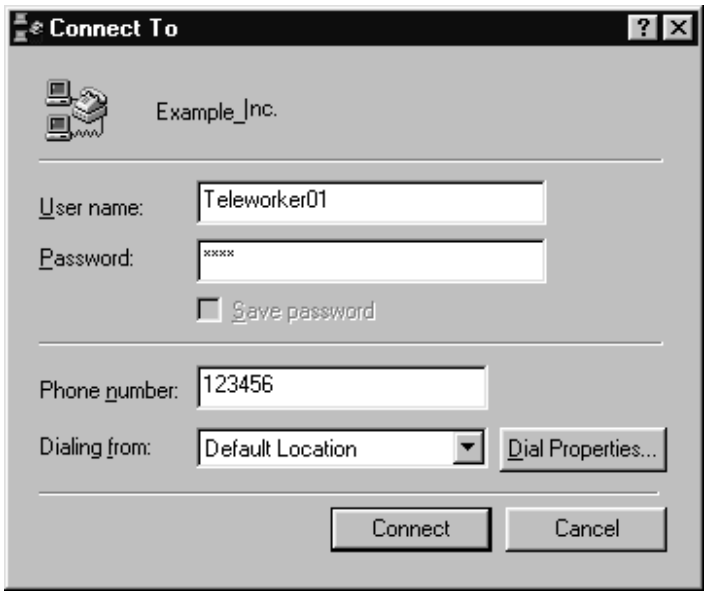
– TCP/IP selected as the network protocol

– 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 and Windows networks on the TCP/IP network. He can find this server by clicking on **Start** ▶ **Find** ▶ **Computer** in the Windows Start menu, for instance.

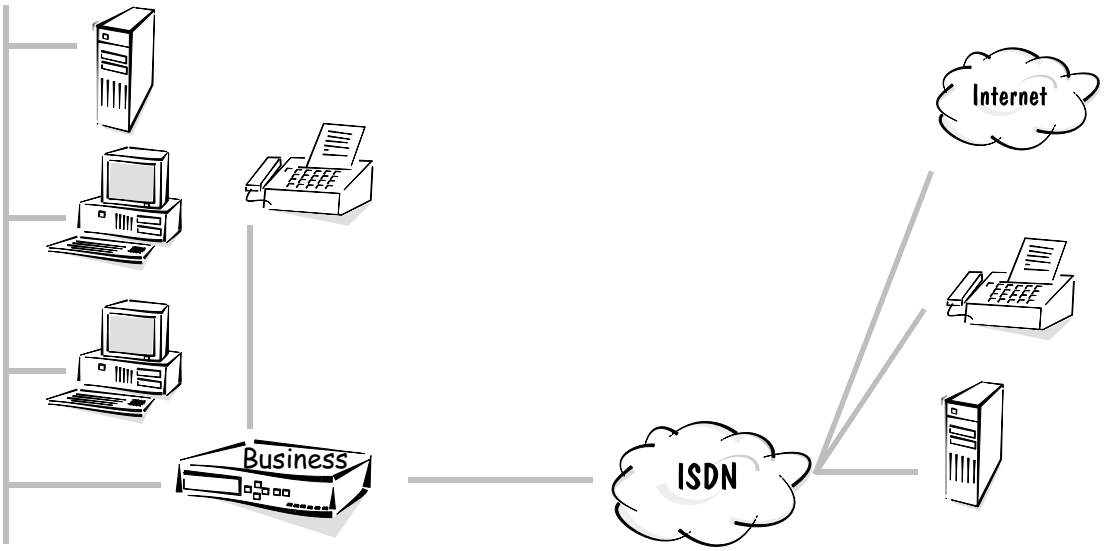
The least-cost router

In this chapter we will show you an example of how you can make significant savings with regard to connect charges.

Once it has been set up, the least-cost router automatically selects the most economical provider and attempts to establish the connection using that provider's network.

Example:

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.



The two employees in this office use the following functions of the *ELSA LANCOM Business*:

- 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*.

Of course, the office in this chapter's example also needs to make connections as cheaply as possible when 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 Glasgow and it has a telephone account with British Telecom. 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 Business* 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.

⑤ First let's take care of the long-distance connections. With this entry you can divert all national calls to another provider, depending on the time of day they are made:

Prefix	Dial-around 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 am – 11:59 pm	YES

⑥ International calls are relatively rare. In this example, therefore, just one entry applies to all international connections:

Prefix	Dial-around number	Days	Time	Fallback
00	01015;01028	Every day	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 Glasgow. On the Internet, the employees have found out which exchanges belong to the local zone. The following entries are now added:

Prefix	Dial-around number	Days	Time	Fallback
02408		Every day	0:00 am – 11:59 pm	YES
02464		Every day	0:00 am – 11:59 pm	YES
02404		Every day	0:00 am – 11:59 pm	YES
02401		Every day	0:00 am – 11:59 pm	YES
02403		Every day	0:00 am – 11:59 pm	YES
02454		Every day	0:00 am – 11:59 pm	YES
02451		Every day	0:00 am – 11:59 pm	YES
02406		Every day	0:00 am – 11:59 pm	YES
02407		Every day	0:00 am – 11:59 pm	YES
02429		Every day	0:00 am – 11:59 pm	YES
02465		Every day	0:00 am – 11:59 pm	YES
02423		Every day	0:00 am – 11:59 pm	YES
02471		Every day	0:00 am – 11:59 pm	YES
02456		Every day	0:00 am – 11:59 pm	YES

Prefix	Dial-around number	Days	Time	Fallback
02473		Every day	0:00 am – 11:59 pm	YES
02409		Every day	0:00 am – 11:59 pm	YES
02402		Every day	0:00 am – 11:59 pm	YES
02405		Every day	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	Dial-around number	Days	Time	Fallback
01		Every day	0:00 am – 11:59 pm	YES
0800		Every day	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	
	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.

Menu	Parameter	Comment or value
	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 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 dial-around provider.
	Fallback	Automatic fallback to your own telephone company if all dial-around 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 they are also not available, the connection will be made via the normal telephone company.

Create all the entries in accordance with this example, using the tables in *ELSA LANconfig* as a reference.

Appendix

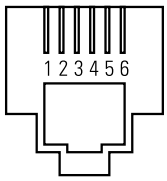
This appendix contains, in addition to the specifications, the pin assignments, and the general terms of warranty.

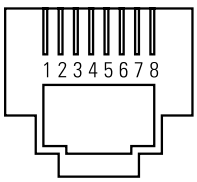
Technical data

Functions:	IP router, IPX router, CAPI server, DHCP server; least cost router for router and CAPI connections, simultaneous operation of all functions possible
LAN connection:	Ethernet IEEE 802.3, 10/100Base-TX (RJ45, node/hub, switch), auto-sense, full duplex operation
Network protocols:	IP router IP, TCP, ICMP, ARP, RIP-1, RIP-2, PROXY ARP, DHCP IPX router: RIP, SAP, Novell NetBIOS, Novell burst mode
Filter possibilities:	IP router TCP, UDP port filtering, source and destination network filter IPX Router: RIP, SAP, IPX and SPX watchdog, sockets, propagated packets
Spoofing:	IPX router: RIP and SAP packets; IPX and SPX watchdogs, Novell NetBIOS, keep-alive-packets
ISDN interface:	Connect: ISDN S0 bus, point-to-point and point-to-multipoint configuration, I.430 D channel: 1TR6, Euro-ISDN (DSS1), auto-sense, Group 0 fixed connections (D64S, D64S2, D64SY) B channel: PPP (asynch./synch.), MLPPP, X.75, HDLC, V.110, CAPI 2.0 over ELSA LANCAPI, Stac data compression
CAPI server:	Virtual CAPI 2.0 for Windows operating systems, NDIS WAN drivers, fax class 1
Line control:	Automatic callback with or without call establishment; line-on-demand (dynamic channel bundling), short-hold mode, round-robin dialing, fast callback, dial backup for leased lines
Charge monitoring:	Maximum number of calling charge units may be set for a specified period of time
Security and firewall functions:	Evaluation of remote-side subscriber number; PAP and CHAP, PPP authentication mechanisms; automatic firewall callback via CLIP, PPP or ELSA protocol; filter options in IP, IPX and bridge mode; protection of configuration using access lists and passwords, recording of most recent connection information, IP masquerading, encryption in development.
IP masquerading:	(NAT/PAT) IP address and port implementation using a single IP address, static/dynamic IP address assignment via PPP, masking of TCP, UDP, ICMP, FTP; DNS forwarding; inverse masquerading intranet IP services
Management:	Via LAN, ISDN (remote maintenance) or V.24, *ELSA LANconfig* and *ELSA LANmonitor* for Windows management software, configuration via SNMP v.1, TFTP, telnet or terminal
Operating security:	Hardware watchdogs, regular self-testing, FirmSafe concept for remote software upgrades
Statistics:	LAN and WAN packet counters; error, connection and charge counters, timer
Display/operation:	LCD display and keypad, LEDs for LAN and WAN status
Power supply:	12 V AC with AC adapter for 230 V, 12 VA

Ambient conditions:	Temperature: 5 – 40°C, humidity: 0 – 80%, non-condensing
Dimensions and design:	Rugged metal case, connections on rear panel; dimensions 230 x 38 x 228 mm (W x H x D)
Package contents:	Accessories: Power adapter, ISDN line connection cable, cable for outband interface, twisted-pair cable (CAT-5), detailed documentation and *ELSA LANCOM* CD-ROM Software: *ELSA LANconfig*, *ELSA LANmonitor*, *ELSA LANCAPI*, TFTP client, *ELSA-RVS-COM* office communications suite, *ELSA-ZOC* terminal program, LapLink for Windows remote maintenance software, CompuServe
Approvals:	For Germany, Switzerland and all other EU countries in preparation
Service and warranty:	6-year warranty
Support:	Via hotline and Internet

Pin assignments

Connector	RJ11 pin	Line
 a/b ports – RJ11	1	free
	2	free
	3	A
	4	B
	5	free
	6	free

Connector	RJ45 pin	Line	IAE
 ISDN – RJ45	1	free	free
	2	free	free
	3	T+	2a
	4	R+	1a
	5	R-	B 1
	6	T-	2b
	7	free	free
	8	free	free

Warranty conditions

The ELSA AG warranty, valid as of June 01, 1998, is given to purchasers of ELSA products in addition to the warranty conditions provided by law and in accordance with the following conditions:

1 Warranty coverage

a) The warranty covers the equipment delivered and all its parts. Parts will, at our sole discretion, be replaced or repaired free of charge if, despite proven proper handling and adherence to the operating instructions, these parts became defective due to fabrication and/or material defects. Also we reserve the right to replace the defective product by a successor product or repay the original purchase price to the buyer in exchange to the defective product. Operating manuals and possibly supplied software are excluded from the warranty.

b) Material and service charges shall be covered by us, but not shipping and handling costs involved in transport from the buyer to the service station and/or to us.

c) Replaced parts become property of ELSA.

d) ELSA are authorized to carry out technical changes (e.g. firmware updates) beyond repair and replacement of defective parts in order to bring the equipment up to the current technical state. This does not result in any additional charge for the customer. A legal claim to this service does not exist.

2 Warranty period

The warranty period for ELSA products is six years. Excepted from this warranty period are ELSA color monitors and ELSA videoconferencing systems with a warranty period of 3 years. This period begins at the day of delivery from the ELSA dealer. Warranty services do not result in an extension of the warranty period nor do they initiate a new warranty period. The warranty period for installed replacement parts ends with the warranty period of the device as a whole.

3 Warranty procedure

a) If defects appear during the warranty period, the warranty claims must be made immediately, at the latest within a period of 7 days.

b) In the case of any externally visible damage arising from transport (e.g. damage to the housing), the transport company representative and ELSA should be informed immediately. On discovery of damage which is not externally visible, the transport company and ELSA are to be immediately informed in writing, at the latest within 7 days of delivery.

c) Transport to and from the location where the warranty claim is accepted and/or the repaired device is exchanged, is at the purchaser's own risk and cost.

d) Warranty claims are only valid if the original purchase receipt is returned with the device.

4 Suspension of the warranty

All warranty claims will be deemed invalid

a) if the device is damaged or destroyed as a result of acts of nature or by environmental influences (moisture, electric shock, dust, etc.),

b) if the device was stored or operated under conditions not in compliance with the technical specifications,

c) if the damage occurred due to incorrect handling, especially to non-observance of the system description and the operating instructions,

d) if the device was opened, repaired or modified by persons not authorized by ELSA,

e) if the device shows any kind of mechanical damage,

f) if in the case of an ELSA Monitor, damage to the cathode ray tube (CRT) has been caused especially by mechanical load (e.g. from shock to the pitch mask assembly or damage to the glass tube), by strong magnetic fields near the CRT (colored dots on the screen), or through the permanent display of an unchanging image (phosphor burnt),

g) if, and in as far as, the luminance of the TFT panel backlighting gradually decreases with time, or

h) if the warranty claim has not been reported in accordance with 3a) or 3b).

5 Operating mistakes

If it becomes apparent that the reported malfunction of the device has been caused by unsuitable software, hardware, installation or operation, ELSA reserves the right to charge the purchaser for the resulting testing costs.

6 Additional regulations

a) The above conditions define the complete scope of ELSA's legal liability.

b) The warranty gives no entitlement to additional claims, such as any refund in full or in part. Compensation claims, regardless of the legal basis, are excluded. This does not apply if e.g. injury to persons or damage to private property are specifically covered by the product liability law, or in cases of intentional act or culpable negligence.

c) Claims for compensation of lost profits, indirect or consequential detriments, are excluded.

d) ELSA is not liable for lost data or retrieval of lost data in cases of slight and ordinary negligence.

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

f) The warranty is valid only for the first purchaser and is not transferable.

g) The court of jurisdiction is located in Aachen, Germany in the case that the purchaser is a merchant. If the purchaser does not have a court of jurisdiction in the Federal Republic of Germany or if he moves his domicile out of Germany after conclusion of the contract, ELSA's court of jurisdiction applies. This is also applicable if the purchaser's domicile is not known at the time of institution of proceedings.

h) The law of the Federal Republic of Germany is applicable. The UN commercial law does not apply to dealings between ELSA and the purchaser.

Declaration of conformity

CE

KONFORMITÄTSERKLÄRUNG

DECLARATION OF CONFORMITY

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

Geräteart: **Type of Device:**	**ISDN Router**
Typenbezeichnung: **Product Name:**	***ELSA Lancom Business***
EG-Baumusterprüfbescheinigungs Nr.: D801080L **Registration No.:**	
Benannte Stelle: **Notified Body:**	**CETECOM ICT Services GmbH** CE 0682 X

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

Niederspannungs Richtlinie (73/23/EWG)
Low Voltage Directive (73/23/EEC)
ISDN Vorschrift (97/346/EG)
ISDN Directive (97/346/EEC)
EMV Richtlinie (89/336/EWG)
EMC Directive (89/336/EEC).

Zur Beurteilung der Konformität wurden folgende **Normen** herangezogen:
The assessment of this product has been based on the following **standards**

EN 50082: 1992 Teil 2: EN 61000-4-2, 3, 4, 5, 6
EN 50081: 1992 Teil 1: EN 55022B: 1994
EN 60950: 1992 +A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997
TBR 3

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

ELSA AG
Sonnenweg 11
D-52070 Aachen

abgegeben durch:
this declaration is submitted by:

Aachen, 8. Februar 1999
Aachen, 8th February 1999

i.V. Peter Wieninger
Bereichsleiter Entwicklung
VP Engineering

Glossary

- **10BaseT –** Twisted pair; 10-Mbit Ethernet connection type; RJ45 network connection
- **10Base2 –** Thin Ethernet; Cheapernet; 10-Mbit Ethernet connection type; BNC network connection
- **10Base5 –** Thick Ethernet; 10-Mbit Ethernet connection type; AUI or SUB-D 15-pin network connection
- **100BaseTX –** Twisted pair; 100-Mbit Fast Ethernet connection type; RJ45 network connection
- **1TR6 –** German national ISDN; formerly common D channel protocol in Germany; only provided by Deutsche Telekom on special request
- **ARP –** Address Resolution Protocol, a protocol of the ➡TCP/IP family. ARP resolves IP addresses to associated MAC addresses.
- **Asynchronous transfer –** A process is required in serial data communications to establish synchronization between the transmitter and receiver, to permit the receiver to identify the beginning and end of a transmitted character. This structure is provided during asynchronous transfer by marking each byte to be transmitted with a start bit and one or two stop bits. This start-stop process is one of the most common transfer processes, especially in the microcomputer sector, as it can be realized technically with relative ease.
- **AUI –** Attachment Unit Interface = Port for general network connections.
- **B-chan. –** ISDN data transfer channel (64 kbps); an ISDN basic rate interface has one D channel and two B channels.
- **Basic Rate Interface –** ISDN subscriber connection with two ➡bearer channels (64 kbps) and a signal channel (16 kbps). The ➡S_0 interface is the subscriber interface used by the Basic Rate Interface.
- **BNC –** Common connector type for Cheapernet (Thin Ethernet). This connector is also known as T-BASE2. A T connector must be used to connect devices equipped with BNC sockets.
- **Bridge –** A bridge is a connection between two networks with identical layer-2 structures in the ➡OSI model. Such a bridge can consist of two devices connected to one another by a data transfer route. This constellation is known as a remote bridge.
- **Broadcast –** Broadcasts are special data packets sent out to all stations set to receive. In Ethernet networks, these data packets are marked with the target address FFh FFh FFh FFh FFh FFh (i.e. to everyone).
- **Burst mode –** Burst mode is a special form of data packet transfer used in Novell networks in which several data packets are sent consecutively without confirmation of receipt.
- **CEPT –** Conférence Européenne des Postes et des Télécommunications = the European telecommunications standards board.
- **Channel bundling –** Bundling of both ISDN B channels to a logical connection in order to double the transfer speed.
- **Client –** Client = Workstation. A client is a user of services provided by a ➡server.
- **CLIP –** Caller Line Identification Parameter = Subscriber number of the caller that can be transmitted in the ISDN.

- **Data compression –** Method for the reduction of the data volume to be transferred; data compression can be used to increase the data throughput of a connection (common processes: V.42bis, STAC, MPPC)
- **D channel –** ISDN signaling channel (dialing, caller line identification, charge information, establishment and termination); an ISDN basic rate interface has one D channel and 2 B channels.
- **Data packet –** A data packet contains a number of characters (control commands) specified by a data network for the transfer of data.
- **DNS –** Domain name server. Designation for a server that provides a name service for every computer of a ➡domain. A computer that only knows the symbolic name of a destination can request the IP address associated with the name from the DNS server.
- **Domain –** A domain is a logically limited section of a network such as corporate network or an Internet provider.
- **DSS1 –** Euro-ISDN; currently a commonly used ISDN D channel protocol
- **Dynamic channel bundling –** Bandwidth-on-demand; the bandwidth is increased by automatically adding further B channels as required.
- **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.
- **EAZ –** The EAZ = is the terminal device selection number used in the 1TR6 protocol to distinguish terminal equipment connected to the same ISDN ➡base rate interface. Callers will attach this digit at the end of the telephone number.
- **Ethernet network –** An Ethernet network is a ➡bus system with ➡CSMA/CD (carrier sense multiple access with collision detection) access and ➡baseband transmission. This local network type was developed in 1979 by DEC, Intel and Xerox. As one of the first ➡LANs, it became a de-facto standard and was adopted as an official standard by the IEEE (Institute of Electrical and Electronics Engineers, standard 802.3). The data transfer takes place via coaxial, twisted-pair, fiber optic or other conductors at a rate of 10 Mbit per second.
- **ETSI –** European Telecommunications Standards Institute. This is the standardization authority which developed the European D channel protocol (DSS1).
- **Firewall –** Mechanism to protect intranets from unauthorized access; the *ELSA LANCOM* supports IP masquerading, port filtering and access lists as firewall mechanisms.
- **Flash ROM –** Flash ROM is type of memory that can be erased and rewritten electrically. Flash ROMs are frequently used in devices in which the firmware can be updated.
- **Gateway –** Network component that provides access to other network components on a layer of the ➡ OSI model (e.g. on layer 3 in Windows 95).
- **HDLC –** High Level Data Link Control. Format of a data packet that is secured using a CRC calculation.
- **Hops –** Number of routers along a specific network connection.
- **Hub –** Network component; distributor; collector; also used for the conversion of one

type of connection to another; one network input – several network outputs for star-shaped distribution.

- **INTERNET –** The Internet is the sum total of all networks connected to one another using ➡TCP/IP.
- **Intranet –** Domain; a network limited to a single company, for example, and that only permits controlled access to and from the outside.
- **IP –** The Internet Protocol is an extensive protocol family developed by the DoD (Department of Defense) in the early 1970s for the interconnection of heterogeneous Wide Area Networks.
- **IPX –** Internet Packet eXchange = a data transport protocol defined by Novell. This protocol is realized on PCs using the IPX.COM or ➡VLM Shell drivers.
- **IP address –** First part of the address with which a network component identifies itself in a TCP/IP network.
- **IP netmask –** Second part of the address with which a network component identifies itself in a TCP/IP network.
- **IP-masquerade –** Single IP address; port address translation; a process for the connection of an intranet (several workstations) to the Internet using a single IP address; the *ELSA LANCOM* is capable of this process.
- **IPX –** Internet Packet eXchange; transport protocol; network protocol used mainly by Novell networks.
- **IPX address –** Consists of the ➡ node ID, IPX network address and socket; used for the precise identification of a network component within an IPX network.
- **IPX watchdog –** Packets sent at specific intervals by the server to monitor a workstation. If the workstation does not answer it is automatically logged off.
- **ISDN –** Integrated Services Digital Network
- **ISO –** International Standardization Organization. The ISO is an international organization that coordinates the development and publication of worldwide standards in all fields. National standards institutes such as DIN (Germany), ANSI (USA), BSI (Great Britain) or AFNOR (France) are members of the ISO.
- **ITU-T –** The telecommunication standardization sector of the International Telecommunications Union (ITU) deals with the standardization of data and telephony services. The ITU-T guidelines of the V. series cover data transfer in telephone networks, for example. The ITU-T is the successor organization of the CCITT (Comité Consultatif International Télégraphique et Téléphonique).
- **LAN –** Local Area Network According to ➡ISO, a local network is a network for the bit-serial transfer of data between linked, independent elements within the property limits and under the legal control of the operator. In other words, a local network is limited to a very small area, generally within a single building or a company headquarters.
- **Layer –** Layer, level (see OSI reference model); layer within a modular connection structure between two communicating systems
- **Line on demand –** Establishment of a connection as required. In the *ELSA LANCOM*, the receipt of data packets from the LAN determines whether a connection is established.

- **MAC –** Media Access Control. A sublevel of layer 2 of the ➡ISO reference model. In Ethernet networks, the source and destination addresses as well as the protocol type belong to the MAC layer data.
- **MPPC –** Microsoft Point-to-Point Compression; data compression process (currently not supported by the *ELSA LANCOM*).
- **MPR –** Multiprotocol router; a router that is capable of routing multiple protocols.
- **MSN –** Multiple Subscriber Number. With the DSS1 protocol, the exchange can assign several subscriber numbers to one ISDN connection. Normally, three numbers are offered, but up to eight are possible. Using these numbers, you can directly address terminal devices attached to the S_0 interface. Unlike the one digit EAZ number that is attached at the end of the telephone number, the MSN can consist of a maximum of 16 digits.
- **Multicast –** Multicasts are special data pakkets sent out to all stations that are set to receive within a group.
- **Multilink PPP –** MLPPP; PPP channel bundling process; (not supported by the *ELSA LANCOM* at the present).
- **NBNS –** Net BIOS Name Server. Designation for a server that provides a name service for every computer of a ➡domain. A computer that only knows the symbolic name of a destination can request the IP address associated with the name from the DNS server.
- **Network –** A network is a multiple-user and multifunctional group of computers and terminal systems that are connected by communications lines to share information and resources.
- **NETX –** NETX = NetWare shell. This program provides an interface between applications and the Novell network operating system.
- **Node –** A node is a device connected to a network that either sends or receives data. These can be individual *ELSA LANCOMs*, workstations, servers or printers shared by network participants.
- **Node-ID –** MAC-address
- **Novell –** The manufacturer of the Novell NetWare network operating system.
- **OSI –** Open System Interconnection. A reference model for networks developed by the ➡ISO (International Standardization Organization) to establish interface standards between computer manufacturers with regard to hardware and software requirements.
- **Outband configuration –** In outband (or out-of-band) configuration, data exchange with the device to be configured is realized via a serial V.24 interface. This configuration connection can remain in operation even in the event of problems with the network connection.
- **Ping –** ICMP command; this command is used to determine the distance of network components in a TCP/IP network in a manner similar to the sonar ping used by submarines.
- **PPP –** Point-to-Point Protocol; protocol family (LCP, IPCP, IPXCP, CBCP, ECP, CCP etc.); protocol for the negotiation of connection parameters for the point-to-point connection of network components (e.g. callback, network protocols, compression)
- **Protocol –** Dialog between connected components for the establishment and maintenance of connections (network, ISDN, analog connections).

- **Proxy ARP –** Proxy ARP ensures that stations that are normally connected directly to a local TCP/IP network and thus have a suitable local IP address are also available through a router (and thus via a WAN connection). The router identifies itself as the remote station during ARP queries in the local network, i.e. revealing its own MAC address. It can then receive data packets and forward them to the remote station.
- **RIP –** Routing Information Protocol; used for the transfer of router information in networks (in this case, Netware IPX).
- **RoundRobin –** A process for dialing up a logical remote station (e.g. company headquarters) using a variety of numbers for different devices. In the event that the default remote station is busy, other remote stations are automatically dialed.
- **Router –** A router is a device to connect two networks with identical layer-3 structures in the ➡OSI model. Such a router can consist of two devices connected to one another by a data transfer route. This constellation is also known as a remote router.
- **RTS –** Request to Send
- **S_0 line connection –** 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. Used for the distribution of services in NetWare networks.
- **Server –** A server is a provider of services used by ➡clients. Many network operating systems use a client-server architecture, i.e. a specific, very powerful computer serves data and programs to a large number of clients (workstations).
- **Short hold mode –** A connection is terminated after a specified period in which no data has been transferred. This can be used to ensure that the connection will be held until no further data is being transferred.
- **SNMP –** Simple Network Management Protocol; standardized protocol for the management of network components; advantage: monitoring of a variety of network components using one and the same user interface (such as HP Openview or Cabletron Spectrum); not specific to any manufacturer; *ELSA LANCOM* supports SNMP Version 1.
- **Socket –** ID number for the service under which a data packet is sent.
- **Spoofing –** Spoofing is a method to avoid unnecessary connection charges. All queries from the LAN side are answered directly by the router without establishing a connection or sending data to the remote station.
- **SPX –** Sequenced Packet eXchange = a protocol defined by Novell for the secure transfer of data in a network. This protocol is realized on PCs using the NETX.COM or similar drivers.
- **SPX watchdog –** Packets sent at specific intervals by the server to monitor an SPX connection.
- **SPV –** Semi-permanent connection = pre-ordered long-term dial-up connection. Semi-permanent connection are currently available for the ➡1TR6 protocol and can be established between any two ISDN connections. 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 may result in savings of communications charges.

- **Stac compression –** Data compression process
- **Stand-alone solution –** The *ELSA LANCOM Business 4100* is a stand-alone solution because no additional computers must be set up or additional software installed on a server as was previously the case with conventional routers. In other words, it is an independent network component.
- **Leased line –** A leased line is a permanent connection between two participants for their exclusive use.
- **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 kbps for ➡Basic Rate Connections or 64 kbps for ➡Primary Multiplex Connections.
- **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. The Internet Protocol is an extensive protocol family developed by the DoD (Department of Defense) in the early 1970s for the secure interconnection of heterogeneous Wide Area Networks. The two foundations of this protocol family are IP, which implements layer 3 of the ➡OSI model, and the corresponding TCP for the fourth layer.
- **Telnet –** Telnet is a protocol of the ➡TCP/IP protocol family. It permits remote access from a workstation to another computer system in the network. As it requires secure bi-directional communications, the telnet protocol uses the ➡TCP protocol for data transfer. A virtual terminal on the host is thus placed at the telnet client's disposal.
- **TFTP –** Trivial File Transfer Protocol; a simple protocol for file transfers such as firmware uploads, or the backup and restoration of configurations.
- **TICS –** System time unit of the *ELSA LANCOM*
- **Transceiver –** A transceiver is a device that transforms the input signal format to a different output format.
- **UDP –** User Datagram Protocol = transfers data in certain IP network services, but unlike TCP does not provide secure data transfer.
- **UNIX –** UNIX is an operating system developed by AT&T for high-performance microcomputers, computers and mainframes.
- **V.24 interface –** Serial interface, port used to connect modems, for example; the *ELSA LANCOM* has a V.24 interface to permit analog dial-ups via a connected modem.
- **V.42bis –** Recommendation of the ➡ITU-T with regard to the compression of data within a data stream.
- **V.110 –** Recommendation of the ➡ITU-T with regard to the adaptation of asynchronous and synchronous serial data streams to the ISDN bit rate of 64 kbps in the ISDN ➡B channel (also known as I.463).

- **VLM –** Virtual Loadable Module = This program provides an interface between applications and the Novell network operating system.
- **WAN –** Wide area networks based on connections using ISDN devices, for example.
- **WORKSTATION –** Designation for a single computer within a network.
- **X.75 –** 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 ➞transfer protocol with automatic error recognition and correction. Data transfer is performed in 128-byte blocks. If a transfer error is identified, the faulty block is sent again. XModem is one of the most commonly used protocols worldwide. It is supported by many standard terminal programs, but has since been superseded by more modern high-performance protocols such as ZModem.
- **Y connection –** Simultaneous connection to two different remote stations, each using one B channel of the same ISDN S_0 connection.

Index

D

M

N

O

P

R

S

T

U

V

W

X

Y

Description of the menu options

The menu tree for *ELSA LANCOM* 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* family. Restrictions with regard to specific models are indicated by the symbol shown here.

You can access the menus when configuring via Telnet or terminal programs and via SNMP (also see 'Configuration Modes').

When configuring with *ELSA LANconfig*, you are provided with an integrated help system that gives you brief descriptions of the individual parameters.

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

Symbols

	Menu	Indicates a further submenu.
	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**
  - Name
  - WAN-module
  - Charges-module
  - LAN-module
  - IPX-module
  - TCP-IP-module
  - IP-router-module
  - SNMP-module
  - DHCP-module
  - NetBIOS-module
  - Config-module
  - LANCAPI-module
  - LCR-module
  - DNS module
  - Time-module
- **Firmware**
  - Version-table
  - Table-firmsafe
  - Mode-firmsafe
  - Timeout-firmesafe
  - Test-firmware
  - Firmware-upload
- **Status**
  - Connection
  - Current-time
  - Operating-time
  - WAN-statistics
  - LAN-statistics
  - PPP-statistics
  - IPX-statistics
  - TCP-IP-statistics
  - IP-router-statistics
  - Config-statistics
  - Queue-statistics
  - Conn.-statistics
  - Info-connection
  - Layer-connection
  - Call-info-table
  - Remote-statistics
  - S_0-bus
  - Channel-statistics
  - Time-statistics
  - LCR-statistics
  - Delete-values
- **Other**
  - Manual-dialing
  - Boot-system
  - Reset-system
  - Upload-system

Status

The Status menu contains information on the current status and the internal sequences of operations in the LAN and WAN, which can relate to the data transmission route (e.g. dialing or connection) or to statistics (e.g. number of calls received or data blocks transmitted). The statistics displays are an important aid for verifying correct functioning and optimizing parameter settings. In addition, they provide valuable information for error analysis when malfunctions occur.

Most status displays are continually updated and can be deleted with a **value** or set to 0 in the current menu.

The menu has the following layout:

Status		Running status displays
Connection		Status of the WAN route
Current-time		Current time in device
Operating-time		Period of time the device has operated since it was last switched on
WAN-statistics		Displays WAN statistics
LAN-statistics		Displays LAN statistics
PPP-statistics		Point-to-point-protocol 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
Connections-statistics		Connection information for each interface
Info-connection		Information on the last connection for each interface
Layer-connection		Information on the B-channel protocol used for each interface
Call-info-table		Information on the last 100 calls received
Remote-statistics		Statistics on the last 100 connections
S_0-bus		Status of the S_0 interface
Channel-statistics		Information of the status of the individual channels.
Time-statistics		Time module information
LCR-statistics		Least-cost router information
Delete-values		Deletes all values except tables with substatistics.

Display and keyboard

The display shows status information and error messages issued by the device. The following display modes are available:

- B channel overview (one character per channel)
- B channel status (one line per channel)
- Device status / Device error messages

A total of six keys are available (cursor keys + “Mode” + “Clr”), as well as a two-line display with 40 characters per line, of which 16 characters each are currently displayed. Depending on the devices settings, the text information is displayed in German or English.

B-channel-overview

In the B channel overview the channels are displayed in the form of a table. The individual fields of the table have the following significance:

P: x (status of port 1, first B channel)	P: X	P: X	P: X
1: x (status of port 1, second B channel)	2: x	3: x	4: x

The following symbols are used for the channel status (shown by x in the table):

.	Channel idle (disabled)
-	Channel idle (enabled)
E (flashing)	An error has occurred on the channel
A (flashing)	Outgoing call
A	Connected (outgoing)
P (flashing)	Incoming call
P	Connected (incoming)
N (flashing)	Negotiation

The cursor keys have no function in this mode.

B channel status display

The B channel status display shows an excerpt from a table with an entry for each B channel. In the event of changes to the status of a channel, the table will jump to the current entry if no cursor key has been used for at least 5 seconds. The status of the channel is displayed in plain text, e.g.:

```
CH11: Connection LC_PPP
CH12: Remote station LC_PPP not responding
```

Error messages are retained for 60 seconds. Information with regard to the enabling and disabling of S_0 interfaces is also displayed.

The up and down cursor keys can be used to scroll through the individual lines; use the left and right cursor keys to navigate within the line itself. Although a width of only 16 characters is available, the display has a total width of 40 characters (the visible section can be moved). The display returns to the start 5 seconds after the last horizontal movement.

Device status and device error messages

Channel-independent device status messages and especially error messages (with simultaneous flashing Power/Msg LED) are displayed in this mode. The unit automatically switches to this mode in the event of an error.

The up and down cursor keys permit scrolling through all available messages. The model number (e.g. "Model 4100") and the firmware version always appear as the final message. This display also appears immediately after switching the unit on, before changing to the last current display mode. The error messages in this mode can also be up to 40 characters long.

The Mode key switches between the display modes described above.

The Clr key clears the errors displayed in the device status and device error message display modes.

Status/Connection

The **Status/Connection** menu option displays the status messages for the individual channels.

/Connection-state		Running status displays
Connection		CH01: Ready; CH02: Ready

Status/Current-time

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

Status/Operating-time

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

Status/WAN-statistics

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

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

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

Byte-transport-statistics

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

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

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

Ifc	Designates the associated channel.
CRx-bytes	Number of bytes received (compressed)
Rx-bytes	Number of bytes received (uncompressed)
Tx-bytes	Number of bytes sent (uncompressed)
CTx-bytes	Number of bytes sent (compressed)

Packet-transport-statistics

For each available interface, the **Status/WAN-statistics/Packet-transport-statistics** menu option provides statistics on the data packets transferred via this interface. The table maintained here has the following layout:

Ifc	Rx	Tx-total	Tx-normal	Tx-reliable	Tx-urgent
Ch01	0	0	0	0	0
Ch02	0	0	0	0	0

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

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

Error-statistics

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

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

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

Ifc	Designates the associated channel.
Rx-I1-error	Number of layer-3 errors in data received (i.e., the protocol header of layer-3 is incorrect)
Rx-I2-error	Number of layer-2 errors in data received (i.e., similar to the layer-3 errors, e.g. defective PPP header)
Rx-I3-error	Number of layer-1 errors in data received (similar to layer-3 errors)
Stack-error	Number of transmission errors that occurred while sending
Tx-error	Number of stack errors for data received. Stack errors are caused when frames are received that cannot be assigned to an internal processing procedure (e.g. IP router).

Throughput-statistics

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

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

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

Ifc	Designates the associated channel.
Rx/s current	Throughput on the channel in the last second in the receiving direction
Tx/s current	Throughput on the channel in the last second in the transmission direction
Rx/s average	Average throughput on the channel in the receiving direction
Tx/s average	Average throughput on the channel in the transmission direction

Status/LAN-statistics

Similarly to the previous menu option, this option allows you to display the statistics relating to the LAN port. The **Status/LAN-statistics** menu has the following layout:

/LAN-statistics	Running status displays	
LAN-rx-packets		Number of data packets received
LAN-tx-packets		Number of data packets sent
LAN-rx-errors		Number of data packets incorrectly received
LAN-tx-errors		Number of data packets incorrectly sent
LAN-stack-errors		Number of packets without a suitable receive module (bridge/ router)
LAN-NIC-errors		Number of data packets discarded by the NIC
LAN-heap-packets		Number of buffers available
LAN-queue-packets		Number of buffers in use
LAN-queue-errors		Number of packets discarded due to a lack of buffers
LAN-collisions		Number of collisions during a send procedure
Link-active		Display of correct Ethernet connection (data transfer possible). Corresponds to the 'Link' LED on the device.
Negotiation done		The negotiation of the transfer mode between the router and the remote station is complete. This is only relevant if Setup/LAN/Connection is set to 'Auto'.

/LAN-statistics		Running status displays
Connector		This item shows the connection type currently being used on the Ethernet connection: 10B-TX: 10 MBit, half-duplex FD10B-TX: 10 MBit, full-duplex 100B-TX: 100 MBit, half-duplex FD100B-TX: 100 MBit, full-duplex If 'Auto' is set under Setup/LAN, then this is the connection type the two units have negotiated. This corresponds to the 'Fast' and 'FDpx' LEDs on the unit. If, on the other hand, a fixed transfer mode has been set, this value will be the same as the one in Setup/LAN/Connection.
LAN-rx-bytes		Number of bytes received from the LAN
LAN-tx-bytes		Number of bytes sent to the LAN
LAN-rx-broadcasts		Number of broadcast packets received from the LAN
LAN-rx-multicasts		Number of multicast packets received from the LAN
LAN-rx-unicasts		Number of directly addressed packets received from the LAN
LAN-tx-broadcasts		Number of broadcasts received from the LAN
LAN-tx-multicasts		Number of multicasts received from the LAN
LAN-tx-unicasts		Number of unicasts received from the LAN
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
CBCP-statistics		Displays PPP/CBCP statistics
IPXCP-statistics		Displays PPP/IPXCP statistics
IPCP-statistics		Displays PPP/IPCP statistics
CCP-statistics		Displays PPP/CCP statistics
ML-statistics		Displays PPP/ML statistics

/PPP-statistics		Running status displays
BACP-statistics		Displays PPP/BACP statistics
Rx-options		Displays the LCP, IPCP and IPXCP information received
Tx-options		Displays the LCP, IPCP and IPXCP information sent
Delete-values		Deletes PPP statistics.

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

PPP-phases

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

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

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

Ifc	Designates the associated channel.
Phase to	Indicates the current phase of the PPP. The possible values are **AUTHENTICAT**, **NETWORK** and **TERMINATE**.
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 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 CBCP 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 *ELSA LANCOM* 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**eceive **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
Authent.	Authentication procedure used (PAP/CHAP)
Callback	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 *ELSA LANCOM* (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 *ELSA LANCOM* 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 *ELSA LANCOM* 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/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 sokket 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 sokket 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
Table-SAP	Number of SAP packets received from the LAN
Delete-values	Deletes SAP statistics

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 computer name	Network address	MAC address of the server	Socket for the service	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
Establish-table	Table of the last 20 packets that required a connection
Delete-values	Deletes IPX router statistics

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 have caused a connection to be established.

An IPX establish table might have the following appearance:

Time	Destination	Source
1T; 16:45:01	00000081 ffffffffffff 0453	00000001 00a05702000a 0453
1T; 10:45:10	00000081 ffffffffffff 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 'ffffffffffff' 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

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

/TCP-IP-statistics		Statistics from the TCP/IP area
ARP-statistics		Statistics from the ARP area
IP-statistics		Statistics from the IP area
ICMP-statistics		Statistics for ICMP packets
TFTP-statistics		Statistics for TFTP operations
TCP-statistics		Statistics for TCP packets from TCP sessions to the router
DCHP-statistics		Statistics from the DCHP server
Delete-values		Deletes TCP/IP statistics
NetBIOS-statistics		NetBIOS module statistics
DNS-statistics		Statistics from the DNS server

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
Table-ARP	Displays ARP table
Delete-values	Deletes ARP statistics

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

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

Status/TCP-IP-statistics/NetBIOS

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

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

B-Nodes

Broadcast nodes. A B node performs name negotiations exclusively via broadcasts. Such a computer is not visible over a router connection, since broadcasts may not be routed.

P-Nodes

Point-to-point nodes. For name negotiations, a P node requires a NetBIOS nameserver (NBNS) as well as a NetBIOS datagram distribution server (NBDD) to transfer datagrams over a router.

M-Nodes

Mixed nodes. This type is a mixture of B and P nodes. It acts as a B node in the local network; if the required partner can't be found in the local network, it attempts to locate it using an NBNS query (P node behavior).

W-Nodes

This type of node is not permissible according to RFC, but was introduced nevertheless by Microsoft as a hybrid node.

Status/TCP-IP-statistics/DNS-statistics

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

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

The hit list has the following structure:

Domain	Requests	Time	IP-address
www.elsa.com	1	00.00.0000 00:00:29	10.0.0.123

The individual fields of this list have the following significance:

Domain	Name of the requested computer
Requests	Total number of requests for this name since its appearance in the table
Time	Time of the last request
IP-address	Address of the computer that last requested this name

This list is sorted according to the frequency of requests. When the table is full, the names that have not been requested for the longest period will be deleted to make room for new entries.

Status/IP-router-statistics

This menu groups together the statistics from the IP router module.

/IP-router-statistics		Statistics from the IP router area
IPr-LAN-rx		Number of data packets to be routed from the LAN
IPr-LAN-tx		Number of data packets routed to the LAN
IPr-LAN-local-routings		Number of packets received from the LAN and routed to the LAN
IPr-LAN-network-errors		Number of LAN packets that were not routed
IPr-LAN-routing-errors		Number of LAN packets that must be sent to another router
IPr-LAN-ttl-errors		Number of LAN packets with an expired time-to-live value
IPr-LAN-filters		Number of LAN packets filtered by the filter table
IPr-LAN-discards		Number of LAN packets discarded
IPr-WAN-rx		Number of data packets to be routed from the WAN
IPr-WAN-tx		Number of data packets routed to the WAN
IPr-WAN-network-errors		Number of WAN packets that were not routed
IPr-WAN-ttl-errors		Number of WAN packets with an expired time-to-live value
IPr-WAN-filters		Number of WAN packets filtered by the filter table
IPr-WAN-discards		Number of WAN packets discarded
IPr-WAN-type-errors		Number of packets from the WAN without an IP router ID
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
Delete values		Deletes IP-router statistics

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	Prot.	D-port	S-port
1T; 16:45:01	192.120.131.40	192.120.130.10	tcp	23	4711
1T; 10:45:10	192.120.131.50	192.120.130.10	udp	53	8123

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

Protocol-table

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

A protocol table might have the following appearance:

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

Status/IP-router-statistics/RIP-statistics

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

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

Table-RIP

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

An IP-RIP table might have the following appearance:

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

Status/Config-statistics

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

/Config-statistics		Remote configuration statistics
LAN-active-connections		Current number of active configuration connections from the LAN
LAN-total-connections		Total number of configuration connections from the LAN up until the present
WAN-active-connections		Current number of active configuration connections from the WAN
WAN-total-connections		Total number of configuration connections from the WAN up until the present
Outband-active-connections		Current number of active outband configuration connections
Outband-total-connections		Total number of previous outband configuration connections up until the present
Outband-bitrate		Bit rate of the last outband configuration session
Login-errors		Total number of defective logins
Login-locks		Number of login locks
Login-rejects		Number of login attempts while the login lock was active
Delete-values		Deletes the config statistics

Status/Queue-statistics

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

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

/Queue-statistics	Statistics on the 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.
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:

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

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

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

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

Status/Info-connection

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

Ifc	Status	Mode	Dialup-remote	Device-name	B1-DT	B2-DT
Ch01 Ch02	Ready Ready				0 0	0 0

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

Ifc	Designates the associated channel.
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 *ELSA LANCOM Business 4100* 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. The following are possible: **Active** (active call establishment = dialing) **Passive** (passive call establishment = call acceptance) **CB** (call establishment via callback)

Dialup-remote	Indicates the call number of the remote station from the name list.
Device-name	Indicates the logical name of the remote station (if it can be detected). The device name is also displayed on the appropriate display line as soon as a logical connection is established.
B1-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:

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

Status/Call-info-table

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

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

System-Time	Ifc	CLIP-Caller	Dial-Caller	Capab.	B-chan.
0T; 00:20:57	S_0	5678	1234	HDLC64K	2
0T; 00:20:46	S_0	4321	1234	HDLC64K	1
0T; 00:19:47	S_0	4321	1234	HDLC64K	1
0T; 00:11:33	S_0	5678	1234	HDLC64K	1
0T; 00:01:13	S_0	4321	1234	HDLC64K	2
0T; 00:01:02	S_0	4321	1234	HDLC64K	1
0T; 00:00:06	S_0	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	Designates the associated interface.
CLIP-Caller	Call number (CLIP) of the caller

Dial-Caller	The MSN/EAZ dialed by the caller
Capab.	The service requested by the caller. Possible values are HDLC64K, HDLC56K and unknown. An analog call is displayed as unknown here.
B-chan.	The B channel used. A value of 0 means that all channels have already been seized, i.e. call waiting is activated.

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

Status/Remote-statistics

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

The table has the following layout:

Conn.-start	Remote-ID	Mode	Ifc	Conn.-time	Charge
0T; 00:20:57	LONDON	Active	Ch01	50	5
0T; 00:20:46	MANCHESTER	Passive	Ch02	230	10

The different entries have the following meaning:

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

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

Status/S_0-bus

This option allows you to display the current status of the S_0 interface. The statistics have the following layout:

/S_0-bus		Running status displays
D-info		Overview of the D channel status
D2-statistics		Breakdown of the Layer-2 information of the D channel for the B channels.

D-info

This table shows general information related to the D channel:

Channel	B-channel identification.
Protocol	D-channel protocol. Either the protocol fixed in the interface table or the protocol detected in the 'Auto' settings at the ISDN terminal.
Layer-2	Activation of layer 2 of the D channel ('Yes' or 'No')
TEI	TEI assigned ('Yes' or 'No')
S_0-activation	Displays activation status ('Yes' or 'No')

D2-statistics

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

Channel	B-channel identification.
TEI	**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/Channel-statistics

This table shows information on the current status of the two B channels. The information from this table is primarily used for output via *ELSA LANmonitor*. Therefore, some values are shown simply as bits with no further explanation.

The table has the following layout:

Channel	State	App	Mode	Cause	Dialup-remote	Sub-address	Charge	Conn.-time	Extra	ISDN-display
S_0-1-ERR	00000000	Router	active	0000	0241123456	00000000	3	0		
S_0-1-B1	00000000	a/b	active	0000	0241123457	00000000	2	20		
S_0-1-B2	00000000	LAN-CAPI	passive	0000	0241123458	00000000	4	180		

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

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

Status/Time-statistics

This menu has information on the current time in the device and on the path over which the *ELSA LANCOM Business* 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
Units	
Delete values	Deletes ISDN statistics

Status/LCR-statistics

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

The menu has the following layout:

/LCR-statistics		Least-cost router statistics
Total calls		Total number of LCR calls
Found-events		Number of calls in which the router found a suitable rule in its tables and successfully rerouted the connection.
Not-found-errors		Number of calls in which the router did not find a suitable rule in its tables and thus could not reroute the connection.
Missing time-errors		Number of calls in which the LCR could not become active due to lack of time
Provider-statistics		A table with all providers used (or their prefixes), the number of successful and unsuccessful calls
Delete values		Deletes LCR statistics

Status/Delete-values

With the exception of the tables, this option allows you to delete all the values in the substatistics. To do so, enter the following command:

```
do delete-values
```

Setup

This menu allows you to query and modify all the system parameters that are necessary to the functioning of the devices.

/Setup		System configuration
Name		Entering the device name
WAN-module		WAN settings
Charges-module		Charge management settings
LAN-module		LAN settings
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

/Setup		System configuration
DHCP-module		DHCP server settings
NetBIOS-module		Settings for the NetBIOS proxy
Config-module		Configuration module settings
LANCAPI-module		*ELSA LANCAPI* settings
LCR-module		Least-cost router settings
DNS module		DNS server settings
Time-module		Time module settings

Name

Here you can enter the device name (maximum 16 characters). The set of characters available includes uppercase and lowercase letters as well as some special characters. You can display the full range of available characters during a configuration session by entering the following command:

```
set \setup\name ?
```

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.

In addition, the device names you assign must be unique. For example, you might match the device names to the location (e.g. Glasgow, London, Provider, etc.).

Setup/WAN-module

This menu groups together all the settings necessary for starting up the WAN interface and controlling connections to logical remote stations.

/WAN-module		WAN settings
Interface-list		S_0 interface settings
Router-interface-list		Router module settings
Channel-list		Settings for the use of the available channels
Name-list		Remote station settings
RoundRobin-list		Settings for different remote station numbers
Layer-list		Settings for the layer combinations used

/WAN-module		WAN settings
PPP-list		Parameter settings for PPP connections
Number-list		Settings for call numbers with access authorization
Script-list		Dial script settings
Manual-dialing		Settings for manual connection control
Protect		Protection for answering incoming calls
CB-attempts		Number of callback attempts when the remote station is busy
Backup-delay-seconds		

Interface-list

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

Ifc	Protocol	LL-B-chan.	Dial-prefix
S0	Auto	1	0

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

`Setup/WAN-module/Router-interface-list`

`setup/lancapi-module`

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

Ifc	Designates the associated interface.
Protocol	D-channel protocol setting. The possible values are: **Auto**: automatic detection of the D-channel protocol **DSS1**: Euro-ISDN **1TR6**: National ISDN **GRP0**: Leased-line connection group 0 **P2P-DSS1**: Point-to-point connection
LL-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.
Dial-prefix	Global dialing prefix for all modules of the devices. The digits entered here (maximum 8) are automatically prefixed to the selected call number in every call. Use this prefix when, for example, the router is connected to a PBX.

Router-interface-list

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

Ifc	MSN/EAZ	YC.	CLIP
S0	123456	Off	On

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

Ifc	Designates the associated interface.
MSN-EAZ	If your device is connected to an ISDN port with 1TR6, enter the EAZ to which the interface is to respond. If your device is connected to an ISDN port with DSS1, enter the MSN to which the interface is to respond. If you wish the interface to respond to several different MSNs, enter them here separated by semicolons. A '#' in the list enables any number of incoming MSNs. For outgoing calls, the first MSN in this list will be reported to the remote station. If no MSN is entered, the switching center sends the main MSN of the terminal.
YC.	This entry can be used to control the interface's ability to establish Y connections. Possible settings are: **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 *LANCAPI* . **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.
CLIP	Calling Line Identification Protocol: Suppresses the outgoing MSNs. Possible values: **Yes**: Activate CLIR, do not send MSN. **No**: Deactivate CLIR, send MSN to remote station. Please note: The "selective suppression of call number transmission" may be a service feature that will have to be obtained from the telephone company.

Channel list

The channel list specifies the number and sequence of the channels to be established.

Device-name	Min	Mx	Order	Backup
LONDON	2	2	1-1;1-2	1
INTERNET	2	2	1-1;1-2;2-1;2-2	0
DEFAULT	1	2	0	

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

Device-name	Name of the remote station that is also used in the name and PPP lists.
Min	Number of static channels. These channels are used during every call establishment to the remote station.

Mx	The maximum number of channels to be used for this remote station. The Max-Min difference is the number of dynamic channels.
Order	This defines which channels are to be established on which S_0 bus. Syntax: [<BusNo>-<ChannelNo>][;<BusNo>-<ChannelNo>].... Possible values: 1 to 4 for the busses, 1 or 2 for the channel. If no entry has been made, a random channel on a random bus will be used. If one or more leased lines are to be used, an entry must be available for each leased line.
Backup	Number of possible backup connections. These connections will be established in the event that all valid leased-line channels are down. Backup connections always use a random channel on a random bus.

Name-list

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

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

Device-name	Dialup-remote	B1-DT	B2-DT	WAN-layer	Callback
GLASGOW	875463	180	0	PPPHDLC	On
LONDON	040785647	20	20	DEFAULT	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.
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	In this column, you can define appropriate connection time-outs (in seconds) for the first B channel. If no data is being transmitted when this time expires, the connection on this channel is released (default: 20). If charging information is transmitted over the ISDN network during the connection, the *ELSA LANCOM* will make full use of every charging unit and will only terminate the connection just before the beginning of the next unit. This function is also referred to as dynamic short-hold.
B2-DT	In this column, you can define appropriate connection time-outs for the second B channel (same as B1-DT, default: 20). The B2 hold time controls the bundling behavior during a channel bundling. Values of 0 or 9999 identify static bundling, values between them dynamic bundling.
WAN-layer	In this column, a name is stored that must also be entered in the layer list. This establishes the transfer protocol required for this connection.
Callback	In this column, you can define whether a callback is to be made for the relevant remote station (Off/Name/Auto/Looser/ELSA; default: Off).

- Callback options

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

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

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

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

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

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

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

Device-name	RoundRobin	Head
GLASGOW	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. GLASGOW#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 an *ELSA LANCOM Business:*

WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
DEFAULT	TRANS	PPP	TRANS	bnd+cmpr	HDLC64K
PPPHDLC	TRANS	PPP	TRANS	none	HDLC64K
MLPPP	TRANS	PPP	TRANS	bnd+cmpr	HDLC64K
RAWHDLC	TRANS	TRANS	TRANS	none	HDLC64K

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

WAN-layer	In this column, you can enter an original name designating the layer combination that you use. These names can then be used in the name list 'layer name' column depending on their spelling to set the protocol. If an entry with the name **DEFAULT** is defined in this column, the settings stored there are always used when no layer name can be assigned (e.g. a caller does not transmit his or her call number). This entry is also used when a group 0 leased-line connection is established. If the **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 *ELSA LANCOM* devices.
	TRANS	No Ethernet header is sent in this setting. Only “pure“ IP data packets are transferred, for example. This setting provides the greatest possible effective data throughput.

Lay-3	In the lay-3 column, you can define additional headers for data transmission in ISDN. You can select from among the following settings:	
	TRANS	No additional header is inserted (higher data throughput). Always select this setting if the remote station sends the data transparently via ISDN layer 3 (e.g. transparent HDLC, transparent X.75LAPB).
	PPP	A negotiation is performed according to the point-to-point protocol.
	APPP	A negotiation is performed as per the asynchronous PPP. APPP is then used when synchronous PPP is not possible because the connection does not permit a synchronous transmission (e.g. for analog modem operation).
	SCPPP	Following completion of script processing, a synchronous PPP negotiation is initiated.
	SCAPPP	Following completion of script processing, an asynchronous APPP negotiation is initiated.
	SCTRANS	Following completion of script processing, a connection exists to the remote station. No further protocol negotiation is performed.
Lay-2	In this column, you can select the protocol for ISDN layer 2:	
	TRANS	The data is packed directly in HDLC packets. Always select this setting if communication is to take place via transparent HDLC.
	X.75LAPB	The data is exchanged in X.75 secured format. Always select this setting if the remote station is to work with X.75 data protection.
L2-Opt.	The L2-opt. enables the setting of an option for the data transfer setting under Lay-2 with an additional *ELSA LANCOM*.	
	none	No data compression or channel bundling is performed.
	compr.	Stac data compression will be used. Compression as per Stac (Hi/fn) must be used in connection with PPP or multilink PPP. Stac compression may also be used in connection with Windows remote stations.
	bundle	Channel bundling is performed via several B channels. Channel bundling is only possible for the Lay-2 settings of 'PPP'.
	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.
	V110_9K6	Data is transferred at 9,600 bps in a V.110 connection, when connecting to GSM mobile phones, for example.
	V110_19K2	Data is transferred at 19,200 bps in a V.110 connection.
	V110_38K4	Data is transferred at 38,400 bps in a V.110 connection.

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

For Internet and remote access, PPP is generally specified.

PPP-list

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

Device-name	Auth.	Key	Time	Try	Conf	Fail	Term	Username	Rights
GLASGOW	CHAP	*******	0	5	10	5	2	ELSA	IP

Not all parameters can be reached via the telnet configuration. Use *ELSA LANconfig* so far as possible.

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

Device-name	In the Device-name column, you can enter the name with which the remote station logs onto the router. In the case of connections via the data transmission network, this is the name entered as "Username". For remote access via the data transmission network, the 'Username' field (see below) is not evaluated! Entries are not case-sensitive!	
Auth.	In this column, you can enter the security procedure to be used for verification of the remote station. Default: PAP	
	None	The router does not negotiate authentication with the remote station when establishing a connection. However, the remote station can itself require authentication from the router. This is the case when dialing up a connection to an ISP, for example.
	PAP	The remote station is checked as per the Password Authentication Protocol.
	CHAP	The remote station is checked as per the Challenge Handshake Authentication Protocol.
Key	A password may be entered in this column. Its presence is indicated by the symbol * and it is used to check the remote station. It may consist of 95 characters (7-bit ASCII, including spaces). Default: None. The `set ?` 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 *ELSA LANconfig* configuration program)!	
Username	The user name (max. 64 characters) transmitted to the remote station during PPP negotiation. The router identifies itself to the remote station with it. If no user name is entered, the device name serves as the user name. Entries are case-sensitive here.	
Rights	Network protocols to be routed over this connection: IP, IPX, NTB (NetBIOS). NetBIOS always requires one of the other two protocols. The routing of IP or NetBIOS via PPP always requires a suitable route (in the IP routing table for IP or in the remote-station table for NetBIOS).	

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 GLASGOW and LONDON 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	GLASGOW
040785647	LONDON

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

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

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

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

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

Script-list

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

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

Device-name	Script
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, an additional entry for the logical remote station may be added as in the round-robin list. The syntax for this is: Device name followed by '#' and a number. The entries are processed from top to bottom.

Setup/WAN-module/Manual-dialing

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

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

to initiate the manual establishment of a connection via remote configuration. The remote station's device name specified as a parameter must also be entered in the name list with a call number.

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

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

Setup/WAN-module/protection

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

- If 'Protect' is set to 'none', all pending calls are answered provided that the remote end supports the connection protocol.

- If this option is set to 'name', calls are accepted only from remote stations for which an entry is found in the name list. This verification provides additional protection. This verification is only available when using PPP.
- If this option is set to 'number', calls are accepted only from remote stations that are entered in the number list as authorized remote stations.
- The 'no./name' setting allows you to select combined protection using a name list and number list. First a verification that there is an entry in the number list is made. If this is not possible, the router will attempt to determine the name using the protocol negotiation.

Setup/WAN-module/CB-attempts

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

Setup/WAN-module/Backup-delay-seconds

The backup start time indicates the number of seconds to elapse before the first backup attempt is started after determining that the leased line is down. If the value 0 is entered, no backup connection will be established actively.

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 device
Spare-heap		Buffers that receive data packets from the local network

Connector

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

Connect	Meaning
Auto	Default setting; enables the Autosense function of the network chip. This automatically sets the router to the port in use without requiring manual configuration of this item.
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 the fast-Ethernet operation, please note that the selected transfer mode must also support the additional terminals.

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

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

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

Setup/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. In the default configuration, the IPX router is deactivated.

When the IPX router 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 router can automatically detect the network number and the binding.

The default value is '00000000' and means that the 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 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.

- **Filt.** 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 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 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. As a result, the maximum number of remote stations that can receive propagated frames corresponds to the number of possible simultaneous connections. 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 256 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).
- **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 512 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).
- **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
ARP-aging-min.		Dwell time for entries in the ARP table
TCP-aging-min.		Time limit for configuration connections that are inactive
TCP-max.-conn.		Max. number of simultaneous configuration connections to the *ELSA LANCOM*

Operating

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

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

IP address

The IP address for the router may be entered here. The default address on delivery is '0.0.0.0'.

If IP masquerading is used, this address takes on a special meaning in connection with the Intranet address:

If the IP address is assigned to the router by the Internet provider by PPP, all computers in the network linked by IP address and IP network mask are normally routed. These computers can then also be accessed directly from the Internet.

IP-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 router itself). This setting (an IP address registered in the Internet with a fully assigned network mask) can be used for masquerading via a raw IP access, such as that offered by the provider of the individual network. With such an access an IP address is not assigned to the router by a PPP negotiation, but it must have a fixed IP address registered in the Internet.

Intranet-address

A second IP address for the router may be entered here. This enables the 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.

In the event that such an address already exists in the network, a different address must be entered via outband configuration (terminal program).

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

Access-list

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

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

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

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

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

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

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

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

IP-address	IP-netmask
192.234.222.0	255.255.255.0

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

DNS-default

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

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

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

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

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

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

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

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

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

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

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

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

Setup/IP-router-module

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

/IP-router-module		IP router module settings
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
Start-WAN-Pool		Start of the address pool for dynamic address assignment for remote access
End-WAN-Pool		End of the address pool.
Routing-method		Routing method for IP packets
RIP-config		Settings for IP-RIP operation
Masquerading		Settings for IP masquerading

Operating

This option allows you to activate or deactivate the IP router module. In the default configuration, the IP router module is activated.

Activating the IP router module also activates the TCP/IP module.

IP-routing-table

The routing table can contain a maximum of 128 entries of destination network addresses or direct IP addresses with netmasks, and the names or IP addresses of other local routers. Alternatively, you can enter a setting by means of which packets to specific destination IP addresses are discarded and are not answered by proxy ARP. This is done by entering 0.0.0.0 for the name of the responsible router.

The 'Masquerade' field indicates whether the route should be masked or not. The following options are offered here:

- **On**: IP masquerading is switched on and functions with dynamic assignment of the IP address by the remote station. In this procedure the router queries the IP address '0.0.0.0' at the remote station and is assigned a random IP address by the remote station, which is then used for further processing.
- **Off**: Masquerading is switched off.
- **Static**: IP masquerading is switched on and functions with assignment of a static IP address previously assigned by the remote station. In this procedure the router queries the IP address entered under 'Setup/TCP-IP-module' at the remote station

and is assigned this address by the remote station. Use this setting when the remote station (e.g. your Internet provider) has assigned you a fixed IP address in the access data. Of course, this procedure will only function when this address has also been entered in the router as the IP address.

The IP routing table is generally sorted as shown below:

- The longest network mask is placed on top.
- For network masks of equal length, the one with the smallest IP address is placed on top.

In order to identify the correct remote station, the router searches the routing table from top to bottom using the destination IP address received. If a matching entry is found, the router name found is used for establishing the connection.

Address ranges that are prohibited in the Internet are excluded from transmission by preset entries in the IP routing table (the router name 0.0.0.0 means that packets to these addresses are not transmitted). The IP routing table below is provided by way of example and also shows the default settings:

IP-address	IP-netmask	Router-name	Distance	Masquerade
192.168.0.0	255.255.0.0	0.0.0.0	0	Off
172.16.0.0	255.240.0.0	0.0.0.0	0	Off
10.0.0.0	255.0.0.0	0.0.0.0	0	Off
224.0.0.0	224.0.0.0	0.0.0.0	0	Off

However, if these addresses are required for Intranet use, for example, it is possible to delete the predefined entries at any time. If the routing table contains no entries with the router name 0.0.0.0, the router processes all IP addresses with valid routes.

- Example
  - The local network address is 192.120.130.0.
  - Three terminal units must be available via proxy ARP with the IP addresses 192.120.130.10, 192.120.130.11 and 192.120.130.12 via an *ELSA LANCOM* 'Leeds'.
  - Two destination networks 192.120.131.0 and 192.120.132.0 can be accessed by the remote stations 'GLASGOW' and 'LONDON'.
  - 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	LEEDS	0	Off
192.120.130.11	255.255.255.255	LEEDS	0	Off
192.120.130.12	255.255.255.255	LEEDS	0	Off
192.120.131.0	255.255.255.0	GLASGOW	0	Off
192.120.132.0	255.255.255.0	LONDON	0	Off
193.140.200.0	255.255.255.0	0.0.0.0	0	Off
193.140.300.0	255.255.255.0	192.120.130.200	0	Off
255.255.255.255	0.0.0.0	PROVIDER	0	On

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

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

LAN-filter-table

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

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

Idx.	D-st.	D-end	S-st.	S-end	Src.-addres	Src-netmask	Prot	Type
WIN	0	0	137	139	255.255.255.255	0.0.0.0	TCP and UDP	Alway s-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	139	0.0.0.0	0.0.0.0	TCP and UDP

The fields in the table have the same meaning as in the LAN filter table, with the following exception:

- Dst-address, Dst-netmask

A subnetwork of the local network for which the filter is valid can be entered here. A destination address of 0.0.0.0 means that the filter is applied to all computers. A network mask of 0.0.0.0 means that the filter is applied to all networks (which also means all computers).

The table entries are sorted in a similar fashion to the IP router table:

- Longest network mask is placed on top.
- For two network masks of equal length, the one with the smaller IP address is placed on top.

Network masks and IP addresses of 0.0.0.0 can be used as "wildcards". Specified computers and networks may be simultaneously subjected to targeted filtering while others pass the router unfiltered.

The tables are processed from top to bottom. As soon as a matching filter is found, the packet is handled accordingly.

Proxy-ARP This option allows you to activate or deactivate the proxy ARP mechanism (default: 'Off'). This function permits data to be transmitted to IP addresses within the same logical network as the sender, e.g. when linking individual workstation computers (teleworkers) to the corporate network via TCP-IP.

Loc.-routing Local routing enables the router to forward data packets via the local network. The local routing is necessary if the router, as the default gateway for the workstations receives packets for destination networks to which it cannot establish a connection itself. If the router cannot return the address of the appropriate router to the workstation via IMCP, it will forward the data to the corresponding router itself (see also 'Local Routing'). Since this setting increases network utilization in the LAN, the default setting is 'Off'.

Start-address-pool Start of the address pool used for the dynamic assignment of IP addresses for devices dialing in. This function is also known as IP pooling and can be used for remote access by several field staff members, for example.

The address pool should be in the same address range as the router. If possible, ensure that the address pool is large enough that an IP address can be assigned to every device dialing in (e.g. one address for each of the available B channels).

If the device dialing in can initially establish a connection, only to have it terminated again during the protocol negotiation, this is a sign of insufficient free IP addresses in the IP pool.

End-address-pool End of the address pool for IP pooling.

Setup/IP-router-module/Routing-method

The router offers two methods for IP routing, which can be separately set for IP and ICMP packets. Both methods are based on the evaluation of the field 'Type-of-service' in the IP header.

The menu has the following layout:

/Routing-method		Routing method settings
Routing-method		Routing method for IP packets
ICMP-routing-method		Routing method for ICMP packets

Routing-method This option allows you to define the routing method used for IP packets:

- If you select 'Normal', all IP packets are handled in the same way as per the routing specifications of the Internet protocol.
- If you select 'Type-of-service', IP packets are placed in the urgent queue or reliable queue, depending on the contents of the 'Type-of-service' field. All other packets are placed in the normal send queue. In this way, transmission is guaranteed, provided that it is possible.

ICMP-routing-method This option allows you to define the routing method used for ICMP packets:

- If you select 'Normal', the ICMP packets are handled like any other IP packets as per the routing specifications of the Internet protocol.
- If you select 'Reliable', all ICMP packets received are placed in the reliable queue.

Setup/IP-router-module/RIP-configuration

This option allows you to enter settings for the management of IP-RIP packets. The menu has the following layout:

/RIP-configuration		Settings for IP-RIP operation
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.
- **CI+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-IP-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)').

The service table (also called the static masquerading table) can contain up to 16 entries and has the following layout:

D-port	Intranet addr.
20	10.1.1.10
21	10.1.1.10

The different columns have the following meaning:

- D-port: Destination port for the particular entry
- Intranet-addr.: Destination IP address for the computer in the local network

Through this assignment, it is possible, for example, to address the relevant service directly via telnet. Enter the IP address of the router and attach the port number, separated by a double point, to the address.

You can use the command

```
telnet 192.38.50.100:27
```

to connect directly to a news server that can be reached via a router with the IP address 192.38.50.100.

Table-masquerading

With IP masquerading, the IP addresses of computers in the local network are rendered invisible to external devices by means of a conversion of addresses and ports in the router. The dynamic masquerading table displays the IP addresses from the local network that the router is currently masking. The dynamic masquerading table can contain up to 2048 entries and has the following layout:

Intranet addr.	S-port	Protocol	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 router to retain targeted trap information. The *ELSA LANmonitor*, for example, queries the channel statistics in this way and converts them to a graphic display (under Windows).

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

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

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

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

Monitor-table The monitor table has the following structure:

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

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

Setup/DHCP-module

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

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

Operating

On: The device operates as a DHCP server

Off: The device does not operate as a DHCP server

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

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

Start-address-pool
End-address-pool

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

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

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

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

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

Netmask

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

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

Broadcast

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

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

Max.-lease-time-minute(s)

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

The DEFAULT value of 6000 minutes equals approximately 4 days.

Default-lease-time-minute(s)

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

The DEFAULT value of 500 minutes equals approximately 8 hours.

Table-DHCP

In the DCHP module, the 'Table-DCHP' 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	Node-ID	Timeout	Hostname	Type
10.1.1.10	00a0570308e1	500	ELSA	new

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

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

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

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

Setup/NetBIOS-module

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

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

Scope-ID

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

NT-Domain

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

Remote-table

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

Name	Type
GLASGOW	Router or workstation

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

Type

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

Host table

The host table has the following structure:

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

Group table

The group table thus looks like this:

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

The fields of the table have the following significance:

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

Flags

The flags have the following significance:

0x0003	This counter increments up each time the validity expires. The entry will be deleted if the name is not refreshed after the second expiration at the latest.
0x0004	This identifies an entry that still needs to be transferred.
0x0008	This identifies an entry that is queued for deletion, i.e. the name has not yet been refreshed after the establishment of a connection.
0x0010	Reserved

0x0020	This identifies a remote station.
0x0040	Reserved
0x0080	Reserved

The server list has the following structure:

Host	Group/ Domain	UPD	IP-address	OS-Ver	SMB-Ver	Server-type	Remote station	Time-out	Flags
REMOTE	WORKGROUP	00	10.0.1.100	0400	010f	0004140b	GLASGOW	13	0020
WORKSTATION	WORKGROUP	07	10.0.0.10	0400	0415	00452003		31	0000

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

The individual fields have the following significance:

Host	Name of the server
Group/Domain	Workgroup or domain in which the server is located.
UPD	Update counter: indicates the number of times that the server has already propagated itself
IP-address	Address of the server
OS-Ver	Operating system version number
SMB-Ver	Version number of the SMB protocol used
Server-type	Bit mask in which the services of the server are coded
Remote station	Name of the remote station from which the server was announced
Timeout	Time until the entry loses its validity (for entries from the LAN) or time until the router propagates a remote entry.
Flags	Corresponds to the flags in the host or group tables.

Setup/Config-module

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

/Config-module		Configuration module settings
LAN-config		Switch for configuring from the LAN side
WAN-config		Switch for configuring from the WAN side
Password-required		Password required on/off if there is no password
Farconfig-(EAZ-MSN)		Subscriber number for remote configuration via PPP
Maximum-connections		Maximum number of simultaneous connections

/Config-module		Configuration module settings
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
Display contrast		
Language		Configuration language

LAN-config

This option allows you to define whether remote configuration from the LAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting for this option is **On**.

WAN-config

This option allows you to define whether remote configuration from the WAN side is possible (**On**), is not possible (**Off**), or is possible only in read mode (**Read**). The default setting for this option is **Off**.

Password-required

This specifies whether a new password should be requested every time a remote configuration is begun (**On**), or the password request should be suppressed (**Off**). The default setting for this option is **On**.

Farconfig-(EAZ-MSN)

This subscriber number permits remote configuration via PPP. If no number is specified here, remote-configuration calls will be accepted on all numbers.

Maximum connections

This option allows you to display the maximum number of remote configuration sessions that can occur simultaneously for the device.

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 device forgets all prior login errors.

Language

This option allows you to select whether you will use the German or English version of the software for performing the configuration.

Setup/*LANCAPI*-module

Configuring *LANCAPI* basically involves answering two questions:

- What call numbers from the telephone network should *LANCAPI* respond to?
- Which of the computers in the local network should be able to access the telephone network via *LANCAPI*?
- Via which UDP port do the *LANCAPI* server and *LANCAPI* clients communicate?

The *LANCAPI* module has the following layout:

/LANCAPI-module		***LANCAPI* settings**
Access-list		List of computers allowed to use the *LANCAPI*
Interface-list		Activation of the *LANCAPI* for the various interfaces and specification of the various subscriber numbers to which the *LANCAPI* should respond.
Priority-list		Priority for the *LANCAPI* versus router connections
UDP-port		UDP port for communication between the *LANCAPI* server and clients

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*.

Interface-table

The interface table appears as follows:

Ifc	**Operating**	**EAZ-MSN(s)**	**Force-Out-MSN**
S0-1	Outgoing	123456	no

The fields of the table have the following significance:

Ifc	Designates the associated interface
Operating	This item determines whether *LANCAPI* operation is permitted on this interface for outgoing calls, incoming and outgoing calls (On) or whether *LANCAPI* operation is disabled completely (Off).
EAZ-MSN(s)	Enter the EAZs or MSNs on which the *LANCAPI* should respond to incoming calls here; these EAZs/MSNs will also be displayed to the exchange during outgoing calls.
Force-Out-MSN	If no outgoing MSN has been configured for the CAPI application, this item can be used to determine whether the *LANCAPI* transfers the first EAZ/MSN on the list.

Priority-table

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 device should the LCR functions be active?
- Which area codes should be diverted when via which dial-around provider?

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 *LANCAPI*, **On** or **Off**
Timetable		Call forwarding table
Celebration-day-table		List of holidays affecting the timetable.

Timetable

The table has 256 entries and the following structure:

Index	Prefix	Days	Start	Stop	Number-list	Fallback
1	0171	192	0:00	23:59	01013;01070	On

The individual entries have the following meaning:

Index	Continuing index of entries in the table.
Prefix	Area code to be diverted.
Days	Validity of the entry for week days and holidays shown in an 8-bit mask: Bit 0 represents Monday, bit 7 holidays. The entry '31' therefore designates all business days, '192' Sundays and holidays.
Start	Beginning time for the validity of the entry on the defined days.
Stop	Termination time for the validity of the entry on the defined days.
Number-list	Network identification number of the dial-around providers.
Fallback	Automatic fallback to your own telephone company if all dial-around numbers are busy.

Example:

`set 1 02 31 1:00 11:59 01030;01090;01070 On` diverts all long-distance calls to region '02' between one and twelve o'clock to the provider with the network identification number '01030'. If this number is busy, the network identification numbers '01090' and '01070' will be attempted. If they are also not available, the connection will be made via the normal telephone company.

Celebration-day-table

The celebration-day-table has 256 entries and the following structure:

Index	Date
1	01010000
2	01050000
3	03100000
4	25120000
5	26120000
6	02041999
7	13051999

The individual entries have the following meaning:

Index	Continuing index of entries in the table
Date	Dates of holidays. Enter the index and the date in full without separators, e.g. 'set 8 13041999' for April 13, 1999 as the eighth entry in the list. Enter '0000' as the year for annually occurring holidays.

Setup/DNS-module

The settings for the DNS server can be modified here as required. The menu contains the following items (incl. their default settings):

Operating		On (default) or off
Domain		Own domain, optional, 32 characters max.
DHCP-usage		Yes (default) or no
NetBIOS-usage		Yes (default) or no
DNS-table		Static DNS table for the manual association of IP addresses to names, 64 entries
Filter-list		Filter list for the exclusion of prohibited domains, 64 entries
Leasetime		Specifies the name validity information to be given to a requesting computer. Default: 2000

DNS-table

The DNS table contains a simple association of local names to IP addresses. The table is sorted alphabetically by names.

The table is restricted to 64 entries, as large networks are configured more effectively using the DHCP server, which can also be used to handle name requests. The table has the following layout:

Hostname	IP-address
Host10	10.0.0.10

The name is restricted to a maximum of 32 characters. Longer names are not necessarily practical in a local network.

Filter-list

The filter list contains the entries for prohibited domains. In addition, it is possible to specify for whom a given domain will be prohibited. This is set using an IP address/ netmask pair. An IP address of 0.0.0.0 prohibits this domain for all computers. A subnet mask of 0.0.0.0 prohibits the domain for all networks. The table has the following layout:

Idx.	Domain	IP-Address	Netmask
F001	*xxx*	0.0.0.0	0.0.0.0

Clear IDs can be freely selected and assigned to the filters in the 'Idx.' field.

Enter the name of the domain to be prohibited in the 'Domain' field. Wildcards such as '?' and '*' may be used. The wildcard '?' replaces exactly one character, while '*' can stand for a random number of characters. Multiple instances of the wildcard '*' can be used. For example, *xxx* filters all names containing the letters xxx in any position within the name.

The IP address and subnet mask fields can be used to specify the subnet for which the domain will be prohibited.

The filter table is sorted according to the subnet masks in descending order (the longest at the top); entries with identical subnet masks are sorted according to the IP addresses in ascending order. In the event of identical IP addresses, the entries are sorted in ascending order according to the domain to be prohibited.

The table is searched from top to bottom and an error message is returned to the requesting computer in the event of a match.

Setup/Time-module

The least-cost router in the device requires correct time information to calculate the call number diversions via call-by-call provider. Precise time information is also desirable for some statistics.

The time may be set manually (with the 'time' command) or automatically read from the ISDN network.

For automatic time comparison when the module is switched on, a previously specified remote station is called directly and the time information is taken from the ISDN network. So long as the time module is switched on, the time will be taken from the ISDN every time the router establishes a connection.

The time module has the following layout:

/Time-module		Time module settings
Operating		Activating the module: **On**, **Off**
Current-time		Displays the current time in the device.
Time-call-number		Call number to which a connection must be established to receive time information from the ISDN.
Call-attempts		Number of possible attempts to receive time information

Firmware

The various firmware parameters can be called up and a firmware upload started from this menu:

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

Version table

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

Ifc	Module	Version	Serial-number
Ifc	LANCOM Business 4100	1.60.0012 / 30.06.1999	8427.000.020

Table firmsafe This table provides the following details for the two firmware versions stored in the device: the position in memory (1 or 2), status information (active or inactive), the version number, the date, the size and the index (sequential number).

Position	Status	Version	Date	Size	Index
1	Inactive	1.60	23061999	690	6
2	Active	1.60	30061999	692	7
3	<loader>	1.60	07061999	64	0

Enter the following command to activate an inactive firmware version:

```
set <position number> active.
```

Mode-firmsafe Only one of the firmware versions stored in the device can be active at any one time. When new firmware is loaded the inactive firmware is overwritten. You can decide which firmware will be activated after the upload:

- 'immediate': The first option is to load the new firmware and activate it immediately. The following situations can result:
  - The new firmware is successfully loaded and then operates as desired. Everything is then in order.
  - However, if the new firmware does not operate correctly, it may not be possible to communicate with the device after the restart. If an error occurs during the upload, the device automatically reactivates the previous firmware version and reboots the device.
- 'login': To prevent problems caused by defective firmware, the second option will load the firmware and start it immediately.
  - In contrast to the first option, the firmsafe will wait until it has successfully logged on over outband or inband (by telnet). In contrast to the first option, the firmsafe will wait until it has successfully logged on (by telnet). The new firmware will only be permanently activated when the login occurs successfully within the time set under 'Timeout firmsafe'.
  - If the device no longer responds and it is therefore impossible to log in, the firmware automatically loads the previous firmware version and reboots the device with it.
- 'manual': The third option allows you to set a period (Timeout firmsafe) beforehand for testing the new firmware. The device will start with the new firmware and wait for the preset period until the loaded firmware is manually activated and therefore becomes permanently effective.

Other

The **Other** menu allows you to manage the following functions:

/Other		Various functions
Manual-dialing		Connection testing
Boot-system		Boots the device.
Reset-system		Resets to factory settings.
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.

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.

Novell SAP numbers

Decimal	Hexadecimal	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	000F	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)
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)

Decimal	Hexadecimal	SAP description
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)
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 Domain
309	0135	Netware Naming Services Profile
311	0137	Netware 386 Print Queue or NNS Print Queue
321	0141	LAN Spool Server (Vap, Intel)
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 Tools
394	018A	NASI services broadcast server (Novell)
432	01b0	GARP Gateway (net research)
433	01b1	Binfview (Lan Support Group)
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 Server
476	01dc	Castille FAX/Xerox 7033 Fax Server/Excel Lan Fax
496	01f0	LEGATO
501	01f5	LEGATO
563	0233	NMS Agent or Netware Management Agent
567	0237	NMS IPX Discovery or LANtern Read/Write Channel
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

Decimal	Hexadecimal	SAP description
780	030c	Intel Netport 2 or HP JetDirect or HP Quicksilver
800	0320	Attachmate Gateway
807	0327	Microsoft Diagnostics
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	ViruSafe 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)
983	03d7	Lexmark printer server (type 4033-011)
984	03d8	Lexmark XLE printer server (type 4033-301)
990	03de	Gupta Sequel Base Server or 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 (Brightworks)
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 Emulex
1312	0520	Site Lock Checks
1321	0529	Site Lock Checks (Brightworks)
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 antivirus
1466	05BA	Compatible Systems Routers
	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

Decimal	Hexadecimal	SAP description
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 LANport
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
61951	f1ff	Site Lock
62723	f503	Microsoft SQL Server
63749	f905	IBM Time and Place/2 application
64507	fbfb	TopCall III fax server
65535	ffff	Any Service or Wildcard

TCP/IP ports

Capab.	Port no.	Protocol
echo	7	tcp
echo	7	udp
discard	9	tcp
discard	9	udp
systat	11	tcp
systat	11	tcp
daytime	13	tcp
daytime	13	udp
netstat	15	tcp
qotd	17	tcp
qotd	17	udp
chargen	19	tcp
chargen	19	udp
ftp-data	20	tcp
ftp	21	tcp
telnet	23	tcp
smtp	25	tcp
time	37	tcp
time	37	udp
rlp	39	udp
name	42	tcp
name	42	udp
whois	43	tcp
domain	53	tcp
domain	53	udp
nameserver	53	tcp
nameserver	53	udp
mtp	57	tcp
bootp	67	udp
tftp	69	udp
rje	77	tcp
finger	79	tcp
www	80	tcp
www	80	udp
link	87	tcp
supdup	95	tcp
hostnames	101	tcp
iso-tsap	102	tcp
dictionary	103	tcp
x400	103	tcp
x400-snd	104	tcp
csnet-ns	105	tcp
pop	109	tcp
pop2	109	tcp
pop3	110	tcp
portmap	111	tcp
portmap	111	udp
sunrpc	111	tcp
sunrpc	111	udp
auth	113	tcp
sftp	115	tcp
path	117	tcp
uucp-path	117	tcp
nntp	119	tcp
ntp	123	udp
nbname	137	udp
nbdatagram	138	udp
nbsession	139	tcp
NeWS	144	tcp
sgmp	153	udp
tcprepo	158	tcp
snmp	161	udp
snmp-trap	162	udp
print-srv	170	tcp
vmnet	175	tcp
load	315	udp
vmnet0	400	tcp

Capab.	Port no.	Protocol
sytek	500	udp
biff	512	udp
exec	512	tcp
login	513	tcp
who	513	udp
shell	514	tcp
syslog	514	udp
printer	515	tcp
talk	517	udp
ntalk	518	udp
efs	520	tcp
route	520	udp
timed	525	udp
tempo	526	tcp
courier	530	tcp
conference	531	tcp
rvd-control	531	udp
netnews	532	tcp
netwall	533	udp
uucp	540	tcp
klogin	543	tcp
kshell	544	tcp
new-rwho	550	udp
remotefs	556	tcp
rmonitor	560	udp
monitor	561	udp
garcon	600	tcp
maitrd	601	tcp
busboy	602	tcp
acctmaster	700	udp
acctslave	701	udp
acct	702	udp
acctlogin	703	udp
acctprinter	704	udp
elcsd	704	udp
acctinfo	705	udp
acctslave2	706	udp

Capab.	Port no.	Protocol
acctdisk	707	udp
kerberos	750	tcp
kerberos	750	udp
kerberos_master	751	tcp
kerberos_master	751	udp
passwd_server	752	udp
userreg_server	753	udp
krb_prop	754	tcp
erlogin	888	tcp
kpop	1109	tcp
phone	1167	udp
ingreslock	1524	tcp
maze	1666	udp
nfs	2049	udp
knetd	2053	tcp
eklogin	2105	tcp
rmt	5555	tcp
mtb	5556	tcp
man	9535	tcp
w	9536	tcp
mantst	9537	tcp
bnews	10000	tcp
rscs0	10000	udp
queue	10001	tcp
rscs1	10001	udp
poker	10002	tcp
rscs2	10002	udp
gateway	10003	tcp
rscs3	10003	udp
remp	10004	tcp
rscs4	10004	udp
rscs5	10005	udp
rscs6	10006	udp
rscs7	10007	udp
rscs8	10008	udp
rscs9	10009	udp
rscsa	10010	udp

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

ELSA LANCOM Business internal

This chapter provides information on the internal functions of the 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

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 *ELSA LANCOM*.

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 *ELSA LANCOM* 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.
SCTRANS	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 RoundRobin 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 *ELSA 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:

WAN-layer	Encaps.	Lay-3	Lay-2	L2-Opt.	Lay-1
CSERVE	TRANS	SCAPPP	X.75LAPB	none	HDLC64K

Name list:

Device name	Dialup-remote	B1-DT	B2-DT	WAN-layer	Callback
CSERVE	0021194260	60	60	CSERVE	Off

PPP list:

Device name	Authent.	Key	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.
[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 (SCAPPP) 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 *ELSA LANCOM*. Such information can aid in finding erroneous configurations easily and securely, both from *ELSA LANCOM* and from other devices connected with an *ELSA LANCOM*.

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, i.e. 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
PPP	Display PPP protocol negotiation
SCRPT	Display script 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 *LANCOM Office*-Router)
Packet dump	Display of the 64 bytes of a packet in hexadecimal format (only *LANCOM Office*-Router)

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 outputs under 'status' describe status changes on a WAN interface (at present only the internal S_0 terminal). They are displayed in the following format:

- Format: [Interface] [Status]
- Example:

  `Ch01: Dial 8700`

  On the first B channel of the internal S_0 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'PPP'

The point-to-point protocol consists of a collection of subprotocols, of which *ELSA LANCOM* 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 in any combination from now on. To terminate a PPP connection it switches into the TERMINATE phase where once again only LCP pakkets 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 ffffffffffff 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 ffffffffffff 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 ffffffffffff 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 (i.e. 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 *ELSA LANCOM* 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 *ELSA LANCOM* 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
190.254.0.0255.255.0.0194.162.38.1623Store
195.126.38.0255.255.255.0194.162.38.1623update
255.255.255.2550.0.0.0194.162.38.1622Discard
194.162.38.0255.255.255.0194.162.38.1622Discard
```

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 *ELSA LANCOM*. 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 *ELSA LANCOM* 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 *ELSA LANCOM*. 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 *ELSA LANCOM* 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 *ELSA LANCOM* 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-routing-method`

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.